# **Титульный лист**

# **Задание на ВКР**

Тема: Автоматизация управления сетевой доступностью в контейнеризированной сети организации

# **Аннотация**

В работе предлагается решение по разработке и внедрению адаптивного алгоритма для обеспечения увеличения скорости конвергенции протокола граничного шлюза (BGP). Апробация алгоритма производится в открытой платформе для автоматизации развертывания и масштабирования контейнеризированных приложений с использованием модуля управления сетевой политикой.

Оглавление

[**Титульный лист** 1](#_Toc193629661)

[**Задание на ВКР** 2](#_Toc193629662)

[**Аннотация** 3](#_Toc193629663)

[**Список используемых сокращений** 5](#_Toc193629664)

[**Введение** 6](#_Toc193629665)

[**Литературный обзор** 7](#_Toc193629666)

[**1.1** **Обоснование выбора BGP** 7](#_Toc193629667)

[**2.1 Контейнеры** 7](#_Toc193629668)

[**Заключение** 9](#_Toc193629669)

[**Список использованных источников** 10](#_Toc193629670)

# **Список используемых сокращений**

ЛВС – Локальная вычислительная сеть

BGP – Borderline gate protocol/Протокол граничного шлюза

EBGP – External borderline gate protocol/Внешний протокол граничного шлюза

IBGP – Internal borderline gate protocol/Внутренний протокол граничного шлюза

CNI – Container networking interface/Сетевой интерфейс контейнера

K8s – Kubernetes

# **Введение**

В современном мире все пользуются сетью интернет и различного рода сервисами. Для реализации сервисов, которыми пользуются миллионы людей, используются такие технологии, как Docker и Kubernetes, в локальных или территориально распределённых вычислительных сетях с использованием технологии BGP для обеспечения маршрутизации между кластерами и контейнерами. Однако, BGP с стандартным набором параметров зачастую не обеспечивает наибольшую сходимость и надежность сети.

Цель моей работы – разработать и внедрить метод автоматизации сетевой доступности в контейнеризированную сеть организации.

Цель проекта определяет список задач работы:

* Планирование и описание сетевой инфраструктуры организации (стенда).
* Рассмотрение и анализ факторов, влияющих на эффективность BGP в описанной ЛВС.
* Реализация стенда(развертывание k8s, с плагином Calico)
* Разработка правил маршрутизации.
* Разработка адаптивного алгоритма.
* Использование программных средств для анализа трафика, позволяющих сделать качественную оценку внедренного решения. (снятие статистической картины с использованием инструментов, не влияющих на утилизацию канала связи)
* Имплементация предложенного решения. (интеграция адаптивного алгоритма в сетевой стек)
* Анализ трафика
* Приведение сравнительной характеристики С решением, и без

Объектом исследования является протокол граничного шлюза и принцип работы модулей для обеспечения взаимодействия между контейнерами и кластерами, а в частности IBGP в реализации CNI Calico.

Предметом исследования является разработка и внедрение адаптивного алгоритма маршрутизации для обеспечения наибольшей сходимости протокола BGP в контейнеризированной сети с использованием k8s и CNI Calico.

# **Литературный обзор**

# **Обоснование выбора BGP**

Что такое бжп, какие протоколы есть, их различие, анализ работы алгоритмов протоколов динамической маршрутации  
rip/bgp/eigrp/белман форд/дейкстра  
  
  
BGP является развитием алгоритма белмана фрода с бОльшим количеством варьируемых параметров, обеспечивающих эффективный инструментарий для обеспечение максимальной сходимости таблицы маршрутизации сети.

# **2.1 Контейнеры**

3.1 K8s обоснование calico

**Практическая часть**  
Выполнена в ходе практики на предприяти.

# **Заключение**

В дальнейшем предлагается и тп и тд  
Применение нейро нечетких сетей и тд.

# **Список использованных источников**

1

20

В данной статье обсуждается вариант решения для обнаружения и предотвращения распространения аномальной маршрутной информации, распространяемой по протоколу BGP-4. Предлагаемое решение не требует модификации стандартного программного обеспечения маршрутизаторов оператора связи, что дает возможность для его плавной интеграции без перерывов в обеспечении услуг связи. Анализ и проверка правильности распространяемых маршрутов базируется на данных из баз данных регистратур маршрутной информации организаций – координаторов межсетевого взаимодействия в сети Интернет. Алгоритм приведенного решения строит проверку пути распространения каждого маршрута в соответствии с декларируемой политикой связности всех операторов связи по цепочке и исключает попадание некорректных маршрутов, появившихся вследствие «утечек», «угонов» или ошибочных конфигураций маршрутизаторов транзитных операторов на любом участке, в таблицы маршрутизации контролируемого данным решением оператора связи. Решение является модульным, и его функциональность может быть расширена и адаптирована как расширением возможностей алгоритма анализа маршрутной информации, так и увеличением числа агентов, выполняющих непосредственное удаленное взаимодействие с пограничными маршрутизаторами контролируемого оператора связи по блокировке поступающих аномальных маршрутов в соответствии со спецификой командного интерфейса управления маршрутизаторов.