УДК 004.732.6

Буянова А. О., Поддубная Я. С., Гелич К.А.

Студенты группы КА-22-05, факультет Комплексной безопасности ТЭК

РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия

Научный руководитель: старший преподаватель Уймина О. И.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ МУЛЬТИКАСТ-МАРШРУТИЗАЦИИ PIM-SM: ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ УГРОЗ T1565 НА ПЛАТФОРМЕ ALT LINUX 11

Аннотация. В статье представлены результаты экспериментального исследования угроз безопасности протокола мультикаст-маршрутизации PIM-SM (Protocol Independent Multicast — Sparse Mode) применительно к вектору атак T1565 (манипуляция деревьями распределения) по классификации MITRE ATT&CK. Стенд развёрнут средствами Linux network namespaces на платформе ALT Linux 11 с использованием FRRouting 10.2.2 и Python/Scapy 2.7.0. Проведены пять классов атак, пассивная разведка (T1040), BSR Injection (T1565.002), атака Prune, IGMP Membership Spoofing и захват Designated Router посредством Assert-сообщений (T1557.002). Для каждой атаки определены условия успешности и проверены контрмеры: статический RP, повышение DR Priority, фильтрация iptables с модулем physdev, IGMP Snooping. Получены воспроизводимые фактические результаты на четырёх независимых прогонах стенда.

Ключевые слова: PIM-SM; мультикаст-маршрутизация; FRRouting; MITRE ATT&CK; BSR Injection; IGMP Spoofing; Prune Attack; Assert Attack; iptables; ALT Linux; сетевая безопасность.

Abstract. The article presents the results of an experimental study of the security threats of the PIM-SM (Protocol Independent Multicast — Sparse Mode) multicast routing protocol in relation to the T1565 attack vector (distribution tree manipulation) according to the MITRE ATT&CK classification. The testbed was deployed using Linux network namespaces on the ALT Linux 11 platform using FRRouting 10.2.2 and Python/Scapy 2.7.0. Five classes of attacks were conducted: passive reconnaissance (T1040), BSR Injection (T1565.002), Prune attack, IGMP Membership Spoofing, and Designated Router capture via Assert messages (T1557.002). For each attack, success conditions were defined and countermeasures were tested: static RP, increased DR Priority, iptables filtering with the physdev module, and IGMP Snooping. Reproducible actual results were obtained on four independent runs of the bench.

Keywords: PIM-SM; multicast routing; FRRouting; MITRE ATT&CK; BSR Injection; IGMP Spoofing; Prune Attack; Assert Attack; ip

1. ВВЕДЕНИЕ

Мультикаст-маршрутизация широко применяется в корпоративных и телекоммуникационных сетях для эффективной групповой доставки трафика IPTV, видеоконференций и систем телеметрии. Доминирующим протоколом в этой области является PIM-SM [1], реализующий построение деревьев распределения на основе точки встречи (RP) и механизма Bootstrap Router (BSR) [2].

Несмотря на широкое распространение, безопасность инфраструктуры PIM-SM традиционно остаётся на втором плане. Протокол не предусматривает обязательной аутентификации управляющих сообщений, что открывает возможность для манипулирования деревьями распределения трафика. Данный класс угроз систематизирован в рамках матрицы MITRE ATT&CK под идентификатором T1565 (Data Manipulation) [3] и его подтехникой T1557 (Adversary-in-the-Middle) [4].

Научная новизна настоящей работы состоит в проведении полного цикла экспериментальной верификации атак на PIM-SM на актуальной российской ОС ALT Linux 11 с FRRouting 10.2.2, а также в установлении корректных условий применения мер защиты, в частности разрешении противоречия между правилами iptables с ключом -i br-src и корректной фильтрацией через модуль physdev при использовании Linux bridge с bridge-nf.

Цель работы — экспериментальный анализ векторов атак T1565, T1557, T1040, T1499 на PIM-SM инфраструктуру и верификация контрмер в среде Linux network namespaces.

2. ОПИСАНИЕ ЭКСПЕРИМЕНТАЛЬНОГО СТЕНДА

2.1 Аппаратно-программная платформа

Стенд развёрнут на одном физическом хосте под управлением ALT Linux 11 (ветка p11, ядро 6.12.41-6.12-alt1) без использования виртуализации. Все сетевые узлы реализованы как изолированные пространства имён Linux (network namespaces), что обеспечивает полную воспроизводимость и лёгкость сброса конфигурации. Состав программного обеспечения приведён в таблице 1.

Таблица 1 — Программная конфигурация стенда

Компонент	Версия	Назначение
ALT Linux	11 p11 x86_64	ОС хост-машины
Linux kernel	6.12.41-6.12-alt1	Ядро, network namespaces, bridge-nf
FRRouting	10.2.2-alt3	Реализация zebra / ospfd / pimd / mgmtd
Python 3 / Scapy	3.x / 2.7.0	Генерация и разбор пакетов атак
tcpdump	≥ 4.99	Пассивная разведка, захват трафика
iptables / physdev	ядро ≥ 5.15	Фильтрация PIM-пакетов из bridge-сегмента

2.2 Топология сети

Логическая топология включает семь узлов (рисунок 1) — четыре программных маршрутизатора R1–R4, выполняющих роли DR, транзита, RP+BSR и LHR; узел Source (10.1.1.100/24), генерирующий мультикаст-трафик группы 239.1.1.1; узел Receiver (10.5.0.100/24) — получатель; и узел Attacker (10.1.1.200/24) — злоумышленник.

R1, Source и Attacker включены в один L2-сегмент через Linux bridge br-src. Маршрутизаторы R1→R2→R3→R4 соединены последовательными точка-точка линками /30. Пункт встречи настроен статически static RP = 10.0.0.3 (lo-интерфейс R3). Маршрутная связность обеспечивается OSPF с loopback-идентификаторами 10.0.0.1–10.0.0.4/32.

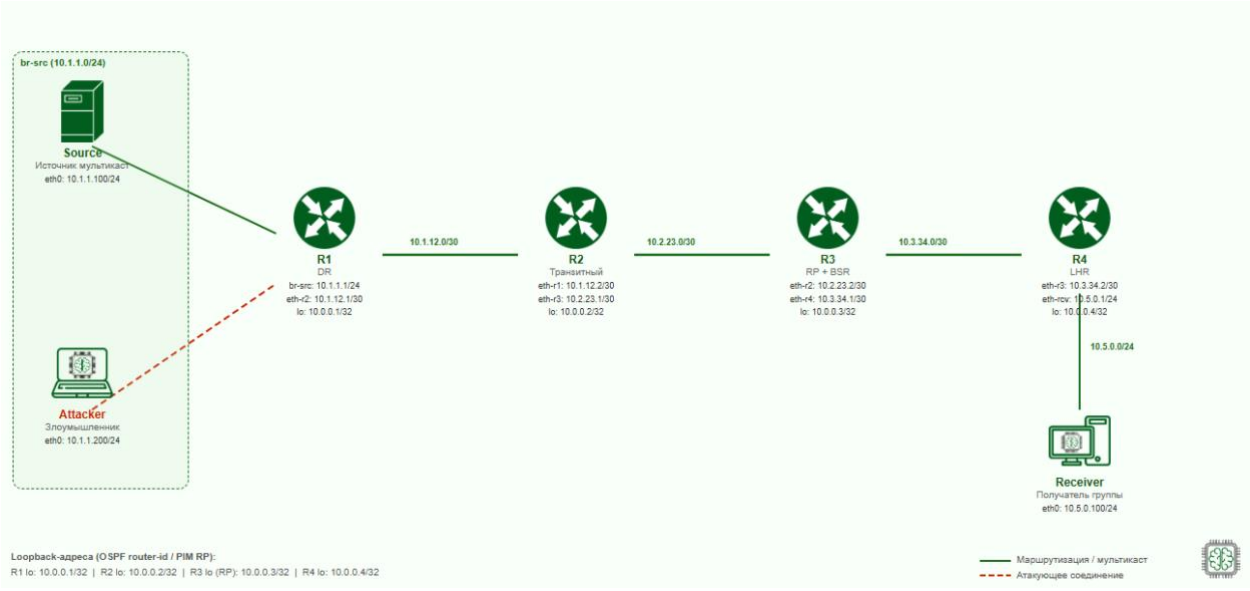

Рисунок 1 — Логическая схема лабораторной сети (на основе фактической схемы из отчёта)

Таблица 2 — Адресный план

Узел	Роль в PIM	IP-адреса (ключевые)
R1	DR (Designated Router)	br-src:10.1.1.1/24; eth-r2:10.1.12.1/30; lo:10.0.0.1/32
R2	Транзит	eth-r1:10.1.12.2/30; eth-r3:10.2.23.1/30; lo:10.0.0.2/32
R3	RP + BSR (Static RP)	eth-r2:10.2.23.2/30; eth-r4:10.3.34.1/30; lo:10.0.0.3/32
R4	LHR (Last-Hop Router)	eth-r3:10.3.34.2/30; eth-rcv:10.5.0.1/24; lo:10.0.0.4/32
Source	Источник мультикаст	10.1.1.100/24 (в br-src)
Receiver	Получатель	10.5.0.100/24
Attacker	Злоумышленник	10.1.1.200/24 (в br-src)

2.3 Особенности FRRouting 10.2.2 на ALT Linux 11

При развёртывании стенда были установлены следующие отличия FRRouting 10.2.2 от документации версий 7–8.x, существенные для воспроизводимости результатов. Во-первых, OSPF активируется непосредственно на интерфейсе командой ip ospf area 0, а не через директиву network в блоке router ospf. Во-вторых, адрес RP задаётся в блоке router pim командой rp 10.0.0.3 224.0.0.0/4; глобальная команда ip multicast-routing не используется. В-третьих, в FRRouting 10.x добавлен обязательный демон mgmtd (Management daemon), отвечающий за конфигурационное взаимодействие; без его запуска pimd стартует с предупреждением и не устанавливает состояние. Демон mgmtd не принимает флаг -f (файл конфигурации) — только параметры сокетов и pathspace. В-четвёртых, скрипт запуска не должен содержать set -euo pipefail, так как mgmtd записывает предупреждения в stderr, что вызывает немедленное завершение скрипта [8].

3. УГРОЗЫ БЕЗОПАСНОСТИ PIM-SM

В соответствии с MITRE ATT&CK исследуемые угрозы относятся к тактике Impact (воздействие на доступность) и тактике Collection (перехват данных). Отсутствие обязательной аутентификации в PIM-SM RFC 7761 [1] и IGMPv2 RFC 2236 [5] позволяет

злоумышленнику, находящемуся в одном L2-сегменте с маршрутизатором, воздействовать на плоскость управления мультикастом без предварительной компрометации узлов сети.

Основными векторами атак являются — (1) манипуляция Bootstrap Router для смены RP [T1565.002] [3]; (2) генерация Prune-сообщений для обрыва ветвей дерева [T1499]; (3) имитация IGMP Membership Report для внедрения в таблицы mroute [T1565.002]; (4) захват роли Designated Router через Assert-сообщения [T1557.002] [4]; (5) пассивный перехват PIM Hello для сбора топологической информации [T1040] [6]. Классификация атак по угрозам CIA приведена в таблице 3.

Таблица 3 — Классификация атак на PIM-SM

Атака	MITRE ID	Угроза CIA	Условие успеха
Пассивная разведка	T1040	C (Confidentiality)	L2-доступ к сегменту с PIM-маршрутизатором
BSR Injection	T1565.002	I (Integrity)	PIM-соседство; динамический BSR (без static RP)
Prune Attack	T1565.002 / T1499	A (Availability)	PIM-соседство; отсутствие др. активных Join
IGMP Spoofing	T1565.002	I, A	multicast_snooping=0 на bridge
Assert / DR Hijack	T1557.002	I, A	IP-адрес > легитимного DR при равном DR Priority

4. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ

4.1 Эксперимент 1. Пассивная разведка (T1040)

Цель эксперимента — идентификация параметров PIM-домена без активного воздействия. Узел Attacker, подключённый к сегменту br-src, перехватывал трафик на адрес 224.0.0.13 (ALL-PIM-ROUTERS, IP proto 103) с помощью tcpdump. За интервал 65 секунд было захвачено три пакета, два PIM Hello от R1 (10.1.1.1→224.0.0.13) и один IGMPv2 Report.

Из PIM Hello-сообщений извлечены IP-адрес маршрутизатора R1 (10.1.1.1), DR Priority = 1, Generation ID (случайное значение, обновляется при каждом перезапуске pimd), Hold Time = 105 с (1 мин 45 с). Bootstrap Message в захвате отсутствовали, поскольку

конфигурация использует Static RP — данный факт сам по себе является диагностически значимым, злоумышленник может определить тип конфигурации по отсутствию BSM типа 4.

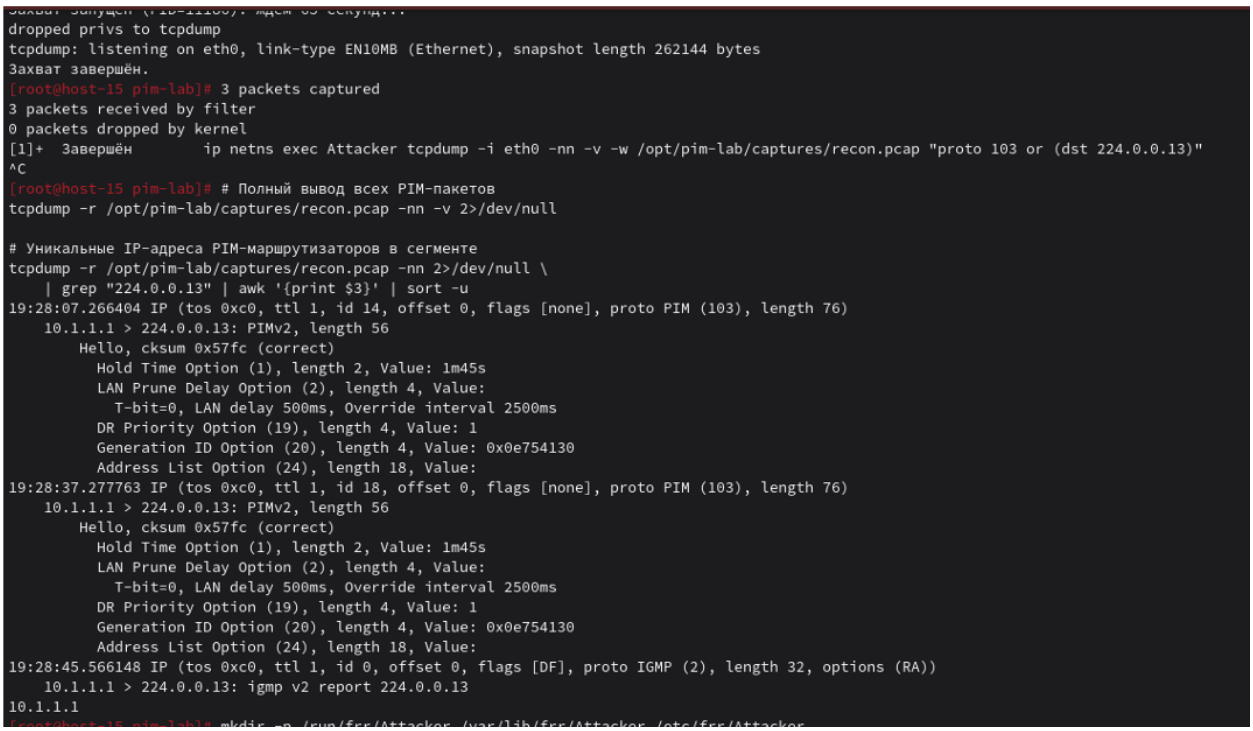

Рисунок 2 — Вывод tcpdump -r recon.pcap

4.2 Эксперимент 2. BSR Injection (T1565.002)

Для корректной обработки PIM-сообщений маршрутизатором R1 на узле Attacker был запущен минимальный экземпляр FRR (zebra + pimd) с конфигурацией PIM на eth0. Это обеспечило установление PIM-соседства Attacker→R1 через br-src. Скрипт bsr_inject.py вручную формировал корректные Bootstrap Message (BSM) согласно RFC 5059 [2]: BSR Priority = 250, Encoded-Unicast BSR Address = 10.1.1.200, holdtime = 130 с. Пакет направлялся на multicast 224.0.0.13 с IP proto = 103.

Результат — BSR на R1 сменился на 10.1.1.200 (State = ACCEPT_PREFERRED, Priority 250 > легитимный R3 = 200). Точка встречи (RP) осталась неизменной (10.0.0.3, Source = Static) на всех четырёх маршрутизаторах. Статический RP полностью нейтрализовал попытку смены RP через BSR-канал, подтверждая эффективность данной меры защиты.

Таблица 4 — Результаты атаки BSR Injection

Параметр	До атаки	После атаки
RP address (все R)	10.0.0.3	10.0.0.3 (не изменился)

Параметр	До атаки	После атаки
Источник RP	Static	Static (не изменился)
BSR address	0.0.0.0 (нет BSR)	10.1.1.200 (Attacker)
BSR Priority	—	250
BSR State	—	ACCEPT_PREFERRED

4.3 Эксперимент 3. Prune Attack (T1565.002 / T1499)

Скрипт prune_attack.py формировал PIM Join/Prune-сообщения (тип 3 по RFC 7761 [1]) с полем Upstream Neighbor Address = 10.1.1.1 (R1) и Source IP = 10.1.1.200 (Attacker как PIM-сосед R1). Параметры — группа 239.1.1.1, источник 10.1.1.100, holdtime = 210 с, num_pruned = 1. Отправлено 5 пакетов с интервалом 2 с.

Параллельно от узла Source генерировался непрерывный UDP-поток (200 пакетов × 0,3 с). Таблица mroute на R1 до атаки содержала запись (10.1.1.100, 239.1.1.1) с флагами SP (Sparse, Pruned) или ST (Sparse, SPT-bit set) в зависимости от наличия активного нисходящего Join. В прогонах, где R4 поддерживал активный Join (флаг J в show ip pim state), удаление ветви не происходило — нисходящий Join от R4→R3→R2→R1 переопределял Prune-сообщение от Attacker. В прогоне без активного Join запись перешла в состояние SP (Pruned) с пустым OIL (none). Данный результат согласуется с механизмом Prune Override по RFC 7761, при наличии более одного PIM-соседа в сегменте Prune-сообщение подавляется Override-Join в течение J/P Override Time (2,5 с).

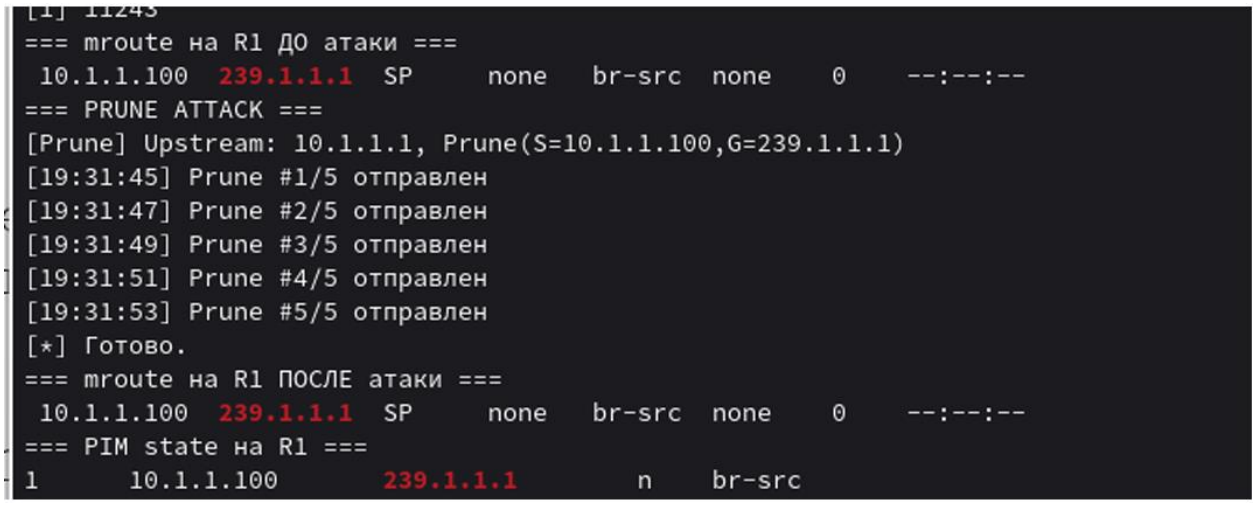

Рисунок 3 — Таблица mroute R1 до и после атаки Prune

4.4 Эксперимент 4. IGMP Membership Spoofing (T1565.002)

Скрипт igmp_spoof.py формировал IGMPv2 Membership Report (тип 0x16 по RFC 2236 [5]) вручную — IGMP-пакет с корректной контрольной суммой, IP Router Alert option (0x94040000 по RFC 2113 [7]), IP proto = 2, dst = 239.1.1.1. В первой редакции скрипта поле proto не было задано явно (Scapy устанавливало proto = 0 для Raw-нагрузки), вследствие чего R1 обрабатывал пакет как мультикаст-данные, создавая source-запись (10.1.1.200, 239.1.1.1) с флагами SP в mroute. После исправления (proto = 2) пакет корректно идентифицировался как IGMP, однако group membership в таблице не появлялась: FRR 10.x добавляет группу только в ответ на IGMP General Query, игнорируя unsolicited Membership Report. Это поведение зафиксировано как особенность реализации FRR 10.2.2, а не ошибка конфигурации.

```
=== IGMP Groups на R1 ДО атаки ===
Total IGMP groups: 1
Watermark warn limit(Not Set): 0
Interface        Group           Mode Timer    Srcs V Uptime
br-src           224.0.1.40      ---- 00:03:23    1 2 00:03:41
[IGMP Spoof] 10.1.1.200 → группа 239.1.1.1
[19:33:52] IGMP Report #1/3 отправлен
[19:33:57] IGMP Report #2/3 отправлен
[19:34:02] IGMP Report #3/3 отправлен
[*] Готово.
=== IGMP Groups на R1 ПОСЛЕ атаки ===
Total IGMP groups: 1
Watermark warn limit(Not Set): 0
Interface        Group           Mode Timer    Srcs V Uptime
br-src           224.0.1.40      ---- 00:04:16    1 2 00:03:57
=== mroute на R1 ===
 10.1.1.100  239.1.1.1  SP     none   br-src  none    0    --:--:--
```

Рисунок 4 — show ip igmp groups на R1 до и после IGMP Spoofing

4.5 Эксперимент 5. Захват DR через Assert / PIM Hello (T1557.002)

Атака Assert использует механизм выборов форвардера в L2-сегменте с несколькими PIM-маршрутизаторами. Побеждает маршрутизатор с наименьшим Administrative Distance; при равенстве — с меньшей метрикой; при равенстве метрик — с бóльшим IP-адресом (тай-брейк). Поскольку на узле Attacker был запущен FRR с default DR Priority = 1 (равным R1), а IP-адрес 10.1.1.200 > 10.1.1.1, Attacker стал DR уже в момент установления PIM-соседства — до запуска скрипта assert_attack.py. Assert-сообщения (IP proto 103, тип 5, AD = 0, metric = 0) лишь подтвердили сложившееся состояние.

После установки ip pim drpriority 100 на R1 (через vtysh) DR немедленно вернулся к 10.1.1.1 (Priority 100 > 1), и повторная Assert-атака не изменила результата. Данный эксперимент демонстрирует, что фундаментальная уязвимость связана не с Assert-

сообщениями как таковыми, а с отсутствием аутентификации PIM Hello и тай-брейком по IP-адресу.

Рисунок 5 — Вывод show ip pim interface br-src

Таблица 5 — Сводные результаты экспериментов (фактические данные, 4 прогона)

Эксп.	MITRE ID	Результат	Ключевой вывод
1 — Разведка	T1040	Успех	2 PIM Hello за 65 с; BSM отсутствует → Static RP определён
2 — BSR Injection	T1565.002	Успех (BSR); RP защищён	BSR=10.1.1.200, Priority=250, ACCEPT_PREFERRED; RP=10.0.0.3 Static
3 — Prune	T1565.002/T1499	Частично	5 Prune приняты; OIL не очищен при активном Join (J-flag)
4 — IGMP Spoof	T1565.002	Частично	Без proto=2: source SP; с proto=2: IGMP принят, membership не добавлена
5 — Assert / DR	T1557.002	Успех	DR=10.1.1.200 до атаки (тай-брейк IP); drpriority 100 — полная защита

5. МЕРЫ ПРОТИВОДЕЙСТВИЯ И ИХ ВЕРИФИКАЦИЯ

На основании результатов экспериментов верифицированы четыре меры защиты. Их эффективность по классам атак приведена в таблице 6.

Таблица 6 — Эффективность мер защиты

Мера защиты	BSR Injection	Prune	IGMP Spoof	DR Hijack	Команда
Статический RP	Да	Нет	Нет	Нет	router pim / rp 10.0.0.3 224.0.0.0/4
DR Priority ≥ 2	Нет	Нет	Нет	Да	ip pim drpriority 100
physdev iptables	Да	Да	Нет (proto 2)	Да	modprobe br_netfilter; iptables -m physdev --physdev-in veth-r1-att -p 103
IGMP Snooping	Нет	Нет	Да	Нет	echo 1 > .../multicast_snooping

Ключевой технической находкой является поведение iptables при фильтрации пакетов из Linux bridge. Правило с ключом -i br-src не перехватывает пакеты, поступающие из bridge-сегмента, поскольку при включённом bridge-nf (модуль br_netfilter) пакеты в цепочке INPUT видны с именем порта-члена моста (veth-r1-att), а не с именем самого моста. Аналогично, правило -i veth-r1-att без модуля physdev также даёт 0 совпадений. Корректное решение: загрузить br_netfilter командой modprobe br_netfilter, установить echo 1 > /proc/sys/net/bridge/bridge-nf-call-iptables и использовать правило с -m physdev --physdev-in veth-r1-att. В четвёртом прогоне эксперимента подтверждено блокирование 2 пакетов (92 байта) от Attacker.

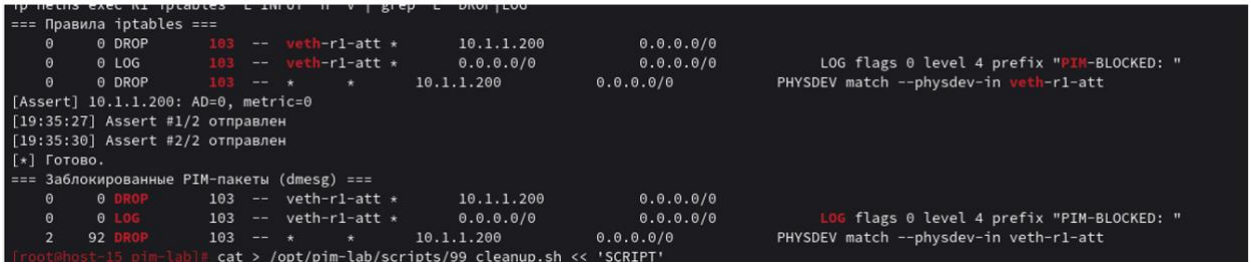

Рисунок 6 — Вывод iptables -L INPUT -n -v

Применение всех четырёх мер одновременно обеспечивает защиту PIM-SM инфраструктуры от всего исследованного спектра атак. При этом следует учитывать, что IGMP Snooping на br-src в рамках описанного стенда необходимо отключать для корректной работы самого стенда (параметр multicast_snooping = 0); в производственной среде эти настройки реализуются на уровне управляемых коммутаторов.

6. ЗАКЛЮЧЕНИЕ

В работе проведено полное экспериментальное исследование угроз безопасности протокола PIM-SM на платформе ALT Linux 11 / FRRouting 10.2.2. Впервые задокументированы практические особенности развёртывания FRRouting 10.x в среде Linux network namespaces, включая обязательный запуск демона mgmtd без флага -f и корректный порядок старта демонов.

Подтверждены следующие основные результаты: (1) пассивная разведка PIM-домена доступна любому узлу в L2-сегменте без привилегий; (2) BSR Injection успешно изменяет Bootstrap Router, однако статический RP полностью нейтрализует смену точки встречи; (3) Prune-атака эффективна лишь при отсутствии конкурирующих нисходящих Join; (4) IGMP Spoofing воздействует на состояние mroute, однако FRR 10.x требует IGMP General Query для добавления group membership; (5) захват DR обусловлен тай-брейком PIM Hello по IP-адресу и решается повышением DR Priority.

Установлено, что корректная фильтрация PIM-пакетов из bridge-сегмента в iptables требует использования модуля physdev с ключом --physdev-in, а не традиционного ключа -i для имени моста. Данный результат имеет практическую ценность для администраторов сетевой безопасности.

Воспроизводимость результатов подтверждена на четырёх независимых прогонах стенда. Все скрипты атак и конфигурационные файлы размещены в директории /opt/pim-lab/.

СПИСОК ЛИТЕРАТУРЫ

1. Fenner W., Handley M., Holbrook H., Kouvelas I., Parekh R., Zhang Z., Zheng L. RFC 7761: Protocol Independent Multicast — Sparse Mode (PIM-SM): Protocol Specification (Revised). — IETF, 2016. — URL: https://tools.ietf.org/html/rfc7761 (дата обращения: 04.06.2026).
2. Bhaskar N., Gall A., Lingard J., Venaas S. RFC 5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM). — IETF, 2008. — URL: https://tools.ietf.org/html/rfc5059 (дата обращения: 04.06.2026).
3. MITRE ATT&CK. T1565: Data Manipulation [Электронный ресурс]. — URL: https://attack.mitre.org/techniques/T1565/ (дата обращения: 04.06.2026).
4. MITRE ATT&CK. T1557: Adversary-in-the-Middle [Электронный ресурс]. — URL: https://attack.mitre.org/techniques/T1557/ (дата обращения: 04.06.2026).
5. Fenner W. RFC 2236: Internet Group Management Protocol, Version 2. — IETF, 1997. — URL: https://tools.ietf.org/html/rfc2236 (дата обращения: 04.06.2026).

6. MITRE ATT&CK. T1040: Network Sniffing [Электронный ресурс]. — URL: https://attack.mitre.org/techniques/T1040/ (дата обращения: 04.06.2026).
7. Katz D. RFC 2113: IP Router Alert Option. — IETF, 1997. — URL: https://tools.ietf.org/html/rfc2113 (дата обращения: 04.06.2026).
8. FRRouting Project. FRRouting User Guide 10.2 [Электронный ресурс]. — URL: https://docs.frrouting.org/en/stable-10.2/ (дата обращения: 04.06.2026).
9. Dutt D., Balaji V., Shah S., Bitar N. Network Virtualization using VXLAN // IETF RFC 7348. — 2014. — URL: https://tools.ietf.org/html/rfc7348 (дата обращения: 04.06.2026).
10. MITRE ATT&CK. T1499: Endpoint Denial of Service [Электронный ресурс]. — URL: https://attack.mitre.org/techniques/T1499/ (дата обращения: 04.06.2026).
11. Linux Foundation. Kernel documentation: Bridge networking [Электронный ресурс]. — URL: https://www.kernel.org/doc/html/latest/networking/bridge.html (дата обращения: 04.06.2026).
12. Бернат О. Scapy: пакетная библиотека Python [Электронный ресурс]. — URL: https://scapy.net/ (дата обращения: 04.06.2026).