качество локализации и классификации. Дополнительно требуется зафиксировать протокол извлечения интервалов из плотных карт и правила сопоставления токенов с истинными событиями, чтобы обеспечить воспроизводимость результатов и однозначную интерпретацию архитектурного вклада.

Список использованных источников

1. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation // Medical Image Computing and Computer-Assisted Intervention (MICCAI). 2015. P. 234–241. DOI: 10.1007/978-3-319-24574-4_28. – Дата доступа: 14.12.2025.

2. Perslev M., Jensen M. H., Darkner S., Jennum P. J., Igel C. U-Time: A Fully Convolutional Network for Time Series Segmentation Applied to Sleep Staging // Advances in Neural Information Processing Systems (NeurIPS 2019). 2019. – Дата доступа: 14.12.2025.

3. Vaswani A., Shazeer N., Parmar N., et al. Attention Is All You Need. arXiv:1706.03762. 2017. – Дата доступа: 15.12.2025.

4. Gu A., Goel K., Ré C. Efficiently Modeling Long Sequences with Structured State Spaces. arXiv:2111.00396. 2021. – Дата доступа: 15.12.2025.

УДК 004.715

МАРШРУТИЗАТОР С ФУНКЦИЯМИ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Е. С. Белоусова[1], В. Л. Мальцев[2], Д. М. Мартинкевич[3], К. О. Янославский[3]

[1] доцент кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники

[2] заведующий лабораторией «Информационная безопасность» УО «Национальный детский технопарк»

[3] учащийся УО «Национальный детский технопарк»

Введение. В соответствии с п. 20 Приказа Оперативно-аналитического центра при Президенте Республики Беларусь № 66 от 20 февраля 2020 г. [1] в системе информационной безопасности критически важного объекта информатизации должны использоваться устройства с функциями межсетевого экранирования и анализа трафика при внутреннем и внешнем информационном взаимодействии по протоколам сетевого и транспортного уровней. На сегодняшний день на большинстве критически важных объектов информатизации Республики Беларусь используются сетевые устройства зарубежных производителей, таких как Huawei, Mikrotik и др. Поэтому актуальным является развитие производства телекоммуникационного обо-

рудования с функциями маршрутизации и анализа сетевого трафика в Республике Беларусь, а также внедрение отечественной продукции в различные организации в том числе для обнаружения и блокировки киберугроз. Авторами реализуется разработка маршрутизатора с функциями анализа сетевого трафика в ходе освоения индивидуальной учебной программы дополнительного образования одаренных детей и молодежи для дистанционной формы получения образования по направлению «Информационная безопасность» в учреждении образования «Национальный детский технопарк». В данной индивидуальной учебной программе авторами планируется добавление функций в разрабатываемый маршрутизатор и создание на его базе программно-аппаратного комплекса для межсетевого экранирования.

Основная часть. Для аппаратной реализации маршрутизатора с функциями анализа сетевого трафика был выбран мини-компьютер Chuwi Larkbox X [2], технические характеристики которого представлены в таблице 1.

Для программной реализации маршрутизатора с функциями анализа сетевого трафика была выбрана операционная система Ubuntu Server 22.04 LTS, так как она характеризуется стабильностью работы, совместимостью с оборудованием, наличием подробной документации, доступностью программного обеспечения.

Таблица 1 – Технические характеристики мини-компьютера Chuwi Larkbox X

Процессор	Intel Processor N100
Количество ядер	4
Максимальная частота	до 3400 МГц
Размеры	127 x 49 x 127 мм
Оперативная память	12 Gb LPDDR5
Накопитель	SSD 512 Gb
Сетевое подключение	2 x 1 Gbit

Для осуществления функций DHCP был выбран Kea DHCP, DHCP сервер с открытым исходным кодом, разрабатываемый Internet Systems Consortium (ISC). Kea DHCP имеет высокую производительность, что позволяет его использовать не только в частных локальных сетях, но и на крупных предприятиях. Для ведения аудита подключенных устройств локальной сети используется возможность Kea DHCP сохранять список устройств, запросивших IP-адрес. Для ведения списка может быть использовано три варианта баз данных

(БД): MySQL, PostgreSQL а также memfile. Выбор БД PostgreSQL обусловлен наличием возможности резервирования IP-адресов без прерывания работы DHCP-сервера, что необходимо для серверов, которым нужен статический IP-адрес. В БД PostgreSQL после добавления адреса в список зарезервированных он не будет использоваться пулом DHCP, что неосуществимо в memfile. По сравнению с MySQL БД PostgreSQL имеет поддержку типов данных, специфических для сетевых технологий (inet, macaddr), что экономит место, так как данные хранятся в бинарном виде, а не как обычная строка.

Для настройки DHCP-сервиса на маршрутизаторе был отредактирован файл конфигурации kea-dhcp4.conf, в котором указывался номер интерфейса маршрутизатора для принятия DHCP-запросов, имя базы данных PostgreSQL для хранения запрашиваемых IP-адресов и для резервирования IP-адресов за определенными MAC-адресами. В файле конфигурации kea-dhcp4.conf также настраиваются параметры управления выдачи IP-адресов, IP-адрес DNS-сервера, диапазон IP-адресов и др. В последнем блоке файла конфигурации настраиваются параметры логирования событий DHCP-сервиса с меткой INFO, соответствующей информационным сообщениям, возникающим в процессе работы.

Для удобного просмотра списка устройств, запросивших IP-адрес, был изменен файл .bashrc (рисунок 1), в который было добавлено обращение к PostgreSQL с целью форматирования вывода результатов выдачи IP-адресов в виде таблицы (рисунок 2).

Рисунок 1 – Фрагмент файла .bashrc

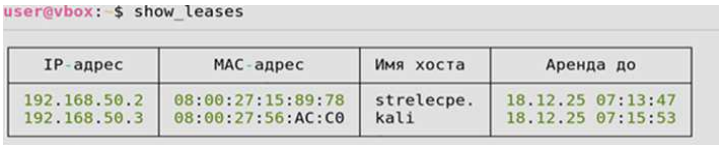

Рисунок 2 – Результат правильной работы DHCP-сервиса на маршрутизаторе

Для настройки функции маршрутизации на мини-компьютере Chuwi Larkbox X был настроен процесс перенаправления трафика IP Forwarding, который необходим для перенаправления трафика от интерфейса, подключенному к внешней сети к интерфейсу, подключенному к внутренней сети, и наоборот LAN. Для включения процесса перенаправления трафика IP Forwarding в операционной системе Ubuntu Server 22.04 LTS необходимо в файле /etc/sysctl.conf установить параметр net.ipv4.ip_forward=1.

Для реализации функции трансляции IP-адресов (NAT, Network Address Traslation) был использован инструмент nftables, который также реализовал функции блокировки подозрительных IP-адресов. На рисунке 3 представлен фрагмент файла nftables.conf в котором добавлена таблица NAT с функцией masquerade, которая необходима для преобразования IP-адресов в пакетах из внутренней сети, при их передаче на внешний интерфейс enp1s0. Результат правильной работы трансляции IP-адресов посредством инструмента tcpdump показан на рисунке 4, на котором видно, что в пакете данных, приходящем на внутренний интерфейс маршрутизатора (enp2s0) осуществляет преобразование IP-адреса 192.168.50.2 в IP-адрес 192.168.100.11, настроенный на внешнем интерфейсе (enp1s0).

```
 GNU nano 6.2          /etc/nftables.conf
table ip nat {
        chain postrouting {
                type nat hook postrouting priority 100;
                oifname "enp1s0" masquerade
        }
```

Рисунок 3 – Фрагмент файла nftables.conf для активации NAT

```
ubuntu@ubuntu:~$ sudo tcpdump -i enp2s0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:02:59.019948 IP 192.168.50.2 > dns.google: ICMP echo request, id 1, seq 40, length 40
22:02:59.034362 IP dns.google > 192.168.50.2: ICMP echo reply, id 1, seq 40, length 40
22:03:00.035012 IP 192.168.50.2 > dns.google: ICMP echo request, id 1, seq 41, length 40
ubuntu@ubuntu:~$ sudo tcpdump -i enp1s0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:03:16.240484 IP 192.168.100.11 > dns.google: ICMP echo request, id 1, seq 43, length 40
22:03:16.253496 IP dns.google > 192.168.100.11: ICMP echo reply, id 1, seq 43, length 40
22:03:17.245697 IP 192.168.100.11 > dns.google: ICMP echo request, id 1, seq 44, length 40
```

Рисунок 4 – Результат проверки работы NAT посредством tcpdump

Разработанный маршрутизатор в процессе маршрутизации трафика анализирует заголовок IP в каждом пакете и автоматически блокирует IP-адреса из списка Firehol IP list [3], представляю-

щий собой постоянно обновляющийся список IP-адресов, с которых были зафиксированы кибератаки. FireHOL [4] – это язык для создания правил межсетевого экранирования и их преобразования и добавления в nftables ОС Linux. Firehol IP list представляет собой высокоуровневое описание правил, которые автоматически преобразуются в наборы правил nftables, что позволяет удобно и быстро добавлять правила для блокировки IP-адресов. Для запуска периодических обновлений был написан скрипт firehol-update.sh (рисунок 5), который загружает актуальный firehol IP list (level2), редактирует файл firehol_leve2.netset, добавляя новые IP-адреса и удаляет из списка локальные IP-адреса, а также обновляет список правил nftables (рисунок 6).

```
 GNU nano 6.2                                    /etc/firehol-update.sh
#!/bin/bash
curl -O https://iplists.firehol.org/files/firehol_level2.netset
grep -Eo '([0-9]{1,3}.){3}[0-9]{1,3}(/[0-9]{1,2})?' firehol_level2.netset |
grep -Ev -E '^127.|^10.|^192.168.|^169.254.|^172.(1[6-9]|2[0-9]|3[0-1]).|^224.|^255.' |
sort -u > firehol_level2.txt

nft -f <(echo "flush set inet filter bad_ips; add element inet filter bad_ips
{ $(tr '\n' ',' < firehol_level2.txt | sed 's/,$//') }")
```

Рисунок 5 – Фрагмент скрипта firehol-update.sh для обновления правил nftables

```
ubuntu@ubuntu:~$ sudo nft list ruleset
table inet filter {
        set bad_ips {
                type ipv4_addr
                flags interval
                elements = { 1.1.179.25, 1.13.79.144,
                             1.13.175.150, 1.14.12.141,
                             1.24.210.27, 1.27.226.158,
                             1.30.20.98, 1.31.80.222,
                             1.55.33.86, 1.62.252.20,
                             1.71.249.167, 1.82.135.154,
                             1.94.67.207, 1.94.145.98,
                             1.95.12.125, 1.95.79.93,
```

Рисунок 6 – Фрагмет правил nftables с добавленными IP-адресами из списка Firehol IP list

Специально был создан сервис update-firehol.service, который запускает автоматическое обновление списка Firehol IP list через 5 минут после его запуска и каждые 3 часа, что определяется update-firehol.timer (рисунок 7).

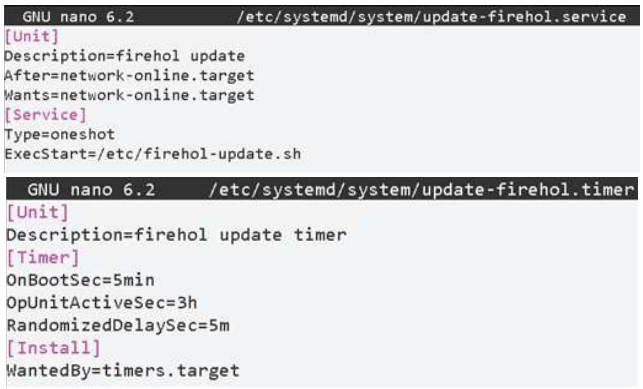

Рисунок 7 – Фрагменты файлов update-firehol.service и update-firehol.timer

Заключение. Таким образом, разработанный маршрутизатор рекомендуется к внедрению в корпоративные сети различных организаций Республики Беларусь, так как имеет весь необходимый функционал. На маршрутизаторе возможно настроить Kea DHCP-сервис, посредством которого можно резервировать IP-адреса, а также добавлять и отслеживать выданные IP-адреса в БД PostgreSQL. Также в маршрутизаторе реализована функция анализа трафика сетевого уровня и преобразования IP-адресов в соответствии с технологией NAT. Посредством конфигурации nftables возможна блокировка или разрешение трафика с разными IP-адресами и протоколами. Функция блокировки IP-адресов с подозрительной активностью, включенных в список firehol IP list, с автоматическим обновлением позволяет упростить процесс конфигурации nftables. В дальнейшей работе авторами планируется добавление следующих функций: DNS-сервис с протоколом DNS-over-HTTPS и проверкой доменов, обнаружения и блокировки вторжений, логирования событий информационной безопасности и инспекции зашифрованного трафика.

Список использованных источников

1. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 20 февр. 2020 г., № 66 / Нац. правовой Интернет-портал Респ. Беларусь. – 2020. – 7/4470.

2. LarkBox X. User Manual / CHUWI [Electronic resource] – Mode of access: https://cdn.shopify.com/s/files/1/0116/2762/6596/files/LarkBoxX-UserGuide.pdf?v=1680059623. – Date of access: 15.12.2025.

3. FireHOL [Electronic resource] – Mode of access: https://firehol.org/documentation/#firehol. – Date of access: 15.12.2025.

4. FireHOL iplists [Electronic resource] – Mode of access: https://iplists.firehol.org/?ipset=firehol_level2. – Date of access: 15.12.2025.