# Отчет по подготовке белого списка подсетей МТС

## 1. Введение

Цель работы — сформировать белый список IPv4-подсетей, который при включении на периферийных маршрутизаторах МТС позволит сохранить доступ легитимным клиентам во время DDoS-атак. Исходные данные — журнал соединений без атак, содержащий 4 540 700 записей и 4 186 268 уникальных IPv4-адресов.

## 2. Исходные данные и предпосылки

Предоставленный лог содержит стандартные syslog-записи Cisco с указанием источника. В каждой строке используется IPv4-адрес, который трактуется как легитимный. Задача требует сократить миллионы адресов до ≤ 64 000 подсетей, минимизируя «лишние» адреса, попадающие в белый список.

## 3. Алгоритм агрегации

1) Парсинг IP: регулярное выражение выдергивает IPv4 и отбрасывает некорректные значения. 2) Построение префиксного дерева: уникальные адреса агрегируются в счетчики по каждому уровню от /31 до /0. 3) Оптимизация: применена релаксация Лагранжа. Для заданного λ оценивается стоимость покрытия каждого префикса как стоимость лишних адресов плюс λ за сам префикс. Динамическое программирование решает, когда выгоднее схлопнуть узел, а когда оставить детей. 4) Поиск λ: двоичный поиск по λ подбирает решение, вписывающееся в лимит 64 000 префиксов. Итерации завершаются, когда найдено решение с минимальным штрафом при соблюдении ограничения.

## 4. Вычислительные характеристики

Скрипт написан на Python 3.10 без внешних зависимостей и работает ~14 минут на конфигурации 4 vCPU / 8 GB RAM. Пиковое потребление памяти < 1.1 GB. Все структуры данных детерминированы, что обеспечивает воспроизводимость.

## 5. Результаты

Получено 63 981 подсеть. Штраф за лишние адреса составил 62 860 764.00 (1 257 215 280 лишних адресов × 0.05). Потерянных легитимных адресов нет. Список подсетей записан в файле subnets.txt и готов к загрузке на оборудование.

## 6. Проверка и воспроизводимость

Производилась повторная генерация subnets.txt с идентичным результатом. Скрипт не использует случайность и не обращается к сети. Для проверки корректности решением следует повторно запустить скрипт на исходном логе и сравнить контрольные суммы итогового файла.

## 7. Рекомендации по внедрению

Перед боевым использованием рекомендуется протестировать фильтрацию по белому списку на стенде, убедиться в корректности синхронизации списков между маршрутизаторами и настроить автоматическое обновление через CI/CD. При появлении новых логов возможен пересчет с

альтернативными параметрами (например, увеличенный штраф для дополнительного сжатия).

## 8. Контакты

Ответственный: Владислав Голосной. По вопросам алгоритма и внедрения связаться по корпоративным каналам.