УДК 004.056.53

Демидова Д. В.
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Комнацкая Е. Д.
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

ВЫЯВЛЕНИЕ И ПРОТИВОДЕЙСТВИЕ УТЕЧКЕ ТОПОЛОГИИ СЕТИ IPv6 ЧЕРЕЗ БАЗУ ДАННЫХ СОСТОЯНИЯ КАНАЛОВ ПРОТОКОЛА OSPFv3 (MITRE ATT&CK T1590)

Аннотация: В статье исследуется утечка топологии сети IPv6 через базу данных состояния каналов (LSDB) протокола OSPFv3 — техника разведки MITRE ATT&CK T1590. В среде эмулятора GNS3 развёрнут гетерогенный стенд, объединяющий в единой зоне маршрутизаторы трёх производителей (Cisco, MikroTik, VyOS). Реализован сценарий атаки с узла под управлением Debian с пакетом FRRouting: пассивный перехват пакетов Hello и активное установление смежности с получением полной LSDB. Подтверждено, что в конфигурации по умолчанию OSPFv3 не выполняет аутентификацию, вследствие чего полное описание автономной системы извлекается независимо от вендора оборудования менее чем за минуту. Разработан комплекс мер защиты (пассивизация интерфейсов, аутентификация IPsec AH с общим ключом, применение алгоритмов SHA-2), а уязвимость классифицирована как уязвимость конфигурации по ГОСТ Р 56546-2015.

Ключевые слова: сетевая безопасность, MITRE ATT&CK, OSPFv3, IPv6, утечка топологии, LSDB, разведка сети, IPsec AH, пассивный интерфейс.

Demidova D. V.
Student
Gubkin Russian State University of Oil and Gas
Komnatskaya E. D.
Student

Gubkin Russian State University of Oil and Gas

DETECTION AND MITIGATION OF IPv6 NETWORK TOPOLOGY LEAKAGE THROUGH THE OSPFv3 LINK-STATE DATABASE (MITRE ATT&CK T1590)

Abstract: This article examines the leakage of IPv6 network topology through the link-state database (LSDB) of the OSPFv3 protocol — the MITRE ATT&CK T1590 reconnaissance technique. A heterogeneous testbed, deployed in the GNS3 emulator, combines routers from three vendors (Cisco, MikroTik, VyOS) within a single routing area. An attack scenario is implemented from a Debian node running FRRouting: passive capture of Hello packets and active establishment of adjacency to obtain the full LSDB. It is confirmed that, in its default configuration, OSPFv3 performs no authentication, so the complete description of the autonomous system is extracted regardless of the equipment vendor in under one minute. A set of protective measures (passive interfaces, IPsec AH authentication with a shared key, use of SHA-2 algorithms) is developed, and the vulnerability is classified as a configuration vulnerability per GOST R 56546-2015.

Keywords: network security, MITRE ATT&CK, OSPFv3, IPv6, topology leakage, LSDB, network reconnaissance, IPsec AH, passive interface.

Введение

Развитие сетей передачи данных существенно изменили условия проведения разведки сетевой инфраструктуры [13]. Адресное пространство IPv6 для отдельной подсети составляет 2^{64} адресов, что делает методы активного сканирования, традиционные для IPv4 сетей, практически неприменимыми. Полный перебор адресов одной подсети /64 при скорости в миллион проверок в секунду занял бы время, превышающее возраст Вселенной. Указанное обстоятельство вынуждает злоумышленника искать альтернативные источники сведений о топологии атакуемой сети.

Одним из таких источников выступает база данных состояния каналов (Link-State Database, LSDB) протокола динамической маршрутизации OSPFv3 (Open Shortest Path First version 3). Указанный протокол применяется

для маршрутизации в сетях IPv6 и хранит в LSDB полное описание топологии автономной системы (Autonomous System, AS): идентификаторы всех маршрутизаторов, объявляемые префиксы, состояние межмаршрутизаторных каналов. Получение доступа к LSDB позволяет восстановить карту сети целиком, минуя необходимость активного сканирования адресного пространства.

Описанный вектор соответствует технике T1590 (Gather Victim Network Information — Сбор информации о сети жертвы) матрицы MITRE ATT&CK [18]. Техника относится к тактике разведки и включает сбор сведений о сетевых диапазонах, топологии и административной организации сети.

Теоретическая основа

1. Нормативно-правовое регулирование

Защита сетевой инфраструктуры в Российской Федерации регулируется комплексом нормативных правовых актов. Основополагающим документом выступает Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1], устанавливающий правовые основы обеспечения безопасности объектов критической информационной инфраструктуры (КИИ). Сети передачи данных операторов связи, государственных органов и организаций ряда отраслей экономики относятся к объектам КИИ, что обуславливает применение к ним установленных законом требований.

Требования к техническим мерам защиты значимых объектов КИИ конкретизированы приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [2]. Приказ устанавливает перечень организационных и технических мер, среди которых присутствуют меры по защите информационной (телекоммуникационной) сети, включающие сегментирование, контроль сетевого взаимодействия и защиту протоколов маршрутизации [3].

Непрерывный мониторинг сетевого трафика, предписываемый приказом для своевременного обнаружения аномалий, непосредственно связан с противодействием рассматриваемой в работе технике разведки.

Классификация и описание уязвимостей, к числу которых относится отсутствие аутентификации в протоколе маршрутизации, регламентируются национальными стандартами ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» [5] и ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» [4]. Согласно классификации ГОСТ Р 56546-2015 [5], рассматриваемая уязвимость относится к уязвимостям конфигурации, возникающим вследствие недостатков настройки программного обеспечения. Общие требования к системам менеджмента информационной безопасности, в рамках которых реализуется защита протоколов маршрутизации, установлены стандартом ГОСТ Р ИСО/МЭК 27001-2021 [6, 7].

2. Протокол OSPFv3

Протокол OSPFv3 представляет собой протокол внутреннего шлюза (Interior Gateway Protocol, IGP), основанный на технологии состояния каналов (link-state). В отличие от дистанционно-векторных протоколов, передающих соседям таблицу маршрутизации, протоколы состояния каналов распространяют сведения о состоянии собственных каналов, на основании которых каждый маршрутизатор самостоятельно строит полную карту сети и вычисляет кратчайшие пути по алгоритму Дейкстры (Shortest Path First, SPF) [9].

Протокол OSPFv3 является адаптацией протокола OSPFv2 для работы в сетях IPv6 и описан в RFC 5340 [14]. Между версиями существуют принципиальные различия.

Во-первых, OSPFv3 функционирует поверх локальных адресов канала (link-local) IPv6 и не переносит сетевую адресацию в заголовках

протокольных пакетов — адресная информация вынесена в отдельные объявления состояния каналов.

Во-вторых, и это ключевое отличие, OSPFv3 не содержит встроенного механизма аутентификации. Если OSPFv2 поддерживает аутентификацию по паролю и по хэшу MD5 непосредственно в протоколе, то в OSPFv3 функция аутентификации полностью делегирована протоколу защиты межсетевого взаимодействия IPsec (Internet Protocol Security) [16]. Указанное обстоятельство означает, что в конфигурации по умолчанию OSPFv3 не выполняет проверку подлинности соседних маршрутизаторов.

База данных состояния каналов LSDB представляет собой совокупность объявлений состояния каналов (Link-State Advertisement, LSA). В протоколе OSPFv3 определены следующие основные типы LSA, значимые для восстановления топологии [14]. Router-LSA (тип 1) описывает состояние интерфейсов маршрутизатора и содержит его идентификатор (Router ID). Network-LSA (тип 2) формируется выделенным маршрутизатором (Designated Router, DR) и описывает множественный сегмент. Intra-Area-Prefix-LSA (тип 9) переносит префиксы IPv6, связанные с маршрутизатором или сегментом. Link-LSA (тип 8) распространяется в пределах одного канала и содержит локальные адреса канала. Совокупность перечисленных объявлений в LSDB образует полное описание автономной системы.

Синхронизация LSDB между соседними маршрутизаторами выполняется в несколько этапов. Маршрутизаторы обнаруживают друг друга посредством пакетов Hello, рассылаемых на групповой адрес FF02::5. После установления двусторонней связи стороны обмениваются пакетами описания базы данных (Database Description, DBD), содержащими перечень имеющихся объявлений. На основании полученного перечня маршрутизатор запрашивает недостающие объявления пакетами запроса состояния канала (Link-State Request, LSR), получает их в пакетах обновления состояния канала (Link-State Update, LSU) и подтверждает приём пакетами подтверждения (Link-State Acknowledgment, LSAck). По завершении обмена

базы данных соседей становятся идентичными, а смежность переходит в состояние полной синхронизации (Full) [14].

Существенным для оценки риска является то обстоятельство, что в конфигурации по умолчанию любой узел, способный сформировать корректные пакеты Hello и получить статус соседа, проходит полную процедуру синхронизации и получает копию LSDB целиком. Поскольку аутентификация в OSPFv3 по умолчанию отсутствует, установление смежности не требует предъявления каких-либо учётных данных. Узел злоумышленника, подключённый к сегменту с работающим OSPFv3, получает полное описание топологии автономной системы.

Важной характеристикой протокола OSPFv3 является механизм выбора выделенного маршрутизатора и резервного выделенного маршрутизатора (Backup Designated Router, BDR) в множественных сегментах. В сегментах с множественным доступом, где потенциально может присутствовать более двух маршрутизаторов, для сокращения числа смежностей выбирается выделенный маршрутизатор, с которым устанавливают смежность все прочие маршрутизаторы сегмента. Выбор основан на значении приоритета интерфейса и идентификатора маршрутизатора. Узел злоумышленника, установив смежность с выделенным маршрутизатором, получает доступ к LSDB наравне с легитимными участниками сегмента. Указанный механизм не привносит дополнительной защиты, поскольку процедура выбора выделенного маршрутизатора также не предусматривает аутентификации.

Идентификатор маршрутизатора (Router ID) в OSPFv3 представляет собой 32-битное значение, записываемое в формате, аналогичном адресу IPv4, однако не связанное с фактической адресацией IPv6 интерфейсов. Идентификатор однозначно определяет маршрутизатор в пределах автономной системы и фигурирует в объявлениях Router-LSA. Получение злоумышленником перечня идентификаторов всех маршрутизаторов автономной системы из LSDB предоставляет основу для построения логической карты сети, независимой от физической адресации.

3. Утечка топологии как угроза безопасности

В сетях IPv4 разведка сетевой инфраструктуры традиционно опирается на активное сканирование: последовательную проверку доступности адресов в известных диапазонах (ping sweep) и сканирование портов (port scan) [8]. Размер типовой подсети IPv4 (например, /24, содержащая 256 адресов) допускает полный перебор за доли секунды. В сетях IPv6 указанный подход неприменим вследствие размера адресного пространства подсети, составляющего 2^{64} адресов.

Невозможность активного сканирования смещает интерес злоумышленника к пассивным источникам топологической информации. Протоколы динамической маршрутизации представляют собой такой источник: их штатное функционирование предполагает распространение полного описания топологии между всеми участниками маршрутизации. Если злоумышленник получает возможность стать участником процесса маршрутизации, он получает и полное описание сети. В этом состоит парадокс безопасности OSPFv3 в сетях IPv6: большое адресное пространство, затрудняющее сканирование, не защищает топологию, поскольку последняя свободно распространяется самим протоколом маршрутизации.

Утечка содержимого LSDB предоставляет злоумышленнику следующие сведения: идентификаторы всех маршрутизаторов автономной системы; полный перечень объявляемых префиксов IPv6, включая адреса интерфейсов обратной связи (loopback) и транзитных каналов; структуру связей между маршрутизаторами, позволяющую построить граф топологии; сведения о выделенных маршрутизаторах сегментов. Указанные сведения соответствуют составу информации, собираемой в рамках техники T1590 матрицы MITRE ATT&CK [18], и образуют основу для планирования последующих этапов атаки — выбора целей, определения критических узлов, подготовки атак на доступность или перехват трафика.

Полученная топологическая информация может быть использована на последующих этапах развития атаки. Знание структуры связей позволяет

идентифицировать критические узлы, выход из строя которых приводит к фрагментации сети, что создаёт предпосылки для целенаправленных атак на доступность. Сведения о префиксах оконечных сетей определяют направления дальнейшей разведки и потенциальные цели. Возможность установления смежности, продемонстрированная в работе, создаёт также предпосылки для активных атак на маршрутизацию — внедрения ложных объявлений с целью перенаправления трафика, что выходит за рамки рассматриваемой техники разведки, однако становится возможным вследствие той же первопричины — отсутствия аутентификации.

В терминах матрицы MITRE ATT&CK [18] рассматриваемая техника относится к тактике разведки и предшествует тактикам получения первоначального доступа и закрепления. Особенность техники T1590 состоит в том, что значительная часть сбора информации может выполняться без непосредственного взаимодействия с целевыми системами, что затрудняет обнаружение разведывательной активности. Применительно к OSPFv3 пассивный перехват протокольных пакетов не оставляет следов в журналах маршрутизаторов, а установление смежности, хотя и регистрируется, может быть замаскировано под легитимное подключение сетевого оборудования.

4. Методы защиты

Защита LSDB протокола OSPFv3 от несанкционированного получения основывается на предотвращении установления смежности с недоверенными узлами и на проверке подлинности протокольных пакетов. В работе рассматриваются три метода защиты, различающиеся механизмом действия и применимостью в условиях разнородного оборудования [11].

Первый метод — назначение интерфейсов пассивными (passive interface). Пассивный интерфейс анонсирует связанный с ним префикс в LSDB, однако не отправляет и не принимает пакеты Hello, вследствие чего не устанавливает смежности. Метод применяется к интерфейсам, направленным в сторону сегментов, где наличие соседних маршрутизаторов не предполагается, — в первую очередь к пользовательским сегментам и

сегментам подключения оконечных устройств. Назначение интерфейса пассивным предотвращает установление смежности злоумышленником, подключённым к данному сегменту, и тем самым исключает получение им LSDB. Метод поддерживается всеми основными производителями сетевого оборудования и не требует согласования параметров между устройствами, что делает его универсальным средством защиты периметра маршрутизации. Ограничением метода является неприменимость к транзитным каналам между маршрутизаторами, где установление смежности необходимо для работы протокола.

Второй метод — аутентификация протокольных пакетов посредством заголовка аутентификации IPsec (Authentication Header, AH) с использованием общего ключа. Протокол IPsec AH, описанный в RFC 4302 [15], обеспечивает проверку подлинности и целостности пакетов без их шифрования. Применение AH, а не протокола инкапсуляции полезной нагрузки (Encapsulating Security Payload, ESP), обусловлено использованием в OSPFv3 групповой адресации: пакеты протокола направляются на групповые адреса, для которых шифрование с индивидуальными ключами получателей неприменимо, тогда как аутентификация без шифрования с общим ключом совместима с групповой рассылкой. Заголовок AH содержит индекс параметров безопасности (Security Parameter Index, SPI), идентифицирующий контекст безопасности, порядковый номер для защиты от повторного воспроизведения и значение проверки целостности (Integrity Check Value, ICV). Маршрутизатор, не обладающий корректным ключом, не может сформировать действительное значение ICV, вследствие чего его пакеты отвергаются, а смежность не устанавливается.

Третий метод связан с выбором криптографического алгоритма вычисления хэша для значения ICV. Алгоритм SHA-1 формирует значение длиной 160 бит и рассматривается как минимально приемлемый [16]. Алгоритмы семейства SHA-2, в частности HMAC-SHA-256, обеспечивают повышенную криптографическую стойкость и рекомендуются к

применению. Исторически в реализациях OSPFv3 применялся также алгоритм MD5, признанный в настоящее время криптографически слабым [10, 12].

Существенным для практического применения является различие в поддержке указанных методов оборудованием различных производителей. Аутентификация OSPFv3 посредством IPsec AH с интеграцией в команды настройки протокола поддерживается не всеми маргрутизаторами. Данное обстоятельство, подробно рассматриваемое в практической части работы, определяет необходимость комбинированного применения методов защиты в реальных гетерогенных сетях.

Описание экспериментального стенда

Экспериментальный стенд построен в среде сетевого эмулятора GNS3 с применением аппаратной виртуализации. Выбор гетерогенной топологии, объединяющей оборудование трёх производителей в единой зоне маршрутизации, обусловлен стремлением приблизить условия эксперимента к реальным сетям операторов связи и крупных организаций, где совместно эксплуатируется оборудование различных вендоров. Такая постановка позволяет одновременно оценить поведение протокола OSPFv3 при межвендорном взаимодействии и проверить применимость мер защиты в разнородной среде.

Все три маршрутизатора включены в единую зону OSPFv3 — магистральную зону с идентификатором 0.0.0.0. Размещение всех маршрутизаторов в одной зоне обеспечивает наличие в LSDB каждого узла полного описания топологии автономной системы, что соответствует цели исследования: продемонстрировать, что злоумышленник, установивший смежность с одним маршрутизатором, получает сведения обо всей сети, включая маршрутизаторы, физически расположенные в других сегментах.

Узел злоумышленника реализован на базе операционной системы Debian с установленным пакетом маршрутизации FRRouting (FRR), обеспечивающим поддержку OSPFv3. Узел подключается поочерёдно к

сегменту каждого из трёх маршрутизаторов, что позволяет реализовать три независимых сценария атаки и провести сравнительный анализ поведения оборудования различных производителей.

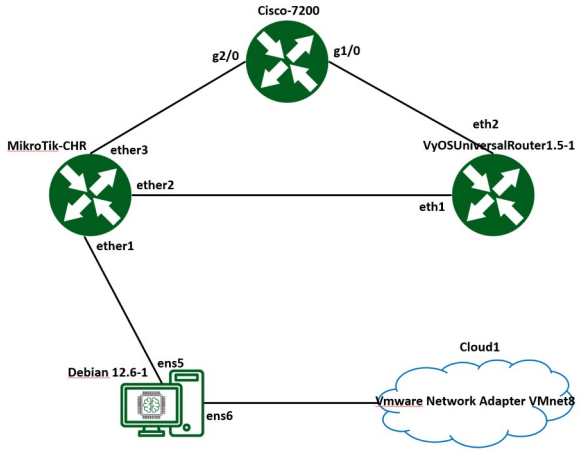


Рисунок 1. Топология для эксперимента

Топология стенда организована таким образом, что три маршрутизатора образуют замкнутый контур: каждый маршрутизатор соединён транзитными каналами с двумя другими. Такая организация обеспечивает наличие альтернативных путей и формирование полноценной LSDB, отражающей все связи автономной системы. Каждый маршрутизатор дополнительно располагает интерфейсом обратной связи (loopback) с уникальным префиксом /128, имитирующим клиентские сети, анонсируемые в маршрутизацию. Наличие таких префиксов в LSDB позволяет продемонстрировать утечку сведений не только о транзитной инфраструктуре, но и об оконечных сетях.

Таблица 1 – Состав оборудования и программного обеспечения стенда

Узел	Платформа	Версия ПО	Идентификатор
R1	Cisco 7206VXR	Cisco IOS 15.2(4)M8	1.1.1.1
R2	MikroTik CHR	RouterOS 7.21.4	2.2.2.2
R3	VyOS Universal Router	VyOS 1.5-stream-2025-Q2	3.3.3.3

Злоумышленник	Debian (FRRouting)	Debian 12, FRR 8.4.4	9.9.9.9

Адресный план стенда построен на основе документального префикса 2001:db8::/32, зарезервированного RFC 3849 [17] для применения в документации и примерах. Распределение адресного пространства по сегментам сети приведено в таблице 2.

Таблица 2 – Адресный план экспериментального стенда

Префикс / адрес	Назначение
2001:db8:12::/64	Транзитный канал R1 (Cisco) — R2 (MikroTik)
2001:db8:13::/64	Транзитный канал R1 (Cisco) — R3 (VyOS)
2001:db8:23::/64	Транзитный канал R2 (MikroTik) — R3 (VyOS)
2001:db8:1::/64	Сегмент подключения злоумышленника к R1 (Cisco)
2001:db8:2::/64	Сегмент подключения злоумышленника к R2 (MikroTik)
2001:db8:3::/64	Сегмент подключения злоумышленника к R3 (VyOS)
2001:db8:100::1/128	Интерфейс обратной связи (loopback) R1 (Cisco)
2001:db8:200::1/128	Интерфейс обратной связи (loopback) R2 (MikroTik)
2001:db8:300::1/128	Интерфейс обратной связи (loopback) R3 (VyOS)

Реализация атаки

Реализация атаки выполнена в три этапа, соответствующих поочерёдному подключению узла злоумышленника к сегменту каждого из маршрутизаторов. Методология каждого этапа включает две фазы: пассивный перехват протокольных пакетов с целью первичного обнаружения

маршрутизатора и активное установление смежности с целью получения полной LSDB.

В фазе пассивного перехвата на узле злоумышленника выполняется захват трафика на групповые адреса OSPFv3 средствами анализатора пакетов. Перехват пакетов Hello позволяет установить факт наличия маршрутизатора в сегменте, его идентификатор и идентификатор зоны, не выдавая присутствия злоумышленника. На данном этапе сведения о топологии автономной системы ограничены, поскольку пакеты Hello не переносят содержимого LSDB.

В фазе активного установления смежности на узле злоумышленника настраивается процесс OSPFv3 с произвольным идентификатором маршрутизатора, после чего узел проходит штатную процедуру установления смежности с атакуемым маршрутизатором. По достижении состояния полной синхронизации (Full) узел получает полную копию LSDB, содержащую описание всей автономной системы.

Инструментальное обеспечение атаки включает анализатор пакетов для перехвата и разбора протокольного трафика, средства языка сценариев для автоматизированного извлечения сведений из перехваченных пакетов, а также пакет маршрутизации FRRouting для установления легитимной с точки зрения протокола смежности. Применение полнофункционального пакета маршрутизации, а не специализированного инструмента подделки пакетов, отражает реалистичный сценарий: злоумышленнику достаточно штатного программного обеспечения с открытым исходным кодом, поскольку отсутствие аутентификации не требует обхода защитных механизмов. Указанное обстоятельство понижает порог реализуемости атаки и повышает её практическую значимость как угрозы.

1. Сценарий 1 – атака на сегмент Cisco

Узел злоумышленника подключён к сегменту маршрутизатора под управлением Cisco IOS. Пассивный перехват трафика подтвердил наличие в

сегменте пакетов Hello, отправляемых маршрутизатором с идентификатором 1.1.1.1 в зоне 0.0.0.0.

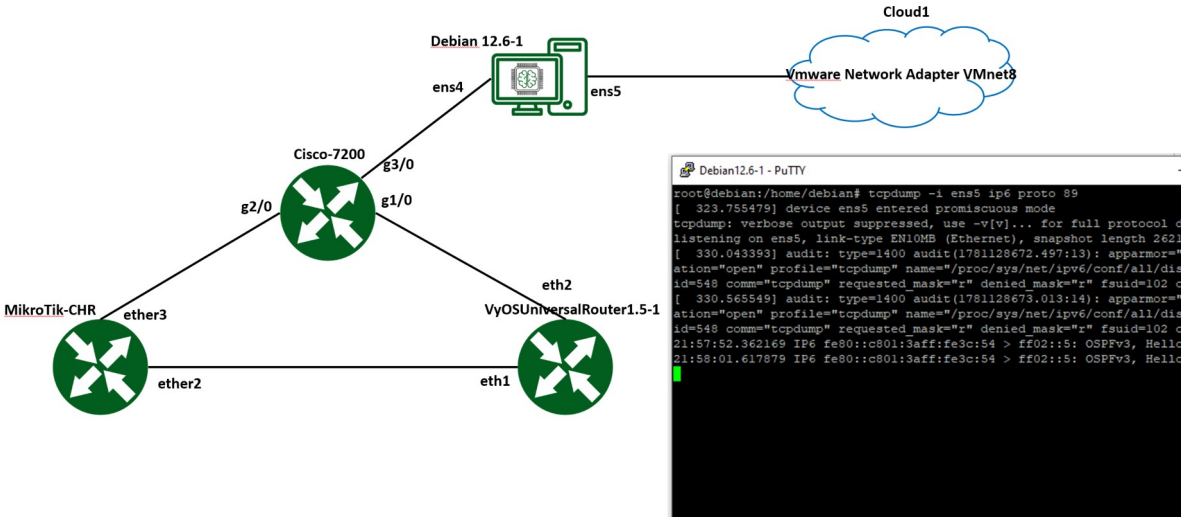


Рисунок 2. Прослушивание Hello-пакетов от маршрутизатора

После проведения анализа Hello-пакетов и настройки процесса OSPFv3 на узле злоумышленника смежность с маршрутизатором перешла в состояние полной синхронизации.

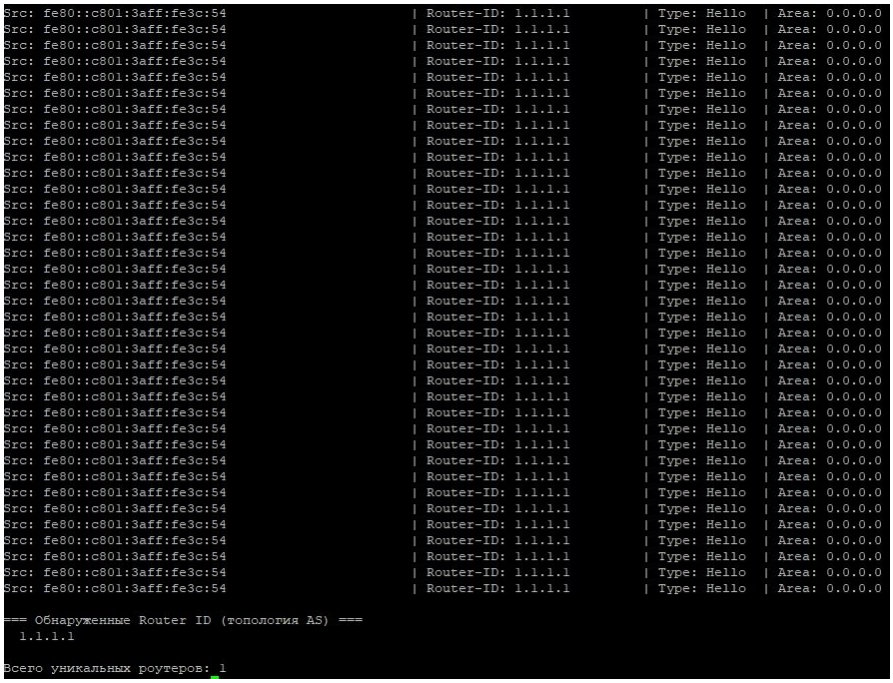
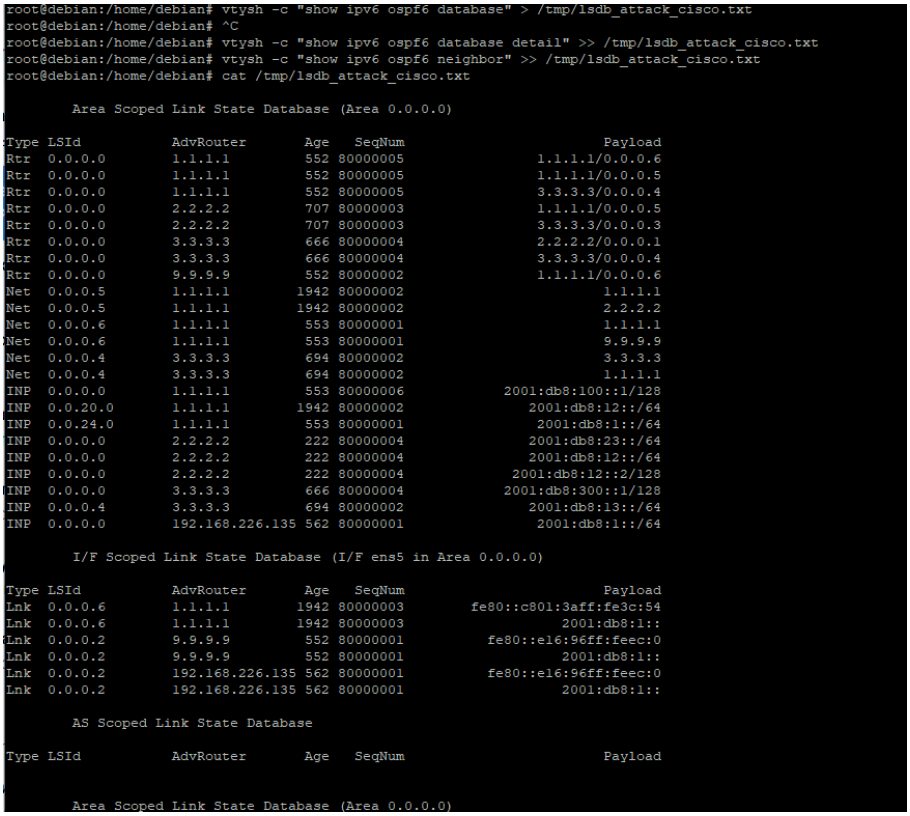


Рисунок 3. Анализ Hello-пакетов с помощью python-скрипта

Анализ полученной LSDB показал наличие в ней объявлений Router-LSA от всех трёх маршрутизаторов автономной системы с идентификаторами 1.1.1.1, 2.2.2.2 и 3.3.3.3, а также объявления от самого узла злоумышленника, ставшего полноправным участником маршрутизации.

В составе объявлений Intra-Area-Prefix-LSA обнаружены все префиксы сети, включая адреса интерфейсов обратной связи маршрутизаторов и транзитных каналов. Таким образом, подключение к сегменту единственного маршрутизатора обеспечило получение полного описания топологии автономной системы.



```
root@debian:/home/debian# vtysh -c "show ipv6 ospf6 database" > /tmp/lsdb_attack_cisco.txt
root@debian:/home/debian# ^C
root@debian:/home/debian# vtysh -c "show ipv6 ospf6 database detail" >> /tmp/lsdb_attack_cisco.txt
root@debian:/home/debian# vtysh -c "show ipv6 ospf6 neighbor" >> /tmp/lsdb_attack_cisco.txt
root@debian:/home/debian# cat /tmp/lsdb_attack_cisco.txt

        Area Scoped Link State Database (Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                      Payload
Rtr  0.0.0.0         1.1.1.1         552 80000005              1.1.1.1/0.0.0.6
Rtr  0.0.0.0         1.1.1.1         552 80000005              1.1.1.1/0.0.0.5
Rtr  0.0.0.0         1.1.1.1         552 80000005              3.3.3.3/0.0.0.4
Rtr  0.0.0.0         2.2.2.2         707 80000003              1.1.1.1/0.0.0.5
Rtr  0.0.0.0         2.2.2.2         707 80000003              3.3.3.3/0.0.0.3
Rtr  0.0.0.0         3.3.3.3         666 80000004              2.2.2.2/0.0.0.1
Rtr  0.0.0.0         3.3.3.3         666 80000004              3.3.3.3/0.0.0.4
Rtr  0.0.0.0         9.9.9.9         552 80000002              1.1.1.1/0.0.0.6
Net  0.0.0.5         1.1.1.1        1942 80000002                     1.1.1.1
Net  0.0.0.5         1.1.1.1        1942 80000002                     2.2.2.2
Net  0.0.0.6         1.1.1.1         553 80000001                     1.1.1.1
Net  0.0.0.6         1.1.1.1         553 80000001                     9.9.9.9
Net  0.0.0.4         3.3.3.3         694 80000002                     3.3.3.3
Net  0.0.0.4         3.3.3.3         694 80000002                     1.1.1.1
INP  0.0.0.0         1.1.1.1         553 80000006          2001:db8:100::1/128
INP  0.0.20.0        1.1.1.1        1942 80000002             2001:db8:12::/64
INP  0.0.24.0        1.1.1.1         553 80000001              2001:db8:1::/64
INP  0.0.0.0         2.2.2.2         222 80000004             2001:db8:23::/64
INP  0.0.0.0         2.2.2.2         222 80000004             2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         222 80000004           2001:db8:12::2/128
INP  0.0.0.0         3.3.3.3         666 80000004          2001:db8:300::1/128
INP  0.0.0.4         3.3.3.3         694 80000002             2001:db8:13::/64
INP  0.0.0.0         192.168.226.135 562 80000001              2001:db8:1::/64

        I/F Scoped Link State Database (I/F ens5 in Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                      Payload
Lnk  0.0.0.6         1.1.1.1        1942 80000003       fe80::c801:3aff:fe3c:54
Lnk  0.0.0.6         1.1.1.1        1942 80000003                  2001:db8:1::
Lnk  0.0.0.2         9.9.9.9         552 80000001         fe80::e16:96ff:feec:0
Lnk  0.0.0.2         9.9.9.9         552 80000001                  2001:db8:1::
Lnk  0.0.0.2         192.168.226.135 562 80000001         fe80::e16:96ff:feec:0
Lnk  0.0.0.2         192.168.226.135 562 80000001                  2001:db8:1::

        AS Scoped Link State Database

Type LSId            AdvRouter       Age   SeqNum                      Payload


        Area Scoped Link State Database (Area 0.0.0.0)
```

Рисунок 4. Доступ к LSDB на узле злоумышленника

2. Сценарии 2 и 3 — атака на сегменты MikroTik и VyOS

Сценарии атаки на сегменты маршрутизаторов под управлением RouterOS и VyOS реализованы по идентичной методологии. В обоих случаях узел злоумышленника установил смежность в состоянии полной синхронизации и получил LSDB, содержащую полное описание автономной системы, совпадающее с результатом первого сценария. Совпадение результатов подтверждает, что объём утекающей информации не зависит от того, к сегменту какого производителя подключён злоумышленник, поскольку LSDB в пределах одной зоны идентична на всех маршрутизаторах.

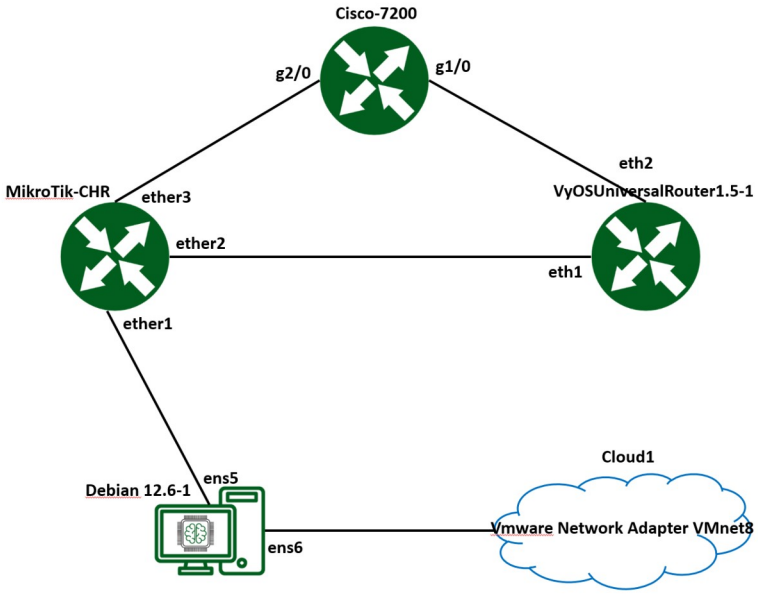


Рисунок 5. Перестроенная топология для атаки на MikroTik

```
debian# show ipv6 ospf6 database

        Area Scoped Link State Database (Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Rtr  0.0.0.0         1.1.1.1         435 80000005              1.1.1.1/0.0.0.5
Rtr  0.0.0.0         1.1.1.1         435 80000005              3.3.3.3/0.0.0.4
Rtr  0.0.0.0         2.2.2.2         223 80000005              1.1.1.1/0.0.0.5
Rtr  0.0.0.0         2.2.2.2         223 80000005              3.3.3.3/0.0.0.3
Rtr  0.0.0.0         2.2.2.2         223 80000005              9.9.9.9/0.0.0.2
Rtr  0.0.0.0         3.3.3.3         408 80000003              2.2.2.2/0.0.0.2
Rtr  0.0.0.0         3.3.3.3         408 80000003              3.3.3.3/0.0.0.4
Rtr  0.0.0.0         9.9.9.9         223 80000004              9.9.9.9/0.0.0.2
Net  0.0.0.5         1.1.1.1         852 80000003                     1.1.1.1
Net  0.0.0.5         1.1.1.1         852 80000003                     2.2.2.2
Net  0.0.0.4         3.3.3.3         436 80000001                     3.3.3.3
Net  0.0.0.4         3.3.3.3         436 80000001                     1.1.1.1
Net  0.0.0.2         9.9.9.9         223 80000001                     9.9.9.9
Net  0.0.0.2         9.9.9.9         223 80000001                     2.2.2.2
INP  0.0.0.0         1.1.1.1         435 80000006          2001:db8:100::1/128
INP  0.0.0.0         1.1.1.1         435 80000006            2001:db8:1::/64
INP  0.0.20.0        1.1.1.1         852 80000003           2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         228 80000005           2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         228 80000005         2001:db8:12::2/128
INP  0.0.0.0         2.2.2.2         228 80000005           2001:db8:23::/64
INP  0.0.0.0         2.2.2.2         228 80000005            2001:db8:2::/64
INP  0.0.0.0         3.3.3.3         408 80000003          2001:db8:300::1/128
INP  0.0.0.4         3.3.3.3         436 80000001           2001:db8:13::/64
INP  0.0.0.2         9.9.9.9         223 80000001            2001:db8:1::/64
INP  0.0.0.2         9.9.9.9         223 80000001            2001:db8:2::/64

        I/F Scoped Link State Database (I/F ens5 in Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Lnk  0.0.0.3         2.2.2.2         228 80000001       fe80::e3b:79ff:fece:0
Lnk  0.0.0.3         2.2.2.2         228 80000001                2001:db8:2::
Lnk  0.0.0.2         9.9.9.9         263 80000005       fe80::e16:96ff:feec:0
Lnk  0.0.0.2         9.9.9.9         263 80000005                2001:db8:1::

        AS Scoped Link State Database

Type LSId            AdvRouter       Age   SeqNum                  Payload
```

Рисунок 6. Доступ к LSDB на узле злоумышленника (MikroTik)

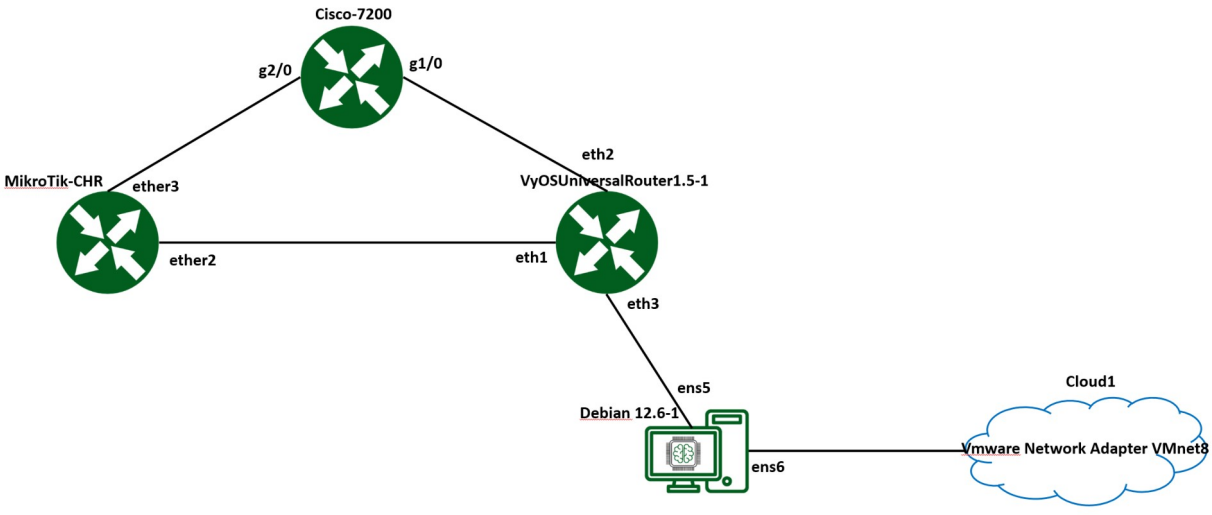
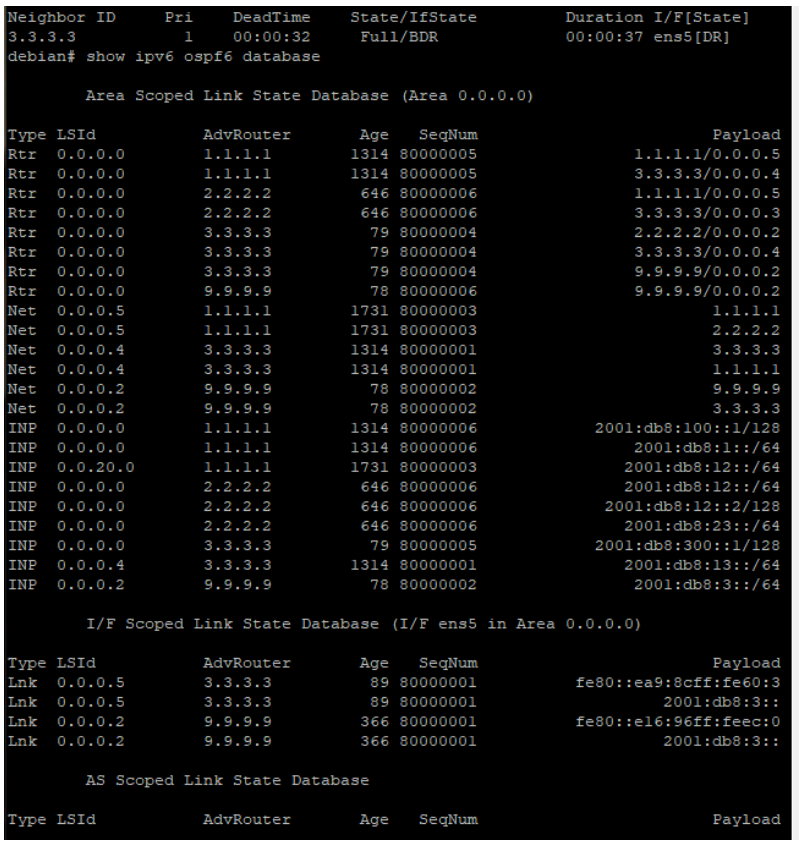


Рисунок 7. Перестроенная топология для атаки на VyOs



```
Neighbor ID     Pri    DeadTime    State/IfState         Duration I/F[State]
3.3.3.3           1    00:00:32     Full/BDR             00:00:37 ens5[DR]
debian# show ipv6 ospf6 database

       Area Scoped Link State Database (Area 0.0.0.0)

Type LSId           AdvRouter       Age   SeqNum                      Payload
Rtr  0.0.0.0        1.1.1.1        1314 80000005               1.1.1.1/0.0.0.5
Rtr  0.0.0.0        1.1.1.1        1314 80000005               3.3.3.3/0.0.0.4
Rtr  0.0.0.0        2.2.2.2         646 80000006               1.1.1.1/0.0.0.5
Rtr  0.0.0.0        2.2.2.2         646 80000006               3.3.3.3/0.0.0.3
Rtr  0.0.0.0        3.3.3.3          79 80000004               2.2.2.2/0.0.0.2
Rtr  0.0.0.0        3.3.3.3          79 80000004               3.3.3.3/0.0.0.4
Rtr  0.0.0.0        3.3.3.3          79 80000004               9.9.9.9/0.0.0.2
Rtr  0.0.0.0        9.9.9.9          78 80000006               9.9.9.9/0.0.0.2
Net  0.0.0.5        1.1.1.1        1731 80000003                     1.1.1.1
Net  0.0.0.5        1.1.1.1        1731 80000003                     2.2.2.2
Net  0.0.0.4        3.3.3.3        1314 80000001                     3.3.3.3
Net  0.0.0.4        3.3.3.3        1314 80000001                     1.1.1.1
Net  0.0.0.2        9.9.9.9          78 80000002                     9.9.9.9
Net  0.0.0.2        9.9.9.9          78 80000002                     3.3.3.3
INP  0.0.0.0        1.1.1.1        1314 80000006          2001:db8:100::1/128
INP  0.0.0.0        1.1.1.1        1314 80000006              2001:db8:1::/64
INP  0.0.20.0       1.1.1.1        1731 80000003             2001:db8:12::/64
INP  0.0.0.0        2.2.2.2         646 80000006             2001:db8:12::/64
INP  0.0.0.0        2.2.2.2         646 80000006           2001:db8:12::2/128
INP  0.0.0.0        2.2.2.2         646 80000006             2001:db8:23::/64
INP  0.0.0.0        3.3.3.3          79 80000005          2001:db8:300::1/128
INP  0.0.0.4        3.3.3.3        1314 80000001             2001:db8:13::/64
INP  0.0.0.2        9.9.9.9          78 80000002              2001:db8:3::/64

       I/F Scoped Link State Database (I/F ens5 in Area 0.0.0.0)

Type LSId           AdvRouter       Age   SeqNum                      Payload
Lnk  0.0.0.5        3.3.3.3          89 80000001       fe80::ea9:8cff:fe60:3
Lnk  0.0.0.5        3.3.3.3          89 80000001                2001:db8:3::
Lnk  0.0.0.2        9.9.9.9         366 80000001       fe80::e16:96ff:feec:0
Lnk  0.0.0.2        9.9.9.9         366 80000001                2001:db8:3::

       AS Scoped Link State Database

Type LSId           AdvRouter       Age   SeqNum                      Payload
```

Рисунок 8. Доступ к LSDB на узле злоумышленника (VyOs)

3. Сравнительный анализ результатов

Сводные результаты трёх сценариев атаки приведены в таблице 3. Во всех трёх случаях смежность установлена без предъявления учётных данных, а полная LSDB получена за время, не превышающее одной минуты.

Таблица 3 – Сводные результаты сценариев атаки

Сценарий	Состояние смежности	LSDB получена	Аутентификация
Cisco 7206VXR	Full / DR	Да (полная)	Отсутствует
MikroTik CHR	Full / DR	Да (полная)	Отсутствует
VyOS 1.5	Full / DR	Да (полная)	Отсутствует

Результаты эксперимента подтверждают, что протокол OSPFv3 в конфигурации по умолчанию не обеспечивает защиту LSDB от несанкционированного получения независимо от производителя оборудования. Уязвимость носит протокольный, а не реализационный характер: отсутствие встроенной аутентификации в OSPFv3 является

свойством самого протокола, вследствие чего оборудование всех трёх производителей оказалось одинаково уязвимым. Полученный результат опровергает возможное предположение о наличии у отдельных производителей встроенных механизмов защиты, активных по умолчанию.

Сопоставление содержимого LSDB, полученной в трёх сценариях, показало полное совпадение перечня объявлений во всех случаях. Данное наблюдение согласуется с принципом работы протоколов состояния каналов: в пределах одной зоны база данных синхронизируется и поддерживается идентичной на всех маршрутизаторах. Следовательно, точка подключения злоумышленника не влияет на объём получаемой информации — подключение к любому сегменту любого маршрутизатора зоны обеспечивает получение полного описания автономной системы. Данное обстоятельство усугубляет рассматриваемую угрозу, поскольку для компрометации топологии всей сети достаточно доступа к единственному её сегменту.

С точки зрения классификации уязвимостей по ГОСТ Р 56546-2015 [5] выявленная уязвимость относится к уязвимостям конфигурации, проявляющимся на уровне сетевого программного обеспечения. Местом возникновения уязвимости является подсистема маршрутизации, областью происхождения — недостатки настройки, связанные с эксплуатацией протокола в конфигурации по умолчанию без активации механизмов аутентификации. Указанная классификация определяет направление устранения уязвимости — изменение конфигурации с активацией мер защиты, рассматриваемых далее.

Разработка и проверка мер защиты

Разработка мер защиты выполнена с учётом ключевого ограничения реальных сетей: разнородности и возможной устарелости оборудования. В сетях, эксплуатируемых длительное время, совместно функционирует оборудование различных производителей и поколений, причём поддержка отдельных механизмов защиты может отсутствовать на устаревших платформах или различаться по способу настройки. Предлагаемый подход

основан на комбинировании методов защиты таким образом, чтобы обеспечить защищённость сети при минимальных требованиях к возможностям оборудования.

Анализ поддержки методов аутентификации OSPFv3 оборудованием стенда выявил существенные различия между производителями. Интеграция аутентификации IPsec AH непосредственно в команды настройки протокола OSPFv3 присутствует в исследованной версии Cisco IOS, где параметры аутентификации задаются на уровне интерфейса командой настройки OSPFv3. В исследованных версиях RouterOS [19] и VyOS [20] прямая интеграция аутентификации IPsec AH в команды OSPFv3 отсутствует: настройка IPsec для защиты протокольного трафика требует отдельной конфигурации подсистемы IPsec, не связанной непосредственно с настройкой протокола маршрутизации. Указанное различие имеет принципиальное значение для построения защиты в гетерогенной сети и обобщено в таблице 4.

Дополнительным ограничением выступает требование согласованности параметров аутентификации между всеми маршрутизаторами одного сегмента. Аутентификация OSPFv3 является симметричной: все маршрутизаторы, образующие смежности в пределах одного канала, должны использовать одинаковый ключ и алгоритм хэширования. В гетерогенной сети это требование осложняется как различиями в синтаксисе настройки, так и возможными расхождениями в поддерживаемых алгоритмах и форматах представления ключа.

Таблица 4 – Поддержка методов защиты OSPFv3 оборудованием стенда

Метод защиты	Cisco IOS	RouterOS	VyOS
Пассивный интерфейс	Поддерживается	Поддерживается	Поддерживается
Аутентификация IPsec AH, встроенная	Поддерживается	Не поддерживается	Не поддерживается

в OSPFv3		напрямую	напрямую
Защита через отдельную подсистему IPsec	Поддерживается	Требует ручной настройки	Требует ручной настройки

1. Двухуровневая стратегия защиты

С учётом выявленных ограничений предложена двухуровневая стратегия защиты, обеспечивающая защищённость сети независимо от полноты поддержки аутентификации отдельными устройствами.

Первый уровень — защита периметра маршрутизации посредством назначения пассивными всех интерфейсов, направленных в сторону недоверенных сегментов. Данный метод поддерживается всеми тремя производителями единообразно по смыслу действия и не требует согласования параметров между устройствами. Назначение пассивным интерфейса, обращённого к пользовательскому сегменту, предотвращает установление смежности злоумышленником, подключённым к данному сегменту. Поскольку именно через такие сегменты наиболее вероятно подключение злоумышленника, первый уровень защиты обеспечивает основной эффект и применим даже к оборудованию, не поддерживающему аутентификацию OSPFv3.

Второй уровень — аутентификация протокольных пакетов на транзитных каналах между маршрутизаторами для оборудования, поддерживающего данную функцию. Аутентификация защищает от подключения злоумышленника непосредственно к транзитному каналу, а также от подмены маршрутизатора. На оборудовании с прямой поддержкой аутентификации OSPFv3 второй уровень реализуется средствами протокола, на прочем оборудовании — средствами подсистемы IPsec либо, при невозможности, компенсируется усилением физической и канальной защиты транзитных каналов.

Применительно к стенду стратегия реализована следующим образом. На маршрутизаторе под управлением Cisco IOS, обладающем прямой

поддержкой аутентификации, на интерфейсе, обращённом к сегменту злоумышленника, настроена аутентификация IPsec AH с алгоритмом SHA-1 и индивидуальным индексом параметров безопасности. На маршрутизаторах под управлением RouterOS и VyOS, для которых прямая настройка аутентификации OSPFv3 недоступна, интерфейсы, обращённые к сегментам злоумышленника, назначены пассивными. Внутренние транзитные каналы между маршрутизаторами в рамках эксперимента оставлены без аутентификации, что отражает типичную ситуацию частичной защищённости реальной сети и позволяет оценить достаточность защиты периметра.

2. Проверка эффективности мер защиты

Проверка эффективности предложенных мер выполнена повторением сценариев атаки после применения защиты. На маршрутизаторе под управлением Cisco IOS применены меры защиты двух уровней применительно к интерфейсу, обращённому к сегменту злоумышленника. Настройка аутентификации посредством заголовка аутентификации IPsec с алгоритмом SHA-1 [15, 16] на данном интерфейсе исключила возможность установления смежности с узлом, не располагающим корректным ключом: протокольные пакеты злоумышленника были отвергнуты маршрутизатором как не прошедшие проверку целостности. Дополнительно интерфейс назначен пассивным, что прекратило отправку пакетов Hello в сегмент злоумышленника и исключило обнаружение маршрутизатора при пассивном перехвате. Совокупное применение обеих мер на одном интерфейсе обеспечило защиту как от пассивной разведки, так и от активного установления смежности.

```
Cisco-7200(config)#int gi3/0
Cisco-7200(config-if)#$spi 258 sha1 6A8C4A34E3B26A56BCF2EEC590531B17F7F75097
Cisco-7200(config-if)#end
```

Рисунок 9. Настройка безопасности на Cisco

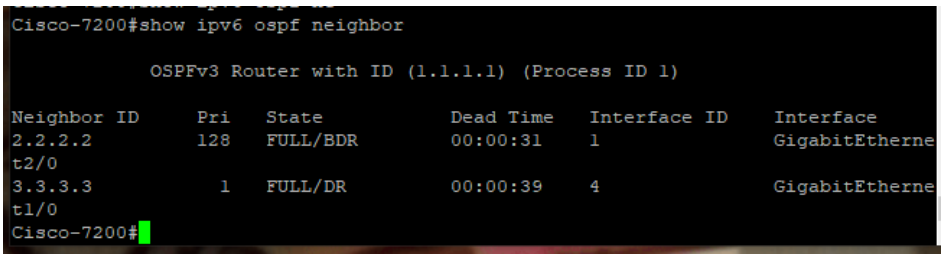


Рисунок 10. Наличие легитимного соседства после настройки безопасности

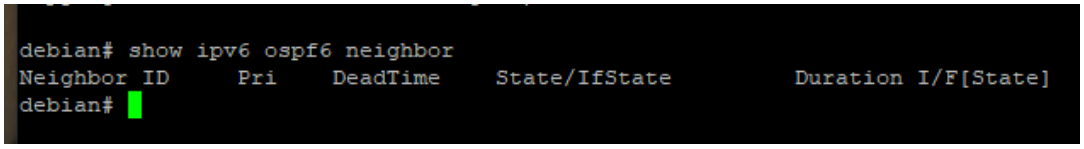


Рисунок 11. Невозможность установить соседство с Cisco после настройки безопасности

На маршрутизаторах под управлением RouterOS и VyOS назначение интерфейса пассивным привело к прекращению отправки пакетов Hello в сегмент злоумышленника, вследствие чего узел злоумышленника не обнаружил маршрутизатор при пассивном перехвате и не смог установить смежность.

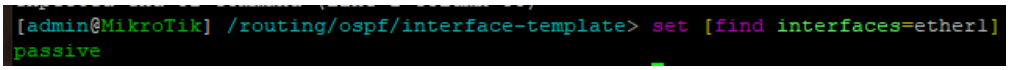


Рисунок 12. Настройка пассивного внешнего интерфейса на MikroTik

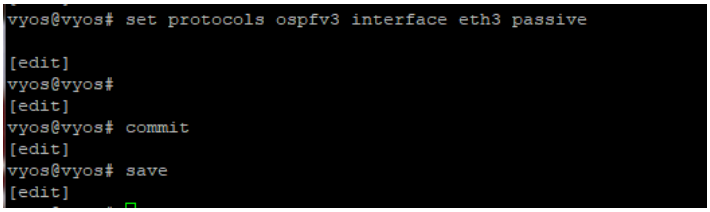


Рисунок 13. Настройка пассивного интерфейса на VyOs

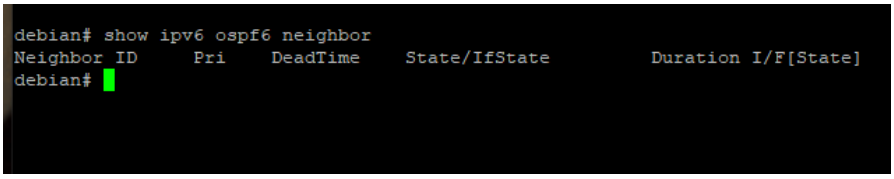


Рисунок 14. Невозможность установить соседство с оставшимися роутерами после настройки безопасности

Заключение

В работе исследована возможность утечки информации о сетевой архитектуре через базу данных состояния каналов протокола OSPFv3 в

условиях большого адресного пространства IPv6. Подтверждено, что техника T1590 матрицы MITRE ATT&CK [18] применительно к OSPFv3 реализуема: узел злоумышленника, подключённый к сегменту сети с работающим протоколом OSPFv3 в конфигурации по умолчанию, устанавливает смежность без предъявления учётных данных и получает полное описание топологии автономной системы за время, не превышающее одной минуты.

Эксперимент, проведённый на оборудовании трёх производителей, показал, что уязвимость носит протокольный характер и не зависит от производителя оборудования: отсутствие встроенной аутентификации является свойством самого протокола OSPFv3. Установлено, что в условиях большого адресного пространства IPv6 значимость данного вектора возрастает, поскольку невозможность активного сканирования смещает интерес злоумышленника к пассивным источникам топологической информации, каковым выступает LSDB.

Выявлено существенное различие в поддержке методов аутентификации OSPFv3 оборудованием различных производителей: прямая интеграция аутентификации IPsec AH в команды настройки протокола присутствует не во всех реализациях. Данное обстоятельство определяет необходимость комбинированного применения методов защиты в реальных гетерогенных сетях. Предложена двухуровневая стратегия защиты, сочетающая защиту периметра маршрутизации посредством пассивных интерфейсов, применимую к оборудованию любого производителя, и аутентификацию каналов. Эффективность стратегии подтверждена экспериментально: после применения защиты получение LSDB узлом злоумышленника оказалось невозможным.

Практическая значимость работы состоит в применимости предложенной стратегии к реальным сетям с разнородным и устаревшим оборудованием, где полная унификация механизмов аутентификации недостижима. Защита периметра маршрутизации обеспечивает основной эффект при минимальных требованиях к возможностям оборудования, что

соответствует требованиям нормативных документов по защите критической информационной инфраструктуры в части контроля сетевого взаимодействия. Направлением дальнейших исследований является изучение защиты транзитных каналов посредством инкапсуляции протокольного трафика OSPFv3 в шифрованные туннели IPsec для оборудования, не поддерживающего встроенную аутентификацию протокола.

Список источников

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. — Текст: электронный // Консультант Плюс: справочно-правовая система. — URL: http://www.consultant.ru (дата обращения: 12.06.2026).
2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239. — Текст: электронный // ФСТЭК России: официальный сайт. — URL: https://fstec.ru (дата обращения: 12.06.2026).
3. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ ФСТЭК России от 21.12.2017 № 235. — Текст: электронный // ФСТЭК России: официальный сайт. — URL: https://fstec.ru (дата обращения: 12.06.2026).
4. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. — Введ. 2016-04-01. — Москва: Стандартинформ, 2015. — 12 с.
5. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. — Введ. 2016-04-01. — Москва: Стандартинформ, 2015. — 16 с.
6. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

информационной безопасности. Требования. — Введ. 2022-01-01. — Москва: Российский институт стандартизации, 2021. — 35 с.
7. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. — Введ. 2009-10-01. — Москва: Стандартинформ, 2009. — 16 с.
8. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд., перераб. и доп. — Москва: ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст: непосредственный.
9. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. — 5-е изд. — Санкт-Петербург: Питер, 2020. — 1008 с. — ISBN 978-5-4461-1426-9. — Текст: непосредственный.
10. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л. К. Бабенко, Е. А. Ищукова. — Москва: Гелиос АРВ, 2006. — 376 с. — Текст: непосредственный.
11. Запечников, С. В. Информационная безопасность открытых систем: учебник: в 2 томах. Том 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. — Москва: Горячая линия — Телеком, 2018. — 558 с. — Текст: непосредственный.
12. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — Москва: ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст: непосредственный.
13. Сергеев, А. Н. Основы локальных компьютерных сетей: учебное пособие / А. Н. Сергеев. — Санкт-Петербург: Лань, 2019. — 184 с. — Текст: непосредственный.
14. RFC 5340. OSPF for IPv6 / R. Coltun, D. Ferguson, J. Moy, A. Lindem. — Internet Engineering Task Force, 2008. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc5340 (дата обращения: 12.06.2026).
15. RFC 4302. IP Authentication Header / S. Kent. — Internet Engineering Task Force, 2005. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc4302 (дата обращения: 12.06.2026).

16. RFC 4552. Authentication/Confidentiality for OSPFv3 / M. Gupta, N. Melam. — Internet Engineering Task Force, 2006. — Текст : электронный. — URL: https://www.rfc-editor.org/rfc/rfc4552 (дата обращения: 12.06.2026).
17. RFC 3849. IPv6 Address Prefix Reserved for Documentation / G. Huston, A. Lord, P. Smith. — Internet Engineering Task Force, 2004. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc3849 (дата обращения: 12.06.2026).
18. MITRE ATT&CK. Gather Victim Network Information (T1590). — Текст: электронный // MITRE Corporation: официальный сайт. — URL: https://attack.mitre.org/techniques/T1590 (дата обращения: 12.06.2026).
19. OSPF: RouterOS documentation. — Текст: электронный // MikroTik: официальный сайт. — URL: https://help.mikrotik.com/docs/spaces/ROS/pages/9863229/OSPF (дата обращения: 12.06.2026).
20. OSPF: VyOS documentation. — Текст: электронный // VyOS: официальный сайт. — URL: https://docs.vyos.io/en/latest/configuration/protocols/ospf.html (дата обращения: 12.06.2026).

References

1. On the Security of the Critical Information Infrastructure of the Russian Federation: Federal Law of July 26, 2017, No. 187-FZ. — Electronic version // Consultant Plus: legal reference system. — URL: http://www.consultant.ru (accessed on June 12, 2026).
2. On Approval of the Requirements for Ensuring the Security of Significant Facilities of the Critical Information Infrastructure of the Russian Federation: Order of the FSTEC of Russia of December 25, 2017, No. 239. — Electronic version // FSTEC of Russia: official website. — URL: https://fstec.ru (accessed on June 12, 2026).
3. On Approval of the Requirements for the Creation of Security Systems for Significant Objects of the Critical Information Infrastructure of the Russian

Federation and Ensuring Their Functioning: Order of the FSTEC of Russia dated 21.12.2017 No. 235. — Text: electronic // FSTEC of Russia: official website. — URL: https://fstec.ru (date of access: 12.06.2026).

4. GOST R 56545-2015. Information Security. Vulnerabilities of Information Systems. Vulnerability Description Rules. — Introduced on 2016-04-01. — Moscow: Standartinform, 2015. — 12 p.
5. GOST R 56546-2015. Information Security. Vulnerabilities of Information Systems. Classification of Information System Vulnerabilities. — Introduced on 2016-04-01. — Moscow: Standartinform, 2015. — 16 p.
6. GOST R ISO/IEC 27001-2021. Information technology. Security methods and means. Information security management systems. Requirements. — Introduced on 2022-01-01. — Moscow: Russian Institute of Standardization, 2021. — 35 p.
7. GOST R 53114-2008. Information protection. Information security in an organization. Basic terms and definitions. — Introduced on 2009-10-01. — Moscow: Standartinform, 2009. — 16 p.
8. Biryukov, A. A. Information security: defense and attack / A. A. Biryukov. — 2nd ed., revised and enlarged. — Moscow: DMK Press, 2017. — 434 p. — ISBN 978-5-97060-435-9. — Text: direct.
9. Olifer, V. G. Computer Networks. Principles, Technologies, Protocols / V. G. Olifer, N. A. Olifer. — 5th ed. — St. Petersburg: Piter, 2020. — 1008 p. — ISBN 978-5-4461-1426-9. — Text: direct.
10. Babenko, L. K. Modern Block Cipher Algorithms and Methods of Their Analysis / L. K. Babenko, E. A. Ishchukova. — Moscow: Helios ARV, 2006. — 376 p. — Text: direct.
11. Zapechnikov, S. V. Information Security of Open Systems: textbook: in 2 volumes. Volume 2. Means of protection in networks / S. V. Zapechnikov, N. G. Miloslavskaya, A. I. Tolstoy, D. V. Ushakov. — Moscow: Goryachaya Liniya-Telecom, 2018. — 558 p. — Text: direct.

12. Shan'gin, V. F. Information Security in Computer Systems and Networks / V. F. Shan'gin. — Moscow: DMK Press, 2012. — 592 p. — ISBN 978-5-94074-637-9. — Text: direct.
13. Sergeev, A. N. Fundamentals of Local Computer Networks: A Tutorial / A. N. Sergeev. — St. Petersburg: Lan, 2019. — 184 p. — Text: direct.
14. RFC 5340. OSPF for IPv6 / R. Coltun, D. Ferguson, J. Moy, A. Lindem. — Internet Engineering Task Force, 2008. — Text: electronic. — URL: https://www.rfc-editor.org/rfc/rfc5340 (date accessed: 12.06.2026).
15. RFC 4302. IP Authentication Header / S. Kent. — Internet Engineering Task Force, 2005. — Text: electronic. — URL: https://www.rfc-editor.org/rfc/rfc4302 (date accessed: 12.06.2026).
16. RFC 4552. Authentication/Confidentiality for OSPFv3 / M. Gupta, N. Melam. — Internet Engineering Task Force, 2006. — Text: electronic. — URL: https://www.rfc-editor.org/rfc/rfc4552 (date accessed: 12.06.2026).
17. RFC 3849. IPv6 Address Prefix Reserved for Documentation / G. Huston, A. Lord, P. Smith. — Internet Engineering Task Force, 2004. — Text: electronic. — URL: https://www.rfc-editor.org/rfc/rfc3849 (date accessed: 12.06.2026).
18. MITRE ATT&CK. Gather Victim Network Information (T1590). — Text: electronic // MITRE Corporation: official website. — URL: https://attack.mitre.org/techniques/T1590 (date accessed: 12.06.2026).
19. OSPF: RouterOS documentation. — Text: electronic // MikroTik: official website. — URL: https://help.mikrotik.com/docs/spaces/ROS/pages/9863229/OSPF (access date: 06/12/2026).
20. OSPF: VyOS documentation. — Text: electronic // VyOS: official website. — URL: https://docs.vyos.io/en/latest/configuration/protocols/ospf.html (access date: 06/12/2026).