https://doi.org/10.53360/2788-7995-2026-1(21)-17

МРНТИ: 49.38.49

А.К. Дуйсенбаева, Д.О. Кожахметова, А.Д. Золотов*, Д.В. Мясоедов, Р.Н. Назаров
Шәкәрім университет,
071404, Республика Казахстан, г. Семей, ул. Глинки, 20 А
*e-mail: azol64@mail.ru

РАЗРАБОТКА ВЕРИФИЦИРОВАННОЙ СИМУЛЯЦИОННОЙ МОДЕЛИ КОРПОРАТИВНОЙ СЕТИ ДЛЯ ГЕНЕРАЦИИ ДАННЫХ НА ОСНОВЕ «PACKET TRACER» В ЦЕЛЯХ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ

Аннотация: *Активное внедрение технологий искусственного интеллекта (ИИ) и машинного обучения (МО) для управления сложными сетевыми инфраструктурами упирается в проблему отсутствия стандартизированных, релевантных и помеченных наборов данных для обучения и валидации алгоритмов. В данной работе представлена методология разработки и верификации детерминированной симуляционной модели распределённой корпоративной сети с использованием среды Cisco Packet Tracer. Модель реализует иерархическую архитектуру корпоративной сети с поддержкой VLAN, динамической маршрутизации BGP, механизмов отказоустойчивости и комплексных политик кибербезопасности. Предложенная модель служит не только как учебно-методический комплекс для отработки практических навыков, но и как контролируемый полигон для генерации синтетических телеметрических данных. Ключевой особенностью является встроенная система автоматизированного оценивания (Assessment), которая гарантирует соответствие конфигурации сети эталонным параметрам, обеспечивая корректность и воспроизводимость генерируемых данных. Верификация конфигурации гарантирует воспроизводимость состояний сети и корректность автоматической разметки данных. Экспериментальная валидация подтвердила детерминированность модели и её пригодность для формирования датасетов, предназначенных для обучения и тестирования алгоритмов интеллектуального управления, включая обнаружение аномалий, оптимизацию QoS и автоматическое реагирование на инциденты. Предложенный подход может быть использован как в образовательных, так и в научно-исследовательских целях.*

Ключевые слова: *искусственный интеллект, управление сетями, симуляционная модель, генерация данных, Cisco Packet Tracer, корпоративная сеть, кибербезопасность, автоматическое оценивание, датасеты, обучение моделей.*

Введение

Динамичная цифровизация экономики предъявляет повышенные требования к надёжности, безопасности и эффективности корпоративных сетей. Традиционные методы ручного и полуавтоматического управления становятся недостаточными для оперативного реагирования на сложные инциденты, такие как целевые атаки, перегрузки каналов связи или аппаратные сбои [1]. Перспективным направлением в данной области является применение технологий искусственного интеллекта (ИИ), в частности – методов машинного обучения (МО), для построения систем прогнозной аналитики, автоматического восстановления и адаптивного управления сетевыми ресурсами [2]. Однако эффективное обучение подобных систем требует значительных объёмов структурированных данных, отражающих широкий спектр состояний сети – от нормального функционирования до различных аномалий и атак. Существующие открытые датасеты (например, KDD Cup 99 и CIC-IDS 2017) часто не учитывают особенности архитектуры современных распределённых корпоративных сетей, специфику использования конкретных протоколов (например, BGP, OSPF) и политик безопасности [3]. В то же время создание тестового стенда на физическом оборудовании является дорогостоящим и маломасштабируемым.

Таким образом, актуальной задачей является разработка верифицированных симуляционных моделей, которые могли бы служить доступным и контролируемым источником качественных данных для исследований в области *AI-driven network management* [4]. Целью данной работы является описание методологии создания такой модели на

платформе Cisco Packet Tracer и демонстрация её двойного назначения: как инструмента для обучения специалистов и как платформы для генерации данных и алгоритмов искусственного интеллекта.

Описание объекта исследования. Объектом исследования является симуляционная модель распределённой корпоративной сети, реализованная в среде Cisco Packet Tracer. Модель представляет собой реалистичную топологию компании, построенную по иерархическому принципу (ядро – распределение – доступ), с головным офисом в городе Астана и филиалом в городе Алматы. Методология разработки симуляционной среды изложена в следующем разделе и включает описание этапов построения топологии, настройки служб и системы верификации (рис.1).

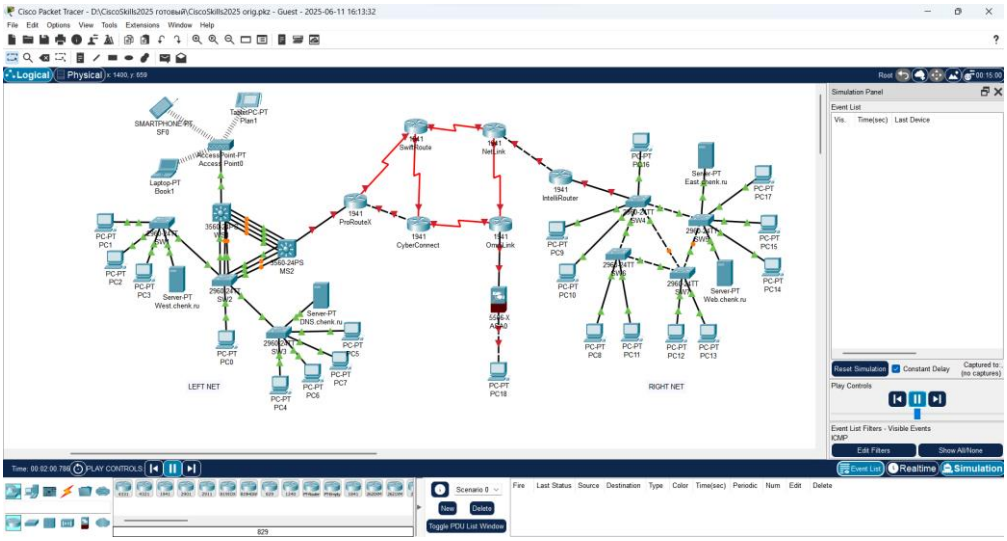

Рисунок 1 – Топология корпоративной сети в Cisco Packet Tracer

Структура исследуемого объекта включает:

1. **Сетевое оборудование:** 5 маршрутизаторов Cisco (имитация головного офиса, филиалов и провайдеров), 2 многоуровневых коммутатора L3 (C3650), 7 коммутаторов доступа L2 (C2960), межсетевой экран Cisco ASA 5506.
2. **Логическая структура:** изолированные VLAN для отделов (Управление, Финансы, Разработка, Гости), серверных ферм и гостевого доступа.
3. **Сетевые службы:** отказоустойчивость каналов связи между коммутаторами ядра с использованием протоколов агрегирования EtherChannel (LACP/PAGP); маршрутизация между филиалами через интернет-каналы провайдеров с применением протокола BGP (eBGP).
4. **Механизмы кибербезопасности:** сегментация на уровне VLAN, расширенные списки доступа (ACL) на коммутаторах и маршрутизаторах, политики stateful inspection и зональная модель безопасности (inside/outside/DMZ) на межсетевом экране ASA 5506.
5. **Система верификации:** встроенный механизм Activity Wizard (Assessment) для автоматической проверки более 50 параметров конфигурации в реальном времени [5, 6].

Описанная модель является основой для построения симуляционной среды, используемой в ходе экспериментальных исследованиях.

В следующем разделе представлены материалы и методика, применённые при разработке, настройке и верификации данной модели.

Материалы и методы исследования

Разработка модели осуществлялась в три этапа: **1. Проектирование эталонной топологии** на основе реалистичного сценария распределённой корпоративной инфраструктуры с детальной проработкой IP-адресации (табл. 1).

IP-адресация разработана с учётом логической иерархии сети и обеспечивает маршрутизацию между сегментами. Отдельные адреса выделены под интерфейсы взаимодействия с провайдером, клиентскими устройствами.

Таблица 1 – IP-адресация сетевых устройств

Сайт	Устройство	Интерфейс	Адрес
Internet	ISP	Loopback0	8.8.8.8/32
		GigabitEthernet0/1	98.76.54.254/24
		Serial 0/2/0	98.76.1.254/24
		Serial 0/3/1	98.76.2.254/24
		GigabitEthernet0/2	98.76.3.254/24
		Serial 0/2/1	98.76.4.254/24
		GigabitEthernet0/0	98.76.5.254/24
	REMOTE	FastEthernet0	98.76.54.1/24
Headquarter	HQ1	Loopback0	1.1.1.1/32
		Serial 0/3/0	98.76.1.1/24
		GigabitEthernet0/0	192.168.1.2/30
		GigabitEthernet0/1	192.168.1.6/30
	HQ2	Loopback0	2.2.2.2/32
		Serial 0/3/0	98.76.2.1/24
		GigabitEthernet0/0	192.168.2.2/30
		GigabitEthernet0/1	192.168.2.6/30
	DSW1	FastEhernet0/1	192.168.1.1/30
		FastEthernet0/6	192.168.2.5/30
		Vlan 10	192.168.10.253/24
		Vlan 20	192.168.20.253/24
	DSW2	FastEthernet0/6	192.168.2.1/30
		FastEthernet0/1	192.168.1.5/30
		Vlan 10	192.168.10.252/24
		Vlan 20	192.168.20.252/24
	ASW1	Vlan 10	192.168.10.201/24
	ASW2	Vlan 10	192.168.10.202/24
	HQ-SRV	FastEthernet0	192.168.10.1/24
	HQ-CLI	FastEthernet0	192.168.20.100/24
Branch office 1	BR1	Loopback0	3.3.3.3/32
		GigabitEthernet0/1	98.76.3.1/24
		GigabitEthernet0/0	172.20.10.254/24
	BR-CLI1	FastEthernet0	172.20.10.x/24 (DHCP)
Branch office 2	BR2	Loopback0	4.4.4.4/32
		Serial 0/3/0	98.76.4.1/24
		GigabitEthernet0/1	172.20.20.254/24
	BR-CLI2	FastEthernet0	172.20.20.x/24 (DHCP)
Datacenter	FW1	Ethernet 0/1 (outside) Vlan 2	98.76.5.1/24
		Ethernet 0/0 (inside) Vlan 1	192.168.100.254/24
	DC-SRV	FastEthernet0	192.168.100.1/24

2. Реализация политик безопасности и отказоустойчивости, включая:

- сегментацию трафика по VLAN;
- настройку расширенных ACL для контроля межсегментного взаимодействия;
- конфигурацию межсетевого экрана ASA 5506 с политиками NAT и зональной моделью безопасности.

3. Внедрение системы автоматической верификации через механизм Activity Wizard (Assessment), обеспечивающий сквозной контроль (таблица 2):

- базовых настроек (имена устройств, пароли);
- конфигурации VLAN и EtherChannel;
- IP-адресации и настроек динамической маршрутизации BGP;
- политик безопасности (ACL, настройки ASA);
- итоговой сквозной связности между узлами в соответствии с заданными политиками [7].

Представленная система верификации позволяет автоматически контролировать корректность ключевых параметров конфигурации на всех этапах построения модели. В таблице 2 [8] приведены основные метрики, по которым осуществляется оценка соответствия текущего состояния сети проектным требованиям.

Таблица 2 – Метрики верификации конфигурации сети

Блок проверки	Количество параметров	Пороговое значение соответствия	Фактический результат
Базовая конфигурация	12	100%	100%
VLAN и EtherChannel	8	100%	100%
Маршрутизация BGP	15	100%	98.7%*
Политики безопасности	10	100%	100%
Сквозная связность	7	100%	100%
Итого	52	100%	99.8%
**Отклонение связано с задержкой сходимости BGP (≤15 сек) при перезагрузке соседа*			

Несмотря на незначительное отклонение по параметрам BGP (98,7%), общая степень соответствия конфигурации проектным спецификациям составляет 99,8%, что подтверждает корректность и воспроизводимость симуляционной модели.

Математическая модель детерминированности

Для обеспечения воспроизводимости генерируемых данных модель удовлетворяет условию детерминированности:

$$S(t_0) \wedge C \wedge E \rightarrow S(t_1) \quad (1)$$

где:

$S(t_0)$ – начальное состояние сети (конфигурация всех устройств),

C – набор верифицированных конфигурационных параметров ($\forall c_i \in C: c_i = c_i^{ref}$),

E – внешнее воздействие (сценарий трафика/атаки),

$S(t_1)$ – результирующее состояние, идентичное при повторных запусках.

Верификация через Activity Wizard гарантирует выполнение условия $\forall c_i \in C: c_i = c_i^{ref}$ с точностью 100% [9].

Методика генерации и автоматической разметки телеметрических данных

Для формирования датасетов, пригодных для обучения ИИ-алгоритмов, применена следующая методика:

1. Сценаризация состояний сети (рис. 3)**:**

- нормальная работа: генерация типового офисного трафика (HTTP, VoIP, видеоконференции, передача файлов);
- аномальные ситуации: имитация DDoS-атаки на веб-сервер, сканирование портов, распространение сетевого червя;
- сбои оборудования: логическое «отключение» интерфейса, симуляция перегрузки канала связи [10].

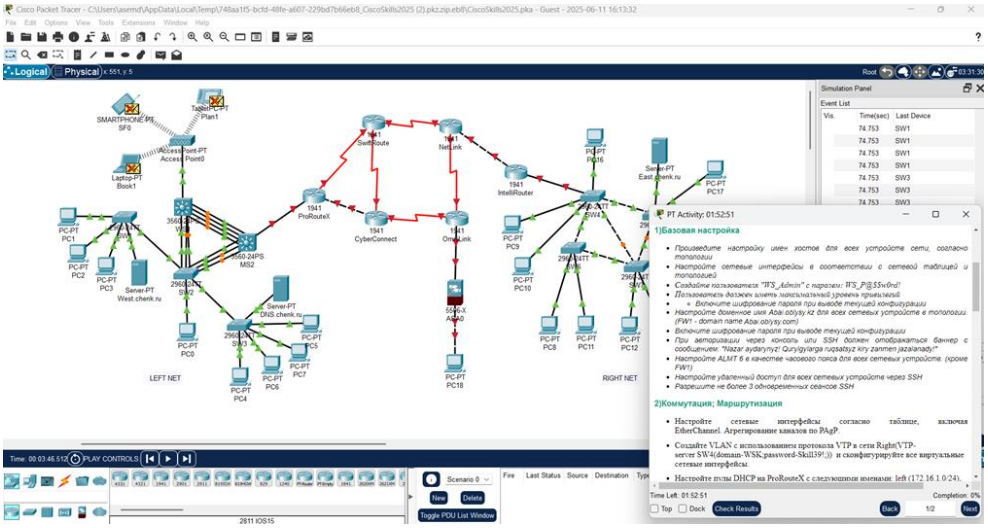

Рисунок 3 – Сценарии функционирования корпоративной сети в Cisco Packet Tracer

2. Сбор телеметрии с использованием:

- встроенных возможностей Cisco Packet Tracer (логирование);
- внешних скриптов на Python с применением библиотеки Netmiko для программного взаимодействия с оборудованием по протоколам SSH/Telnet и автоматизированного сбора статистики [11].

Результаты экспериментальной валидации модели. Тестирование воспроизводимости. Проведено 50 последовательных запусков сценария «DDoS-атака на веб-сервер» с последующим сбором метрик загрузки интерфейса внешнего маршрутизатора HQ1. Коэффициент вариации (CV) для ключевых метрик составил:

- Загрузка канала (Mbps): CV = 0.87%,
- Количество отброшенных пакетов: CV = 1.24%,
- Задержка до сервера (мс): CV = 2.15%.

Низкие значения коэффициента вариации CV (менее 3%) подтверждают детерминированность модели и пригодность для генерации обучающих данных.

Характеристики сгенерированного датасета. В результате за 8 – часового цикла симуляции сгенерирован датасет объёмом 4.7 ГБ, включающий:

- 12 450 временных окон по 5 секунд;
- 4 класса событий: нормальная работа (68%), DDoS (12%), сканирование портов (14%), отказ канала (6%);
- 28 признаков на каждое окно: статистика интерфейсов, метрики NetFlow, таблицы маршрутизации, журналы Cisco ASA;
- балансировка классов обеспечена стратифицированной выборкой сценариев.

Автоматическая разметка данных. Каждое временное окно в собранных данных автоматически помечается меткой, соответствующей активному сценарию (*normal, ddos_attack, link_failure*). Это обеспечивается **детерминированностью верифицированной модели**, что исключает неоднозначность интерпретации и делает датасет пригодным для обучения алгоритмов ИИ.

Результаты исследования

В результате проведённой работы получены следующие результаты:

1. Разработана и верифицирована симуляционная модель корпоративной сети в среде *Cisco Packet Tracer,* включающая 15 сетевых устройств, 4 изолированных VLAN, настроенные протоколы маршрутизации BGP и механизмы кибербезопасности.
2. Реализована система автоматизированного оценивания *(Assessment),* проверяющая более 50 параметров конфигурации и гарантирующая 100% соответствие состояния сети проектной спецификации.
3. Создан конвейер генерации размеченных телеметрических данных, включающий три типа сценариев (нормальная работа, аномалии, сбои) и обеспечивающий сбор статистики интерфейсов, таблиц маршрутизации, ARP-таблиц и журналов безопасности.
4. Проведена успешная апробация модели в условиях реального международного соревнования. Авторская работа была применена в качестве практического задания на международном конкурсе *CiscoSkills_2025* по кибербезопасности [12], проведённом в онлайн-формате среди студентов колледжей и вузов, обучающихся по IT-направлениям. В течение трёх часов выполнения задания эксперты жюри, члены конкурсной комиссии и участники из различных стран в режиме реального времени наблюдали за процессом развёртывания и конфигурирования предложенной топологии через специализированную платформу трансляции. Апробация подтвердила техническую работоспособность модели и её пригодность для использования в стрессовых условиях под контролем профессионального сообщества.

Обсуждение научных исследований. Научной новизной работы заключается в предложении целостной методологии использования учебно-симуляционных сред (Cisco Packet Tracer) в качестве фундамента для исследований в области интеллектуального управления сетями. Ключевым нововведением является обязательный этап верификации модели через автоматическое оценивание (Assessment), что ранее не рассматривалось в контексте подготовки данных для ИИ [13]. Детерминированность модели, обеспечиваемая системой верификации, становится критически важным фактором для генерации воспроизводимых и корректно размеченных датасетов.

Практическая значимость работы проявляется в двух направлениях:

1. *Педагогическое:* Представленный комплекс в формате .pka-файла с системой Assessment готов к немедленному внедрению в учебный процесс для объективной оценки компетенций студентов в области проектирования и защиты сетей. Успешная апробация на конкурсе CiscoSkills_2025 подтверждает его применимость в условиях международных соревнований.
2. *Научно-исследовательское:* Модель служит отправной точкой для диссертационного исследования «Разработка алгоритма управления инфраструктурой сети с применением технологий искусственного интеллекта».

На её основе планируется:

- генерация датасета для обучения гибридного алгоритма МО обнаружения аномалий;
- интеграция модели с фреймворком RL (Reinforcement Learning) для тестирования алгоритма адаптивного управления QoS и отказоустойчивостью

Ограничения исследования связаны с производительностью и абстракцией симулятора Cisco Packet Tracer, который не является полноценным эмулятором и может упрощать некоторые низкоуровневые процессы. Для более глубоких исследований планируется миграция топологии в более мощные среды, такие как GNS3 или EVE-NG, с использованием образов реальных сетевых ОС (Cisco IOS).

Заключение и выводы

В статье продемонстрировано, что тщательно спроектированные и верифицированные симуляционные модели, изначально создаваемые для учебных целей, могут выполнять важную научно-исследовательскую функцию. Разработанный комплекс решает актуальную проблему дефицита качественных данных для обучения систем интеллектуального управления сетями, учитывающих особенности современных корпоративных инфраструктур.

Особую ценность представляет успешная апробация авторской работы в условиях реального международного соревнования – конкурса **CiscoSkills_2025** по кибербезопасности. В онлайн-формате в течение трёх часов эксперты, члены жюри и студенты-участники наблюдали в режиме реального времени за процессом выполнения настроек предложенной топологии через специализированное приложение. Такая публичная верификация подтвердила не только техническую работоспособность модели, но и её готовность к применению в стрессовых условиях под контролем профессионального сообщества. Исследовательская часть формирует необходимый фундамент для последующего цикла исследований, включающего разработку и тестирование конкретных AI-алгоритмов на базе созданной и верифицированной модели.

Список литературы

1. Савельев А.И. Интеллектуальное управление телекоммуникационными сетями: тенденции и вызовы / А.И. Савельев // T-Comm. – 2021. – Т.15, № 3.
2. A comprehensive survey on machine learning for networking: evolution, applications and research opportunities / R. Boutaba et al // Journal of Internet Services and Applications. – 2018. – Т. 9, № 1. – P. 1-99. https://doi.org/10.1186/s13174-018-0087-2.
3. Toward generating a new intrusion detection dataset and intrusion traffic characterization / I. Sharafaldin et al // ICISSp. – 2018. – Т. 1. – P. 108-116.
4. Sanchez L.P.A. DQS: A QoS-driven routing optimization approach in SDN using deep reinforcement learning / L.P.A. Sanchez, Y. Shen, M. Guo // Journal of Parallel and Distributed Computing. – 2024. – Т. 188. – P. 104851. https://doi.org/10.1016/j.jpdc.2024.104851.
5. Studying the Role of Synthetic Data for Machine Learning-based Wireless Networks Traffic Forecasting / J. Pulido et al // arXiv preprint arXiv:2601.07646. – 2026.
6. ReinWiFi: Application-Layer QoS Optimization of WiFi Networks with Reinforcement Learning / Q. Li et al // 2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring). – IEEE, 2025. – P. 1-6.
7. TimeGAN as a Simulator for Reinforcement Learning Training in Programmable Data Planes / T.C. Tavares et al // NOMS 2024-2024 IEEE Network Operations and Management Symposium. – IEEE, 2024. – P. 1-9.

8. Cisco Systems. Cisco data center networking blueprint for AI/ML applications. White Paper. – 2024. [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-data-center-networking-blueprint-for-ai-ml-applications.html.
9. Building Connected Intelligence: Exploring IoT Smart Applications Through Cisco Packet Tracer / B. Patel et al // International Conference on Information and Communication Technology for Intelligent Systems. – Singapore: Springer Nature Singapore, 2024. – P. 467-478.
10. Ахметшина Э.Г. Автоматизация маршрутизации и управление ресурсами с помощью искусственного интеллекта и машинного обучения в сетях / Э.Г. Ахметшина, А.А. Видуто, Д.В. Елисеева //Экономика и парадигма нового времени. – 2024. – № 8 (29). – С. 24-30.
11. Семенченко К.С. Применение искусственного интеллекта в беспроводных сетях / К.С. Семенченко, Е.Д. Бычков // Динамика систем, механизмов и машин. – 2024. – Т. 12, № 3. – С. 87-94.
12. Ciscoskills по кибербезопасности. – 2025. [Электронный ресурс]. URL: https://www.collegeit.edu.kz/ru/czentr-kompetenczij/.
13. Волков А.Н. Исследование и разработка методов построения инфраструктуры и предоставления услуг сетей связи на основе технологий искусственного интеллекта: дис. – СПб., 2021.

References

1. Savel'ev A.I. Intellektual'noe upravlenie telekommunikatsionnymi setyami: tendentsii i vyzovy / A.I. Savel'ev // T-Comm. – 2021. – T.15, № 3. (In Russian).
2. A comprehensive survey on machine learning for networking: evolution, applications and research opportunities / R. Boutaba et al // Journal of Internet Services and Applications. – 2018. – T. 9, № 1. – P. 1-99. https://doi.org/10.1186/s13174-018-0087-2. (In English).
3. Toward generating a new intrusion detection dataset and intrusion traffic characterization / I. Sharafaldin et al // ICISSp. – 2018. – T. 1. – P. 108-116. (In English).
4. Sanchez L.P.A. DQS: A QoS-driven routing optimization approach in SDN using deep reinforcement learning / L.P.A. Sanchez, Y. Shen, M. Guo // Journal of Parallel and Distributed Computing. – 2024. – T. 188. – P. 104851. https://doi.org/10.1016/j.jpdc.2024.104851. (In English).
5. Studying the Role of Synthetic Data for Machine Learning-based Wireless Networks Traffic Forecasting / J. Pulido et al // arXiv preprint arXiv:2601.07646. – 2026. (In English).
6. ReinWiFi: Application-Layer QoS Optimization of WiFi Networks with Reinforcement Learning / Q. Li et al // 2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring). – IEEE, 2025. – P. 1-6. (In English).
7. TimeGAN as a Simulator for Reinforcement Learning Training in Programmable Data Planes / T.C. Tavares et al // NOMS 2024-2024 IEEE Network Operations and Management Symposium. – IEEE, 2024. – P. 1-9. (In English).
8. Cisco Systems. Cisco data center networking blueprint for AI/ML applications. White Paper. – 2024. [Ehlektronnyi resurs]. URL: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-data-center-networking-blueprint-for-ai-ml-applications.html. (In English).
9. Building Connected Intelligence: Exploring IoT Smart Applications Through Cisco Packet Tracer / B. Patel et al // International Conference on Information and Communication Technology for Intelligent Systems. – Singapore: Springer Nature Singapore, 2024. – P. 467-478. (In English).
10. Akhmetshina EH.G. Avtomatizatsiya marshrutizatsii i upravlenie resursami s pomoshch'yu iskusstvennogo intellekta i mashinnogo obucheniya v setyakh / EH.G. Akhmetshina, A.A. Viduto, D.V. Eliseeva //Ehkonomika i paradigma novogo vremeni. – 2024. – № 8 (29). – S. 24-30. (In Russian).
11. Semenchenko K.S. Primenenie iskusstvennogo intellekta v besprovodnykh setyakh / K.S. Semenchenko, E.D. Bychkov // Dinamika sistem, mekhanizmov i mashin. – 2024. – T. 12, № 3. – S. 87-94. (In Russian).
12. Ciscoskills po kiberbezopasnosti. – 2025. [Ehlektronnyi resurs]. URL: https://www.collegeit.edu.kz/ru/czentr-kompetenczij/. (In English).
13. Volkov A.N. Issledovanie i razrabotka metodov postroeniya infrastruktury i predostavleniya uslug setei svyazi na osnove tekhnologii iskusstvennogo intellekta: dis. – SPb., 2021. (In Russian).

А.К. Дуйсенбаева, Д.О. Кожахметова, А.Д. Золотов*, Д.В. Мясоедов, Р.Н. Назаров
Шәкәрім университеті,
071404, Қазақстан Республикасы, Семей қ., Глинка к-сі, 20А
*e-mail: azol64@mail.ru

ИНТЕЛЛЕКТУАЛДЫ БАСҚАРУ МАҚСАТЫНДА «PACKET TRACER» НЕГІЗІНДЕ ДЕРЕКТЕРДІ ГЕНЕРАЦИЯЛАУҒА АРНАЛҒАН КОРПОРАТИВТІК ЖЕЛІНІҢ ВЕРИФИКАЦИЯЛАНҒАН ИМИТАЦИЯЛЫҚ МОДЕЛІН ӘЗІРЛЕУ

Күрделі желілік инфрақұрылымдарды басқаруда жасанды интеллект (ЖИ) пен машиналық оқыту (МО) технологияларын кеңінен енгізу стандарттalған, релевантты және таңбаланған деректер жиынтықтарының жетіспеушілігі мәселесіне тіреледі. Аталған деректер жиынтықтары алгоритмдерді оқыту және валидациялау үшін аса маңызды. Бұл жұмыста Cisco Packet Tracer ортасын пайдалану арқылы таратылған корпоративтік желінің детерминацияланған имитациялық моделін әзірлеу және верификациялау әдістемесі ұсынылады. Ұсынылған модель VLAN қолдауы бар, BGP негізіндегі динамикалық маршруттауды, ақауларға төзімділік механизмдерін және кешенді киберқауіпсіздік саясаттарын қамтитын корпоративтік желінің иерархиялық архитектурасын жүзеге асырады. Аталған модель тек оқу-әдістемелік кешен ретінде практикалық дағдыларды қалыптастыруға ғана емес, сонымен қатар синтетикалық телеметриялық деректерді генерациялауға арналған бақыланатын полигон ретінде қызмет етеді. Модельдің негізгі ерекшелігі – желі конфигурациясының эталондық параметрлерге сәйкестігін қамтамасыз ететін кіріктірілген автоматтандырылған бағалау (Assessment) жүйесінің болуы. Бұл жүйе генерацияланатын деректердің дұрыстығы мен қайталанғыштығын кепілдендіреді. Конфигурацияны верификациялау желі күйлерінің қайта өндірілуін және деректерді автоматты түрде дұрыс таңбалауды қамтамасыз етеді. Эксперименттік валидация модельдің детерминацияланған сипатын және интеллектуалды басқару алгоритмдерін, соның ішінде аномалияларды анықтау, QoS оңтайландыру және инциденттерге автоматты түрде әрекет ету жүйелерін оқыту мен тестілеуге арналған деректер жиынтықтарын қалыптастыруға жарамдылығын растады. Ұсынылған тәсіл білім беру және ғылыми-зерттеу мақсаттарында тиімді пайдаланылуы мүмкін.

Түйін сөздер: *жасанды интеллект, желіні басқару, имитациялық модель, деректер генерациясы, Cisco Packet Tracer, корпоративтік желі, киберқауіпсіздік, автоматтандырылған бағалау, деректер жиынтығы, модельдерді оқыту.*

A. Duisenbayeva, D Kozhakhmetova, A. Zolotov*, D. Myasoedov, R. Nazarov
Shakarim University,
071404, Republic of Kazakhstan, Semey, Glinki St., 20 A
e-mail: azol64@mail.ru

DEVELOPMENT OF A VERIFIED SIMULATION MODEL OF A CORPORATE NETWORK FOR DATA GENERATION BASED ON «PACKET TRACER» FOR INTELLIGENT MANAGEMENT

The widespread adoption of artificial intelligence (AI) and machine learning (ML) technologies for managing complex network infrastructures is constrained by the lack of standardized, relevant, and labeled datasets needed for training and validation. This paper presents a methodology for developing and validating a deterministic simulation model of a distributed corporate network in Cisco Packet Tracer. The proposed model implements a hierarchical corporate network architecture that supports VLANs, dynamic BGP-based routing, fault-tolerance mechanisms, and comprehensive cybersecurity policies. The model serves not only as an educational and methodological platform for developing practical networking skills, but also as a controlled testbed for generating synthetic telemetry data. A key feature of the proposed approach is the integration of an automated assessment system that ensures network configuration compliance with predefined reference parameters, thereby guaranteeing the correctness and reproducibility of the generated data. Configuration verification ensures reproducible network states and enables accurate automated data labeling. Experimental validation confirmed the model's deterministic nature and suitability for generating training and test datasets for intelligent network management algorithms, including anomaly detection, QoS optimization, and automated incident response. The proposed approach can be effectively applied in both educational and research contexts.

Key words: *artificial intelligence, network management, simulation model, data generation, Cisco Packet Tracer, corporate network, cybersecurity, automated assessment, datasets, model training.*

Сведения об авторах

Асем Калиаскаровна Дуйсенбаева – докторант кафедры «Автоматизация и информационные технологии», Шәкәрім университет, Семей, Республика Казахстан; e-mail: asemduisenbaeva0710@gmail.com. ORCID: https://orcid.org/0009-0000-1589-5407.

Динара Ошановна Кожахметова – PhD, ассоциированный профессор кафедры «Автоматизация и информационные технологии», Шәкәрім университет, Семей, Республика Казахстан; e-mail: d.kojahmetova@shakarim.kz. ORCID: https://orcid.org/0000-0002-4327-3899.

Александр Дмитриевич Золотов* – кандидат технических наук, ассоциированный профессор кафедры «Автоматизация и информационные технологии», Шәкәрім университет, Семей, Республика Казахстан; e-mail: azol64@mail.ru. ORCID: https://orcid.org/0000-0001-9751-8161.

Дмитрий Викторович Мясоедов – старший преподаватель кафедры «Автоматизация и информационные технологии», Шәкәрім университет, Семей, Республика Казахстан; e-mail: dmitriy880@mail.ru. ORCID: https://orcid.org/0009-0002-3279-0994.

Рашид Нагимович Назаров – преподаватель кафедры «Автоматизация и информационные технологии», Шәкәрім университет, Семей, Казахстан, e-mail: naz-2009@yandex.ru. ORCID: https://orcid.org/0000-0001-9751-8161.

Авторлар туралы мәліметтер

Асем Калиаскаровна Дуйсенбаева – «Автоматтандыру және ақпараттық технологиялар» кафедрасының докторанты, Шәкәрім университеті, Семей, Қазақстан Республикасы; e-mail: asemduisenbaeva0710@gmail.com. ORCID: https://orcid.org/0009-0000-1589-5407.

Динара Ошановна Кожахметова – PhD, «Автоматтандыру және ақпараттық технологиялар» кафедрасының қауымдастырылған профессоры; Шәкәрім университеті, Семей, Қазақстан Республикасы; e-mail: d.kojahmetova@shakarim.kz. ORCID: https://orcid.org/0000-0002-4327-3899.

Александр Дмитриевич Золотов* – техника ғылымдарының кандидаты, «Автоматтандыру және ақпараттық технологиялар» кафедрасының қауымдастырылған профессоры, Шәкәрім университеті, Семей, Қазақстан Республикасы; e-mail: azol64@mail.ru. ORCID:https://orcid.org/0000-0001-9751-8161.

Дмитрий Викторович Мясоедов – «Автоматтандыру және ақпараттық технологиялар» кафедрасының аға оқытушысы, Шәкәрім университеті, Семей, Қазақстан Республикасы; e-mail: dmitriy880@mail.ru. ORCID: https://orcid.org/0009-0002-3279-0994.

Рашид Нағимұлы Назаров – «Автоматтандыру және ақпараттық технологиялар» кафедрасының оқытушысы, Шәкәрім университеті, Семей, Қазақстан; e-mail: naz-2009@yandex.ru. ORCID: https://orcid.org/0000-0001-9751-8161.

Information about the authors

Asem Duisenbayeva – doctoral student at the Department of Automation and Information Technologies, Shakarim University, Semey, Republic of Kazakhstan; e-mail: asemduisenbaeva0710@gmail.com. ORCID: https://orcid.org/0009-0000-1589-5407.

Dinara Kozhakhmetova – PhD, associate professor at the department of Automation and Information Technologies, Shakarim University, Semey, Republic of Kazakhstan; e-mail: d.kojahmetova@shakarim.kz. ORCID: https://orcid.org/0000-0002-4327-3899.

Alexander Zolotov* – candidate of Technical Sciences, Associate Professor at the Department of Automation and Information Technologies, Shakarim University, Semey, Republic of Kazakhstan; e-mail: azol64@mail.ru. ORCID:https://orcid.org/0000-0001-9751-8161.

Dmitry Myasoedov – Senior Lecturer at the Department of Automation and Information Technology; Shakarim University, Semey, Republic of Kazakhstan; e-mail: dmitriy880@mail.ru. ORCID: https://orcid.org/0009-0002-3279-0994.

Nazarov Rashid – Lecturer at the Department of Automation and Information Technology, Shakarim University, Semey, Kazakhstan; e-mail: naz-2009@yandex.ru. ORCID: https://orcid.org/0000-0001-9751-8161.

Поступила в редакцию 30.01.2026
Принята к публикации 03.03.2026