ПОЛИТЕХ
Высшая школа
кибербезопасности

Министерство науки и высшего образования Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
Высшая школа кибербезопасности

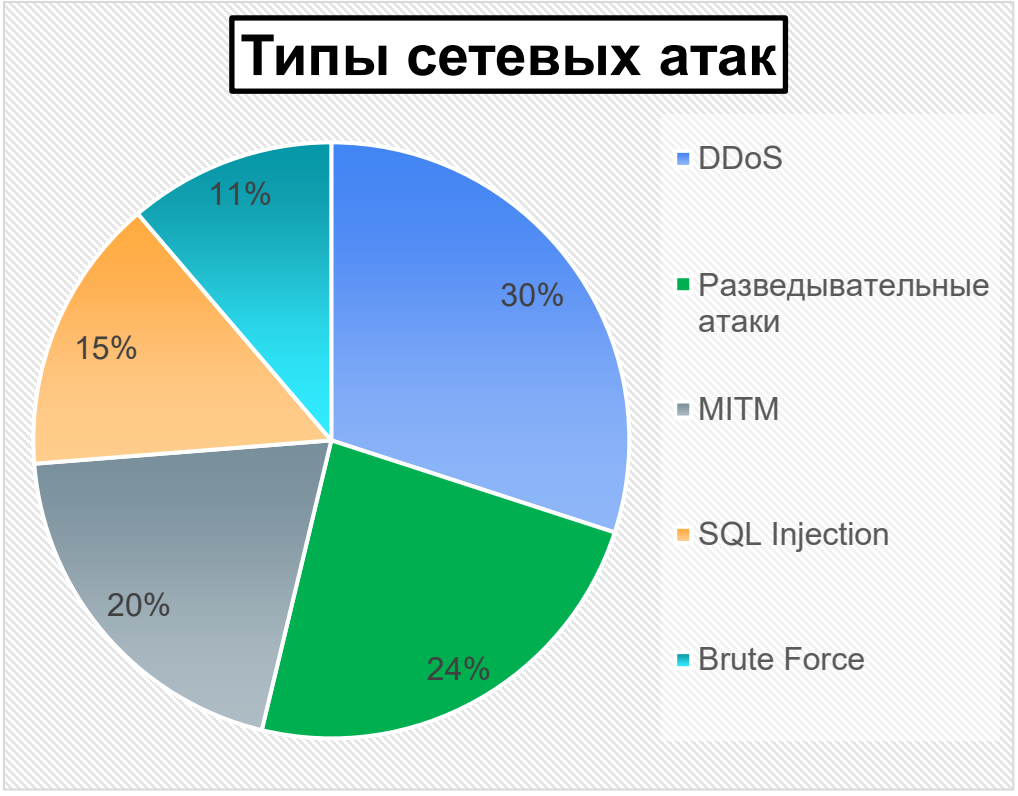
ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА АДАПТИВНОЙ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК НА ОСНОВЕ РЕКОНФИГУРАЦИИ СЕТИ

ВШК ИКНК И.А. Горецкий

Профессор ВШК ИКНК,
д.т.н., доцент
Д.С. Лаврова

Санкт-Петербург – 2025

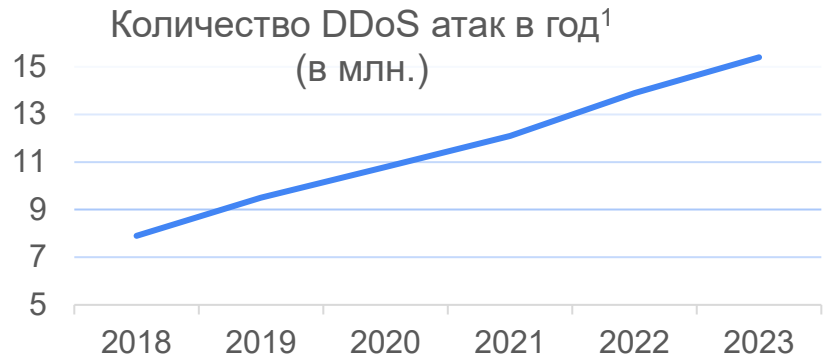
Сетевые атаки и методы противодействия им

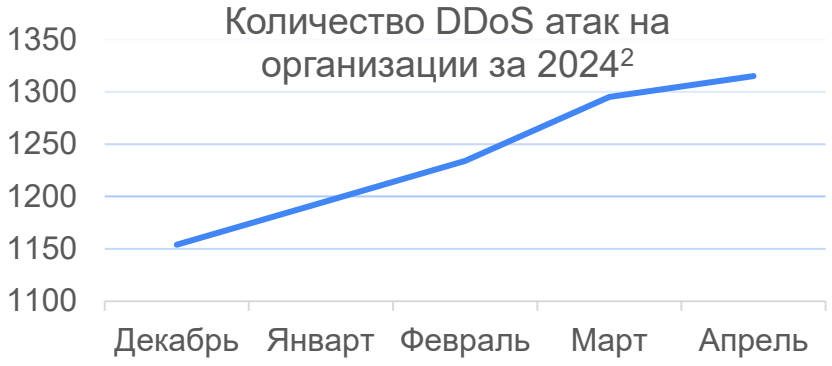


Атака	Метод противодействия
DDoS	Изменение топологии сети, Фильтрация пакетов
Разведывательные атаки	Использование межсетевого экрана с блокировкой сканирования сети
MITM	Завершение сессии, активация шифрования соединения
SQL Injection	Фильтрация SQL запросов
Brute Force	Блокировка сессии злоумышленника

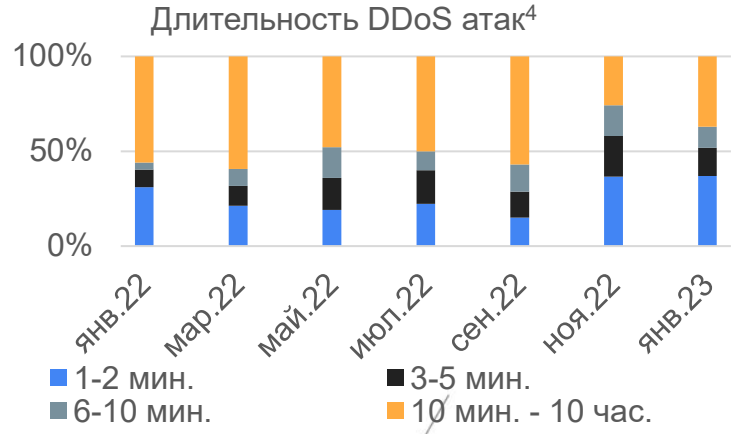
A Review of Cybersecurity Challenges in Small Business https://www.scirp.org/journal/paperinformation?paperid=130449

DDoS Сегодня





- Ежегодное увеличение числа сетевых атак составляет 10%
- Ежедневная частота инцидентов безопасности возрастает на 8% каждый месяц
- 121 сетевая атака в минуту[3]



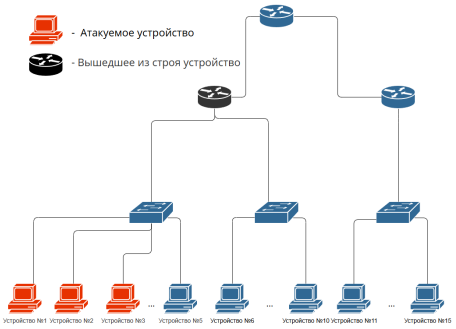
1. Shifting Attack Landscapes and Sectors in Q1 2024 with a 28% increase in cyber attacks globally https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/
2. Cisco Annual Internet Report (2018–2023) White Paper https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
3. Интерактивная карта киберугроз https://cybermap.kaspersky.com/ru/stats#country=213&type=IDS&period=m
4. DDoS attack trends and insights https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights

ПОЛИТЕХ МЫСЛИТЬ БУДУЩИМ

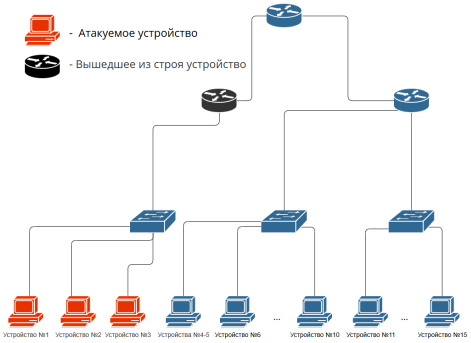
Противодействия атакам при помощи реконфигурации сети

Перестроение топологии

До :

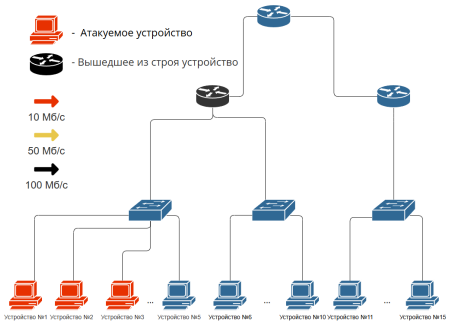


После:

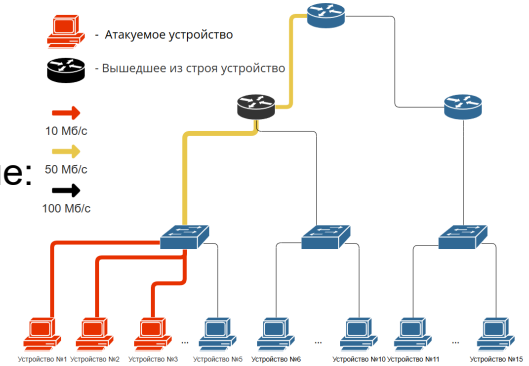


Изменение ширины каналов

До :



После:



Основным недостатком данной меры является большая вариативность. Для 40 устройств может быть $\approx 2^{1120}$ разнообразных топологий. Кроме того помимо генерации нужно так же производить оценку сгенерированным топологиям

Достоинства рекомендательной системы

- Генерация различных вариантов топологий
- Ранжирование сгенерированных топологии

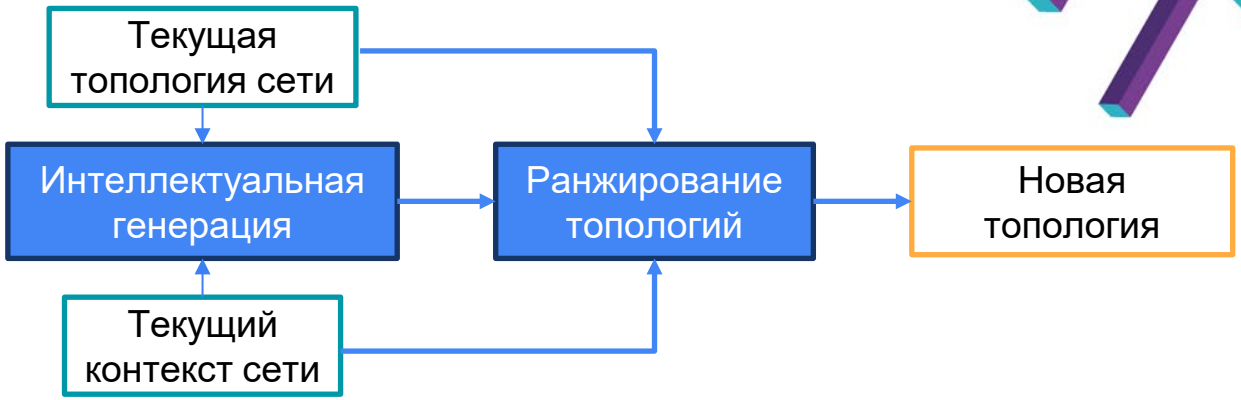
Так как для оценки и генерации топологий необходимо их применять то в основе рекомендательной системы будет лежать обучение с подкреплением

Рекомендательная система

Недостатки существующих решений:

- Не производят оценки новых топологий
- Генерируют только один вариант сети
- Генерируют либо новую топологию сети, либо новую пропускную способность каналов, но не обе одновременно

Схема работы:



- Контекстом сети является количество мегабайт переданных на каждом интерфейсе, текущая нагрузка устройств, а так же атакуемые устройства
- Выходными данными является вариант перестроения сети с оценкой пропускной способности
- Время генерации и оценки топологии не должно превышать 30 секунд
- Основано на обучении с подкреплением модели Актер-критик (A2C)

Ранжирование топологий:

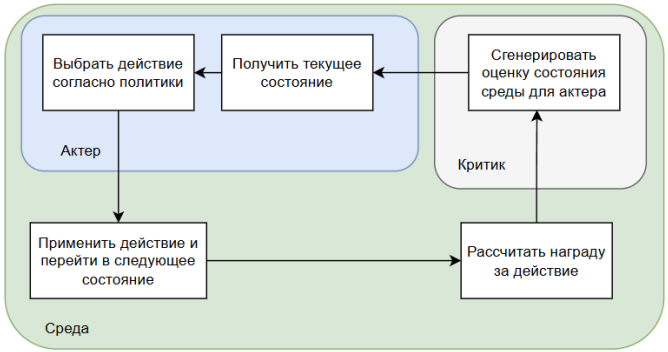
- Реализовано как рекомендательная система с контентной фильтрацией
- Оценивает среднюю пропускную способность топологии
- Оценка реализована в виде критика

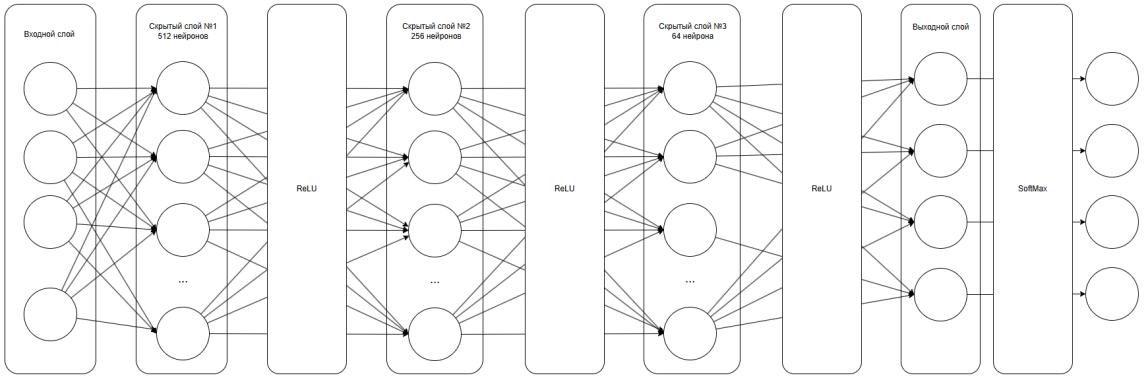
Интеллектуальная генерация:

- Генерация представлена виде актера
- Производит генерацию новых топологий сетей

Интеллектуальная генерация

- Метод основан на обучении с подкреплением моделью актер-критик
- Генерация представлена виде критика
- Задача актера – генерировать новые топологии сети
- Пространство состояний представлено квадратными матрицами топологий
- Пространство действия состоит из 4 элементов: увеличении/уменьшении пропускной способности канала между устройствами, включении/выключении канала между устройствами и переход к следующему элементу матрицы
- Актер и критик имеют одинаковое количество нейронов скрытого слоя, но имеют разное количество входов и выходов (ниже представлена схема нейронной сети актера)



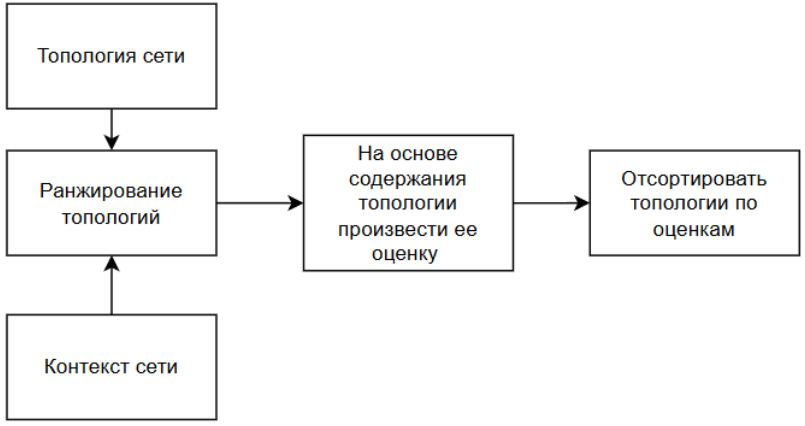


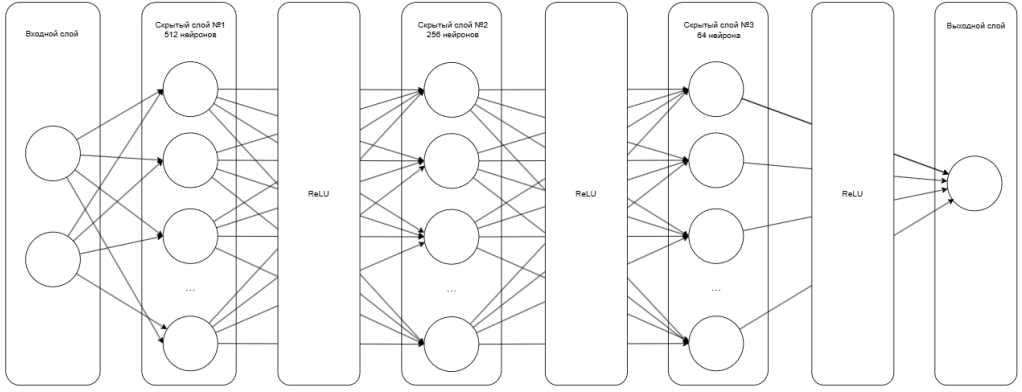
Ранжирование топологий

- Объект – сеть
- Элементы рекомендаций – различные топологии сети
- Метод рекомендаций – Фильтрация на основе содержания
- Ранжирование топологий представлено в виде критика

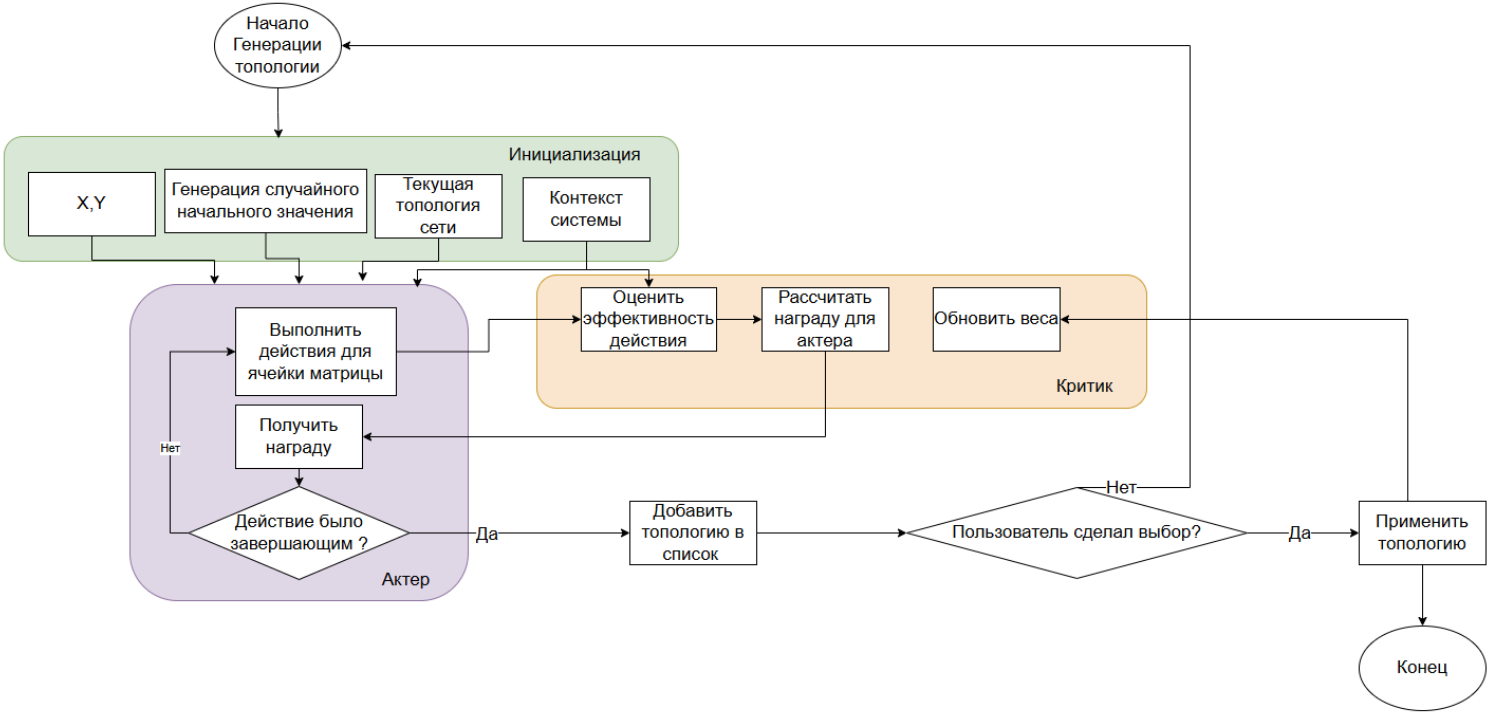
Характеристики среды кртика:

- Задача критика – предсказывать среднюю пропускную способность топологии
- Ниже представлена схема нейронной сети критика
- Нейронная сеть принимает на вход топологию сети и ее контекст





Блок схема работы рекомендательной системы



Метрики оценки рекомендательной системы

Для оценки ранжирования топологий были использованы среднеквадратичная ошибка и средняя абсолютная процентная ошибка:

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(x_i - x_i')^2\,;\ \mathrm{MAPE} = \frac{100\%}{n}\sum_{i=1}^{n}\left|\frac{x_i - x_i'}{x_i}\right|,$$

где параметры

x_i – предсказанное значение

x_i' – реальное значение

n – количество элементов для ранжирования

Для оценки модуля генерации были использованы списочное сходство (ILS) и относительное изменение пропускной способности сети (K) :

$$\mathrm{ILS}(M,N) = \frac{1}{n^2}\sum_{i=1}^{m}\sum_{j=1}^{n} sim\left(M_{ij}, N_{ij}\right);\ K = 100\% * \frac{y_i' - y_i}{y_i},$$

где параметры

$sim\left(M_{ij}, N_{ij}\right)$ – косинусное расстояние

n – количество сгенерированных элементов

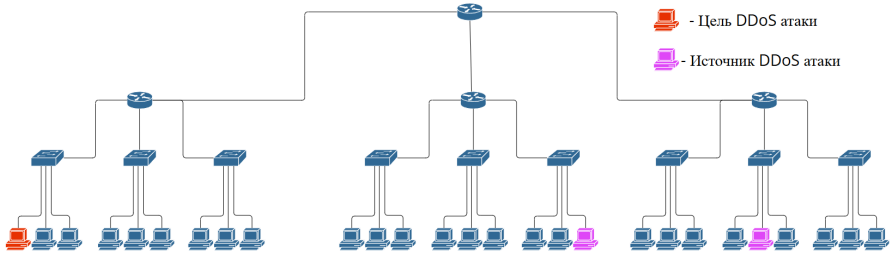
y_i – средняя пропускная способность сети в исходной топологии

y_i' – средняя пропускная способность сети в новой топологии

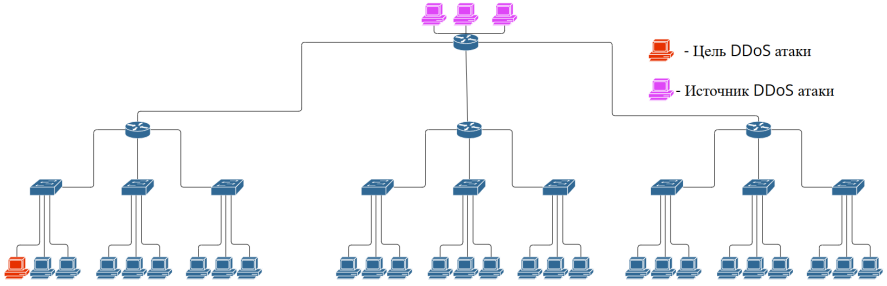
Стенд тестирования

- Эмуляция SDN сети при помощи Mininet и Ryu-controller
- Обучение и тестирование производилось в 3 средах маршрутизации: OSPF, EIGRP и статической маршрутизацией
- Вся настройка устройств происходит централизованно из SDN контроллера
- В сети выбиралось 15% атакующих узлов и 5% атакуемых узлов, все остальные узлы воспроизводили полезную нагрузку отправляя случайным узлам данные
- Тестировалось два шаблона с внутренними и внешними нарушителями

Внутренние нарушители:



Внешние нарушители:



Оценка эффективности новых топологий

Нарушитель	Количество устройств	Среднее значение K в STATIC	Среднее значение K в OSPFv3	Среднее значение K в EIGRP
Внешний	20	**31 %**	27 %	30 %
Внутренний	20	**58** %	56 %	57 %
Внешний	40	**31 %**	24 %	29 %
Внутренний	40	**59** %	55 %	57 %
Внешний	80	28 %	24 %	**39 %**
Внутренний	80	58 %	59 %	**64** %

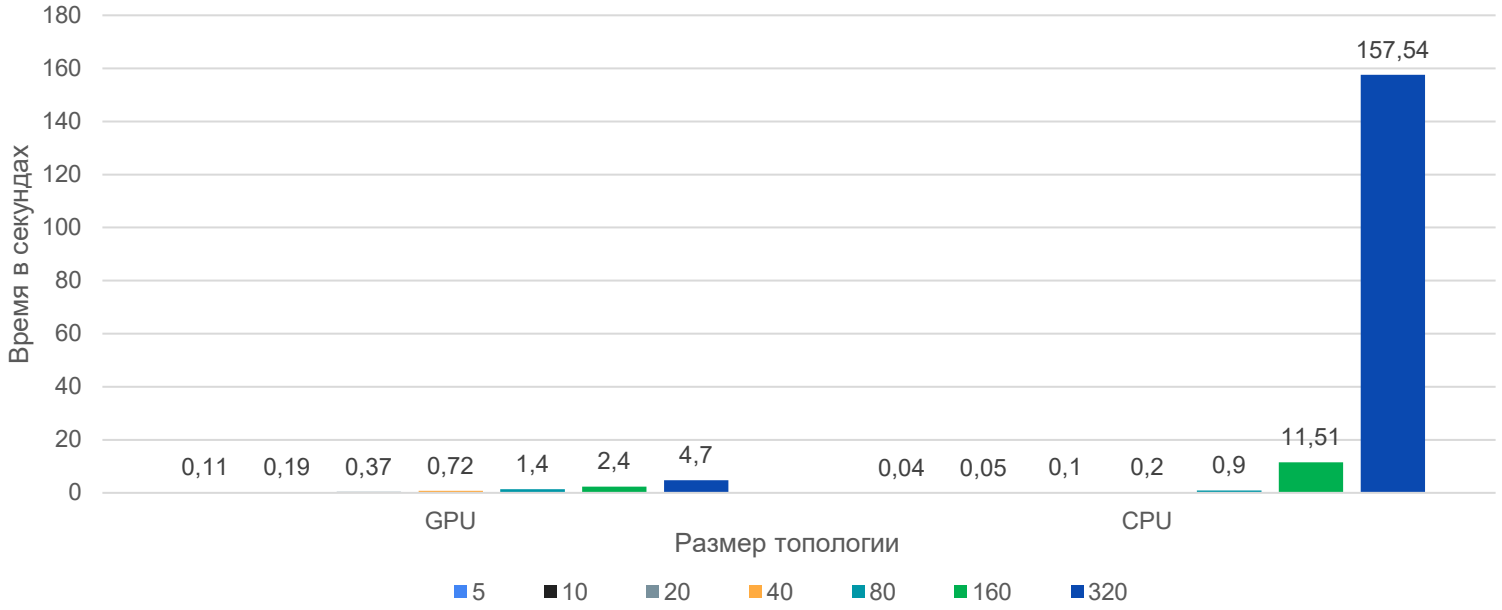
Метрика K – показывает на сколько процентов увеличилась средняя пропускная способность сети в новой топологии

Значения после 1000 запусков для каждого типа маршрутизации

ПОЛИТЕХ

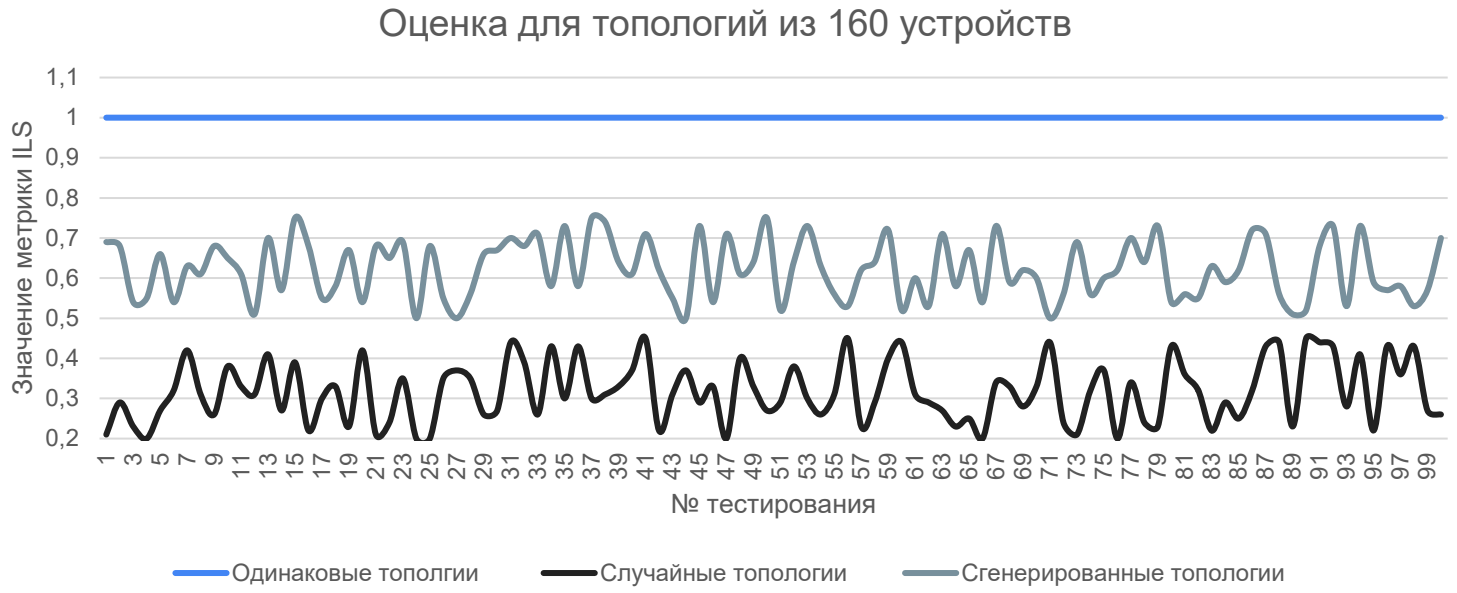
МЫСЛИТЬ БУДУЩИМ

Оценка времени генерации и оценки топологий



При использовании GPU система способна быстро сгенерировать различные топологии даже для больших сетей с 320 устройствами

Оценка разнообразности интеллектуального метода генерации вариантов перестроения сети



Среднее значение ILS = 0,62 показывает, что генератор создает не однотипные топологии

Оценка работы модуля анализа

Значения метрик $\mathrm{M}SE = 384$ и $\mathrm{M}APE = 18{,}7\ \%$, что примерно равно размеру погрешности для, топологии из 160 устройств

Результаты

1. Была разработана архитектура интеллектуального метода автоматической выработки вариантов перестроения сети, в основе которого лежит обучение с подкреплением

2. Экспериментальное тестирование показало, что разработанная интеллектуальная система генерирует новые топологии, снижающие эффективность атак в среднем на 46%

Контакты: goretskij.ia@edu.spbstu.ru