Создание многофункционального исследовательского стенда для изучения IT-технологий интернета вещей и анализа данных

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

Институт вычислительного моделирования СО РАН

si@krasn.ru

***Аннотация*. В статье представлены технологические решения многофункционального исследовательского стенда, предназначенного для организации инновационной образовательной среды, способствующей развитию компетенций в области искусственного интеллекта, и телекоммуникационных технологий. Архитектура стенда основана на концепции интернета вещей и включает сенсорный, транспортный, сервисный и прикладной функциональные уровни. Стенд позволяет собирать данные с устройств, фиксировать сетевой трафик и моделировать распределённые угрозы для исследования аспектов информационной безопасности. За время работы стенда собраны значительные объёмы информации, которые служат основой для практического освоения современных методов предобработки, очистки и анализа больших данных.**

Ключевые слова: инновационные инструменты обучения; исследовательский стенд; интернет вещей; сетевые протоколы; информационная безопасность; анализ данных

I. Введение

В условиях бурного развития информационных технологий их функциональные возможности становятся объектом пристального внимания педагогических исследований, определяющих перспективные направления модернизации образовательных процессов [1]. Цифровизация образования представляет собой один из ключевых инновационных трендов, в связи с чем, особую значимость приобретают не только вопросы организационного обеспечения цифрового образования, но и направления поиска эффективных инструментов, способных гармонично интегрироваться в учебную среду [2].

Российский рынок труда неуклонно демонстрирует рост интереса к специалистам IT-направлений. Педагогическая эффективность их подготовки напрямую зависит от применения исследовательских форм обучения, ориентированных не только на представление предложенных знаний, но на формирование навыков самостоятельного решения задач, развивающих научные и креативные компетенции. Такой подход, согласно введённой в [3] классификации определяет «исследовательскую форму» взаимодействия с образовательным ресурсом, при которой учебные задачи не внедрены в образовательный контент, а предоставляют обучающимся свободу самостоятельного выбора путей их решения.

Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (Соглашение 075-02-2025-1606)

В этой связи возникает необходимость в разработке дополнительных инструментов, ориентированных на практическое применение знаний и навыков ведения IT-проектов в реальных условиях. Одним из таких инструментов является исследовательский стенд, предоставляющий возможность практического изучения современных информационных технологий и методов их применения. Специализированные учебные стенды создаются для детального освоения принципов настройки и функционирования оборудования, работы телекоммуникационных систем, систем умного дома и других устройств, предназначенных для управления и контроля [4].

Одним из ключевых приоритетов исследовательской деятельности Красноярского математического центра является разработка инновационных образовательных инструментов, нацеленных на подготовку специалистов, владеющих компетенциями в таких областях, как искусственный интеллект, анализ больших данных, информационная безопасность, сетевые и телекоммуникационные технологии, интернет вещей и смежные направления. В настоящей статье представлены разработанные архитектурные и технологические решения для создания многофункционального исследовательского стенда, в задачи которого входит наглядная демонстрация масштабируемой сетевой инфраструктуры, обеспечивающей механизмы межуровневого взаимодействия распределённых устройств и приложений по технологии интернета вещей [5], а также сбор данных для возможности последующего анализа. Стенд применяется для практических занятий по дисциплинам: «Информационные и вычислительные сети», «Информационная безопасность», «Интеллектуальные системы».

II. Архитектурные решения

Архитектурные принципы разработанного исследовательского стенда основаны на концепции интернета вещей (Internet of Things – IoT), которая описывает методы организации вычислительных сетей, состоящих из распределённых устройств и приложений, объединяющих физические и виртуальные объекты, взаимодействующие между собой для предоставления цифровых услуг [6]. IoT является платформой для обеспечения автономности сбора данных, их совместимости и развёртывания независимых сервисов и приложений [7]. Для успешного функционирования в структуру такой платформы входит четыре функциональных уровня [8, 9], схема которых приведена на рис. 1.

Рис. 1. Функциональные уровни IoT

Описание функциональных уровней IoT-платформы:

- Сенсорный уровень отвечает за сбор информации о состоянии наблюдаемых объектов.
- Транспортный уровень включает шлюзы и сети передачи данных.
- Сервисный уровень обеспечивает хранение и распределение данных.
- Прикладной уровень предназначен для решения задач предметной области.

Одной из задач нашего стенда является демонстрация особенностей организации коммуникаций на транспортном функциональном уровне. Стенд обеспечивает возможность сбора данных с IoT-устройств, а также фиксации журналов сетевого трафика для анализа информации, поступающей по протоколам на различных участках сети. Примеры сетевых протоколов, с помощью которых обеспечивается возможность взаимодействия устройств IoT и их соответствие сетевой модели OSI (Open Systems Interconnection model) и TCP/IP представлены в табл. 1.

ТАБЛИЦА I. СЕТЕВЫЕ ПРОТОКОЛЫ

Уровни сетевой модели		**Протоколы**
Модель OSI	***Модель TCP/IP***	
Прикладной	Прикладной	HTTP, HTTPS, FTP, MQTT, CoAP
Представления		
Сеансовый		
Транспортный	Транспортный	TCP, UDP
Сетевой	Межсетевой	IPv4, IPv6, ICMP
Канальный	Канальный	Ethernet, Wi-Fi, BLE, Zigbee, Z-Wave, LoRa
Физический		

В настоящий момент канальный (физический) уровень реализован по протоколу Ethernet и Wi-Fi, на транспортном уровне собираются данные по протоколу TCP, в качестве прикладного протокола выбран MQTT (Message Queuing Telemetry Transport) [10]. Эти протоколы выполняют функции по упаковке, форматированию и доставке данных.

Прикладной протокол MQTT является открытым стандартом международной организацией по развитию стандартов (OASIS), предназначенным для межмашинного взаимодействия в сетях Интернета вещей. Для функционирования сети реализована схема «Издатель-Брокер-Подписчик», где издатели – IoT-устройства, брокеры – сервера с развёрнутым на них программным обеспечением, собирающим и распределяющим данные по подписчикам – системам их анализирующим (рис. 2).

В качестве IoT-устройств рассматриваются датчики мониторинга окружающей среды (CL-210-E производства ICP DAS), подключенными посредством проводного протокола Ethernet (100BASE-TX) одновременно являющейся и источником питания по технологии Power over Ethernet стандарта IEEE 802.3af.

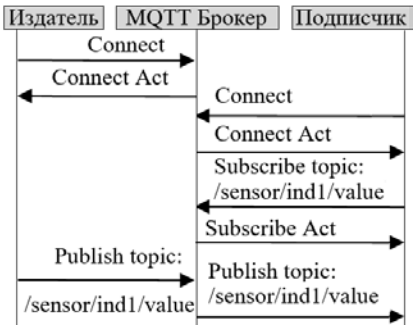

Рис. 2. Схема протокола MQTT

Сбор, хранение и анализ выполняется на кластере Kubernetes (K8s), вычислительная структура которого размещена на 3-х физических серверах и отказоустойчивом кластере виртуальных машин с системой виртуализации Hyper-V. На всех узлах кластера K8s использована операционная система Ubuntu Server. Кластер K8s развернут поверх системы контейнеризации Docker. Централизованное управление жизненными циклами контейнеров выполняется на платформе orchestration Rancher. Такая схема на основе использования контейнеризации позволяет встраивать получаемые обучающимися программные решения в существующие механизмы функционирования исследовательского стенда.

Для реализации функций брокеров выбраны и развёрнуты несколько популярных программных платформ: Eclipse Mosquitto, EMQX, NanoMQ и VerneMQ [11]. Каждая из этих платформ была установлена на отдельном виртуальном сервере с уникальной конфигурацией настроек безопасности. Такой подход позволяет наблюдать и анализировать сетевые аномалии, возникающие при взаимодействии с IoT-устройствами. Конфигурации серверов (табл. 2) различаются по нескольким параметрам: способ доступа (с авторизацией через Login/Password или анонимный доступ), использование протокола шифрования TLS (Transport Layer Security) или его отсутствие, а также ограничение доступа – только из внутренней корпоративной сети или из интернета.

ТАБЛИЦА II. КОНФИГУРАЦИИ СЕРВЕРОВ (ДЛЯ БРОКЕРОВ)

Обозначение	**Авторизация**	**Шифрование**	**Доступ**
auth_priv	Login/Password	Open	Private
anon_priv	Anonymous	Open	Private
auth_priv_tls	Login/Password	TLS	Private
anon_priv_tls	Anonymous	TLS	Private
auth_pub_tls	Login/Password	TLS	Public
anon_pub_tls	Anonymous	TLS	Public

Для каждой программной платформы были настроены серверы с учётом указанных политик безопасности. Всего реализовано 24 варианта конфигураций брокеров, что позволяет гибко подбирать параметры для достижения баланса между доступностью сервисов и обеспечением целостности данных. При этом сохраняется функциональность и учитываются ограничения по потреблению ресурсов в условиях одинаковых сценариев использования. Для обеспечения публикации данных и их передачи между отдельными

сегментами сети на каждую инсталляцию создан реплицирующий брокер. Такая схема позволяет в режиме реального времени изменять различные настройки брокеров и выполнять доступ к данным для проведения исследований.

III. Инструменты сбора данных

Для сбора сетевого трафика созданы и размещены в распределённой среде исследовательского стенда программные агенты [12]. На рис. 3 приведён фрагмент схемы сбора данных.

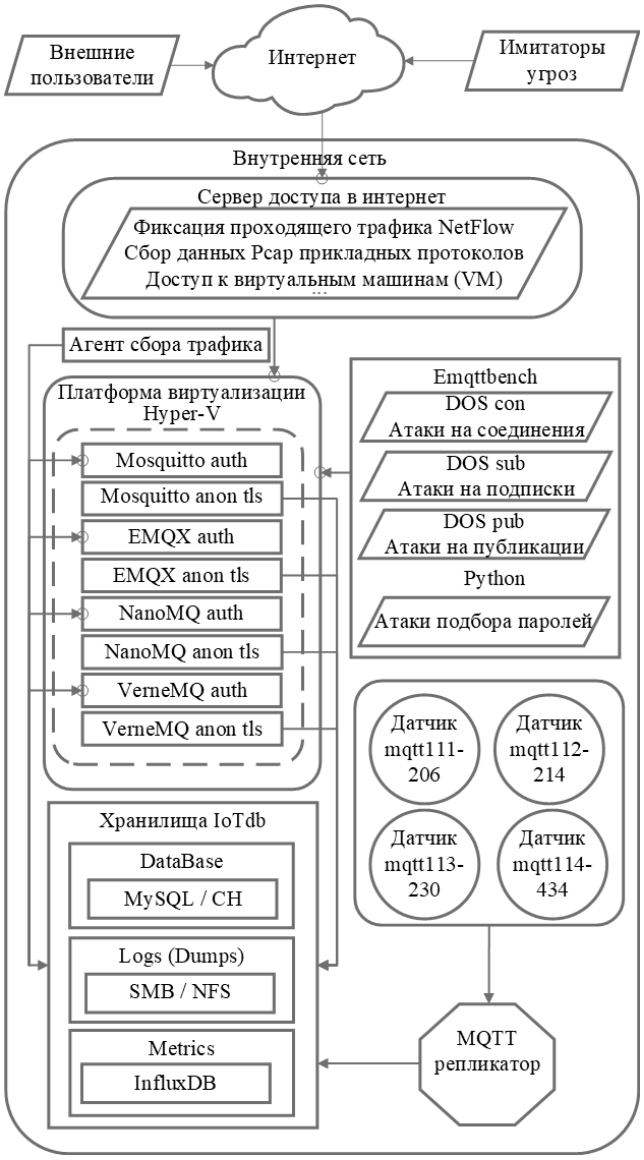

Рис. 3. Схема сбора данных

Сбор сетевого трафика осуществляется с помощью инструментов, размещённых на сервере доступа в Интернет и серверах брокеров. Для брокеров, доступных из глобальной сети, данные, собираются на сервере доступа и включают информацию о всем сетевом трафике в формате Netflow, а также данные всех пакетов для исследуемого прикладного протокола в формате Pcap (Packet Capture). Программные агенты, функционирующие на серверах брокеров, фиксируют как внешний, так и внутренний трафик, поступающий на стандартные порты протокола MQTT (1883, 8883).

Помимо данных из сетевых журналов, осуществляется сбор метрик серверов, включая показатели использования процессора, оперативной памяти, сетевого канала, а также количество операций ввода/вывода и другие параметры. Дополнительно фиксируются метрики, предоставляемые программным обеспечением брокеров, содержащие сведения об активности клиента, получаемых и отправляемых сообщениях и пр.

От IoT-устройств поступают данные, полученные с датчиков для измерения температуры, влажности и концентрации мелкодисперсной пыли. Для их хранения создано специализированное хранилище, доступ к которому предоставляется различным подписчикам. Собранные данные применяются для практического освоения современных методов предобработки, очистки и анализа больших объёмов информации с использованием методов машинного обучения и технологий интеллектуального анализа данных.

Для исследования вопросов сетевой безопасности требуется не только анализ реального трафика из сетевых журналов, но и моделирование трафика, возникающего при имитации потенциальных угроз сети интернета вещей. Для этих целей используется инструмент тестирования производительности eMQTT-Bench. На данный момент ведётся сбор данных аномального трафика, имитирующего следующие типы атак:

- Массовая отправка запросов на подключение к брокеру в течение короткого промежутка времени.
- Большое количество запросов на подписку к брокеру за ограниченный период.
- Множество запросов брокеру на публикацию сообщений в короткий промежуток времени.
- Перебор комбинаций логин/пароль для брокеров с настроенной аутентификацией.

Реализованы единичные источники атак и варианты угроз из нескольких распределённых источников. Сбор данных об угрозах, характерных для систем интернета вещей, позволяет исследовать устойчивости к атакам при использовании различных платформ брокеров, оценивать влияние способов конфигурирования политик безопасности и выявить уязвимости сети.

Исследовательский стенд функционирует на протяжении более двух лет и позволил собрать более 1 ТБ сетевого трафика Netflow и около 50Гб данных Pcap, поступающих с IoT-устройств. В процессе работы с данными многофункционального исследовательского стенда учащиеся получают возможность сосредоточиться на решении практических задач в условиях, максимально приближенных к реальным.

IV. Заключение

В работе предложен подход к созданию многофункционального исследовательского стенда, позволяющего формировать навыки самостоятельного решения задач по дисциплинам, связанным с информационными и вычислительными сетями, информационной безопасностью и методами интеллектуального анализа данных. Стенд представляет масштабируемую сетевую инфраструктуру для изучения особенностей организации межмашинного взаимодействия в концепции интернета вещей.

Одним из ключевых преимуществ стенда является его гибкость. Реализованные конфигурации брокеров на базе популярных программных платформ позволяют исследовать влияние различных политик безопасности и параметров на производительность и устойчивость IoT-сети. Сбор данных осуществляется как с физических устройств, так и с программных агентов, размещённых на устройствах, через которые проходит сетевой трафик. Это даёт возможность анализировать реальный трафик, а также моделировать потенциальные угрозы.

Таким образом, разработанный исследовательский стенд представляет собой эффективный инструмент для подготовки высококвалифицированных специалистов. Работая с данными стенда, обучающиеся могут углублённо изучать технологии и методы их применения, решать прикладные задачи и развивать навыки, необходимые для успешной работы в IT-сфере.

Проведение дальнейших исследований будет направлено на расширение функциональности стенда, интеграцию в него инструментов визуализации и анализа данных для совершенствования механизмов обеспечения информационной безопасности.

Список литературы

[1] Лаптева С.В. Информационные технологии в высшем образовании // Современное педагогическое образование, 2023, №2, С. 120-125.

[2] Бородина Н.А., Подгорская С.В., Анисимова О.С. Информационные технологии в образовании: монография: Донской ГАУ, 2021, 168 с.

[3] Чернявская В.С. Методологические основы формирования современной цифровой образовательной среды: монография: «ООО «Изд-во «Элит», 2018, 174 с.

[4] Калиберда Е.А., Шабалин А.М. Программно-аппаратный стенд как современное средство обучения студентов настройке беспроводных сетей // Russian Journal of Education and Psychology, 2022, № 6, С. 45-58.

[5] 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, pp. 040030.

[6] Самсонов М.Ю., Гребешков А.Ю., Росляков А.В., Ваняшин С.В. Стандартизация интернета вещей // «Электросвязь», 2013, № 8, С. 10-13.

[7] Atzori L., Iera A., Morabito G. The internet of things: A survey // Computer Networks, 2010, № 54(15), pp. 2787-2805.

[8] Javed A., Heljanko K., Buda A., Främling K. CEFIoT: A fault-tolerant IoT architecture for edge and cloud // IEEE World Forum on Internet of Things, 2018, pp. 813-818.

[9] Ermolenko D., Kilicheva C., Muthanna A., Khakimov A. Internet of things services orchestration framework based on Kubernetes and edge computing // IEEE Conference of russian young researchers in electrical and electronic engineering, 2021, pp. 12-17.

[10] MQTT: The Standard for IoT Messaging [Электронный ресурс]. URL: https://mqtt.org/ (дата обращения: 28.04.2025)

[11] 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, pp. 1–5.

[12] 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.