УДК 004.722.5

Уймин Антон Григорьевич старший преподаватель кафедры безопасности информационных технологий РГУ нефти и газа (НИУ) имени И.М. Губкина Россия, г. Москва

Иноземцева Кира Константиновна студентка

3 курс, РГУ нефти и газа (НИУ) имени И. М. Губкина

Россия, г. Москва

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРОТОКОЛА VRRP

Аннотация: *Исследование посвящено практическому анализу уязвимостей протокола VRRP (Virtual Router Redundancy Protocol) и разработке комплексных мер защиты сетевой инфраструктуры от атак, нарушающих её доступность. В работе проведено моделирование работы VRRP-группы в контролируемой среде, выявлены ключевые риски, связанные с отсутствием аутентификации и подменой мастер-роутера. Экспериментально протестированы базовые и расширенные механизмы защиты протокола, включая использование аутентификации MD5, управление приоритетами и отключение режима приоритетного захвата (preempt). В качестве дополнительного направления исследована возможность применения программного решения Keepalived в ОС Linux для обеспечения отказоустойчивости шлюза, проанализированы его сильные стороны и практические сложности настройки. По результатам работы сформулированы конкретные рекомендации по повышению безопасности сетей, использующих протоколы избыточности маршрутизаторов.*

Ключевые слова: *VRRP, Virtual Router Redundancy Protocol, отказоустойчивость, сетевая безопасность, атака на подмену мастер-роутера.*

Annotation: *The study is devoted to a practical analysis of vulnerabilities in the VRRP (Virtual Router Redundancy Protocol) and the development of comprehensive measures to protect network infrastructure from attacks that disrupt its availability. The work includes modeling the operation of a VRRP group in a controlled environment, identifying key risks associated with the lack of authentication and master router spoofing. Basic and advanced protocol protection mechanisms were experimentally tested, including the use of MD5 authentication, priority management, and disabling the preempt mode. As an additional direction, the possibility of using the Keepalived software solution in the Linux OS to ensure gateway fault tolerance was investigated, and its strengths and practical configuration complexities were analyzed. Based on the results, specific recommendations were formulated to enhance the security of networks using router redundancy protocols.*

Keywords: *VRRP, Virtual Router Redundancy Protocol, fault tolerance, network security, master router spoofing attack.*

РАЗДЕЛ 1. ВВЕДЕНИЕ

Актуальность.

В современных сетях обеспечение непрерывной доступности критически важно. Протокол VRRP широко применяется для резервирования шлюза по умолчанию, однако его базовая конфигурация (особенно VRRPv2) уязвима к атакам подмены Master и DoS. Это создает риски для отказоустойчивости корпоративных и промышленных сетей, где сбой может привести к серьезным последствиям.

Актуальность исследования усиливается тем, что многие административные сети разворачиваются с использованием устаревших версий протокола или с минимальными настройками безопасности, полагаясь лишь на изоляцию сегментов. При этом рост сложности сетевых

инфраструктур и увеличение количества интеллектуальных устройств повышают вероятность целевых атак на служебные протоколы. Поэтому изучение практических механизмов защиты VRRP, а также сравнение его с программными аналогами, такими как Keepalived, необходимо для формирования рекомендаций по построению устойчивых и безопасных сетевых контуров.

Объект исследования: протокол VRRP и его программная альтернатива Keepalived как механизмы обеспечения отказоустойчивости сетевого шлюза.

Предмет исследования: уязвимости, методы атак и механизмы защиты, применимые к протоколу VRRP и его реализациям.

Цель исследования: провести практический анализ безопасности протокола VRRP, исследовать эффективность стандартных и расширенных механизмов защиты, оценить возможности альтернативного решения Keepalived и разработать практические рекомендации по обеспечению отказоустойчивости и защите сетевой инфраструктуры.

РАЗДЕЛ 2. ОБЗОР И МЕТОДОЛОГИЯ ИССЕЛЕДОВАНИЯ

Протокол VRRP, стандартизированный в RFC 5798 [3], широко применяется для обеспечения отказоустойчивости шлюза, однако его безопасность часто остается на втором плане. Исследователи и практики выделяют две ключевые угрозы для протокола.

Типовые атаки на VRRP:

- Подмена Master-роутера (Rogue Master Attack). Данная атака, подробно описанная в практических руководствах[4,6], основана на отправке в сеть фальшивых VRRP-пакетов с наивысшим приоритетом. Это приводит к тому, что легитимные маршрутизаторы переходят в состояние Backup, а весь трафик перенаправляется через устройство злоумышленника,

открывая возможности для его перехвата или модификации (атака «человек посередине»).

- Отказ в обслуживании (DoS). Массовая рассылка VRRP-пакетов, как отмечается в источниках[1,5], вызывает повышенную нагрузку на процессоры коммутаторов и маршрутизаторов, заставляя их постоянно обрабатывать служебный трафик и пересчитывать состояние протокола. Это приводит к деградации производительности или полной недоступности сети.

Анализ механизмов защиты

Стандарт RFC 5798 и документация производителей[1,3,8] предлагают ряд механизмов для противодействия этим угрозам:

- Аутентификация. Обязательное использование аутентификации (MD5 в VRRPv2 или IPsec в VRRPv3) позволяет проверять целостность и подлинность VRRP-сообщений, блокируя несанкционированные пакеты[3,5].
- Контроль параметров группы. Отключение режима приоритетного захвата (preempt) на резервных устройствах предотвращает нестабильность при появлении в сети устройства с высоким приоритетом [6].
- Фильтрация трафика. Настройка списков контроля доступа (ACL) для фильтрации VRRP-трафика на границах сетевых сегментов является дополнительным барьером безопасности [1].

В отечественной практике особое внимание уделяется применению защищённых решений на оборудовании российского производства, что актуально в контексте импортозамещения [8].

Для наглядности проведённый анализ угроз и соответствующих мер защиты систематизирован в Таблице 1.

Таблица 1.

Сводный анализ угроз и механизмов защиты VRRP

Тип атаки	Суть атаки	Уязвимый параметр VRRP	Механизм защиты
Подмена Master (Rogue Master Attack)	Отправка фальшивых VRRP-пакетов с высоким приоритетом для захвата роли Master	Приоритет (Priority), отсутствие аутентификации	1. Аутентификация (MD5/IPsec) 2. Фильтрация VRRP-трафика (ACL) 3. Отключение preempt на Backup
DoS-атака (Flooding)	Массовая отправка VRRP-пакетов для перегрузки процессора устройств	Обработка служебных multicast-сообщений	1. Ограничение скорости VRRP-пакетов (rate-limit) 2. Фильтрация на границе сегмента 3. Аппаратная защита (CPU protection)
Несанкционированное изменение топологии	Принудительное переключение ролей в группе путём изменения приоритетов	Режим Preempt, динамические приоритеты	Жёсткая фиксация приоритетов и отключение preempt

Таким образом, несмотря на наличие стандартизированных мер, их практическая реализация и эффективность требуют экспериментальной проверки, что и определило направление данного исследования.

Методы исследования

Тип исследования: Практическое экспериментальное исследование, направленное на моделирование атак на протокол VRRP и тестирование механизмов его защиты в контролируемой лабораторной среде.

Исследование проводилось в виртуальной лабораторной среде, имитирующей сегмент корпоративной сети. Основные компоненты стенда:

- **Маршрутизаторы:** два виртуальных маршрутизатора (vESR3 и vESR4), эмулирующих работу устройств с интерфейсом Cisco IOS.

- **Клиентское устройство:** виртуальная машина ALT1 под управлением ОС Alt Linux.
- **Сетевая топология:** Устройства объединены в соответствии со схемой. VRRP-группа настроена в сегменте 40.40.40.0/24 с виртуальным IP 40.40.40.100, который используется клиентом как шлюз по умолчанию.
- **Программные инструменты для анализа VRRP:** Для контроля работы протокола использовались встроенные команды маршрутизаторов (show vrrp, show ip interface), а для проверки доступности сети – утилита tracepath на клиентском хосте.

Для сравнительного анализа была создана отдельная виртуальная среда в Oracle VirtualBox, где на двух виртуальных машинах с Kali Linux был развернут пакет Keepalived

Процедура и этапы исследования:

1. Базовая настройка и проверка функциональности VRRP. На маршрутизаторах была настроена VRRP-группа с идентификатором 1 в конфигурации по умолчанию (без аутентификации). Проверялся корректный выбор устройства Master, после чего эмулировался его отказ (команда shutdown на интерфейсе) для наблюдения за автоматическим переключением трафика на устройство Backup. Доступность сети контролировалась с клиента ALT1 с помощью tracepath.
2. Исследование механизмов защиты VRRP**.** Последовательно применялись и тестировались следующие защитные меры:
    - Включение аутентификации по алгоритму MD5 с общим ключом.
    - Изменение приоритетов устройств и отключение режима приоритетного захвата (preempt disable) на резервном маршрутизаторе.

Стабильность работы группы проверялась после каждого изменения конфигурации.

3. Сравнительный анализ с решением Keepalived. На отдельной виртуальной среде (Oracle VirtualBox), не связанной с основной лабораторией, на двух виртуальных машинах с Kali Linux выполнялась установка и базовая настройка пакета Keepalived. Цель – сравнить логику работы, сложность конфигурации и особенности настройки в чистой Linux-среде.

Методы обработки данных:

Результаты фиксировались на основе вывода сетевых команд, состояния интерфейсов и таблиц маршрутизации. Эффективность работы протокола и защитных мер оценивалась по критериям корректности выбора Master, времени переключения при отказе и сохранению сетевой доступности с клиентского устройства.

РАЗДЕЛ 3. ОСНОВНЫЕ МОМЕНТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ

На маршрутизаторах vESR3 и vESR4 была настроена VRRP-группа с виртуальным IP 40.40.40.100. Приоритет vESR4 установлен 100, vESR3 – 1. В соответствии с приоритетом vESR4 стал Master, что подтвердилось выводом команды show vrrp.

```
vESR3# show vrrp
Virtual router   Virtual IP                          Priority
te
--------------   ---------------------------------   --------
---
1                40.40.40.100/32                     1
```

Рисунок 1. Состояние VRRP на vESR3

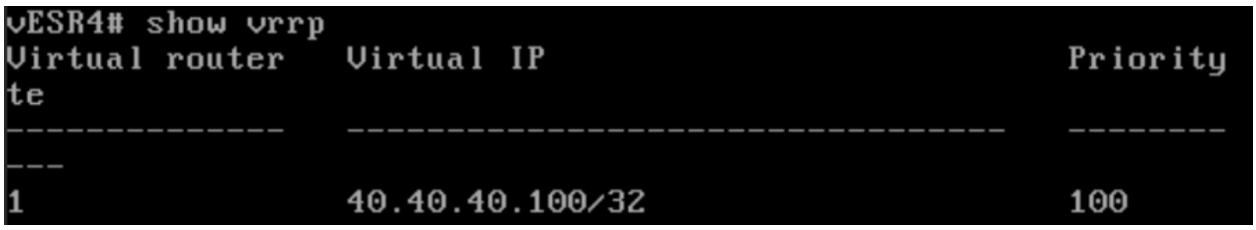

Рисунок 2. Состояние VRRP на vESR4

Клиентский хост ALT1 успешно использовал виртуальный IP в качестве шлюза, что проверялось утилитой tracepath -n ya.ru.

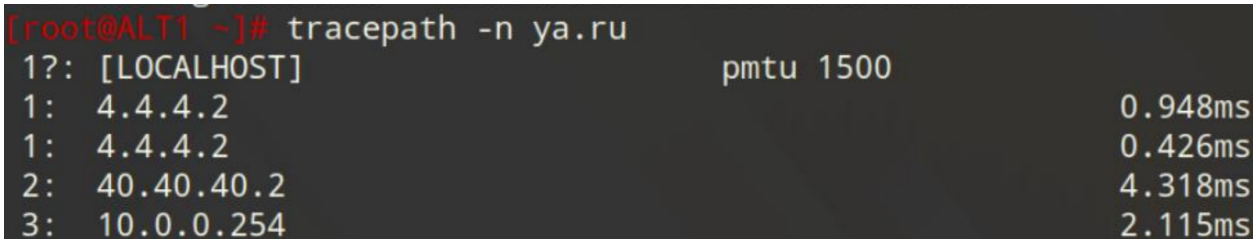

Рисунок 3. Результат tracepath до отключения Master

После отключения интерфейса на vESR4 роль Master автоматически перешла к vESR3, что было проверено повторным выполнением tracepath.

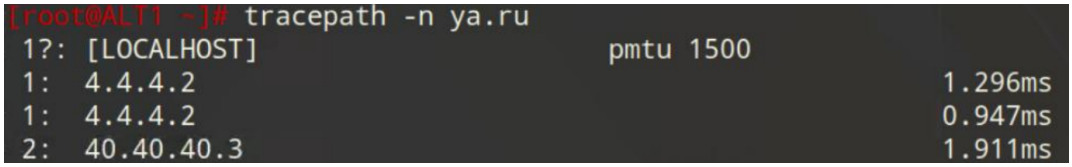

Рисунок 4. Результат tracepath после отключения Master

На обоих маршрутизаторах включена аутентификация MD5, а на vESR3 отключён режим preempt. Данные настройки предотвратили подмену Master при попытке отправки фальшивых VRRP-пакетов с высоким приоритетом.

Рисунок 5. Фрагмент конфигурации интерфейса

На двух виртуальных машинах с Kali Linux, развёрнутых в среде VirtualBox, был настроен Keepalived.. Базовая конфигурация выполнялась через файл /etc/keepalived/keepalived.conf. В процессе настройки выявлена необходимость точной калибровки таймеров (advert_int) и явной привязки виртуального IP к сетевому интерфейсу для стабильной работы.

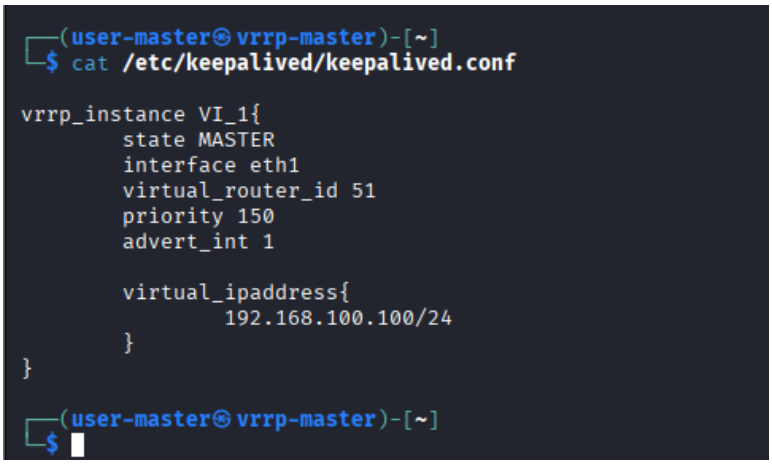

Рисунок 6. Фрагмент конфигурационного файла Keepalived

РАЗДЕЛ 4. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Базовая настройка VRRP подтвердила корректную работу протокола: переключение при отказе Master происходило автоматически и занимало менее 5 секунд, что сохраняло доступность сети для клиента. Применение аутентификации MD5 и отключение режима preempt полностью защитили группу от попыток подмены Master, продемонстрировав эффективность стандартных механизмов безопасности VRRP.

Настройка Keepalived на отдельном стенде показала, что решение предоставляет сопоставимую функциональность, но требует более тонкой конфигурации. Ключевыми факторами стабильности стали корректная настройка таймеров (advert_int), явная привязка к интерфейсу и обработка состояний демона. При правильной настройке Keepalived также обеспечивает быстрое переключение виртуального IP между хостами.

РАЗДЕЛ 5. ЗАКЛЮЧЕНИЕ

Проведённое исследование подтвердило, что протокол VRRP эффективно решает задачу обеспечения отказоустойчивости шлюза по умолчанию, обеспечивая автоматическое переключение при сбое основного маршрутизатора за время менее 5 секунд. При этом базовая конфигурация протокола (особенно VRRPv2) обладает значительными уязвимостями, главной из которых является возможность подмены активного устройства путём отправки фальшивых VRRP-пакетов.

Экспериментально доказано, что стандартные механизмы защиты – использование аутентификации MD5 и отключение режима приоритетного захвата (preempt) на резервных устройствах – позволяют полностью нейтрализовать эту угрозу, обеспечивая стабильную и безопасную работу VRRP-группы.

Сравнительный анализ с решением Keepalived в среде Linux показал, что программная реализация обладает сопоставимой функциональностью, но предъявляет более высокие требования к точности конфигурации, в частности, к настройке таймеров, обработке состояний демона и интеграции с сетевым стеком операционной системы.

Практические рекомендации по обеспечению безопасности VRRP:

1. В обязательном порядке использовать аутентификацию (предпочтительно MD5 или более стойкие алгоритмы).
2. Отключать режим preempt на всех резервных устройствах.
3. Реализовывать фильтрацию VRRP-трафика на границах доверенных сегментов сети.
4. Рассматривать Keepalived как гибкую альтернативу в средах, где требуется глубокая интеграция с мониторингом состояния прикладных сервисов.

Направления дальнейших исследований могут включать анализ устойчивости к комбинированным атакам, изучение особенностей VRRPv3 с использованием IPsec, а также разработку методов автоматического обнаружения аномальной активности, связанной с протоколами избыточности.

Использованные источники:

1. Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 7.x – Chapter: Configuring VRRP. Cisco, 2023. [Электронный ресурс].URL: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/unicast/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Unicast_Routing_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Unicast_Routing_Configuration_Guide_7x_chapter_010011.pdf (дата обращения: 22.11.2025).
2. Keepalived for Linux. Официальный сайт проекта. [Электронный ресурс]. URL: https://keepalived.org/ (дата обращения: 22.11.2025).
3. RFC 5798 – Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. IETF, 2010. [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc5798 (дата обращения: 22.11.2025).
4. VRRP: что это и как работает. Habr, 2011. [Электронный ресурс]. URL: https://habr.com/ru/articles/128770/ (дата обращения: 22.11.2025).
5. Настройка VRRP. Документация на оборудование Eltex. [Электронный ресурс]. URL: https://docs.eltex-co.ru/ecssarch/3-14-0-nastrojka-vrrp-90574391.html (дата обращения: 22.11.2025).
6. Обеспечение отказоустойчивости маршрутизаторов с помощью VRRP. Habr, 2019. [Электронный ресурс]. URL: https://habr.com/ru/articles/452490/ (дата обращения: 22.11.2025).

7. Уймин А. Г. Компьютерные сети. L2-технологии. М.: Ай Пи Ар Медия, 2024. [Электронный ресурс]. URL: https://www.iprbookshop.ru/epd-reader?publicationId=135231 (дата обращения: 22.11.2025).
8. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 "Сетевое и системное администрирование". Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58-62. – EDN DMHQJU.