

Автоматическая генерация сетевых конфигураций по текстовому описанию с использованием нейросети GPT-5.1

Саяпин Никита Анатольевич

Приамурский государственный университет им.Шолом-Алейхема

Студент

Аннотация

Целью данного исследования является демонстрация процесса автоматической генерации конфигураций сетевого оборудования (на примере Cisco IOS, Juniper Junos и MikroTik RouterOS) на основе текстового описания с использованием мультимодальной нейросети GPT-5.1. В работе рассматриваются принципы интерпретации текстового запроса, формирование структуры конфигурации и анализ соответствия сгенерированных настроек исходным требованиям.

Ключевые слова: искусственный интеллект, нейросеть, GPT-5.1, сети, автоматизация настройки, конфигурация, Cisco, Juniper, MikroTik.

Automatic generation of network configurations from textual description using the GPT-5.1 neural network

Sayapin Nikita Anatolyevich

Sholom-Aleichem Priamursky State University

Student

Abstract

The purpose of this study is to demonstrate the process of automatic generation of network device configurations (Cisco IOS, Juniper Junos, MikroTik RouterOS) from textual descriptions using the GPT-5.1 multimodal neural network. The paper examines how the model interprets textual prompts, constructs configuration structures, and how well the generated setups match the initial requirements.

Keywords: artificial intelligence, neural network, GPT-5.1, networking, automation, configuration, Cisco, Juniper, MikroTik.

1. Введение

1.1 Актуальность

Современные компьютерные сети становятся всё более сложными: растёт количество устройств, протоколов маршрутизации и политик безопасности. Ручная разработка конфигураций для оборудования различных вендоров (Cisco, Juniper, MikroTik и др.) требует высокой квалификации и занимает значительное время. Ошибки в конфигурации могут приводить к простоям, нарушению безопасности и снижению качества сервиса.

В этих условиях особенно актуальны подходы, позволяющие автоматизировать подготовку конфигураций на основе высокого уровня абстракции — текстового описания требований к сети: топологии, протоколов, адресных планов, политик доступа.

Мультимодальные модели нового поколения, такие как GPT-5.1, способны не только обрабатывать текст, но и генерировать структурированный технический код: конфигурации, скрипты, шаблоны. Использование GPT-5.1 в задачах text-to-config позволяет сократить трудозатраты инженеров, уменьшить вероятность ошибок и ускорить этапы проектирования и внедрения.

1.2 Обзор исследований

А. О. Суворов и В. А. Суворова рассмотрели применение методов интеллектуального анализа сетевого трафика для построения систем обнаружения вторжений, показав, что использование искусственных нейронных сетей позволяет повысить качество идентификации сетевых атак за счёт автоматизированного выделения информативных признаков в потоках данных [1]. А. М. Митрахович выполнил сравнительный анализ алгоритмов искусственного интеллекта, применяемых для защиты компьютерных сетей, и продемонстрировал, что эффективность различных методов машинного обучения существенно зависит от типа атак и характеристик контролируемой сети [2]. И. Б. Саенко исследовал эволюцию подходов к искусственному интеллекту и современное состояние исследований в этой области, уделив особое внимание задачам информационно-телекоммуникационных систем и отметив тенденцию перехода от локальных экспертных решений к комплексным интеллектуальным платформам управления инфраструктурой [3]. Е. Долматов проанализировал подходы к применению технологий искусственного интеллекта для решения задач автоматизированного управления в сложных технических системах, обосновав целесообразность использования ИИ-моделей для поддержки принятия решений и повышения степени автономности таких систем [4]. В. В. Аллакин предложил общий подход к построению перспективных систем мониторинга технических объектов, включая сетевое оборудование, показав, что интеллектуальная обработка телеметрии и автоматическая генерация предупреждений и отчётов позволяют повысить надёжность функционирования распределённой инфраструктуры [5].

1.3 Цель исследования

Цель исследования — продемонстрировать процесс автоматической генерации конфигураций сетевого оборудования по текстовому описанию с использованием нейросети GPT-5.1 и оценить точность интерпретации сетевых требований в разных сценариях.

2 Материалы и методы

В рамках исследования использовалась мультимодальная нейросеть GPT-5.1, обладающая возможностью преобразовывать текстовое описание сетевой инфраструктуры в структурированный конфигурационный код, совместимый с различными сетевыми платформами, такими как Cisco IOS, Juniper Junos и MikroTik RouterOS. Процесс генерации рассматривался как последовательность логически связанных этапов, начинающихся с формулировки текстового требования к будущей конфигурации. На этом этапе задавались ключевые параметры сети: протоколы маршрутизации, адресное пространство, топология, домены отказоустойчивости, требования к безопасности и особенности конкретного вендора.

3. Результаты

3.1 Настройка VLAN и доступа на коммутаторе Cisco

В первом сценарии, связанном с Cisco IOS, модель уверенно обработала описание, включающее создание двух VLAN, назначение access-портов в определённые диапазоны и настройку trunk-цепи с ограниченным набором VLAN. Кроме того, GPT-5.1 корректно настроила интерфейс управления и маршрут по умолчанию.

Промпт:

Generate a Cisco IOS switch configuration.

Requirements:

- create VLAN 10 “Users” and VLAN 20 “Servers”;
- access ports: Fa0/1–10 in VLAN 10, Fa0/11–15 in VLAN 20;
- trunk on Gi0/1 (allowed VLANs 10,20);
- set management IP 192.168.100.2/24 on VLAN 10, gateway 192.168.100.1.

Конфигурация корректно отражала структуру, заданную в описании. При этом модель автоматически добавила базовые команды (включение IP-маршрутизации для управляемого интерфейса, описание портов), что улучшило читаемость и эксплуатационные качества конфигурации.

Итоговая конфигурация отражала все заданные требования и отличалась структурной аккуратностью, что позволило быстро оценить её практическую применимость (Рис.1).

```
hostname SW-ACCESS-1

! Create VLANs
vlan 10
  name Users
vlan 20
  name Servers

! Access ports Fa0/1-10 in VLAN 10 (Users)
interface range FastEthernet0/1 - 10
  switchport mode access
  switchport access vlan 10
  spanning-tree portfast
  spanning-tree bpduguard enable

! Access ports Fa0/11-15 in VLAN 20 (Servers)
interface range FastEthernet0/11 - 15
  switchport mode access
  switchport access vlan 20
  spanning-tree portfast
  spanning-tree bpduguard enable

! Trunk on Gi0/1, allowed VLANs 10,20
interface GigabitEthernet0/1
  description Uplink-Trunk
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  spanning-tree portfast trunk

! Management SVI on VLAN 10
interface Vlan10
  ip address 192.168.100.2 255.255.255.0
  no shutdown

! Default gateway for management
ip default-gateway 192.168.100.1
```

Рисунок 1 – Создание конфигурации коммутатора Cisco

3.2 Конфигурация OSPF для небольшой сети (Juniper Junos)

Второй сценарий касался протокола OSPF в среде Juniper Junos. Здесь модель продемонстрировала понимание концепции разбиения сети на области и особенностей интерфейсной конфигурации Junos (Рис.2). Промпт:

Design a Juniper OSPF configuration for a small network.

Router has three interfaces:

- ge-0/0/0: 10.0.0.1/24 (area 0);
- ge-0/0/1: 10.0.1.1/24 (area 0);
- ge-0/0/2: 10.0.2.1/24 (area 1);

Set router ID 1.1.1.1 and advertise all connected networks in OSPF

```
junos

## Interfaces with IPs
set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.1/24

## Global router ID
set routing-options router-id 1.1.1.1

## OSPF – advertise all connected interfaces by enabling OSPF on them
## Area 0: ge-0/0/0 and ge-0/0/1
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0

## Area 1: ge-0/0/2
set protocols ospf area 0.0.0.1 interface ge-0/0/2.0
```

Рисунок 2 – Конфигурация небольшой сети

Сгенерированный фрагмент содержал корректный router-id, разделение интерфейсов между area 0 и area 1, а также точную структуру объявления протокола. GPT-5.1 показала способность адаптироваться под различия между конфигурационными моделями вендоров и учитывала специфичные для Junos принципы работы с протоколами.

3.3 Настройка BGP-пиринга между двумя автономными системами (MikroTik RouterOS)

Третий сценарий иллюстрировал установление BGP-пиринга в MikroTik RouterOS.

Промпт:

Generate a MikroTik RouterOS configuration for BGP peering.

Requirements:

- local AS 65001, remote AS 65002;
- local address 203.0.113.1, neighbor 203.0.113.2;
- establish IPv4 eBGP session;
- advertise local network 10.10.0.0/16;
- ensure basic inbound filter that only accepts prefixes up to /24.

Модель успешно обработала описание, в котором требовалось указать локальную и удалённую автономные системы, адреса соседей, правила анонса локальной сети и ограничения по длине принимаемых префиксов (Рис.3).

```
# WAN / BGP-facing interface
/ip address
add address=203.0.113.1/30 interface=ether1 comment="BGP link to 203.0.113.2"

# LAN / local network
add address=10.10.0.1/16 interface=bridge-local comment="Local LAN 10.10.0.0/16"

# -----
# BGP Instance
# -----
/routing bgp instance
set default as=65001 router-id=1.1.1.1

# -----
# BGP Filters
# -----
# Inbound: accept only prefixes up to /24, drop the rest
/routing filter
add chain=BGP-IN prefix-length=0-24 action=accept comment="Allow only prefixes up to /24"
add chain=BGP-IN action=discard comment="Drop more-specifics (/25+ etc.)"

# Outbound: only advertise 10.10.0.0/16
/routing filter
add chain=BGP-OUT prefix=10.10.0.0/16 prefix-length=16-16 action=accept comment="Advertise local 1"
add chain=BGP-OUT action=discard comment="Do not advertise other routes"

# -----
# BGP Peer (IPv4 eBGP)
# -----
/routing bgp peer
add name=EBGP-TO-65002 \
    remote-address=203.0.113.2 \
    remote-as=65002 \
    in-filter=BGP-IN \
    out-filter=BGP-OUT
```

Рисунок 3 – Конфигурация BGP-пиринга между отдельными системами

GPT-5.1 корректно сформировала конфигурацию, продемонстрировав способность учитывать как базовые параметры протокола BGP, так и дополнительные элементы безопасности, связанные с фильтрацией маршрутов.

3.4 Сравнение трех типов сценариев

Сравнение трёх сценариев позволяет выделить следующие наблюдения:

Объём и структурированность промпта напрямую влияют на качество конфигурации. Краткие запросы приводят к генерации минимально жизнеспособного набора команд, тогда как подробные описания с указанием VLAN, IP-адресов, протоколов и политик позволяют получить конфигурацию, близкую к «боевой».

GPT-5.1 корректно учитывает особенности конфигурационных языков разных вендоров (IOS, Junos, RouterOS), если это явно указано в запросе.

Модель проявляет склонность использовать best practices: добавлять описания интерфейсов, базовые настройки безопасности, фильтрацию маршрутов. Это повышает практическую ценность результата.

Основные ограничения связаны с тем, что модель не всегда учитывает существующую инфраструктуру (например, уже заданные политики или шаблоны), поэтому сгенерированная конфигурация требует обязательной проверки инженером перед применением в production-среде.

4 Выводы

Проведённое исследование подтверждает, что использование GPT-5.1 для автоматической генерации сетевых конфигураций по текстовому описанию является перспективным направлением развития инструментов автоматизации в сфере сетевых технологий.

Полученные результаты показывают:

- высокую чувствительность модели к деталям текстового запроса (addressing, протоколы, политики);
- способность GPT-5.1 адаптироваться под различные конфигурационные диалекты (Cisco IOS, Juniper Junos, MikroTik RouterOS);
- применимость подхода text-to-config для типовых задач: настройка VLAN, OSPF, BGP, базовых фильтров и политик.

Использование GPT-5.1 не отменяет необходимости участия сетевого инженера, но позволяет:

- ускорить подготовку черновых конфигураций;
- снизить количество синтаксических и типовых логических ошибок;
- использовать текстовое описание сети как удобный и понятный интерфейс взаимодействия с системой автоматизации.

Перспективными направлениями дальнейших исследований являются интеграция генерации конфигураций с системами верификации (эмуляторы, тестовые стенды), а также связка GPT-5.1 с инструментами NetDevOps (Ansible, Terraform, Nornir) для построения полностью автоматизированного конвейера «текстовое описание → конфигурация → проверка → развёртывание».

Библиографический список

1. Суворов А. О., Суворова В. А. Интеллектуальный анализ сетевого трафика для идентификации компьютерных вторжений // Искусственный интеллект и принятие решений. 2019. № 1. С. 62–73.
2. Митрахович А. М., Митрахович Ю. М. Сравнительный анализ алгоритмов искусственного интеллекта для защиты компьютерных сетей // Хроники цифровых трансформаций : Материалы межкафедрального круглого стола, Москва, 19–26 мая 2022 года. Т. 4. Волгоград: ИП Черняева Юлия Игоревна (Издательский дом «Сириус»), 2022. С. 93–99.
3. Саенко И. Б. Искусственный интеллект: история и современное состояние исследований // Применение искусственного интеллекта в информационно-телекоммуникационных системах: сборник материалов научно-практической конференции, Санкт-Петербург, 31 марта 2021 года / Военная академия связи. Санкт-Петербург: Федеральное государственное казённое военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Будённого» Министерства обороны Российской Федерации, 2021. С. 5–10.
4. Долматов Е. А. Подходы к применению технологий искусственного интеллекта для решения задач автоматизированного управления в сложных организационно-технических системах // Применение искусственного интеллекта в информационно-телекоммуникационных системах : сборник материалов научно-практической конференции, Санкт-Петербург, 31 марта 2021 года / Военная академия связи. Санкт-Петербург: Федеральное государственное казённое военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Будённого» Министерства обороны Российской Федерации, 2021. С. 62–68.
5. Аллакин В. В., Будко Н. П., Васильев Н. В. Общий подход к построению перспективных систем мониторинга распределённых информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 4. С. 125–227.