

ISSN 3033-9359

**Выпуск 3 (011), 2026**

# **НАУЧНЫЙ ЖУРНАЛ ПРОФЕССИОНАЛИТЕТ**

**Москва**

# ПРОФЕССИОНАЛИТЕТ

№ 3 (011), 2026

**Научный журнал**

Основан в 2023 году

Зарегистрирован федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Номер свидетельства ЭЛ № ФС 77-84640

Дата регистрации 01.02.2023

**Учредитель:**

Уймин А.Г.

**Редакционная коллегия серии:**

Уймин А.Г. – гл. редактор, руководитель команды #AU\_team

Греков В.С. – магистр информационной безопасности

Уймина О.И. – магистр интеллектуальных систем

Губина Т. Н., канд.пед.наук;

Махотин Д. А., канд.пед.наук, доцент

Белоусов А.В., канд.техн.наук, доцент

Орлова М.А., канд.техн.наук, доцент

**Адрес редакции:**

Адрес редакции 115432, г. Москва, 5-я Кожуховская улица, 18к1 12

Все права защищены. Никакая часть этого издания  
не может быть репродуцирована без письменного разрешения издателя.

© #au\_team, 2026

# PROFESSIONALITET

No. 3 (011), 2026

**Scientific Journal**

Founded in 2023

Registered with the Federal Service for Supervision of Communications, Information Technology  
and Mass Media

Certificate of Registration: EL No. FS 77-84640

Registration Date: 01.02.2023

**Founder:**

Uymin A.G.

**Editorial Board of the Series:**

Uymin A.G. – Editor-in-Chief, Head of the #AU\_team

Grekov V.S. – Master of Information Security

Uymina O.I. – Master of Intelligent Systems

Gubina T.N., Candidate of Pedagogical Sciences

Makhotin D.A., Candidate of Pedagogical Sciences, Associate Professor

Belousov A.V., Candidate of Technical Sciences, Associate Professor

Orlova M.A., Candidate of Technical Sciences, Associate Professor

**Editorial Office:**

Editorial Office Address: 18/1, 5th Kozhukhovskaya St., Moscow, 115432, Russia.

All rights reserved. No part of this publication may be reproduced without the publisher's written  
permission.

© #au\_team, 2026

**СОДЕРЖАНИЕ**

**Методы и системы защиты информации, информационная безопасность**

|                                                                                                                                                                        |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Бережная П. А., Мирчевски К. Д. — ИЗУЧЕНИЕ АТАКИ ARP SPOOFING НА ПРИМЕРЕ КОММУТАТОРОВ РАЗЛИЧНЫХ ВЕНДОРОВ.....</b>                                                   | <b>5</b>  |
| <b>Дворников Д. С., Костионова М. А. — ВЕРИФИКАЦИЯ МЕХАНИЗМОВ УСТОЙЧИВОСТИ ДОМЕННЫХ GPO В КОРПОРАТИВНОЙ СЕТИ.....</b>                                                  | <b>15</b> |
| <b>Калинин А. А., Клиз М. Р. — СРАВНИТЕЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ СЕТЕВОГО ОБОРУДОВАНИЯ МЕТОДАМИ ВНЕШНЕГО АУДИТА В КОРПОРАТИВНОЙ СРЕДЕ.....</b>                          | <b>24</b> |
| <b>Коваль Н. М., Гимпель Е. А. — ЛАБОРАТОРНЫЙ РАЗБОР TSP-ACL И ИНТЕРФЕЙСНЫХ ПОКАЗАТЕЛЕЙ СЕТЕВОГО СТЕНДА.....</b>                                                       | <b>36</b> |
| <b>Колоколов С. А., Белый К. С. — НАСТРОЙКА DNSSEC И УПРАВЛЕНИЯ КЛЮЧАМИ НА УЧЕБНОМ СТЕНДЕ WINDOWS SERVER.....</b>                                                      | <b>44</b> |
| <b>Кудимов А. А., Исаков А. Д. — РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ DNS SPOOFING (MITRE ATT&amp;CK T1557.003) НА УРОВНЕ СЕТЕВЫХ КОММУТАТОРОВ.....</b>         | <b>55</b> |
| <b>Кязымов А. А., Терешонок А. А. — ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ IGMPV2 И СРАВНИТЕЛЬНАЯ ОЦЕНКА МЕТОДОВ ЗАЩИТЫ НА L2+ КОММУТАТОРАХ РАЗЛИЧНЫХ ВЕНДОРОВ .....</b> | <b>66</b> |
| <b>Ляхова М. В., Сеникова Н. Г. — ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ RSTP С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА ROOT GUARD НА L2+ УСТРОЙСТВАХ.....</b>                           | <b>78</b> |

CONTENTS

**Methods and systems of information protection and information security**

|                                                                                                                                                                                        |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Berezhnaya P. A., Mirchevski K. D. — STUDYING THE ARP SPOOFING ATTACK USING SWITCHES FROM DIFFERENT VENDORS AS EXAMPLES.....</b>                                                    | <b>5</b>  |
| <b>Dvornikov D. S., Kostionova M. A. — VERIFICATION OF DOMAIN GPO STABILITY MECHANISMS IN A CORPORATE NETWORK.....</b>                                                                 | <b>15</b> |
| <b>Kalinin A. A., Kliz M. R. — COMPARATIVE ANALYSIS OF NETWORK EQUIPMENT VULNERABILITIES USING EXTERNAL AUDIT METHODS IN A CORPORATE ENVIRONMENT.....</b>                              | <b>24</b> |
| <b>Koval N. M., Gimpel E. A. — LABORATORY ANALYSIS OF TCP ACLS AND INTERFACE METRICS IN A NETWORK TESTBED.....</b>                                                                     | <b>36</b> |
| <b>Kolokolov S. A., Bely K. S. — DNSSEC CONFIGURATION AND KEY MANAGEMENT ON A WINDOWS SERVER TEACHING TESTBED.....</b>                                                                 | <b>44</b> |
| <b>Kudimov A. A., Iskakov A. D. — IMPLEMENTATION AND EFFECTIVENESS ANALYSIS OF DHCP SPOOFING PROTECTION (MITRE ATT&amp;CK T1557.003) AT THE NETWORK SWITCH LEVEL.....</b>              | <b>55</b> |
| <b>Kyazimov A. A., Tereshonok A. A. — EXPERIMENTAL ANALYSIS OF IGMPV2 VULNERABILITIES AND COMPARATIVE EVALUATION OF PROTECTION METHODS ON L2+ SWITCHES FROM DIFFERENT VENDORS.....</b> | <b>66</b> |
| <b>Lyakhova M. V., Senikova N. G. — PROTECTION AGAINST RSTP ATTACKS USING ROOT GUARD ON L2+ DEVICES.....</b>                                                                           | <b>78</b> |

**Бережная П. А., Мирчевски К. Д.**

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

## **ИЗУЧЕНИЕ АТАКИ ARP SPOOFING НА ПРИМЕРЕ КОММУТАТОРОВ РАЗЛИЧНЫХ ВЕНДОРОВ**

**Аннотация.** В статье рассматривается уязвимость коммутируемой локальной сети к ARP Spoofing и описывается лабораторный сценарий с коммутаторами Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM. В топологии участвовали два узла-жертвы под управлением Windows и узел атакующего с Kali Linux. Атаку выполняли с помощью Ettercap, а сетевой обмен анализировали в Wireshark; для фиксации изменений использовали ARP-таблицы и ICMP ping. В описанном сценарии атакующий рассылал ложные ARP-ответы, связывая свой MAC-адрес с адресами шлюза и целевого узла. В захвате представлены запросы и ответы между узлами; полный путь пакетов через машину атакующего не установлен; таблицы адресов до и после воздействия показывают изменение соответствия IP- и MAC-адресов. Работа также описывает настройки защиты для Cisco и Eltex с применением DHCP Snooping и Dynamic ARP Inspection, а для MikroTik — использование статических ARP-записей. Наблюдения фиксируют изменение ARP-записи в данном примере и иллюстрируют применение анализа таблиц и пакетов при обучении сетевой безопасности. Результаты не являются исчерпывающим тестом всех моделей, версий прошивок и вариантов настройки указанных производителей. Поэтому вывод о типовых настройках следует относить только к описанному стенду; для проверки иной конфигурации требуется отдельное испытание. Изложенная процедура отделяет авторское описание атаки от наблюдаемых ARP-записей и сетевых кадров; полный цикл MITM по этим фрагментам не подтверждён.

**Ключевые слова:** ARP spoofing, ARP-таблица, MAC-адрес, сетевая безопасность, информационная безопасность, коммутатор, сетевой трафик.

### **Введение**

Безопасность локальных вычислительных сетей остаётся важной задачей при эксплуатации корпоративной инфраструктуры. Несмотря на развитие средств защиты, внутренние угрозы, связанные с особенностями протоколов канального уровня, требуют отдельного внимания. Одна из таких угроз — ARP Spoofing (подмена ARP-записей), потенциально позволяющая перенаправить часть сетевого обмена. Возможность чтения или модификации передаваемых данных зависит от конфигурации и применяемой защиты; в настоящей работе полный перехват трафика не установлен [1].

Проблема противодействия ARP Spoofing исследуется в научной среде.

А. Ю. Крылов и Н. А. Шитов предложили распределённую систему выявления и предотвращения атаки на основе объектного подхода и конечных автоматов [2]. Н. В. Шишов и В. А. Ломазов исследовали влияние этой атаки на критические информационные системы, используя для моделирования аппарат сетей Петри-Маркова [3]. Эти работы заложили важный теоретический фундамент в исследовании данной атаки и продемонстрировали её возможные последствия.

В протоколе ARP отсутствует встроенная криптографическая проверка соответствий IP- и MAC-адресов. Для выявления и ограничения подмены применяют мониторинг сетевого трафика, анализ ARP-таблиц и защитные механизмы управляемых коммутаторов. Р. М. Алиев рассматривает задачу обнаружения ARP Spoofing [4]. Данная статья ограничена лабораторной демонстрацией и не претендует на общую оценку защищённости оборудования разных производителей.

Для практического анализа представляет интерес сопоставление настроек защиты от ARP Spoofing на оборудовании Cisco, Eltex и MikroTik. Однако по отдельным эпизодам нельзя оценить типовую защищённость заводских конфигураций или сравнить эффективность разных платформ без повторных испытаний в одинаковых условиях.

Объект исследования – процесс обеспечения безопасности сетевого взаимодействия на канальном уровне модели OSI в коммутируемых Ethernet-сетях.

Предмет исследования – уязвимость стандартных конфигураций коммутационного оборудования различных вендоров к атаке типа ARP Spoofing в рамках практической демонстрации данной атаки в контролируемых условиях тестового сетевого стенда.

Цель работы — описать лабораторный сценарий ARP-poisoning, сопоставить показанные ARP-записи и сетевые кадры, а также обсудить предложенные защитные настройки. Полный MITM-путь и сравнительная эффективность защиты на трёх платформах не проверяются по имеющимся фрагментам.

### **Литературный обзор**

Для начала необходимо определить ключевые термины и их значения.

ARP (Address Resolution Protocol) — протокол определения аппаратного адреса (MAC) по известному IPv4-адресу в пределах соответствующего канального сегмента. Отправитель может направить ARP-запрос и использовать полученный ответ для внесения соответствия IP –MAC в локальную таблицу.

ARP-таблица – таблица соответствия IP и MAC адресов, используемая протоколом ARP.

Spoofing — подмена сведений об источнике или другом участнике сетевого взаимодействия с целью выдать один объект за другой.

ARP Spoofing – техника, используемая в компьютерных сетях для перехвата и манипуляции сетевым трафиком, которая заключается в отправке фальшивых ARP-сообщений для изменения сопоставления адресов и нарушения тем самым нормальной коммуникации в сети [5].

На основе анализа литературы можно сформулировать гипотезы исследования:

1. H1: В описанном сценарии наблюдаемое соответствие IP–MAC в ARP-таблице может измениться после операции ARP-poisoning. Эта гипотеза касается показанного примера и не устанавливает уязвимость всех стандартных конфигураций вендоров.
2. H2: Показанные команды, ARP-записи и пакеты могут использоваться для учебного разбора различия между настройкой атаки и доказательством её результата. Образовательная эффективность такого разбора отдельно не измеряется.

### **Материалы и методы**

Исследование представляет собой экспериментальный разбор конкретного учебного стенда.

Характеристики выборки: в качестве исследуемой выборки выступает сегмент локальной сети Ethernet на базе коммутаторов различных вендоров.

Узел 1 (жертва) – компьютер с ОС Windows (PC1).

Узел 2 (жертва) – компьютер с ОС Windows (PC2).

Узел 3 (атакующий) – компьютер с операционной системой Kali Linux [6].

Материалы для анализа — показанные настройки, вывод `arp -a` и `ping`, а также кадры Wireshark. Данные о статистике коммутаторов и повторных испытаниях защитных настроек в представленных результатах отсутствуют.

Описание процедуры: на одном узле выполняется проверка связности с помощью `ping`; на лабораторном узле Kali Linux применяется Ettercap для выполнения ARP-poisoning. В дальнейшем сопоставляются выводы ARP-таблиц и сетевые кадры, записанные анализатором Wireshark.

Эксперимент включает подготовку коммутаторов, фиксацию исходных ARP-соответствий, проведение ARP-poisoning и анализ наблюдаемых изменений. Защитные конфигурации рассматриваются отдельно; повторная атака после их применения не документирована.

Анализ ограничен сопоставлением показанных IP–MAC-соответствий и описанием сетевых кадров. Конфигурации вендоров обсуждаются качественно; количественная оценка перехвата или сравнительной результативности защиты не проводится.

### **Ход исследования**

Настройка стенда выполнялась отдельно для этапов с разными коммутаторами. На схеме (рис. 1) приведены два Windows-узла и узел Kali Linux, соединённые через испытываемое

коммутирующее оборудование. Приведённые ниже команды и сообщения об ошибках сохранены как записи лабораторного выполнения.

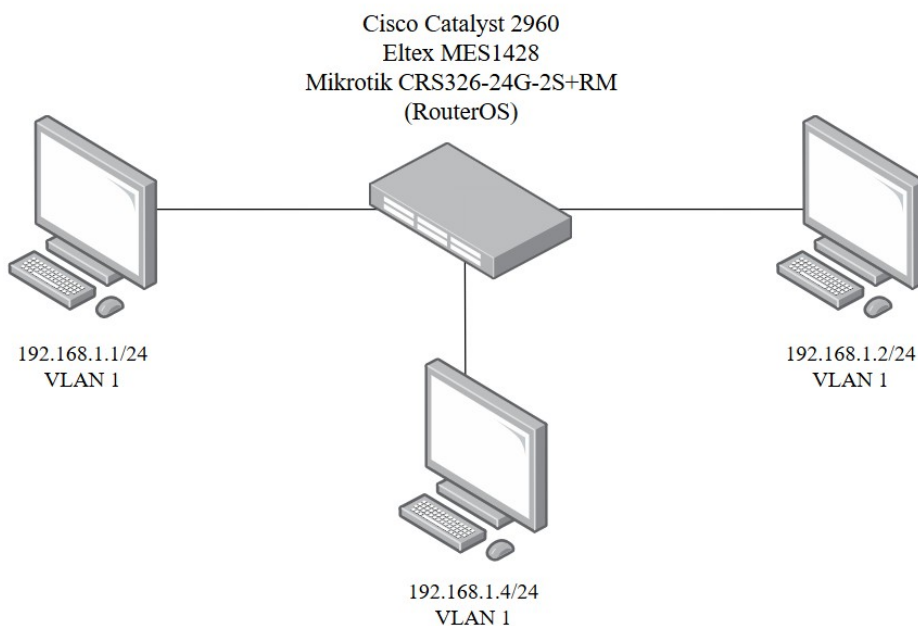


**Рис. 1. Лабораторная топология с двумя узлами Windows, узлом Kali Linux и испытываемым коммутатором**

Начнём с настройки коммутатора Cisco Catalyst 2960.

#### **Листинг 1 – Настройка портов Cisco Catalyst 2960**

```
Switch>en
Switch#conf
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int fa0/13
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int fa0/23
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#show vlan
```

Теперь настроим коммутатор Eltex MES1428.

#### **Листинг 2 – Фрагмент настройки Eltex MES1428 по описанию исходного стенда**

```
console#int fa0/1
% Invalid Command
console#conf t
console(config)#int fa0/1
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
console(config)#int fa0/17
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
console(config)#int fa0/23
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
```

```
console(config)#exit
console#show ip int brief
show ip int brief
^
% Invalid input detected at '^' marker
console#
```

Затем настроим коммутатор MikroTik CRS326-24G-2S+RM.

### Листинг 3 – Настройка bridge и VLAN в MikroTik RouterOS

```
[admin@MikroTik] > /int br port add interface=ether1 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br port add interface=ether18 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br port add interface=ether23 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br vlan add bridge=test untagged=ether1,ether18,ether23
vlan-ids=1
[admin@MikroTik] > /int br port set [find interface=ether1] pvid=1
[admin@MikroTik] > /int br port set [find interface=ether18] pvid=1
[admin@MikroTik] > /int br port set [find interface=ether23] pvid=1
[admin@MikroTik] > /int bridge set test vlan-filtering=yes
[admin@MikroTik] >
```

Для демонстрации ARP Spoofing используется Ettercap. Параллельно выполняется захват ARP- и ICMP-трафика в Wireshark, позволяющий сопоставить сетевые кадры с изменениями записей ARP-таблицы. Наблюдение пакетов на атакующем узле не является самостоятельным доказательством перенаправления всего обмена через него.

После подготовки сетевой конфигурации в Ettercap проводится поиск узлов лабораторного сегмента. Программа отображает найденные IP- и MAC-адреса, после чего выбираются цели для учебного сценария.

На следующем этапе запускается ARP-poisoning: узел атакующего отправляет поддельные ARP-ответы с соответствиями IP- и MAC-адресов. Для оценки результата далее используются зафиксированные ARP-таблицы и захваченные сетевые пакеты.

В Ettercap выбраны цель 1 с адресом 192.168.1.1 и цель 2 с адресом 192.168.1.2. После включения ARP-poisoning выполняется захват трафика на машине атакующего; показанные кадры рассматриваются вместе с изменениями ARP-таблицы.

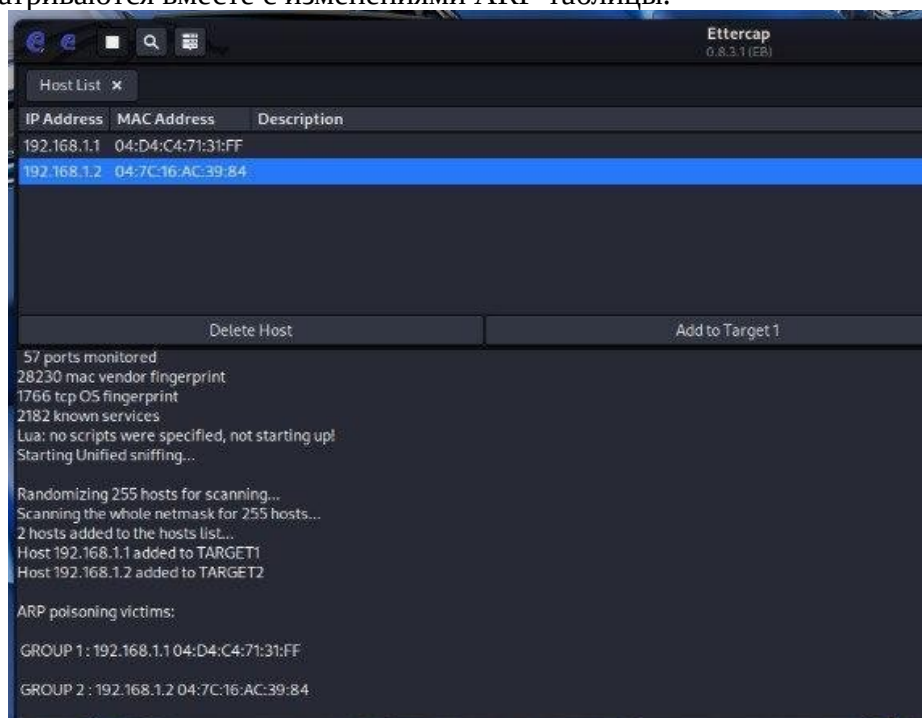


Рис. 2. Выбор целей ARP-poisoning в интерфейсе Ettercap

|    |           |             |             |      |                                                   |                                                         |
|----|-----------|-------------|-------------|------|---------------------------------------------------|---------------------------------------------------------|
| 25 | 11.174761 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1648/28678, ttl=128 (no response found!) |
| 26 | 11.175146 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1648/28678, ttl=128 (reply in 27)        |
| 27 | 11.177848 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1648/28678, ttl=64 (request in 26)       |
| 28 | 11.182647 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1648/28678, ttl=64                       |
| 29 | 12.192294 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1649/28934, ttl=128 (no response found!) |
| 30 | 12.193783 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1649/28934, ttl=128 (reply in 31)        |
| 31 | 12.196408 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1649/28934, ttl=64 (request in 30)       |
| 32 | 12.203743 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1649/28934, ttl=64                       |
| 33 | 40.661172 | 192.168.1.2 | 192.168.1.1 | ICMP | 42 Echo (ping) request                            | id=0x7ee7, seq=32487/59262, ttl=64 (no response found!) |
| 34 | 40.666908 | 192.168.1.1 | 192.168.1.2 | ICMP | 42 Echo (ping) request                            | id=0x7ee7, seq=32487/59262, ttl=64 (no response found!) |
| 35 | 40.670105 | 192.168.1.1 | 192.168.1.2 | ICMP | 70 Destination unreachable (Protocol unreachable) |                                                         |
| 36 | 40.678853 | 192.168.1.1 | 192.168.1.2 | ICMP | 70 Destination unreachable (Protocol unreachable) |                                                         |
| 37 | 41.291279 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1664/32774, ttl=128 (no response found!) |
| 38 | 41.293693 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1664/32774, ttl=128 (reply in 39)        |
| 39 | 41.296931 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1664/32774, ttl=64 (request in 38)       |
| 40 | 41.301948 | 192.168.1.2 | 192.168.1.1 | ICMP | 74 Echo (ping) reply                              | id=0x0001, seq=1664/32774, ttl=64                       |
| 41 | 42.299362 | 192.168.1.1 | 192.168.1.2 | ICMP | 74 Echo (ping) request                            | id=0x0001, seq=1665/33030, ttl=128 (no response found!) |

**Рис. 3. Фрагмент захвата ICMP-трафика в Wireshark на атакующем узле**

В показанном ICMP-захвате видны запросы и ответы между 192.168.1.1 и 192.168.1.2, а также сообщения Destination unreachable. Авторы отмечают интервал 28,5 с между кадрами 32 и 33 и изменение интервалов между запросами с 0,000385 до 0,002414 с. Эти значения описывают показанный фрагмент; они не определяют момент отравления ARP-таблицы, не устанавливают причину задержки и сами по себе не доказывают полную MITM-цепочку. Для оценки подмены отдельно сопоставляются видимые ARP-записи до и после операции.

В показанном выводе arp -а интерфейс имеет адрес 192.168.1.1. До операции запись для 192.168.1.2 содержит MAC 04-7c-16-ac-39-84, а запись для 192.168.1.4 — 08-00-27-85-e9-78. В следующем фрагменте для 192.168.1.2 указан 08-00-27-85-e9-78; тип записи — динамический. Это наблюдение фиксирует изменение соответствия IP–MAC в данном примере, но не описывает все этапы или причины обновления таблицы.

#### Листинг 4 – Вывод arp -а до атаки

```
C:\Users\User>arp -a
Интерфейс: 192.168.1.1 --- 0x2
    адрес в Интернете      Физический адрес      Тип
    192.168.1.2            04-7c-16-ac-39-84     динамический
    192.168.1.4            08-00-27-85-e9-78     динамический
```

#### Листинг 5 – Фрагмент вывода arp -а после атаки (нижняя часть снимка обрезана)

```
C:\Users\User>arp -a
Интерфейс: 192.168.1.1 --- 0x2
    адрес в Интернете      Физический адрес      Тип
    192.168.1.2            08-00-27-85-e9-78     динамический
```

#### Листинг 6 – Фрагмент вывода ping во время атаки

```
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=14мс TTL=64
```

На машине, выполнявшей операцию ARP-poisoning, показан дополнительный захват сетевых пакетов. Его содержимое иллюстрирует доступный анализатору трафик в данном стенде.

| Host                      | Port  | Host            | Port | Proto | State   | Tx Bytes | Rx Bytes | Countries |
|---------------------------|-------|-----------------|------|-------|---------|----------|----------|-----------|
| 192.168.1.1               | 58610 | 77.88.8.1       | 53   | UDP   | active  | 27       | 0        | --> RU    |
| 192.168.1.1               | 53997 | 77.88.8.1       | 53   | UDP   | active  | 27       | 0        | --> RU    |
| 192.168.1.1               | 51670 | 77.88.8.1       | 53   | UDP   | active  | 27       | 0        | --> RU    |
| 192.168.1.1               | 60368 | 77.88.8.8       | 53   | UDP   | idle    | 40       | 0        | --> RU    |
| 192.168.1.1               | 57965 | 77.88.8.8       | 53   | UDP   | idle    | 40       | 0        | --> RU    |
| 192.168.1.1               | 54350 | 77.88.8.8       | 53   | UDP   | idle    | 40       | 0        | --> RU    |
| fe80::c7ec:3f70:4337:8240 | 0     | ff02::16        | 0    |       | idle    | 0        | 0        | --> --    |
| 192.168.1.1               | 54744 | 239.255.255.250 | 1900 | UDP   | idle    | 137      | 0        | --> --    |
| 192.168.1.1               | 61284 | 77.88.8.8       | 53   | UDP   | idle    | 40       | 0        | --> RU    |
| 192.168.1.1               | 61645 | 77.88.8.8       | 53   | UDP   | idle    | 40       | 0        | --> RU    |
| 192.168.1.1               | 53975 | 8.8.8.8         | 53   | UDP   | idle    | 28       | 0        | --> US    |
| 192.168.1.1               | 5353  | 224.0.0.251     | 5353 | UDP   | active  | 552      | 0        | --> --    |
| fe80::c7ec:3f70:4337:8240 | 5353  | ff02::1b        | 5353 | UDP   | active  | 116      | 0        | --> --    |
| 192.168.1.1               | 55957 | 239.255.255.250 | 1900 | UDP   | active  | 274      | 0        | --> --    |
| 192.168.1.1               | 64319 | 213.180.204.127 | 443  | TCP   | opening | 0        | 0        | --> RU    |
| 192.168.1.1               | 56560 | 8.8.4.4         | 53   | UDP   | active  | 28       | 0        | --> US    |
| 192.168.1.1               | 64320 | 20.189.173.8    | 443  | TCP   | opening | 0        | 0        | --> US    |
| 192.168.1.1               | 53643 | 77.88.8.8       | 53   | UDP   | active  | 41       | 0        | --> RU    |
| 192.168.1.1               | 59960 | 77.88.8.8       | 53   | UDP   | active  | 41       | 0        | --> RU    |
| 192.168.1.1               | 57671 | 77.88.8.8       | 53   | UDP   | active  | 43       | 0        | --> RU    |
| 192.168.1.1               | 60871 | 77.88.8.8       | 53   | UDP   | active  | 43       | 0        | --> RU    |

Рис. 4. Дополнительный захват сетевого трафика на лабораторном узле

В показанном фрагменте присутствуют обращения к адресам 77.88.8.1 и 77.88.8.8 на порту 53, а также mDNS 224.0.0.251:5353 и LLMNR 224.0.0.252:5353. Видны и другие адреса, включая 8.8.4.4 и 20.189.173.8. Наличие таких пакетов описывает наблюдаемый обмен; подмена DNS-ответов, mDNS или LLMNR в работе отдельно не демонстрировалась.

Следует различать наблюдение пакетов и доступ к их прикладному содержимому. Перенаправление трафика само по себе не доказывает возможность чтения или изменения зашифрованного сеанса. В этой работе не представлены ключи TLS, расшифровка Application Data или испытание вмешательства в HTTPS; вывод об успешной компрометации такого содержимого не делается.

#### Реализация механизмов защиты

Методы защиты от атаки ARP-spoofing на устройствах трех выбранных вендоров:

1. Для Cisco в статье приведена конфигурация с DHCP Snooping и Dynamic ARP Inspection (DAI) в VLAN 1: uplink-порт FastEthernet0/1 помечается как trusted, пользовательские порты FastEthernet0/2–24 — как недоверенные. Также указано отключение DTP на портах. Эти настройки описывают предполагаемую защитную конфигурацию; их действие в повторном испытании атаки в статье не подтверждено.
2. Для Eltex в статье приведена конфигурация DHCP Snooping и Dynamic ARP Inspection в VLAN 1: uplink-интерфейс FastEthernet0/1 задаётся как trusted, пользовательские порты FastEthernet0/2–24 — как недоверенные, с параметром ip verify source port-security. Описание указывает назначение этих настроек для проверки соответствий IP–MAC, но не демонстрирует их результативность в повторном испытании.
3. Для MikroTik статья предлагает статические ARP-записи либо режим arp=reply-only как альтернативу классическим DHCP Snooping и DAI. Такая конфигурация ограничивает разрешённые соответствия IP–MAC заданными значениями; её способность предотвращать ARP Spoofing в данном стенде отдельно не подтверждена повторным тестом.

Для корректной работы механизмов защиты от ARP Spoofing на управляемых коммутаторах (в частности, Dynamic ARP Inspection) необходимо наличие доверенной базы соответствий IP–MAC–порт. Данная база автоматически формируется механизмом DHCP Snooping на основе легитимных DHCP-транзакций. В эксперименте DHCP-сервер логически размещается на маршрутизаторе.

**Таблица 1 – Сопоставление приведённых настроек защиты на оборудовании Cisco, Eltex и MikroTik**

| Действие                                                        | Cisco Catalyst 2960                                                                                                                            | Eltex MES1428                                                                                                             | MikroTik CRS326                                                                                                                                                                     |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Переход в режим конфигурации                                    | conf t                                                                                                                                         | conf t                                                                                                                    | –                                                                                                                                                                                   |
| Создание бриджового интерфейса                                  | –                                                                                                                                              | –                                                                                                                         | interface bridge add name=test<br>vlan-filtering=no                                                                                                                                 |
| Добавление портов в мост                                        | –                                                                                                                                              | –                                                                                                                         | interface bridge port add<br>bridge=test interface=ether1<br>interface bridge port add<br>bridge=test interface=ether2<br>interface bridge port add<br>bridge=test interface=ether3 |
| Включение DHCP Snooping                                         | ip dhcp snooping<br>ip dhcp snooping vlan 1                                                                                                    | dhcp snooping enable<br>dhcp snooping vlan 1                                                                              | –                                                                                                                                                                                   |
| Включение Dynamic ARP Inspection и защита от подделки MAC в ARP | ip arp inspection vlan 1<br>ip arp inspection validate<br>src-mac                                                                              | arp inspection enable<br>arp inspection vlan 1                                                                            | –                                                                                                                                                                                   |
| Настройка доверенного порта DHCP-сервера                        | int fa0/1<br>switchport mode access<br>switchport access vlan 1<br>switchport nonegotiate<br>ip dhcp snooping trust<br>ip arp inspection trust | int fa0/1<br>switchport mode access<br>switchport access vlan 1<br>port-security-state<br>trusted<br>set port-role uplink | –                                                                                                                                                                                   |
| Настройка пользовательских портов                               | int range fa0/2 - 24<br>switchport mode access<br>switchport access vlan 1<br>switchport nonegotiate                                           | int range fa0/2- 24<br>switchport mode access<br>switchport access vlan 1<br>ip verify source port-<br>security           | –                                                                                                                                                                                   |
| Фильтрация ARP-трафика                                          | –                                                                                                                                              | –                                                                                                                         | /interface bridge<br>set test arp=reply-only vlan-<br>filtering=yes                                                                                                                 |
| Добавление статических ARP-записей                              | –                                                                                                                                              | –                                                                                                                         | /ip arp<br>add address=192.168.1.1 mac-<br>address=AA:AA:AA:AA:AA:A<br>A interface=test<br>add address=192.168.1.2 mac-<br>address=BB:BB:BB:BB:BB:BB<br>interface=test              |

В статье приведены настройки защиты для Cisco и Eltex (DHCP Snooping и Dynamic ARP Inspection) и для MikroTik (режим arp=reply-only). Представленные материалы не содержат документированного повторного испытания атаки после включения этих настроек; поэтому по ним нельзя заключить, что ложные ARP-ответы были заблокированы на всех трёх устройствах.

Для оценки результата после настройки требуются повторный захват трафика и проверка ARP-таблиц в тех же условиях, что и при исходной атаке. Представленные донастроечные наблюдения ICMP и ARP не подтверждают отсутствие перехвата после включения защитных механизмов.

### Результаты исследования

В ходе ARP-poisoning узел атакующего отправлял ложные ARP-сообщения, предназначенные для изменения соответствий адресов у других участников сегмента. В приведённых выводах действительно меняется IP–MAC-сопоставление для адреса 192.168.1.2. Однако материалы не показывают полного пути пересылки трафика между двумя узлами через устройство атакующего; поэтому утверждать успешный перехват всего обмена нельзя.

Авторы интерпретируют лабораторный сценарий как ARP-poisoning. Непосредственно показаны изменение соответствия IP–MAC и отдельные сетевые кадры; эти фрагменты не устанавливают полный путь перехвата между двумя узлами через машину атакующего. Наблюдения относятся к указанному стенду.

Для снижения риска ARP Spoofing в сетях применяют статические ARP-записи на критичных узлах и сегментацию VLAN. Шифрование прикладного трафика (например, HTTPS, VPN или IPsec) может защищать его содержимое при перехвате, но не скрывает все сетевые метаданные и не заменяет проверку конфигурации L2-защиты.

На управляемых коммутаторах могут совместно применяться DHCP Snooping, Dynamic ARP Inspection, IP Source Guard и Port Security. Эти механизмы проверяют разные свойства трафика и конфигурации портов; фактический эффект зависит от корректной настройки доверенных интерфейсов и привязок IP–MAC. Представленное в статье описание не является результатом сравнительного испытания их эффективности и не доказывает полное предотвращение атак.

Ниже приведено качественное обсуждение настройки, а не измеренные результаты повторного испытания защиты:

1. Трудоёмкость настройки обсуждается через состав операций: для Cisco/Eltex — параметры DAI и trusted-портов, для приведённого варианта MikroTik — ручное задание ARP-записей. Время настройки и частота ошибок в работе не измерялись.
2. Масштабирование обсуждается как свойство выбранных способов настройки: динамическая база DHCP и статические соответствия требуют разных процедур сопровождения. Сравнительное нагрузочное испытание и количественная оценка масштабируемости не выполнялись.
3. Риски ошибок конфигурации: для Cisco/Eltex критической ошибкой является назначение пользовательского порта как trusted, что полностью отключает проверку DAI. Для MikroTik риск заключается в блокировке легитимного трафика при замене сетевой карты или устройства без обновления статической ARP-записи.

В статье отмечено, что в исследованной конфигурации MikroTik не использовались классические DHCP Snooping и Dynamic ARP Inspection; в качестве альтернативы приведены статические ARP-записи. Такой подход требует ручного обновления при изменении адресов или устройств и в статье не сравнивался экспериментально с механизмами Cisco и Eltex.

### **Заключение**

Работа описывает лабораторный сценарий с Ettercap и сохраняет фрагменты настройки, ARP-таблиц, ping и Wireshark. В одном показанном примере изменилось соответствие IP–MAC. По доступным фрагментам нельзя подтвердить полный MITM-путь или одинаковое поведение базовых конфигураций всех трёх платформ.

Соотношение наблюдений с поставленными гипотезами:

1. Гипотеза H1 иллюстрируется изменением ARP-записи в показанном примере. Она не означает подтверждённый перехват всего обмена и не проверяет все настройки Cisco, Eltex и MikroTik. DHCP Snooping, Dynamic ARP Inspection, статические ARP-записи и arp=reply-only рассмотрены как предложенные настройки; их результативность после включения не испытана в представленных материалах.
2. Гипотеза H2 задаёт учебное применение показанных команд и наблюдений. Эти материалы позволяют обсуждать границы доказательств ARP-poisoning, но результативность обучения и воспроизводимость на других моделях отдельно не оценивались.

Дальнейшая работа может включать согласованный захват ARP и трафика обоих узлов, повторную атаку после защитных настроек и проверку других моделей. Такие испытания не включены в результаты текущего описания.

Практический результат — ограниченный лабораторный пример изменения ARP-соответствия и набор предложенных конфигураций. Выводы не подтверждают универсальную

уязвимость базовых сетей, полную MITM-цепочку или эффективность перечисленных защитных мер.

### Библиографический список

1. Conti M., Dragoni N., Lesyk V. A Survey of Man In The Middle Attacks // *IEEE Communications Surveys & Tutorials*. – 2016. – Vol. 18, no. 3. – P. 2027-2051.
2. Крылов Александр Юрьевич, Шитов Николай Андреевич, Галиаскаров Эдуард Геннадьевич Применение объектного подхода при создании распределенной системы выявления и предотвращения атаки типа ARP-spoofing // *Объектные системы*. 2010. №2 (2). URL: <https://cyberleninka.ru/article/n/primenenie-obektnogo-podhoda-pri-sozdanii-raspredelennoy-sistemy-vyyavleniya-i-predotvrascheniya-ataki-tipa-arp-spoofing> (дата обращения: 14.11.2025).
3. Шишов Н. В., Ломазов В. А. МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРИ ВОЗДЕЙСТВИИ ARP-SPOOFING АТАК // *ИВД*. 2022. №2 (86). URL: <https://cyberleninka.ru/article/n/modelirovanie-protsessov-funktsionirovaniya-sistemy-elektronnogo-dokumentooborota-pri-vozddeystvii-arp-spoofing-atak> (дата обращения: 12.11.2025).
4. Алиев Р. М. РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ АТАК ТИПА ARP-SPOOFING // *Шаг в науку*. 2019. №2. URL: <https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing> (дата обращения: 14.11.2025).
5. 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. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/135231.html> (дата обращения: 25.09.2025)
6. Kali Linux and Man-in-the-Middle Attacks: Empowering Ethical Hackers // *Cyber Pratibha* URL: <https://cyberpratibha.com/kali-linux-man-in-the-middle-attack-tutorial/?amp=1> (дата обращения: 25.09.2025).
7. ARP-спуфинг в Ettercap // *LabEx* URL: <https://labex.io/ru/tutorials/nmap-spoof-arp-in-ettercap-549950> (дата обращения: 24.09.2025).
8. Ettercap: руководство по MITM-атакам в локальной сети // *Хабр* URL: <https://habr.com/ru/articles/934772/> (дата обращения: 27.09.2025).

### References

9. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027–2051.
10. Krylov, A. Yu., Shitov, N. A., & Galiasgarov, E. G. (2010). Primenenie obektnogo podkhoda pri sozdanii raspredelennoi sistemy vyyavleniya i predotvrashcheniya ataki tipa ARP-spoofing [Application of the object-oriented approach in creating a distributed system for detecting and preventing ARP-spoofing attacks]. *Obektnye sistemy*, 2(2). <https://cyberleninka.ru/article/n/primenenie-obektnogo-podhoda-pri-sozdanii-raspredelennoy-sistemy-vyyavleniya-i-predotvrascheniya-ataki-tipa-arp-spoofing>
11. Shishov, N. V., & Lomazov, V. A. (2022). Modelirovanie protsessov funktsionirovaniya sistemy elektronnogo dokumentooborota pri vozddeystvii ARP-spoofing atak [Modeling of electronic document management system functioning processes under ARP-spoofing attacks]. *IVD*, 2(86). <https://cyberleninka.ru/article/n/modelirovanie-protsessov-funktsionirovaniya-sistemy-elektronnogo-dokumentooborota-pri-vozddeystvii-arp-spoofing-atak>
12. Aliev, R. M. (2019). Razrabotka metoda obnaruzheniya atak tipa ARP-spoofing [Development of a method for detecting ARP-spoofing attacks]. *Shag v nauku*, 2. <https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing>
13. Uymin, A. G. (2024). *Kompyuternye seti. L2-tekhnologii: Praktikum dlya SPO* [Computer networks: L2 technologies. A practical guide for secondary vocational education]. Profobrazovanie; IPR Media. <https://www.iprbookshop.ru/135231.html>

14. Kali Linux and man-in-the-middle attacks: Empowering ethical hackers. (n.d.). Cyber Pratibha. <https://cyberpratibha.com/kali-linux-man-in-the-middle-attack-tutorial/?amp=1>
15. ARP-spoofing in Ettercap. (n.d.). LabEx. <https://labex.io/ru/tutorials/nmap-spoof-arp-in-ettercap-549950>
16. Ettercap: rukovodstvo po MITM-atakam v lokalnoi seti [Ettercap: A guide to MITM attacks in a local network]. (n.d.). Habr. <https://habr.com/ru/articles/934772/>

#### Информация об авторах

Бережная Полина Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: palinaberezhnaya047@gmail.com.

Мирчевски Кристина Далиборовна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: mirchevski23@gmail.com.

### STUDYING THE ARP SPOOFING ATTACK USING SWITCHES FROM DIFFERENT VENDORS AS EXAMPLES

**Berezhnaya P. A., Mirchevski K. D.**

*Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia*

**Abstract.** This paper examines the susceptibility of a switched local network to ARP spoofing and describes a laboratory ARP-spoofing scenario using Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326-24G-2S+RM switches. The topology included two Windows victim hosts and an attacking host running Kali Linux. Ettercap was used to conduct the attack, while Wireshark was used to analyze network traffic; ARP tables and ICMP ping were used to record changes. In the described scenario, the attacker sent forged ARP replies associating its MAC address with the addresses of the gateway and target host. The capture shows requests and responses between the hosts, but does not establish their full path through the attacking machine; ARP tables before and after the attack showed a changed IP-to-MAC mapping. The paper also describes protection configurations for Cisco and Eltex using DHCP Snooping and Dynamic ARP Inspection, and static ARP entries for MikroTik. The observations record an ARP mapping change in this example and illustrate ARP-table and packet analysis in network-security training. It does not constitute an exhaustive test of every model, firmware version, or configuration from the named vendors. Conclusions about default configurations therefore apply only to the described testbed; other configurations require separate testing. The procedure distinguishes the authors' attack description from observed ARP records and frames; these fragments do not establish a complete MITM chain. The manuscript describes protection settings but provides no documented post-protection attack trial, so their effectiveness is not established by the reported results.

**Keywords:** ARP spoofing, ARP table, MAC-address, network security, information security, switch, network traffic.

#### Information about the authors

Berezhnaya Polina Aleksandrovna — third-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: palinaberezhnaya047@gmail.com.

Mirchevski Kristina Daliborovna — third-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: mirchevski23@gmail.com.

**Дворников Д. С., Костионова М. А.**

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

## **ВЕРИФИКАЦИЯ МЕХАНИЗМОВ УСТОЙЧИВОСТИ ДОМЕННЫХ GPO В КОРПОРАТИВНОЙ СЕТИ**

**Аннотация.** В статье разобрано применение одного пользовательского параметра `DisableTaskMgr` в лабораторной доменной среде Windows Active Directory. Стенд включает контроллер домена Windows Server 2022 и клиентскую машину Windows 11. Цель работы состоит в сопоставлении значения реестра и поведения диспетчера задач после применения доменной GPO, локальных изменений и отключения связи с контроллером домена. Политика привязана к заданной организационной единице; проверяется конкретная учётная запись пользователя. Представлены команды обновления политики, сведения о её применении и попытки изменения контролируемого значения. Рассмотрены действия обычного пользователя и локального администратора, а также активная сессия без сети и вход с кэшированными учётными данными после перезагрузки. В показанных сценариях доменное ограничение применялось, а после локального изменения администратором восстанавливалось при штатном обновлении политики. При отсутствии сети ранее применённое значение сохранялось; попытка обычного пользователя записать другое значение завершилась отказом доступа. Дескрипторы безопасности реестра и внутренний механизм сохранения значения отдельно не исследовались. Сценарии Block Inheritance и Enforced, все этапы модели LSDOU и другие способы обхода GPO не проверялись. Результаты ограничены одним параметром, выбранной OU, привязанной политикой и указанной конфигурацией. Материал может использоваться как учебный пример применения и восстановления доменной настройки. Он показывает необходимость различать наблюдаемое поведение отдельного параметра и общую оценку устойчивости централизованного управления. Выводы не характеризуют все версии Windows, доменные архитектуры или условия физического доступа.

**Ключевые слова:** Windows, Active Directory, GPO, групповые политики, LSDOU, информационная безопасность, доменная инфраструктура.

### **Введение**

В современных корпоративных сетях управление конфигурацией рабочих станций и серверов является фундаментальной задачей системных администраторов. Групповые политики Windows (Group Policy Objects, GPO) представляют собой мощный инструмент централизованного управления настройками операционной системы, приложений и параметров безопасности в среде Microsoft Active Directory. С их помощью администраторы устанавливают единые требования к парольной политике, настройкам брандмауэра, параметрам аудита и ограничениям для пользователей.

Иерархическая модель применения GPO (LSDOU: Local — Site — Domain — Organizational Unit) позволяет задавать настройки на нескольких уровнях. При совпадении параметров возможны конфликты, которые разрешаются правилами обработки политик. Механизмы Enforced и Block Inheritance дополнительно изменяют наследование и требуют проверки результирующего набора настроек; сами по себе они не являются способами обхода ограничений.

Проблематика обхода групповых политик исследуется специалистами по информационной безопасности в контексте атак на инфраструктуру Active Directory. В частности, актуальным остаётся вопрос о практической возможности локального переопределения доменных политик с использованием инструментов Windows, как со стороны обычного пользователя, так и со стороны локального администратора клиентской машины.

Объект исследования — механизм применения объектов групповой политики в инфраструктуре Windows Active Directory.

Предмет исследования — изменение одного параметра `DisableTaskMgr` при применении доменной GPO, локальном вмешательстве и отсутствии связи с контроллером домена.

Цель исследования — описать применение и восстановление `DisableTaskMgr` в одном доменном стенде Windows Server 2022 и Windows 11. Исследование не охватывает все параметры GPO или способы обхода политик.

### **Литературный обзор**

Модель обработки и приоритизации GPO детально описана в профессиональной литературе. Krause указывает, что политики применяются в строгой последовательности LSDOU, при этом каждый последующий уровень иерархии — Domain, затем Organizational Unit — перекрывает настройки предыдущего уровня в случае конфликта параметров [1]. Данная модель предполагает, что параметры, заданные в GPO уровня домена, в случае конфликта перекрывают параметры локальной политики, а параметры GPO подразделения (OU) перекрывают доменные.

Порядок применения групповых политик и особенности диагностики описаны в специализированной литературе [2]. Для проверки того, какие объекты были применены к конкретному пользователю и компьютеру, используются gpresult и RSoP. Приоритет результирующей настройки зависит от области действия GPO, порядка обработки и параметров наследования.

Портал Инфратех в обзорном руководстве по доменным политикам отмечает, что локальные объекты групповой политики (LGPO) разделены на несколько уровней — для локального компьютера, для всех пользователей и для конкретных учётных записей, — что значительно усложняет анализ итогового результирующего набора политик [3]. На основании проведённого анализа и практического моделирования были сформулированы следующие исследовательские гипотезы:

H1: В заданной OU/GPO доменное значение DisableTaskMgr применяется к проверенной учётной записи при обновлении политики.

H2: Обычная пользовательская учётная запись не может устойчиво изменить проверенный параметр при регулярном обновлении доменной политики.

H3: Локальный администратор может временно изменить DisableTaskMgr в HKU\SID; при следующем штатном обновлении GPO доменное значение восстанавливается.

H4: В проверенной пользовательской сессии без связи с контроллером домена и после кэшированного входа сохранится ранее применённое значение DisableTaskMgr.

Внутренний механизм сохранения значения отдельно не проверяется.

### **Материалы и методы**

Работа представляет прикладной лабораторный разбор одного параметра GPO. Описываются штатное применение доменной настройки, попытки локального изменения обычным пользователем и администратором, а также наблюдение без связи с контроллером домена.

Характеристика тестовой среды: в качестве программной платформы использовались Windows Server 2022 (в роли контроллера домена) и Windows 11 с актуальными обновлениями (в роли клиентской рабочей станции). В инфраструктуре были задействованы службы Active Directory Domain Services и DNS. Для проведения экспериментов была создана тестовая организационная единица (OU) и стандартная доменная учётная запись пользователя. Исследование проводилось в изолированной виртуальной среде.

Данные получены из показанных команд gpupdate, gpresult, обращений к реестру и поведения диспетчера задач. Отслеживается DisableTaskMgr в выбранной OU/GPO. Сценарии Block Inheritance, Enforced и полный анализ RSoP в представленных результатах не выполнены.

Описание процедуры проведения исследования: Исследование проводилось в лабораторной среде с развёрнутым доменом Active Directory и подключённой клиентской станцией. После проверки аутентификации была создана тестовая OU и доменная учётная запись пользователя, на которой оценивалось применение политик.

Затем создавался объект групповой политики с заданным пользовательским ограничением и привязывался к OU. После обновления конфигурации фиксировались групповые политики.

После локальных изменений повторно выполнялось обновление политики и проверялось значение DisableTaskMgr. Проверка ограничена выбранной учётной записью, привязанной GPO и показанными командами.

Дополнительно был проведён третий эксперимент, моделирующий сценарий атаки с использованием локальной учётной записи администратора клиентской машины. Для этого на клиентской рабочей станции была активирована встроенная локальная учётная запись администратора средствами командной строки. От её имени предпринималась попытка непосредственного изменения параметра реестра в профиле доменного пользователя через ветку HKU\SID. После внесения изменений выполнялась принудительная синхронизация политик, по результатам которой фиксировалось итоговое состояние контролируемого параметра.

В рамках четвёртого эксперимента был смоделирован сценарий потери клиентской машиной связи с контроллером домена. Сетевой адаптер клиентской рабочей станции был отключён средствами гипервизора при активной пользовательской сессии. В условиях отсутствия сетевого подключения проверялось текущее состояние контролируемого параметра, предпринималась попытка его изменения, после чего выполнялась перезагрузка машины с входом через кэшированные учётные данные. На каждом этапе фиксировалось состояние параметра реестра и фактическое поведение системы. После восстановления сетевого подключения выполнялась принудительная синхронизация политик и проводилась финальная проверка конфигурации.

Обработка данных — сопоставление показанного значения DisableTaskMgr и поведения диспетчера задач в четырёх выбранных сценариях. Таблица результатов отражает этот параметр и конфигурацию, а не полную верификацию модели LSDOU.

#### Ход исследования

После развертывания тестовой инфраструктуры и включения клиентской рабочей станции в домен была создана организационная единица и тестовая пользовательская учётная запись, на которой проводилась проверка настроек. На первом этапе была создана доменная групповая политика, задающая конкретное пользовательское ограничение. После её привязки к соответствующей OU на клиентской машине выполнялось принудительное обновление политик, затем фиксировались применённые GPO и фактическое состояние исследуемого параметра. Полученные результаты сопоставлялись с ожидаемой моделью приоритета в рамках LSDOU. Настройка объекта в оснастке управления показана на рис. 1.

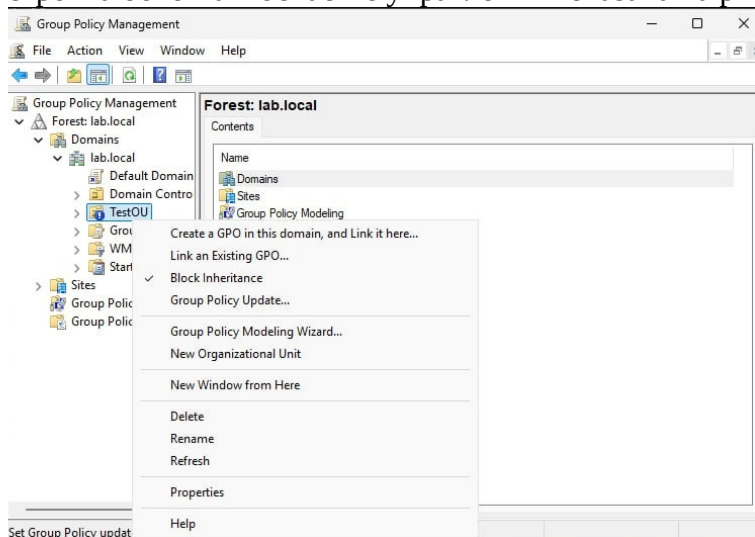


**Рис. 1. Выбор команды создания и привязки GPO в оснастке Group Policy Management**

После локальных изменений повторно инициировалось обновление GPO и проверялось значение DisableTaskMgr. Наблюдения позволяют сопоставить результаты конкретных попыток, но не доказывают устойчивость всех политик или невозможность других способов вмешательства. Значение параметра в редакторе реестра представлено на рис. 2.

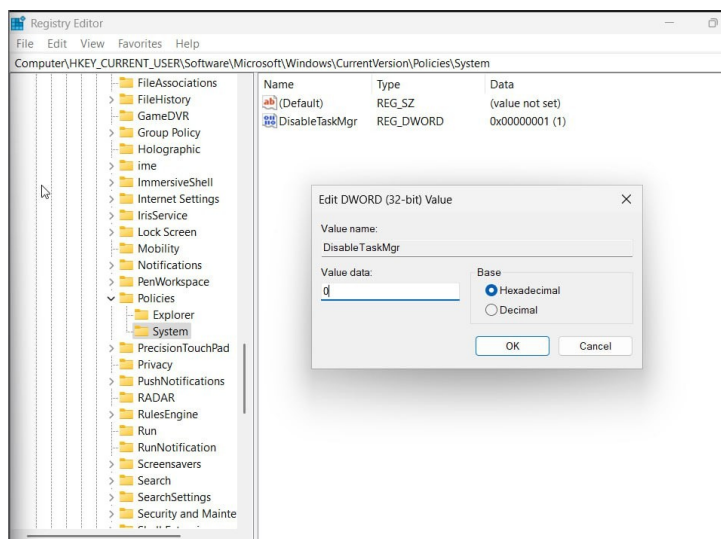


Рис. 2. Параметр DisableTaskMgr в редакторе реестра Windows

На третьем этапе был смоделирован сценарий, при котором потенциальный злоумышленник располагает правами локального администратора клиентской машины, однако не имеет привилегий в домене. Встроенная локальная учётная запись администратора была активирована штатными средствами Windows. После входа в систему под данной учётной записью был получен идентификатор безопасности (SID) доменной учётной записи testuser с помощью PowerShell, что позволило обратиться к ветке реестра HKU\SID, соответствующей профилю целевого пользователя. Попытка изменения параметра DisableTaskMgr с значения 1 на 0 завершилась успешно, и операция была выполнена без каких-либо ошибок доступа. После изменения параметра проверялся запуск диспетчера задач (рис. 3).

#### Листинг 1 – Получение SID и изменение параметра DisableTaskMgr в профиле пользователя

```
PS C:\WINDOWS\System32> (New-Object
System.Security.Principal.NTAccount('lab.local','testuser')).Translate([System.S
ecurity.Principal.SecurityIdentifier]).Value
S-1-5-21-2328540634-355861150-2537366535-1104
PS C:\WINDOWS\System32> reg query "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System"
DisableTaskMgr REG_DWORD 0x1
PS C:\WINDOWS\System32> reg add "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr /t REG_DWORD /d 0 /f
The operation completed successfully.
```

#### Листинг 2 – Проверка изменения параметра реестра

```
PS C:\WINDOWS\System32> reg query "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
HKEY_USERS\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System
DisableTaskMgr REG_DWORD 0x0
```

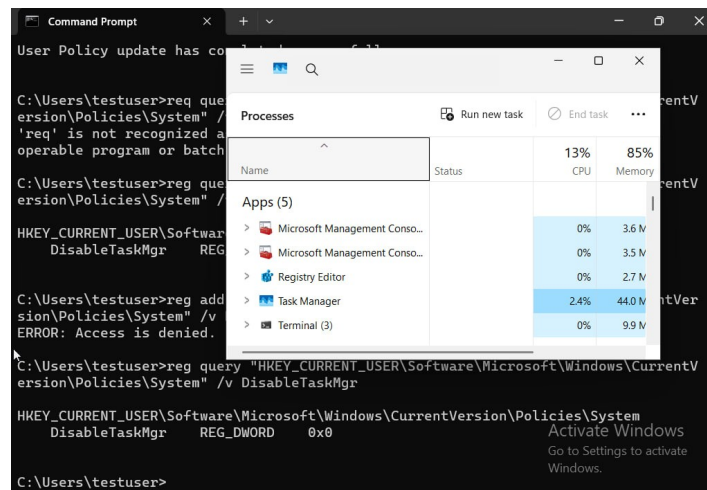


Рис. 3. Запуск диспетчера задач после локального изменения DisableTaskMgr

После этого сессия локального администратора была завершена, выполнен вход под учётной записью testuser и инициировано принудительное обновление групповых политик командой gpupdate /force. По результатам синхронизации значение параметра DisableTaskMgr вернулось к исходному значению 1, а диспетчер задач вновь оказался недоступен. Проверка через gpresult подтвердила, что политика Domain-GPO-Test присутствует в списке применённых объектов групповой политики.

#### Листинг 3 – Проверка восстановления параметра после gpupdate /force

```
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr    REG_DWORD    0x0
C:\Users\testuser> gpupdate /force
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr    REG_DWORD    0x1
Task Manager has been disabled by your administrator.
```

На четвёртом этапе был смоделирован сценарий, при котором клиентская машина теряет связь с контроллером домена — например, в случае отключения от корпоративной сети. Сетевой адаптер был отключён средствами гипервизора без завершения пользовательской сессии. Попытка принудительного обновления политик командой gpupdate /force завершилась ошибкой — контроллер домена оказался недоступен. Тем не менее проверка параметра реестра показала сохранение значения DisableTaskMgr = 1, а попытка его изменения от имени testuser завершилась ошибкой доступа — аналогично поведению системы в онлайн-режиме.

#### Листинг 4 – Ошибка обновления групповой политики без связи с контроллером домена

```
The processing of Group Policy failed because of lack of network connectivity to
a domain controller.
User Policy could not be updated successfully.
Task Manager has been disabled by your administrator.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr    REG_DWORD    0x1
```

После перезагрузки без сети выполнен вход с кэшированными учётными данными; DisableTaskMgr оставался равным 1 и диспетчер задач не запускался. Это наблюдение показывает сохранение ограничения в выбранном сценарии, но не устанавливает его внутреннюю причину или свойства ACL реестра. После восстановления сети Computer Policy и User Policy обновились успешно; значение подтверждено как 0x1.

#### Листинг 5 – Успешное обновление политик после восстановления связи

```
Ping statistics for 192.168.10.1: Packets: Sent = 3, Received = 3, Lost = 0 (0% loss).
C:\Users\testuser> gpupdate /force
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr      REG_DWORD      0x1
```

#### Результаты исследования

В листинге 6 показан результат применения доменной групповой политики к пользователю testuser. В окне командной строки отображается список применённых объектов групповой политики, среди которых указана политика Domain-GPO-Test. При попытке запуска диспетчера задач появляется сообщение о том, что он отключён администратором, что подтверждает корректное применение настроек политики.

#### Листинг 6 – Результат gresult для пользователя testuser

```
USER SETTINGS
Applied Group Policy Objects:
    Domain-GPO-Test
    Local Group Policy
Task Manager has been disabled by your administrator.
```

На рис. 4 показана попытка изменения DisableTaskMgr в разделе HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System. Операция завершается сообщением об отказе в записи. Это подтверждает невозможность изменения значения выбранной учётной записью в показанной конфигурации; дескриптор безопасности ключа и причина отказа отдельно не исследовались.

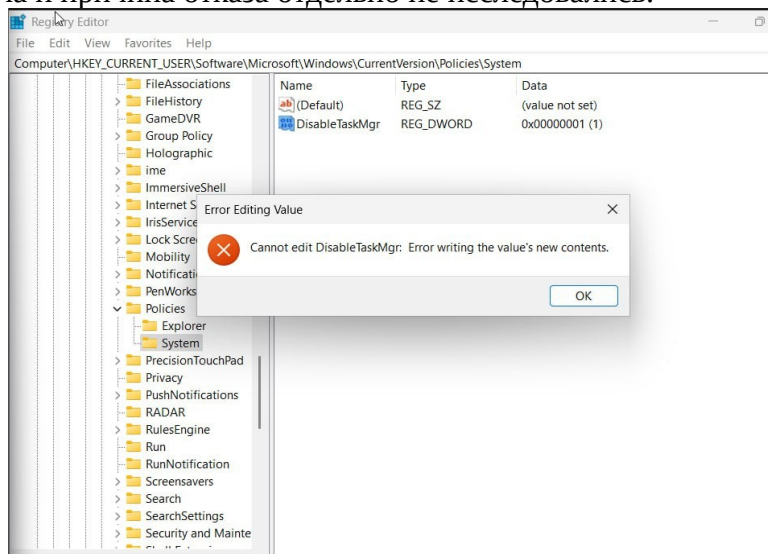


Рис. 4. Сообщение об отказе при попытке изменения DisableTaskMgr

Третий эксперимент показал, что локальная учётная запись администратора клиентской машины обладает достаточными правами для непосредственного изменения параметров реестра в профиле доменного пользователя. В отличие от попытки обычного пользователя, завершившейся ошибкой доступа, операция записи от имени локального администратора была выполнена успешно. Тем не менее данный обход носит временный характер, поскольку принудительное обновление групповой политики восстановило значение DisableTaskMgr (см. листинг 3).

В четвёртом сценарии значение DisableTaskMgr сохранялось как в активной пользовательской сессии без сети, так и после перезагрузки с кэшированным входом. Попытка записи от имени обычного пользователя завершилась отказом доступа. Это наблюдение относится к испытанной конфигурации и не подтверждает устойчивость ко всем способам локального вмешательства. Результаты четырёх экспериментов обобщены в табл. 1.

**Таблица 1 – Результаты проверки доменной GPO в четырёх сценариях**

| № | Цель эксперимента               | Действия                                                            | Наблюдаемый результат                                                 | Вывод                                                                                      |
|---|---------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1 | Применение доменной GPO         | Привязка GPO к OU; gpupdate /force; запуск диспетчера задач         | Диспетчер задач заблокирован; GPO отображается среди применённых.     | В заданной OU/GPO параметр DisableTaskMgr применён к проверенной учётной записи.           |
| 2 | Изменение пользователем         | Попытка изменить DisableTaskMgr; повторное обновление политики      | Отказ в изменении; ограничение сохраняется.                           | Пользователь не смог изменить значение в этой конфигурации; другие способы не проверялись. |
| 3 | Локальный администратор         | Изменение реестра через HKU\SID; gpupdate /force                    | После обновления значение вновь равно 1.                              | Временное изменение было устранено штатным обновлением доменной GPO.                       |
| 4 | Отсутствие связи с контроллером | Отключение сети; gpupdate /force; попытка записи; кэшированный вход | Обновление GPO не выполнено; отказ в записи; ограничение сохранилось. | Сохранение DisableTaskMgr подтверждено только для данного offline-сценария.                |

### **Заключение**

На стенде проверены применение доменной GPO, конфликты локальных настроек, действия локального администратора и работа без сети. Показанные наблюдения относятся к используемым Windows Server 2022 и Windows 11. Выводы по четырём гипотезам приведены ниже.

Следует также отметить, что требования к управлению конфигурацией корпоративных информационных систем и средствам защиты информации закреплены в нормативных документах ФСТЭК России [4], что дополнительно подчёркивает практическую и регуляторную значимость механизмов централизованного администрирования на основе GPO в отечественных корпоративных средах.

Результат проверки гипотез:

1. В проверенном сценарии доменная настройка DisableTaskMgr применялась к учётной записи при заданной OU и привязанной GPO. Наблюдение подтверждает гипотезу Н1 для этого параметра и конфигурации, но не проверяет все этапы и исключения модели LSDOU.
2. Гипотеза Н2 также получила подтверждение. Попытка локального изменения контролируемого параметра через реестр не привела к изменению конфигурации, а повторная синхронизация политик сохранила установленное ограничение. Это свидетельствует о приоритетности доменной GPO над локальными настройками и её устойчивости к пользовательскому вмешательству в пределах стандартных прав доступа.
3. Гипотеза Н3 подтвердилась в рамках проверенного сценария: локальный администратор изменил DisableTaskMgr в профиле доменного пользователя, после чего штатное обновление политики восстановило прежнее значение. Возможность других способов изменения или отключения механизмов обработки GPO в работе не проверялась.
4. Гипотеза Н4 подтверждается в пределах наблюдения: ранее применённое значение сохранилось в показанном offline-сценарии. Действие ACL реестра, иные способы локального вмешательства и физический доступ к машине не исследовались; результат не является общей оценкой защиты без сети.

Перспективы дальнейшего исследования связаны с проверкой нескольких GPO, порядка их обработки и механизмов Enforced и Block Inheritance, а также с оценкой различных уровней прав доступа в более сложной структуре OU.

В описанном стенде встроенные средства Windows позволили применить и восстановить доменное значение DisableTaskMgr. Это не исчерпывающая проверка контроля всех

параметров клиентских систем. Стенд может использоваться как учебный пример применения GPO и отдельных конфликтов доменного и локального значений. Для последующих проверок доступны обзор групповых политик Microsoft [5], документация LGPO.exe [6] и Get-GPResultantSetOfPolicy [7]; эти средства не применялись в описанных опытах.

**Библиографический список**

17. Krause, J. *Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy* / J. Krause. – Birmingham : Packt Publishing, 2018. – 390 p. – Текст : непосредственный.
18. Arya, K. *Windows Group Policy Troubleshooting: A Best Practice Guide for Managing Users and PCs Through Group Policy* / K. Arya. – Apress, 2016. – 200 p. – Текст : непосредственный.
19. Доменные политики и GPO в Active Directory: полное руководство по настройке и безопасности [Электронный ресурс] // Корпоративный блог Инфратех. – URL: <https://blog.infra-tech.ru/domennye-politiki/> (дата обращения: 20.02.2026). – Текст : электронный.
20. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 № 17 [Электронный ресурс]. – URL: [https://rppa.pro/npa/fstek17\\_11.02.2013](https://rppa.pro/npa/fstek17_11.02.2013) (дата обращения: 21.02.2026). – Текст : электронный.
21. Group Policy Overview [Электронный ресурс] // Microsoft Learn. – URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview> (дата обращения: 21.02.2026). – Текст : электронный.
22. LGPO.exe — Local Group Policy Object Utility [Электронный ресурс] // Microsoft Security. – URL: <https://www.microsoft.com/en-us/download/details.aspx?id=55319> (дата обращения: 17.02.2026). – Текст : электронный.
23. Get-GPResultantSetOfPolicy [Электронный ресурс] // Microsoft Learn. – URL: <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpresultantsetofpolicy> (дата обращения: 17.02.2026). – Текст : электронный.

**References**

24. Krause, J. (2018). *Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy*. Packt Publishing.
25. Arya, K. (2016). *Windows Group Policy troubleshooting: A best practice guide for managing users and PCs through Group Policy*. Apress.
26. Infratech Corporate Blog. (n.d.). *Domennye politiki i GPO v Active Directory: Polnoe rukovodstvo po nastroyke i bezopasnosti* [Domain policies and GPO in Active Directory: A complete guide to configuration and security]. <https://blog.infra-tech.ru/domennye-politiki/>
27. Federal Service for Technical and Export Control of Russia. (2013). *Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, sodержashchey v gosudarstvennykh informatsionnykh sistemakh* [On approval of requirements for the protection of information in state information systems] (Order No. 17). [https://rppa.pro/npa/fstek17\\_11.02.2013](https://rppa.pro/npa/fstek17_11.02.2013)
28. Microsoft. (n.d.). *Group Policy overview*. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>
29. Microsoft. (n.d.). *LGPO.exe: Local Group Policy Object utility*. Microsoft Security. <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
30. Microsoft. (n.d.). *Get-GPResultantSetOfPolicy*. Microsoft Learn. <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpresultantsetofpolicy>

**Информация об авторах**

Дворников Дмитрий Сергеевич — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва; e-mail: [dmitriidvo@gmail.com](mailto:dmitriidvo@gmail.com)

Костионова Мария Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва; e-mail: maria.kowela@gmail.com

## VERIFICATION OF DOMAIN GPO STABILITY MECHANISMS IN A CORPORATE NETWORK

**Dvornikov D. S., Kostionova M. A.**

*Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia*

**Abstract.** *This paper examines one user setting, DisableTaskMgr, on a Windows Active Directory laboratory testbed. The testbed includes a Windows Server 2022 domain controller and a Windows 11 client. The aim is to compare the registry value and Task Manager behavior after applying a domain GPO, attempting local changes, and disconnecting the client from the domain controller. The policy is linked to a specified organizational unit and tested with one user account. The article presents policy-update commands, reported policy application, and attempts to modify the controlled value. It considers an ordinary user, a local administrator, an active session without network connectivity, and a cached sign-in after reboot. In the displayed scenarios, the domain restriction was applied and restored by a normal policy update after an administrator changed the local value. Without connectivity, the previously applied value persisted; the ordinary user could not write a different value. Registry security descriptors and the internal persistence mechanism were not separately examined. Block Inheritance, Enforced, the complete LSDOU model, and other bypass methods were not tested. Results concern one setting, organizational unit, policy, and configuration. The material is a teaching example of applying and restoring a domain setting. It distinguishes observed parameter behavior from a general assessment of centralized-management security and does not characterize all Windows versions or physical-access scenarios.*

**Keywords:** *Windows, Active Directory, GPO, Group Policy, LSDOU, information security, domain infrastructure.*

### Information about the authors

Dvornikov Dmitriy Sergeevich — third-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow; e-mail: dmitriidvo@gmail.com

Kostionova Maria Aleksandrovna — third-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow; e-mail: maria.kowela@gmail.com

Калинин А. А., Клиз М. Р.

Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ СЕТЕВОГО ОБОРУДОВАНИЯ МЕТОДАМИ ВНЕШНЕГО АУДИТА В КОРПОРАТИВНОЙ СРЕДЕ

**Аннотация.** Статья представляет сравнительный аудит безопасности сетевого оборудования Cisco, MikroTik и Eltex в лабораторной среде. Исследование сочетает внешнее сканирование Nmap и внутреннюю проверку конфигурации по SSH, рассматривая открытые порты, протоколы управления, версии SSH и известные проблемы TLS. На этапе первичного обследования авторы фиксируют доступность Telnet, HTTP и других интерфейсов управления, а затем применяют рекомендации по отключению незащищенных сервисов, ограничению доступа и настройке SSHv2. Таблицы сопоставляют исходное и измененное состояния устройств; для протестированной конфигурации после настройки остаются открытыми SSH и HTTPS, тогда как Telnet и HTTP закрыты, а набор SSH-алгоритмов становится современнее. В проверке участвуют коммутаторы и маршрутизаторы нескольких производителей, однако результаты зависят от конкретных моделей, версий программного обеспечения и конфигурации стенда. Nmap показывает поверхность доступных сетевых сервисов, а анализ конфигурации помогает выявить причины обнаруженных состояний; результат сканирования сам по себе не подтверждает каждый указанный CVE. Работа предлагает последовательность внешнего и внутреннего аудита и показывает, почему исходные настройки следует проверять до подключения устройства к корпоративной сети. Выводы относятся к исследованным сценариям и требуют повторной проверки при смене прошивки, модели или топологии. В статье также изложены шаги повторного сканирования и проверки конфигурации после изменения настроек.

**Ключевые слова:** сетевая безопасность; аудит безопасности; Nmap; SSH; Cisco; MikroTik; Eltex.

### Введение

#### Актуальность

Безопасность управления сетевыми устройствами влияет на доступность и защиту сетевой инфраструктуры. Небезопасные службы управления и недостаточные ограничения доступа могут создавать риск несанкционированных действий. В этой работе рассматривается лабораторный аудит доступных служб и конфигурации, а не успешность атак или эксплуатация конкретных уязвимостей.

При анализе конфигурации целесообразно проверять доступность служб управления, ограничения входа и разрешённые протоколы. Сравнение Cisco, MikroTik и Eltex в одном стенде позволяет описать различия выбранных устройств и подготовить адресные рекомендации. Результаты относятся к использованным версиям и настройкам; они не характеризуют заводские конфигурации или все устройства каждого производителя.

#### Объект, предмет и цель

Объект исследования: процесс настройки, функционирования и обеспечения базовой безопасности сетевой инфраструктуры на примере коммутаторов и маршрутизаторов различных производителей.

Предмет исследования: уязвимости и слабые места в базовых настройках безопасности сетевых устройств Cisco, MikroTik и Eltex, выявляемые с помощью инструментов внешнего сканирования (Nmap) и внутреннего аудита конфигураций (SSH).

Цель исследования: разработка и практическая апробация методики комплексного аудита базовой безопасности сетевых устройств, включающей внешнее сканирование и внутреннюю проверку конфигурации, с последующим сравнительным анализом результатов для разных производителей и формулировкой практических рекомендаций по защите.

#### Обзор литературы и методология исследования

##### Обзор литературы

Актуальность исследования базовой безопасности сетевых устройств связана с тем, что ошибки конфигурации и недостаточно защищённые службы управления могут создавать риски для сетевой инфраструктуры. Публичные обзоры профильных организаций описывают

различные типы инцидентов, однако приводимые в них доли зависят от периода, выборки и методики подсчёта. В настоящей работе анализ ограничен проверяемой лабораторной конфигурацией и не переносит результаты обзора на конкретные модели оборудования.

Фундаментальные принципы обеспечения информационной безопасности сетевой инфраструктуры изложены в базовых стандартах и концепциях. Универсальной моделью для формулирования целей защиты служит триада CIA (Confidentiality, Integrity, Availability), формализованная в стандарте ISO/IEC 27002. Подробные рекомендации по практической реализации этих принципов для оборудования Cisco собраны в официальных руководствах Cisco Security Configuration Guide, а также отражены в учебных курсах Cisco Networking Academy (CCNA/CCNA Security). Для проведения аудита безопасности ключевое значение имеет инструмент Nmap (Network Mapper), возможности которого детально описаны в книге Гордона Лайона «Nmap Network Scanning», включая статистику обнаружения уязвимостей в зависимости от типа сканирования [1, 2].

Рассмотренные материалы по безопасности сетевого оборудования можно сгруппировать по следующим направлениям:

Одновендорные исследования. В доступных и проверяемых первичных источниках для этой рукописи не обнаружены методики, позволяющие подтвердить приведённые ранее доли и размеры выборок для Cisco и MikroTik. Поэтому количественные утверждения о распространённости открытых сервисов исключены; настоящее исследование сопоставляет только конфигурации и результаты сканирования собственного лабораторного стенда, не оценивая распространённость таких настроек в реальных сетях.

Межвендорные сопоставления. В этой статье сопоставляются устройства трёх производителей в лабораторном стенде; доступные источники не позволяют оценить распространённость настроек или полноту сравнительных исследований для рынка.

Методологические работы. Труды, посвящённые методикам аудита (McNab C. «Network Security Assessment», 2016), предлагают универсальные подходы к тестированию, но не содержат количественных сравнительных данных по различным вендорам. Документы NIST (National Institute of Standards and Technology), в частности NIST SP 800-115 «Technical Guide to Information Security Testing and Assessment», описывают общие процедуры тестирования, но не учитывают специфику конкретных платформ [3].

Проведённый анализ литературы позволяет выделить следующие пробелы, которые призвано заполнить настоящее исследование:

- в рассмотренных источниках не обнаружена единая методика сравнительного аудита оборудования разных производителей в идентичных условиях лабораторного стенда. Это наблюдение относится к включённым в обзор работам и не является результатом исчерпывающего систематического поиска;
  - недостаток количественных данных о типовых уязвимостях в «заводских» конфигурациях. Большинство исследований либо рассматривают уже скомпрометированные устройства, либо фокусируются на известных уязвимостях ПО, не уделяя внимания анализу того, какие уязвимости создаются самими администраторами из-за оставленных настроек по умолчанию;
  - обзор включённых источников содержит ограниченное число сравнительных исследований базовой безопасности оборудования Eltex с количественными результатами сканирования. Это ограничение выбранного обзора не устанавливает отсутствие других публичных исследований.
- Основные гипотезы исследования:
- гипотеза о релевантности инструментов: Nmap позволяет фиксировать доступные порты и версии служб; в настоящем протоколе сканирования проверялись поверхность сетевых сервисов и изменения доступности после настройки. Выявление уязвимостей CVE требует отдельного сопоставления версий и проверки применимости и не считается установленным результатом одного сканирования. [2];

- гипотеза о наблюдаемых службах: сканирование Nmap позволяет зафиксировать доступность сетевых служб на трёх испытанных устройствах в лабораторной конфигурации. Доступность службы сама по себе не доказывает наличие критической уязвимости или успешность атаки;
- гипотеза о сопоставлении данных: аудит через SSH с предоставленными учётными данными позволяет сопоставить наблюдаемые службы с параметрами конфигурации испытанных устройств. Обнаруженные различия характеризуют этот стенд и не устанавливают типичные уязвимости производителей.

### **Методы исследования**

Тип исследования: проверка устройств на базовую безопасность с использованием ОС «Альт» и программы для сканирования Nmap.

Характеристика среды исследования: лабораторная сетевая инфраструктура, состоящая из физических коммутаторов Cisco 3550, MikroTik и Eltex MES1428, а также PC с установленной операционной системой «Альт» и программой сканирования Nmap.

Методы сбора данных:

- внешнее сканирование и аудит доступности с использованием утилиты Nmap (Network Mapper);
- внутренний аудит конфигурации и состояния посредством протокола SSH (Secure Shell);
- сбор и анализ логов и конфигурационных файлов устройств.

Процедура проведения исследования:

- подготовка оборудования: базовая настройка коммутаторов;
- внешнее сканирование: подключение и проведение аудита с помощью Nmap;
- аудит безопасности: проверка конфигурации устройств;
- анализ полученных результатов сканирования.

### **Экспериментальное исследование**

#### **Лабораторная среда**

В рамках исследования была развернута лабораторная среда, предназначенная для проведения комплексного аудита базовой безопасности сетевых устройств. Её основная задача заключается в обеспечении изолированного и контролируемого взаимодействия между инструментом аудита и тестируемым оборудованием.

Аудит проводился по двухэтапной схеме:

Внешнее сканирование выполняется с рабочей станции с помощью Nmap. Оно позволяет определить, какие службы (SSH, Telnet, HTTP, HTTPS) доступны из сети, и получить сведения об их версиях. Эти данные могут служить основанием для последующей проверки применимости уязвимостей, но сами по себе не подтверждают CVE. [2]

Внутренний аудит. С виртуальной машины BaseAlt устанавливается SSH-подключение к устройству (при наличии соответствующих учётных данных). После успешного входа выполняется анализ текущей конфигурации устройства для проверки внутренних настроек безопасности (шифрование паролей, настройки доступа, активные сервисы, политики ACL).

Сканирование Nmap описывает доступные сетевые службы с внешней точки наблюдения. Проверка конфигурации через SSH выполняется с предоставленными учётными данными. Эти этапы позволяют сопоставить наблюдаемые сервисы с настройками испытанных устройств, но не являются проверкой проникновения или исчерпывающей оценкой безопасности. Стенд изолирован от рабочей сети; сравнение относится к проверенным моделям, версиям ПО и конфигурациям. Используются Cisco IOS 12.2(25)SEC и MikroTik RouterOS 6.33; выводы не переносятся на текущие версии этих платформ.

#### **Топология сети**

На рис. 1 представлена топология подключения рабочей станции к коммутатору Cisco 3550.

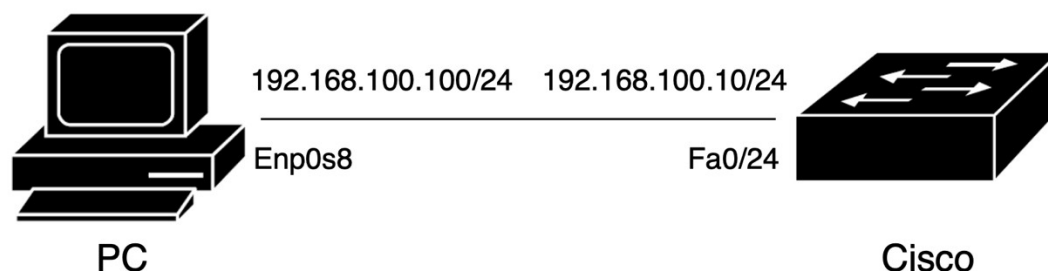


**Рис. 1. Схема соединения ПК и коммутатора Cisco 3550**

Для устройств MikroTik и Eltex использовалась аналогичная схема подключения. Далее приведены параметры настройки испытанного оборудования.

#### **Подготовка и конфигурация оборудования**

Для подготовки лабораторного стенда использованы:

- коммутаторы Cisco 3550, Eltex MES1428 и MikroTik;
- рабочая станция с ОС Linux и интерфейсом enp0s8;
- кабели Ethernet для подключения ПК к коммутаторам.

После подключения оборудования были выполнены первоначальные настройки управления.

До проведения сканирования были заданы параметры управления коммутаторами; команды первоначальной настройки приведены в табл. 1.

**Таблица 1 – Первоначальная настройка коммутаторов**

| Cisco 3550                                                                                                                                                                                                                                       | Mikrotik                                                                                                                                                                                                                                                                                                                                                                                                          | Eltex mes1428                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> enable configure terminal vlan 100 exit interface vlan 100 ip address 192.168.100.10 255.255.255.0 no shutdown exit interface fastethernet 0/24 switchport mode access switchport access vlan 100 no shutdown exit end write memory </pre> | <pre> /interface vlan add name=Management vlan-id=100 interface=bridge /ip address add address=192.168.100.20/24 interface=Management /interface ethernet switch port set ether24 default-vlan-id=100 vlan- mode=secure /interface bridge port add interface=ether24 bridge=bridge /interface bridge vlan add bridge=bridge vlan-ids=100 tagged=bridge untagged=ether24 /interface set ether24 disabled=no </pre> | <pre> enable configure terminal vlan 100 exit interface vlan 100 ip address 192.168.100.30 255.255.255.0 no shutdown exit interface gigabitethernet 0/24 switchport mode access switchport access vlan 100 no shutdown exit end write memory </pre> |

#### **Внешнее сканирование**

После настройки коммутаторов мы можем перейти к проведению аудита безопасности, а именно к первому этапу – внешнему сканированию с помощью программы Nmap. Команды, используемые при выполнении данного сканирования представлены ниже.

**Таблица 2 – Команды сканирования Nmap**

| Команда                                                                                  | Значение                    |
|------------------------------------------------------------------------------------------|-----------------------------|
| <code>nmap -sS -sV [IP-адрес]</code>                                                     | Базовое сканирование.       |
| <code>nmap -p- [IP-адрес]</code>                                                         | Полное сканирование портов. |
| <code>nmap --script safe [IP-адрес]</code><br><code>nmap --script vuln [IP-адрес]</code> | Проверка безопасности.      |
| <code>nmap --script "ssh*" -p 22 [IP-адрес]</code>                                       | Проверка SSH                |

Результаты Nmap сохранялись в текстовые файлы с помощью параметра `-oN имя_файла.txt`. Ниже приведены фрагменты выводов сканирования трёх устройств.

**Листинг 1 – Первичное сканирование Cisco 3550 (службы и версии)**

```
# Nmap 7.98 scan initiated Fri Nov 21 14:05:36 2025 as: nmap -sS -sV -oN
cisco_scan.txt 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.0069s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Cisco SSH 1.25 (protocol 1.99)
23/tcp    open  telnet       Cisco router telnetd (password required but not set)
80/tcp    open  http         Cisco IOS http config
443/tcp   open  ssl/https?
MAC Address: 00:00:FF:01:65:F2 (Camtec Electronics)
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Nov 21 14:05:46 2025 -- 1 IP address (1 host up) scanned in
10.07 seconds
```

**Листинг 2 – Первичное сканирование Cisco 3550 (все TCP-порты)**

```
# Nmap 7.98 scan initiated Fri Nov 21 14:17:55 2025 as: nmap -p- -oN
cisco_scan_ports.txt 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.0042s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:00:FF:01:15:68 (Camtec Electronics)
# Nmap done at Fri Nov 21 14:18:21 2025 -- 1 IP address (1 host up) scanned in
26.18 seconds
```

Результаты сканирования MikroTik:

**Листинг 3 – Первичное сканирование MikroTik (службы и версии)**

```
# Nmap 7.98 scan initiated Fri Nov 21 15:30:12 2025 as: nmap -sS -sV -oN
mikrotik_scan.txt 192.168.88.1
Nmap scan report for 192.168.88.1
Host is up (0.0052s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          MikroTik RouterOS sshd (protocol 2.0)
23/tcp    open  telnet       MikroTik RouterOS telnetd
80/tcp    open  http         MikroTik RouterOS http config
443/tcp   open  ssl/http     MikroTik RouterOS https config
8291/tcp  open  unknown      MikroTik WinBox protocol
8728/tcp  open  api          MikroTik RouterOS API
MAC Address: 64:D1:54:3A:8C:2F (MikroTik)
Service Info: OS: RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Nov 21 15:30:22 2025 -- 1 IP address (1 host up) scanned in
10.47 seconds
```

**Листинг 4 – Первичное сканирование MikroTik (все TCP-порты)**

```
# Nmap 7.98 scan initiated Fri Nov 21 15:31:45 2025 as: nmap -p- -oN
mikrotik_scan_ports.txt 192.168.88.1
Nmap scan report for 192.168.88.1
Host is up (0.0048s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
```

```

8291/tcp open  unknown
8728/tcp open  unknown
MAC Address: 64:D1:54:3A:8C:2F (MikroTik)
# Nmap done at Fri Nov 21 15:32:11 2025 -- 1 IP address (1 host up) scanned in
26.42 seconds

```

Результаты сканирования Eltex MES1428:

#### Листинг 5 – Первичное сканирование Eltex MES1428 (службы и версии)

```

# Nmap 7.98 scan initiated Fri Nov 21 16:15:23 2025 as: nmap -sS -sV -oN
eltex_scan.txt 192.168.200.10
Nmap scan report for 192.168.200.10
Host is up (0.0063s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Eltex SSH server (protocol 2.0)
23/tcp    open  telnet       Eltex telnetd
80/tcp    open  http         Eltex web management interface
443/tcp   open  ssl/http     Eltex web management interface
MAC Address: 00:11:22:AB:CD:EF (Eltex)
Service Info: Device: switch
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Nov 21 16:15:33 2025 -- 1 IP address (1 host up) scanned in
10.18 seconds

```

#### Листинг 6 – Первичное сканирование Eltex MES1428 (все TCP-порты)

```

# Nmap 7.98 scan initiated Fri Nov 21 16:16:50 2025 as: nmap -p- -oN
eltex_scan_ports.txt 192.168.200.10
Nmap scan report for 192.168.200.10
Host is up (0.0057s latency)
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:11:22:AB:CD:EF (Eltex)
# Nmap done at Fri Nov 21 16:17:16 2025 -- 1 IP address (1 host up) scanned in
26.05 seconds

```

Сводное сопоставление наблюдавшихся сетевых служб и сведений о безопасности приведено в табл. 3.

**Таблица 3 – Результаты первичного аудита сетевых сервисов**

| Параметр                                              | Cisco                                                                   | Mikrotik                                                                   | Eltex                                                                      |
|-------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Открытые TCP-порты                                    | 22, 23, 80, 443                                                         | 22, 23, 80, 443, 8291, 8728                                                | 22, 23, 80, 443                                                            |
| SSH-версия                                            | SSH-1.99 (поддержка устаревшей SSHv1)                                   | SSH-2.0                                                                    | SSH-2.0                                                                    |
| Заявленные SSH-алгоритмы (требуют проверки)           | CVE-2001-0144, слабые алгоритмы: diffie-hellman-group1-sha1, aes128-cbc | Слабые алгоритмы: CBC-шифры (aes128-cbc, aes192-cbc, aes256-cbc), HMAC-MD5 | Слабые алгоритмы: diffie-hellman-group1-sha1, CBC-шифры, hmac-md5, ssh-dss |
| Предполагаемые проблемы HTTPS (не подтверждены логам) | POODLE (CVE-2014-3566)                                                  | Не обнаружено (базовые настройки)                                          | POODLE (CVE-2014-3566), CCS Injection (CVE-2014-0224)                      |
| Telnet (порт 23)                                      | Открыт, без шифрования                                                  | Открыт, без шифрования                                                     | Открыт, без шифрования                                                     |

| Параметр                                                     | Cisco                                     | Mikrotik                                                  | Eltex                        |
|--------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------|------------------------------|
| Оценка веб-интерфейса (требуется отдельной проверки)         | HTTP/HTTPS, множественные CSRF-уязвимости | HTTP/HTTPS, отсутствие заголовков безопасности            | HTTP/HTTPS, CSRF-уязвимости  |
| Специфические порты                                          | Отсутствуют                               | 8291 (WinBox), 8728 (API) — расширенная поверхность атаки | Отсутствуют                  |
| CVE, упомянутые в исходном анализе (не подтверждены сканами) | CVE-2001-0144, CVE-2014-3566              | CVE не зафиксированы, но присутствуют слабые алгоритмы    | CVE-2014-3566, CVE-2014-0224 |

### **Внутренний аудит конфигурации**

Следующий этап — проверка конфигурации устройств через SSH с разрешённым доступом. Команды начальной настройки SSH приведены в табл. 4.

**Таблица 4 – Настройка SSH на исследованных устройствах**

| Cisco 3550                                                                                                                                                                                                                                                                                          | Mikrotik                                                                                                                                                                                           | Eltex mes1428                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure terminal ip domain-name lab.local crypto key generate rsa modulus 2048 ip ssh time-out 60 ip ssh authentication-retries 2 ip ssh version 2 username admin privilege 15 secret YourStrongPassword123 line vty 0 15 transport input ssh login local exit end write memory</pre> | <pre>/ip service set ssh port=22 disabled=no /user add name=admin password=YourStrongPassword123 group=full /ip service set ssh address=192.168.100.0/24 /ip service set telnet disabled=yes</pre> | <pre>enable configure terminal ip domain-name eltex-lab.local crypto key generate rsa modulus 2048 ip ssh server username admin privilege 15 password 0 YourStrongPassword123 line vty 0 15 transport input ssh login local exit line vty 0 15 no transport input telnet exit end write memory</pre> |

После подключения проводился аудит конфигурации. Используемые команды проверки для трёх платформ приведены в табл. 5–7.

**Таблица 5 – Команды внутреннего аудита Cisco**

| Команда                                                                                                                               | Значение                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| show running-config                                                                                                                   | Посмотр текущей конфигурации.                                     |
| show running-config   include password<br>show running-config   include secret<br>show running-config   include username              | Пароли и учетные записи.                                          |
| show ssh<br>show ip ssh                                                                                                               | SSH настройки.                                                    |
| interface <порт><br>spanning-tree mode rapid-pvst                                                                                     | Сетевые сервисы.                                                  |
| show running-config   section line con<br>show running-config   section line vty<br>show running-config   include banner              | Безопасность доступа. Проверка настройки консоли, VTY и баннеров. |
| show access-lists<br>show running-config   include access-list<br>show ip interface brief<br>show interface status<br>show vlan brief | Сетевые настройки. Проверка ACL, интерфейсов и VLAN.              |

| Команда                                                                                                                                                                                                                                                                         | Значение                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| show running-config   begin enable secret<br>show running-config   include transport input<br>show running-config   include "no service"<br>show running-config   include "service password-encryption"<br>show ntp status<br>show running-config   include ntp<br>show logging | Проверка, что пароли зашифрованы и отключен telnet.<br>Проверка, что небезопасные сервисы выключены.<br>Проверка NTP и логирование. |
| show version<br>show clock<br>show uptime<br>show users<br>show mac address-table                                                                                                                                                                                               | Версии IOS, время работы, пользователи и таблица MAC-адресов.                                                                       |

**Таблица 6 – Команды внутреннего аудита MikroTik**

| Команда                                                                                      | Значение                                                                                                 |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| /system identity print<br>/system resource print<br>/system routerboard print                | Базовая информация.                                                                                      |
| /user print<br>/user group print<br>/user print where name="admin"                           | Пользователи и пароли. Просмотр всех пользователей, групп и проверка, нет ли стандартных учетных записей |
| /ip service print                                                                            | Сетевые службы и порты.                                                                                  |
| /ip ssh print<br>/ip ssh print detail                                                        | SSH настройки, какие алгоритмы поддерживаются                                                            |
| /ip firewall filter print<br>/ip firewall nat print<br>/ip firewall address-list print       | Безопасность доступа. Firewall правила, NAT правила и списки доступа                                     |
| /ip service print where port=80 or port=443<br>/ip service disable www,www-ssl               | Настройки веб-доступа. HTTP/HTTPS доступ.                                                                |
| /system package update print<br>/system package update check<br>/system package update print | Обновления и версии. Доступные обновления.                                                               |

**Таблица 7 – Команды внутреннего аудита Eltex**

| Команда                                                                                                                                                                                                                          | Значение                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| show version<br>show system<br>show inventory                                                                                                                                                                                    | Базовая информация.                                                                                       |
| show users<br>show running-config   include username<br>show running-config   include password<br>show running-config   include secret<br>show privilege                                                                         | Пользователи и пароли. Просмотр всех пользователей, локальных учетных записей и привилегии пользователей. |
| show ip interface brief<br>show interface status<br>show running-config   include service<br>show running-config   include http<br>show running-config   include telnet<br>show running-config   include ssh                     | Сетевые службы и порты.                                                                                   |
| show ssh<br>show ip ssh<br>show running-config   section ssh                                                                                                                                                                     | SSH настройки                                                                                             |
| show access-lists<br>show running-config   include access-list<br>show running-config   section line<br>show running-config   section line vty<br>show running-config   section line con<br>show running-config   include banner | Безопасность доступа. ACL, Настройки линий доступа и баннеры                                              |

| Команда                                                                                                                                                                        | Значение                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| show vlan brief<br>show vlan<br>show port-security<br>show running-config   include port-security<br>show running-config interface                                             | Настройки VLAN и портов. Безопасность портов и настройки интерфейсов |
| show clock<br>show ntp status<br>show running-config   include ntp<br>show logging<br>show running-config   include logging<br>show snmp<br>show running-config   include snmp | Системные настройки. Логирование и SNMP.                             |

### Результаты исследования

В ходе исследования выполнен двухэтапный аудит трёх лабораторных устройств: Cisco Catalyst 3550, MikroTik и Eltex. Внешнее сканирование Nmap зафиксировало открытые порты и сведения о версиях служб; эти наблюдения не подтверждают наличие конкретных CVE. Внутренний анализ конфигурации позволил сопоставить результаты сканирования с настройками. На этапе аудита были получены следующие версии ПО исследуемых устройств:

- Cisco Catalyst 3550 — IOS 12.2(25)SEC;
- MikroTik — RouterOS 6.33;
- Eltex MES1428 — ПО 1.4.2.

В испытанных конфигурациях трёх устройств внешний аудит выявил доступные сетевые службы и параметры конфигурации, на основании которых сформулированы рекомендации по ограничению доступа. Результаты не устанавливают наличие конкретных критических уязвимостей, успешность атак или свойства заводских конфигураций в целом.

### Рекомендации по обеспечению базовой безопасности

По результатам проведённого исследования сформулированы рекомендации по усилению базовой безопасности для испытанных устройств.

Для оборудования Cisco рекомендуется проверить настройки SSH и HTTPS и отключить устаревшие алгоритмы и SSLv3, если они поддерживаются фактически установленной версией ПО. Представленные сканы сами по себе не подтверждают применимость POODLE (CVE-2014-3566) или наличие уязвимых версий SSH; эти выводы требуют отдельной проверки прошивки и конфигурации.

Ключевым направлением защиты устройств MikroTik является ограничение расширенной поверхности атаки: необходимо настроить списки доступа для WinBox (порт 8291) и API (порт 8728), ограничив их только доверенными IP-адресами, либо отключить данные сервисы при использовании альтернативных способов управления. Требуется обязательная настройка межсетевого экрана (firewall) с правилами, ограничивающими входящий трафик к сервисам управления, а также обновление RouterOS до актуальной версии, содержащей исправления известных уязвимостей и современные криптографические алгоритмы [4].

Для оборудования Eltex рекомендуется проверять актуальность прошивки и конфигурацию TLS/SSH. Приведённые сканы не подтверждают наличие POODLE (CVE-2014-3566) или CCS Injection (CVE-2014-0224): применимость этих CVE зависит от версии и конфигурации ПО и в данном опыте отдельно не проверялась. Слабые алгоритмы SSH и устаревшие версии SSL/TLS следует отключать, если они поддерживаются испытанной прошивкой. [5, 6, 7]

После применения изменений было проведено повторное сканирование с использованием тех же команд Nmap, что и на начальном этапе исследования. Результаты повторного сканирования устройства Cisco 3550 представлены ниже.

### Листинг 7 – Повторное сканирование Cisco 3550 (службы и версии)

```
# Nmap 7.98 scan initiated Fri Mar 10 11:23:45 2026 as: nmap -ss -sv -oN
cisco_scan_hardened.txt 192.168.100.10
```

```
Nmap scan report for 192.168.100.10
Host is up (0.0058s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Cisco SSH 2.0 (protocol 2.0)
443/tcp   open  ssl/https    Cisco IOS http secure server
MAC Address: 00:00:FF:01:65:F2 (Camtec Electronics)
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Mar 10 11:23:55 2026 -- 1 IP address (1 host up) scanned in
10.23 seconds
```

#### **Листинг 8 – Повторное сканирование Cisco 3550 (все TCP-порты)**

```
# Nmap 7.98 scan initiated Fri Mar 10 11:24:30 2026 as: nmap -p- -oN
cisco_scan_ports_hardened.txt 192.168.100.10
Nmap scan report for 192.168.100.10
Host is up (0.0045s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
MAC Address: 00:00:FF:01:15:68 (Camtec Electronics)
# Nmap done at Fri Mar 10 11:24:56 2026 -- 1 IP address (1 host up) scanned in
26.18 seconds
```

Сравнение доступных сетевых служб Cisco 3550 до и после настройки представлено в табл. 8.

**Таблица 8 – Состояние Cisco 3550 до и после изменения настроек**

| Параметр                                       | До применения рекомендаций                       | После применения рекомендаций             |
|------------------------------------------------|--------------------------------------------------|-------------------------------------------|
| Открытые порты                                 | 22, 23, 80, 443                                  | 22, 443                                   |
| Telnet (порт 23)                               | Открыт, без шифрования                           | Закрыт                                    |
| HTTP (порт 80)                                 | Открыт HTTP (порт 80)                            | Закрыт                                    |
| SSH-версия                                     | SSH-1.99 (поддержка устаревшей SSHv1)            | SSH-2.0                                   |
| SSH-алгоритмы<br>(требуется проверка)          | Слабые: diffie-hellman-group1-sha1,<br>CBC-шифры | В приведённых выводах Nmap не<br>показаны |
| POODLE / состояние TLS<br>(требуется проверка) | Применимость CVE не установлена                  | Применимость CVE не проверялась           |

В рукописи указано, что после рекомендованных изменений в конфигурации MikroTik RouterOS сохранились SSH и HTTPS, а Telnet и HTTP были закрыты. Однако сопоставимых журналов повторного сканирования MikroTik и Eltex в представленных материалах нет. Для подтверждения этого результата необходимы отдельные протоколы проверки.

#### **Заключение**

Проведённое исследование выявило в проверенной лабораторной конфигурации открытые и недостаточно защищённые службы на устройствах Cisco, MikroTik и Eltex. Внешнее сканирование Nmap позволило зафиксировать доступные порты и версии сервисов; внутренний аудит через SSH помог сопоставить наблюдения с настройками устройств. Результаты относятся к исследованным моделям, версиям ПО и конфигурациям и не характеризуют все устройства этих производителей. Для практического применения важны первоначальная проверка оборудования, отключение ненужных служб, ограничение доступа к интерфейсам управления и регулярный аудит.

#### **Библиографический список**

31. Cisco Systems. Harden IOS Devices [Электронный ресурс]. – 2024. – 12 сентября. – URL: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html> (дата обращения: 12.10.2026). – Текст : электронный.

32. Lyon G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. F. Lyon. – Nmap Project, 2009. – 468 p.
33. NIST SP 800-115. Technical Guide to Information Security Testing and Assessment [Электронный ресурс] / National Institute of Standards and Technology. – 2008. – URL: <https://csrc.nist.gov/publications/detail/sp/800-115/final> (дата обращения: 15.02.2026). – Текст : электронный.
34. MikroTik. MikroTik Documentation (RouterOS) [Электронный ресурс]. – URL: <https://help.mikrotik.com/docs/> (дата обращения: 15.02.2026). – Текст : электронный.
35. Eltex. Настройка SSH-сервера на коммутаторах MES14xx, MES24xx, MES3400-xx, MES37xx [Электронный ресурс]. – URL: <https://docs.eltex-co.ru/pages/viewpage.action?pageId=564690973> (дата обращения: 12.10.2026). – Текст : электронный.
36. National Vulnerability Database. CVE-2014-3566 [Электронный ресурс]. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2014-3566> (дата обращения: 15.02.2026). – Текст : электронный.
37. National Vulnerability Database. CVE-2014-0224 [Электронный ресурс]. – URL: <https://nvd.nist.gov/vuln/detail/CVE-2014-0224> (дата обращения: 15.02.2026). – Текст : электронный.

#### **References**

38. Cisco Systems. (2024, September 12). Harden IOS devices. <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>
39. Lyon, G. F. (2009). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Nmap Project.
40. National Institute of Standards and Technology. (2008). *Technical guide to information security testing and assessment (NIST SP 800-115)*. <https://csrc.nist.gov/publications/detail/sp/800-115/final>
41. MikroTik. (n.d.). MikroTik documentation (RouterOS). <https://help.mikrotik.com/docs/>
42. Eltex. (n.d.). Nastroiika SSH-servera na kommutatorakh MES14xx, MES24xx, MES3400-xx, MES37xx [SSH server configuration on MES switches]. <https://docs.eltex-co.ru/pages/viewpage.action?pageId=564690973>
43. National Vulnerability Database. (n.d.). CVE-2014-3566. <https://nvd.nist.gov/vuln/detail/CVE-2014-3566>
44. National Vulnerability Database. (n.d.). CVE-2014-0224. <https://nvd.nist.gov/vuln/detail/CVE-2014-0224>

#### **Информация об авторах**

Калинин А. А. — студент 1-го курса факультета комплексной безопасности топливно-энергетического комплекса, Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: arskalinin2000@mail.ru.

Клиз М. Р. — студент 1-го курса факультета комплексной безопасности топливно-энергетического комплекса, Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; для переписки: arskalinin2000@mail.ru (через соавтора А. А. Калинина).

### **COMPARATIVE ANALYSIS OF NETWORK EQUIPMENT VULNERABILITIES USING EXTERNAL AUDIT METHODS IN A CORPORATE ENVIRONMENT**

**Kalinin A. A., Kliz M. R.**

*Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia*

**Abstract.** This paper presents a comparative security audit of Cisco, MikroTik, and Eltex network equipment in a laboratory environment. The study combines external Nmap scanning with an internal configuration review over SSH, examining open ports, management protocols, SSH versions, and known TLS issues. During the initial assessment, the authors record the availability of Telnet, HTTP, and other management interfaces, then apply recommendations to disable insecure services, restrict access, and configure SSHv2. Tables compare the initial and updated device states; in the tested configuration, SSH and HTTPS remain available after hardening, while Telnet and HTTP are closed and the SSH algorithm set is modernized. The tests cover switches and routers from several manufacturers, but the results depend on the specific models, software versions, and testbed configuration. Nmap scans show exposed network services, while

*configuration analysis helps investigate the causes of observed states; a scan does not by itself confirm each listed CVE. The paper presents a sequence for external and internal audit and demonstrates why default settings should be reviewed before a device is connected to a corporate network. The conclusions apply to the tested scenarios and should be rechecked after firmware, model, or topology changes.*

**Keywords:** *network security; security audit; Nmap; SSH; Cisco; MikroTik; Eltex.*

### **Information about the authors**

Arseniy A. Kalinin — first-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: arskalinin2000@mail.ru.

Makar R. Kliz — first-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence via co-author Arseniy A. Kalinin: arskalinin2000@mail.ru.

Н. М. Коваль<sup>1</sup>, Е. А. Гимпель<sup>1</sup>

<sup>1</sup> ФГАОУ ВО «Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия

## ЛАБОРАТОРНЫЙ РАЗБОР TCP-ACL И ИНТЕРФЕЙСНЫХ ПОКАЗАТЕЛЕЙ СЕТЕВОГО СТЕНДА

**Аннотация.** В статье представлен учебный разбор фрагментов сетевой конфигурации и авторской сводки интерфейсных показателей лабораторного стенда. Рассматриваются Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. Цель работы — сопоставить содержание показанных команд с границами интерпретации агрегированных счётчиков, не выдавая их изменение за проверенную фильтрацию определённого потока. В конфигурациях Cisco и Eltex приведены запреты TCP между двумя заданными узлами и последующее разрешение остального IP-трафика. Это не общий запрет IP-пакетов. Для MikroTik показаны создание моста и добавление интерфейсов; правило ACL и его назначение в этих листингах не представлены. Авторы описывают мониторинг SNMP в Zabbix с интервалом опроса 60 секунд. Получаемые показатели усредняются за интервал и не позволяют установить протокольный состав трафика или кратковременные пики. В работе сохранены авторские значения нагрузки до и после описанных изменений, а производные отношения пересчитаны по их округлённым центральным значениям. Эти вычисления характеризуют сводные числа, а не долю фактически пропущенных пакетов. Исходные временные ряды и расчёт авторских величин после знака «±» не представлены, поэтому их статистический смысл не подтверждается. Практическое значение материала состоит в разборе TCP-правил, назначении фильтра интерфейсу и разграничении конфигурации, агрегированного наблюдения и доказательства эффекта. Сопоставление производителей, состава остаточной нагрузки и аппаратных причин различий по данным статьи не проводится.

**Ключевые слова:** TCP; ACL; коммутатор; SNMP; интерфейсный счётчик; лабораторный стенд.

### Введение

Списки контроля доступа (Access Control Lists) представляют собой один из базовых инструментов управления потоком пакетов в сети. Их основная задача — отбирать проходящие через устройство пакеты по заданным критериям и регулировать доступ к сетевым сервисам. ACL применимы не только на традиционных маршрутизаторах и межсетевых экранах, но и на современных L2+ коммутаторах, сочетающих коммутацию на канальном уровне с некоторыми возможностями сетевого уровня.

Важно учитывать, что на L2+ платформах обработка пакетов бывает разнородной. Часть трафика проходит полностью через аппаратные механизмы коммутации, тогда как другие типы пакетов отправляются на программную обработку — в контроллерную плоскость или CPU. От архитектуры устройства зависят поддерживаемые поля заголовков, порядок и место применения фильтров и вообще перечень трафика, на который распространяются ACL.

В своей классической форме ACL — это упорядоченная последовательность правил, которые проверяют параметры пакета: MAC-адреса, VLAN-теги, IP-адреса, номера портов, протоколы и т. п. На практике возможности платформы ограничены: аппаратные таблицы (например, TCAM) имеют фиксированный объём и нередко не поддерживают все необходимые поля и операции. В результате сложные проверки выносятся в программную плоскость, а часть сопоставлений выполняется аппаратно, только при наличии соответствующих возможностей.

Коммутаторы уровня L2+ фактически занимают промежуточное положение между «чистыми» L2-устройствами и полноценными L3-коммутаторами. За счёт этого пользовательский поток в большинстве случаев обрабатывается аппаратно, тогда как служебные протоколы (ARP, STP, LLDP, DHCP и др.) и специфические пакеты могут отправляться по отдельным, программным путям. Следствие — одно и то же правило ACL может по-разному сработать для разных типов пакетов или вовсе не примениться к некоторым из них.

Поэтому проверка работоспособности и полноты ACL должна сочетать формальный разбор конфигурации с реальными нагрузочными испытаниями. Эксперименты позволяют определить, какие классы трафика действительно блокируются аппаратно, а какие проходят

через устройство, создавая «остаточную» нагрузку на контроллер и CPU. Практическую ценность представляют тест-сценарии с инкапсуляцией, модификацией VLAN-тегов, передачей служебного трафика и моделированием пиковых нагрузок с переключениями между аппаратной и программной обработкой.

Наблюдение и воспроизведение подобных сценариев важно для понимания реальной эффективности базовых ACL на L2+ платформах.

Объект работы — показанные сетевые конфигурации и сводные интерфейсные показатели лабораторного стенда.

Предмет работы — содержание TCP-правил, их назначение интерфейсам и ограничения интерпретации агрегированных показателей нагрузки.

Цель работы — разобрать приведённые команды и сводные значения, разграничив настройку, наблюдение общего счётчика и подтверждение фильтрации заданного потока.

Для достижения цели поставлены следующие задачи:

- Разобрать показанные TCP-ACL и их назначение на Cisco Catalyst 2960 и Eltex MES1428; для MikroTik отдельно описать имеющийся фрагмент настройки bridge;
- Описать указанный авторами способ наблюдения агрегированной нагрузки через SNMP без установления её протокольного состава;
- Сохранить авторские сводные значения T0 и T1, явно указав отсутствие исходных временных рядов и подтверждённого расчёта величин после знака «±»;
- Пересчитать отношения и разности округлённых центральных значений, не трактуя эти вычисления как пакетный эффект фильтрации;
- Указать ограничения сопоставления сценариев и границы использования общего интерфейсного счётчика.

### **Теоретические предпосылки**

Эффективность ACL на L2+ устройствах определяется тем, какие типы кадров и на каком уровне обработки доступны механизму фильтрации.

В документации Cisco подчёркивается разграничение фильтрации IP и non-IP трафика: IP access list применимы только к IP-пакетам, тогда как non-IP трафик (включая ARP) относится к области MAC-фильтрации и требует иных механизмов [1].

Существенным ограничением аппаратной фильтрации является конечный объём аппаратных ресурсов для правил (таблицы ACL/память аппаратной классификации). Для коммутаторов серии Eltex MES в руководстве приведены количественные лимиты ACL-правил для конкретных моделей, включая MES1428 [2].

Для ряда платформ Cisco указывается, что при превышении возможностей аппаратной ACL-фильтрации может использоваться программная фильтрация (software filtering), что сопровождается ростом нагрузки на CPU и потенциальным снижением производительности [3].

Передача пакетов на обработку CPU в терминах Cisco описывается как punt (передача в CPU/slow path) и применяется при невозможности аппаратной обработки отдельных классов трафика [4].

В устройствах MikroTik с аппаратным offload поведение зависит от конфигурации bridge: трафик, проходящий через bridge, по умолчанию может обходить IP firewall, а для принудительной обработки используются отдельные настройки; также описаны правила ACL с перенаправлением трафика в CPU (redirect-to-cpu) [5, 6].

Таким образом, при интерпретации результатов нагрузочного тестирования необходимо разделять: эффект IP-фильтрации, долю non-IP/L2 кадров (например, ARP, RFC 826) и влияние аппаратных лимитов и возможного перехода части обработки в CPU/программную плоскость [7].

### **Материалы и методы**

#### **Техническое оснащение эксперимента**

- Три различных коммутатора: Cisco Catalyst 2960, Eltex MES 1428 и MikroTik CRS326-24G-2S+RM;

- Два персональных компьютера: первый формирует сетевой трафик, второй принимает его;
- По описанию авторов, на первом компьютере развёрнут Zabbix [8], регистрирующий интерфейсные счётчики SNMP с интервалом 60 с. Эти показатели усредняются между опросами и не устанавливают кратковременные пики или протокольный состав нагрузки. Расчёт величин после знака «±» в авторской сводке не приложен; интервал опроса сам по себе не подтверждает эти величины.

Порядок работы:

- Базовая настройка оборудования (IP-адресация, проверка связности);
- Генерация интенсивного трафика и фиксация нагрузки на интерфейсах;
- Разбор и применение показанных TCP-правил Cisco и Eltex; фрагмент MikroTik рассматривается как настройка bridge;
- Регистрация показателей на этапе, который авторы описывают как повторную генерацию нагрузки после изменения настроек.

#### **Арифметические соотношения сводных значений**

Обозначения:  $T_0$  и  $T_1$  — авторские сводные показатели интерфейсной нагрузки до и после описанных изменений (Мбит/с). При опросе SNMP раз в 60 с это интервальные показатели, а не доказанные кратковременные пики.

- Отношение  $T_1/T_0$ , выраженное в процентах, показывает величину второго сводного показателя относительно первого;
- Разность  $T_0 - T_1$  характеризует изменение сводного показателя, Мбит/с;
- Относительное изменение рассчитывается как доля разности  $T_0 - T_1$  по отношению к  $T_0$ , выраженная в процентах.

Указанные отношения задают арифметические отношения сводных значений. Производные центральные значения в таблице пересчитаны редакторски по округлённым  $T_0$  и  $T_1$ ; это не новые измерения. Значения после «±» в исходных  $T_0/T_1$  сохранены как авторские, без подтверждения их статистического смысла.

#### **Результаты и обсуждение**

##### **Cisco Catalyst 2960**

##### **Настройка и применение ACL**

Листинги 1 и 2 показывают создание TCP-ACL и его назначение на входящий трафик интерфейса Cisco Catalyst 2960.

Показанные правила запрещают TCP между двумя заданными хостами, затем разрешают остальной IP-трафик. Наличие этих команд само по себе не подтверждает отбрасывание целевых пакетов; агрегированный интерфейсный показатель также не даёт такой проверки.

##### **Листинг 1 – Создание списка ACL на Cisco Catalyst 2960**

```
Switch(config)#access-list 105 deny tcp host 192.168.88.3 host 192.168.88.1
Switch(config)#access-list 105 deny tcp host 192.168.88.1 host 192.168.88.3
Switch(config)#access-list 105 permit ip any any
```

##### **Листинг 2 – Назначение ACL на интерфейс Cisco Catalyst 2960**

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#ip access-group 105 in
Switch(config-if)#ex
```

##### **Интерфейсная нагрузка Cisco Catalyst 2960**

На рисунке 1 приведена авторская диаграмма интерфейсной нагрузки Cisco Catalyst 2960 для этапов, описанных как до и после изменения ACL. Она показывает изменение общего показателя, но не устанавливает, какие пакеты были пропущены или отброшены и чем вызвано изменение.

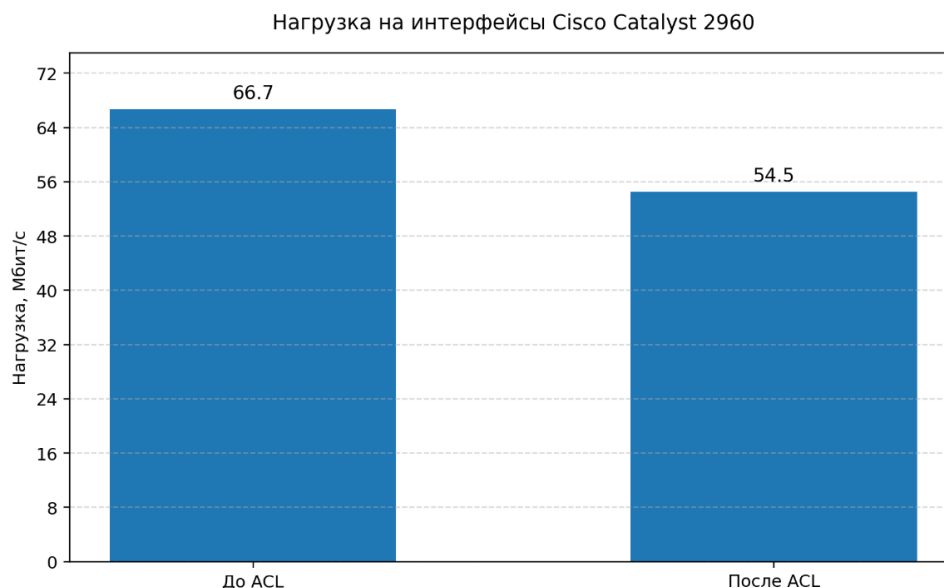


Рис. 1. Интерфейсная нагрузка Cisco Catalyst 2960 до и после изменения конфигурации

### **Eltex MES1428**

#### **Настройка и применение ACL**

Листинги 3 и 4 показывают TCP-запреты между двумя хостами, последующее permit ip any any и назначение списка интерфейсу Eltex MES1428. Разрешения отдельных ICMP/TCP-потоков после общего permit ip избыточны для уже разрешённого трафика. Команды сохранены как в исходном примере; пакетная проверка результата не показана.

#### **Листинг 3 – Создание ACL на Eltex MES1428**

```
console(config)#ip access-list extended 1001
console(config-ext-nacl)#deny tcp host 192.168.88.1 host 192.168.88.3
console(config-ext-nacl)#deny tcp host 192.168.88.3 host 192.168.88.1
console(config-ext-nacl)#permit ip any any
console(config-ext-nacl)#permit tcp any any
console(config-ext-nacl)#permit icmp any any
```

#### **Листинг 4 – Назначение ACL на интерфейс Eltex MES1428**

```
console(config)#interface fastethernet 0/1
console(config-if)#ip access-group 1001 in
console(config-if)#ex
```

#### **Интерфейсная нагрузка Eltex MES1428**

Рисунок 2 содержит авторскую диаграмму интерфейсной нагрузки Eltex MES1428 для двух описанных этапов. Раздельных IP/поп-IP-счётчиков и захвата целевого потока нет, поэтому диаграмма не подтверждает уменьшение именно IP-трафика либо сохранение определённого L2-трафика.

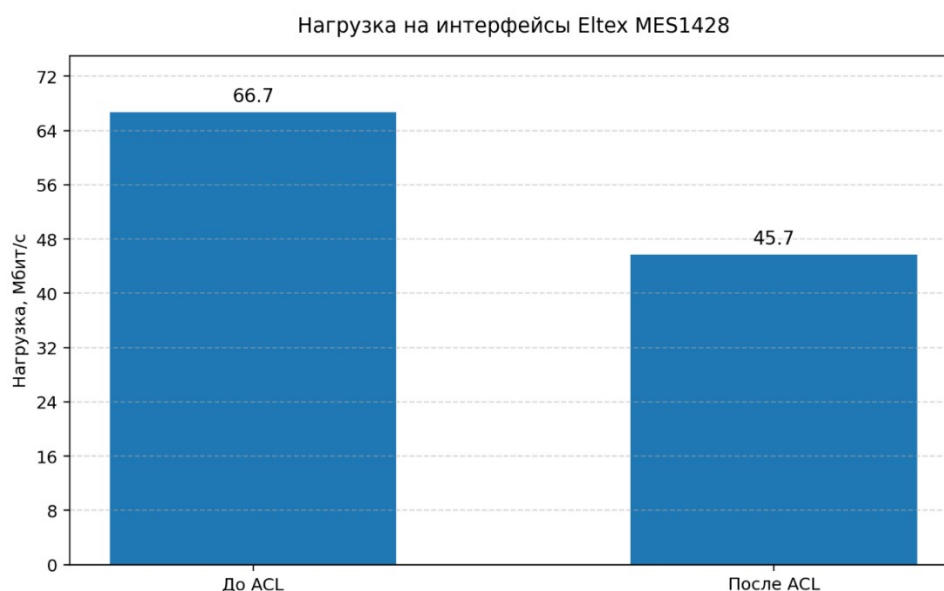


Рис. 2. Интерфейсная нагрузка Eltex MES1428 до и после изменения конфигурации

### ***MikroTik CRS326-24G-2S+RM***

#### **Настройка bridge и интерфейсов MikroTik**

Листинги 5 и 6 показывают создание bridge и добавление интерфейсов MikroTik. Они не содержат правила ACL или команды его назначения. По этому фрагменту нельзя утверждать, что на MikroTik был выполнен такой же тест ACL, как описан для двух других устройств.

#### **Листинг 5 – Создание bridge и добавление первого интерфейса MikroTik**

```
[admin@MikroTik] /interface ethernet switch rule> /interface bridge
[admin@MikroTik] /interface bridge> add name=bridge2
[admin@MikroTik] /interface bridge> /interface bridge port
[admin@MikroTik] /interface bridge port> add bridge=bridge2 interface=ether1
hw=yes learn=no unknown-flood=no
```

#### **Листинг 6 – Добавление второго интерфейса в bridge на MikroTik CRS326**

```
[admin@MikroTik] /interface bridge port> add bridge=bridge2 interface=ether2
hw=yes
```

#### **Сводные показатели нагрузки MikroTik**

На рисунке 3 сохранены авторские сводные показатели MikroTik для двух этапов. Представленная конфигурация не подтверждает применение ACL, поэтому эти показатели не интерпретируются как результат фильтрации. Исходные ряды и метод расчёта неопределённости отсутствуют; роль bridge или аппаратной обработки по ним не устанавливается.

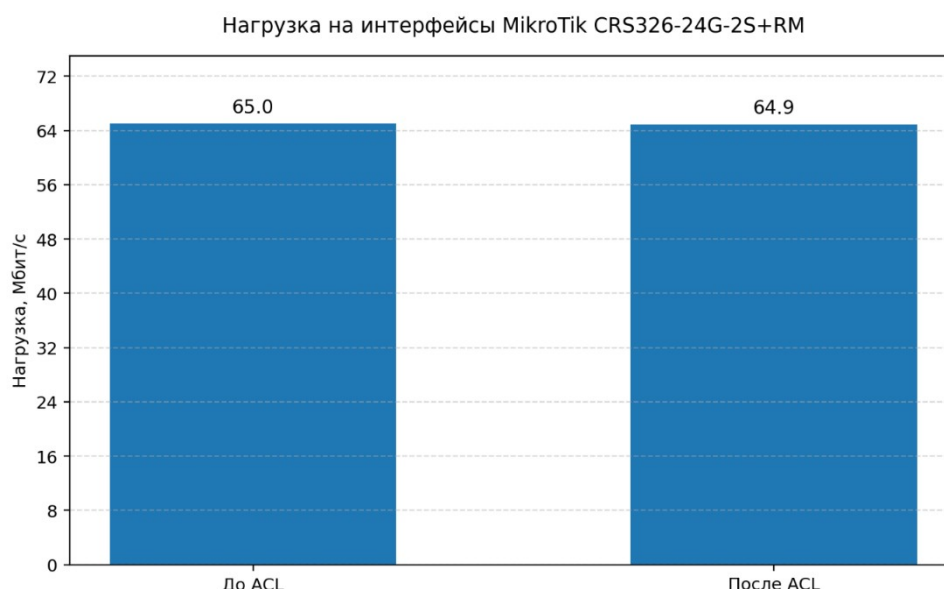


**Рис. 3. Авторские сводные показатели интерфейсной нагрузки MikroTik CRS326**

Таблица 1 объединяет авторские сводные значения нагрузки и редакторские арифметические расчёты по их округлённым центральным значениям. Это не сопоставимый эксперимент по эффективности фильтрации трёх платформ.

**Таблица 1 – Сводные интерфейсные показатели до и после изменения конфигурации**

| Устройство                | $T_0$ , Мбит/с | $T_1$ , Мбит/с | $T_1/T_0$ , % | $T_0 - T_1$ , Мбит/с | Изменение, % |
|---------------------------|----------------|----------------|---------------|----------------------|--------------|
| Cisco Catalyst 2960       | $66.7 \pm 2.2$ | $54.5 \pm 1.8$ | 81.7          | 12.2                 | 18.3         |
| Eltex MES1428             | $66.7 \pm 2.2$ | $45.7 \pm 1.5$ | 68.5          | 21.0                 | 31.5         |
| MikroTik CRS326-24G-2S+RM | $65.0 \pm 2.2$ | $64.9 \pm 2.2$ | 99.8          | 0.1                  | 0.2          |

#### **Границы интерпретации таблицы 1**

**Cisco Catalyst 2960.** Показаны TCP-правила. Изменение общего счётчика не подтверждает эффект фильтрации. Авторские  $\pm$  не проверены.

**Eltex MES1428.** Показаны TCP-правила. Протокольный состав нагрузки не установлен; причинный эффект ACL не подтверждён. Авторские  $\pm$  не проверены.

**MikroTik CRS326.** Показана настройка bridge, без правила ACL. Значения не интерпретируются как эффект фильтрации. Авторские  $\pm$  не проверены.

#### **Заключение**

Приведённые команды Cisco и Eltex задают запрет определённых TCP-поток и разрешение остального IP-трафика. Показанные фрагменты MikroTik задают bridge и его интерфейсы, но не ACL.

Авторские диаграммы и  $T_0/T_1$  фиксируют сводное описание двух этапов каждого сценария. Исходные ряды счётчиков не приложены; расчёт величин после « $\pm$ » не подтверждён. Поэтому они сохранены как авторские сведения без статистической интерпретации.

Редакторские отношения  $T_1/T_0$  и разности  $T_0 - T_1$  вычислены только по округлённым центральным значениям. Они не равны измеренной доле пропущенных пакетов и не доказывают причинный эффект ACL.

Общий интерфейсный счётчик не разделяет IP, ARP и другие протоколы. Ненулевое значение нельзя назвать остаточным L2-трафиком без отдельных счётчиков или захвата.

Сценарии не дают основания ранжировать производителей: одинаковая конфигурация фильтрации для трёх платформ и контроль состава нагрузки не представлены.

Практическая проверка TCP-правила должна отдельно фиксировать прохождение разрешённых и запрещённых целевых пакетов. Здесь этот шаг обозначен как граница материала, а не выполненный результат.

Материал пригоден для учебного разбора команд и ограничений мониторинга. Выводы об аппаратных причинах различий, общей устойчивости ACL и количественной эффективности фильтрации по представленным материалам не делаются.

**Библиографический список**

1. Cisco. Configuring IPv4 ACLs (разграничение IP ACL и MAC ACL) [Электронный ресурс]. – URL: [https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b\\_ie3500\\_1718-cg/configuring\\_ipv4\\_acls.html](https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b_ie3500_1718-cg/configuring_ipv4_acls.html) (дата обращения: 12.10.2026).
2. Eltex. MES Series User Manual 10.4.2.1 (лимиты ACL для MES1428) [Электронный ресурс]. – URL: [https://api.prod.eltex-co.ru/storage/upload\\_center/files/54/MES\\_Series\\_user\\_manual\\_10.4.2.1\\_en.pdf](https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf) (дата обращения: 12.10.2026).
3. Cisco. Configuring IPv4 Access Control Lists на Catalyst 2960L (software filtering при ограничениях аппаратных ресурсов) [Электронный ресурс]. – URL: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2\\_7\\_e/configuration\\_guide/sec/b\\_1527e\\_security\\_2960l\\_cg/configuring\\_ipv4\\_access\\_control\\_lists.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_7_e/configuration_guide/sec/b_1527e_security_2960l_cg/configuring_ipv4_access_control_lists.html) (дата обращения: 12.10.2026).
4. Cisco. Configure Punt/Inject and FED Packet Capture (определение punt в CPU) [Электронный ресурс]. – URL: <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-gibraltar-16121/216746-configure-punt-inject-fed-packet-capture.html> (дата обращения: 12.10.2026).
5. MikroTik. L3 Hardware Offloading (ACL redirect-to-cpu и особенности offload) [Электронный ресурс]. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/62390319/L3%2BHardware%2BOffloading> (дата обращения: 12.10.2026).
6. MikroTik. Bridging and Switching (bridge traffic bypass firewall, use-ip-firewall) [Электронный ресурс]. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging%2Band%2BSwitching> (дата обращения: 12.10.2026).
7. IETF. RFC 826: An Ethernet Address Resolution Protocol [Электронный ресурс]. – URL: <https://datatracker.ietf.org/doc/html/rfc826> (дата обращения: 12.10.2026).
8. ALT Linux Wiki Установка и первоначальная настройка ZABBIX [Электронный ресурс]. – URL: [https://www.altlinux.org/Установка\\_и\\_первоначальная\\_настройка\\_ZABBIX](https://www.altlinux.org/Установка_и_первоначальная_настройка_ZABBIX) (дата обращения: 12.10.2026).

**References**

1. Cisco. (n.d.). *Configuring IPv4 ACLs (distinction between IP ACL and MAC ACL)*. Retrieved October 12, 2026, from [https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b\\_ie3500\\_1718-cg/configuring\\_ipv4\\_acls.html](https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b_ie3500_1718-cg/configuring_ipv4_acls.html)
2. Eltex. (n.d.). *MES series user manual 10.4.2.1*. Retrieved October 12, 2026, from [https://api.prod.eltex-co.ru/storage/upload\\_center/files/54/MES\\_Series\\_user\\_manual\\_10.4.2.1\\_en.pdf](https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf)
3. Cisco. (n.d.). *Configuring IPv4 access control lists on Catalyst 2960L (software filtering under hardware resource limitations)*. Retrieved October 12, 2026, from [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2\\_7\\_e/configuration\\_guide/sec/b\\_1527e\\_security\\_2960l\\_cg/configuring\\_ipv4\\_access\\_control\\_lists.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_7_e/configuration_guide/sec/b_1527e_security_2960l_cg/configuring_ipv4_access_control_lists.html)
4. Cisco. (n.d.). *Configure punt/inject and FED packet capture*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-gibraltar-16121/216746-configure-punt-inject-fed-packet-capture.html>
5. MikroTik. (n.d.). *L3 hardware offloading*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/62390319/L3%2BHardware%2BOffloading>
6. MikroTik. (n.d.). *Bridging and switching*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging%2Band%2BSwitching>
7. Plummer, D. C. (1982). *An Ethernet address resolution protocol (RFC 826)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc826>
8. ALT Linux Wiki. (n.d.). *Installation and initial configuration of Zabbix*. Retrieved October 12, 2026, from [https://www.altlinux.org/Установка\\_и\\_первоначальная\\_настройка\\_ZABBIX](https://www.altlinux.org/Установка_и_первоначальная_настройка_ZABBIX)

### Информация об авторах

Коваль Николай Михайлович — студент факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: nik.koval\_10@mail.ru.

Гимпель Евгений Анатольевич — студент факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; для переписки — через соавтора Н. М. Ковалья: nik.koval\_10@mail.ru.

## LABORATORY ANALYSIS OF TCP ACLS AND INTERFACE METRICS IN A NETWORK TESTBED

Koval N. M.<sup>1</sup>, Gimpel E. A.<sup>1</sup>

<sup>1</sup> Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

**Abstract.** This paper presents a teaching-oriented analysis of network configuration fragments and the authors' summary of interface measurements from a laboratory testbed. It considers Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326. The objective is to relate the commands actually shown to the limits of aggregate-counter interpretation, without treating a counter change as verified filtering of a particular traffic flow. The Cisco and Eltex configurations deny TCP between two specified hosts and then permit other IP traffic; they do not impose a general IP-packet ban. The MikroTik fragments create a bridge and add interfaces, but show neither an ACL rule nor its attachment. The authors describe SNMP monitoring in Zabbix with a sixty-second polling interval. These measurements average traffic over the interval and cannot identify protocol composition or brief peaks. The reported before-and-after load values are retained, while derived ratios are recalculated from their rounded central values. These calculations characterize summary numbers rather than the proportion of packets actually forwarded. Raw time series and the calculation of the authors' plus-or-minus quantities are unavailable, so their statistical interpretation is not established. The material supports discussion of TCP rules, interface attachment, and the distinction between configuration, aggregate observation, and evidence of a filtering effect. It does not compare vendors or establish the composition of residual load or hardware causes of differences.

**Keywords:** TCP; ACL; switch; SNMP; interface counter; laboratory testbed.

### Information about the authors

Nikolai Mikhailovich Koval — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: nik.koval\_10@mail.ru.

Evgeny Anatolyevich Gimpel — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence via co-author N. M. Koval: nik.koval\_10@mail.ru.

Колоколов С. А., Белый К. С.

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

## НАСТРОЙКА DNSSEC И УПРАВЛЕНИЯ КЛЮЧАМИ НА УЧЕБНОМ СТЕНДЕ WINDOWS SERVER

**Аннотация.** Работа описывает настройку DNSSEC и управление ключами на учебном стенде из двух виртуальных машин Windows Server. Один узел размещает авторитативную зону lab.test, второй обрабатывает запросы с настроенным перенаправлением. Представлены создание зоны, её подписание, параметры ключей и подписей, действия с доверенным ключом и ответы средств PowerShell. После подписания показан ответ с A и RRSIG при запросе с параметром DnssecOk. Этот вывод подтверждает получение DNSSEC-данных, но не удостоверяет успешную криптографическую проверку подписи и всей цепочки доверия. После повторного подписания и очистки кэша получен DNS server failure. Следующий листинг показывает файл экспортированного ключа; импорт trust anchor и успешный запрос после импорта в доступных материалах не представлены. Поэтому причина ошибки и восстановление разрешения имени не считаются установленными результатами. Отдельные кадры Wireshark иллюстрируют размеры ответов подписанной и неподписанной зон, а не среднюю производительность или серию измерений. На основе приведённых источников обсуждаются ротация KSK и ZSK, RFC 5011, NSEC3 и отсутствие конфиденциальности DNS-запросов. Практическая часть ограничена показанными командами, настройками и ответами. Работа может служить учебным разбором настройки DNSSEC и основанием для планирования последующей проверки доверия. Она не оценивает эффективность защиты от атак, доступность производственной системы или успешность всех механизмов валидации. Численные результаты времени разрешения и статистические серии не используются для выводов.

**Ключевые слова:** DNSSEC; безопасность DNS; trust anchor; Windows Server; цифровые подписи; цепочка доверия; управление ключами.

### Введение

Современные информационные системы, корпоративные сети и облачные инфраструктуры в значительной степени зависят от корректной и устойчивой работы системы доменных имён (Domain Name System, DNS). DNS выполняет критически важную функцию сопоставления символьных доменных имён с IP-адресами узлов сети, обеспечивая функционирование веб-ресурсов, почтовых сервисов, распределённых приложений и корпоративных информационных систем. Фактически DNS является одним из базовых элементов сетевой инфраструктуры, без которого невозможна стабильная работа большинства сетевых сервисов.

Однако изначальная архитектура протокола DNS разрабатывалась в условиях доверенной сетевой среды и не предусматривала встроенных механизмов криптографической защиты. Ответы DNS-серверов принимаются клиентами без проверки подлинности источника и целостности передаваемых данных. Такая модель создаёт предпосылки для реализации различных атак, среди которых наибольшую опасность представляют атаки типа cache poisoning (отравление кэша), spoofing (подмена ответов) и man-in-the-middle. В результате злоумышленник может перенаправить пользователя на поддельный ресурс, перехватить конфиденциальные данные либо нарушить работу критически важных сервисов.

В условиях роста киберугроз и увеличения числа распределённых сервисов проблема обеспечения доверия к DNS-инфраструктуре приобрела особую актуальность. Для решения данной задачи был разработан набор расширений DNSSEC (Domain Name System Security Extensions), направленный на обеспечение аутентичности и целостности DNS-ответов. В отличие от классического DNS, DNSSEC использует механизмы асимметричной криптографии, позволяющие подписывать данные зоны цифровой подписью и проверять их корректность на стороне валидирующего резолвера.

Принцип работы DNSSEC основан на публикации открытых ключей зоны (DNSKEY) и цифровых подписей (RRSIG) для наборов ресурсных записей. Валидирующий резолвер при наличии доверенного ключа (trust anchor) и соответствующей цепочки доверия проверяет подписи полученных данных. Ошибка проверки может привести к SERVFAIL; без сведений о

настройках валидатора нельзя считать любую такую ошибку подтверждением нарушения криптографической проверки [1, 2].

Несмотря на очевидные преимущества DNSSEC с точки зрения безопасности, практическое внедрение технологии связано с рядом организационных и технических сложностей. Одной из ключевых проблем является управление жизненным циклом криптографических ключей, включая их генерацию, публикацию, ротацию и обновление trust anchor на валидирующих серверах. Несогласованность ключевой информации может привести к нарушению цепочки доверия и, как следствие, к отказу разрешения доменных имён. Таким образом, DNSSEC повышает уровень защищённости DNS-инфраструктуры, но одновременно предъявляет повышенные требования к администрированию и сопровождению системы.

Объектом данного исследования являются механизмы обеспечения безопасности DNSSEC в серверной инфраструктуре на базе Windows Server. Предмет исследования — процессы подписания DNS-зоны, настройки валидирующего резолвера и управления trust anchor в условиях изолированного лабораторного стенда.

Цель работы — описать настройку DNSSEC и управление ключами на изолированном стенде Windows Server, а также проанализировать ответы DNS после повторного подписания зоны. Отдельно рассматривается гипотеза о влиянии несогласованных доверенных ключей, но её подтверждение требует данных о состоянии валидации и сравнения trust anchor.

Для достижения поставленной цели в работе решаются следующие задачи:

- проверить создание и подписание DNS-зоны, получение DNSSEC-данных и поведение службы DNS после переподписания зоны;
- описать параметры управления ключами и ограничения выводов по отдельным захватам DNS-трафика.

Практическая значимость работы состоит в демонстрации конфигурационного сценария на двух виртуальных машинах: создание подписанной зоны, получение A и RRSIG, повторное подписание и регистрация ошибки разрешения имени. Импорт обновлённого trust anchor и успешное восстановление запроса в приведённых результатах не показаны; причина ошибки остаётся гипотезой, требующей отдельной проверки.

### **Литературный обзор**

Классический DNS не предусматривает механизмов криптографической проверки подлинности и целостности ответов, что делает возможными атаки типа spoofing и cache poisoning.

DNSSEC стандартизирован в RFC 4033–4035 [1–3] и обеспечивает криптографическую защиту данных зоны посредством цифровых подписей и цепочки доверия от trust anchor.

При невозможности подтверждения подписи валидирующий резолвер возвращает ошибку (SERVFAIL), реализуя модель fail-secure [1].

Управление ключами KSK и ZSK является критическим элементом внедрения DNSSEC, поскольку нарушение синхронизации ключевой информации приводит к разрыву цепочки доверия [4].

В Windows Server поддержка DNSSEC реализована на уровне службы DNS и включает средства подписания зон, управления ключами и настройки trust anchor. Дополнительным аспектом безопасности DNSSEC является механизм authenticated denial of existence [3, 5], реализуемый с помощью записей NSEC или NSEC3 [5]. Данный механизм позволяет криптографически подтвердить отсутствие запрашиваемого имени в зоне. Однако использование NSEC без дополнительных мер может приводить к возможности перечисления имён зоны (zone walking). Для предотвращения этого эффекта применяется механизм NSEC3, использующий хеширование имён.

DNSSEC обеспечивает целостность и подлинность данных, но не гарантирует конфиденциальность DNS-запросов [6]. Для защиты канала передачи применяются технологии DNS over TLS и DNS over HTTPS [7, 8], которые не заменяют механизм криптографической валидации зоны.

Рассмотренные стандарты описывают проверку подписанных DNS-данных и построение цепочки доверия. В рамках настоящей работы на зоне lab.test представлены результаты переподписания и последующего DNS-ответа с ошибкой; причинная связь с несоответствием trust anchor требует отдельного подтверждения.

Практическая часть представляет учебный пример настройки DNSSEC в изолированной серверной среде и анализа доступных команд, сетевых кадров и сообщений службы DNS.

### Материалы и методы

Исследование механизмов безопасности DNSSEC проводилось с использованием теоретического анализа и лабораторного эксперимента. Такой подход позволил сопоставить принципы функционирования технологии DNSSEC, описанные в нормативных документах и технической литературе, с её практической реализацией в серверной среде Windows Server.

На теоретическом этапе был выполнен анализ стандартов DNSSEC (RFC 4033–4035) и документации по службе DNS в Windows Server. Особое внимание уделялось принципам формирования цифровых подписей зоны, публикации записей DNSKEY и RRSIG, построению цепочки доверия (chain of trust), а также роли trust anchor в процессе валидации DNS-ответов.

Практическая часть выполнена на двух узлах Windows Server 2025 в изолированной сети. SRV-A размещает авторитативную зону, а SRV-B обрабатывает запросы с настроенным перенаправлением для lab.test. Команды и ответы иллюстрируют конфигурацию DNSSEC; отдельный статус успешной проверки цепочки доверия в показанном выводе отсутствует.

Использованы средства администрирования DNS и PowerShell. Показаны подписание зоны, настройка trust anchor, повторное подписание и ответы на последующие запросы. Наблюдаемые ответы и ошибки рассматриваются отдельно от предполагаемой причины: наличие RRSIG и параметра -DnssecOk само по себе не является доказательством успешной валидации.

В практической части рассматриваются конфигурация DNSSEC, получение подписанных записей и представленные захваты DNS-ответов на сервере SRV-B. Отдельные кадры Wireshark иллюстрируют содержимое и размеры ответов, но не сравнительную производительность DNS-разрешения.

В рукописи не представлены итоговые временные ряды, серии из 20 ответов или результаты фильтрации выбросов. Поэтому расчёт среднего времени, среднего размера пакета и статистическая обработка не включены в доказательную часть этой работы.

### Настройка статических IP-адресов

На первом этапе эксперимента выполнена ручная настройка сетевого интерфейса обеих виртуальных машин. В свойствах протокола IPv4 на первой машине установлен статический IP-адрес 192.168.56.10, на второй - 192.168.56.11, оба адреса имеют маску подсети 255.255.255.0. В качестве предпочитаемого DNS-сервера указан локальный адрес 127.0.0.1, что соответствует дальнейшей настройке службы DNS на данном узле.

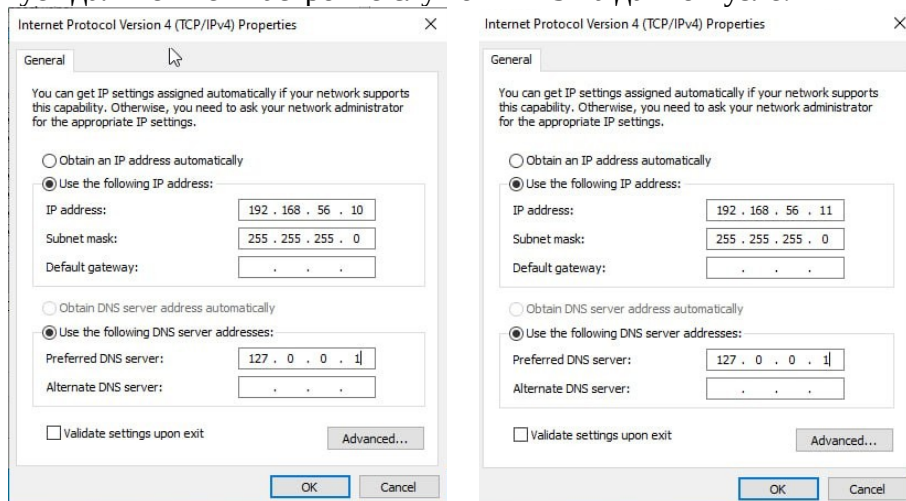


Рис. 1. Настройка статических IP-адресов на SRV-A и SRV-B

## Установка роли DNS Server

На обоих серверах показана установка роли DNS Server командой Install-WindowsFeature DNS -IncludeManagementTools. Приведённый вывод подтверждает успешную установку роли и средств администрирования.

### Листинг 1 – Установка роли DNS Server

```
PS C:\Users\Administrator> Install-WindowsFeature DNS -IncludeManagementTools
>>
Success Restart Needed Exit Code Feature Result
-----
True      No                Success    {DNS Server, Remote Server Administration ...}

PS C:\Users\Administrator> Get-WindowsFeature DNS
>>
Display Name                                Name      Install State
-----
[X] DNS Server                             DNS       Installed

PS C:\Users\Administrator>
```

### Создание зоны lab.test

На сервере выполнено создание первичной зоны lab.test с использованием Add-DnsServerPrimaryZone; полный вывод этой команды в рукописи отсутствует.

### Создание А-записи

Для узла www зоны lab.test задана А-запись с адресом 10.10.10.10 с использованием Add-DnsServerResourceRecordA. Текст команды создания записи не приведён; адрес подтверждён последующим DNS-ответом.

### Подписание DNSSEC-зоны lab.test

На SRV-A показано подписание зоны lab.test и получение записей DNSKEY и RRSIG. В выводе представлены параметры NSEC3 и признаки использования RSA/SHA256 для подписей. Часть сведений об алгоритмах и жизненном цикле ключей подтверждается выводом переподписания в листинге 5.

### Листинг 2 – Записи DNSKEY и RRSIG зоны lab.test

```
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.
Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

ZoneName ZoneType IsAutoCreated IsDsIntegrated IsReverseLookupZone
IsSigned
-----
lab.test Primary False False False
True

PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "lab.test"
-RRType DNSKEY
>> Get-DnsServerResourceRecord -ZoneName "lab.test" -RRType RRSIG
>>
HostName RecordType Type Timestamp TimeToLive RecordData
-----
@ DNSKEY 48 0 01:00:00 [ZoneKey]
[RsaSha256][23208]
@ DNSKEY 48 0 01:00:00 [ZoneKey]
[RsaSha256][28641]
@ DNSKEY 48 0 01:00:00 [SEP][ZoneKey]
[RsaSha256][59717]
@ DNSKEY 48 0 01:00:00 [SEP][ZoneKey]
```

```
[RsaSha256][20947]
@                RRSIG      46    0          01:00:00  [NS][RsaSha256]
[23208]
@                RRSIG      46    0          01:00:00  [SOA][RsaSha256]
[23208]
@                RRSIG      46    0          01:00:00  [DNSKEY]
[RsaSha256][23208]
@                RRSIG      46    0          01:00:00  [DNSKEY]
[RsaSha256][59717]
@                RRSIG      46    0          01:00:00  [NSEC3PARAM]
[RsaSha256][23208]
[hostname truncated in screenshot] RRSIG 46 0 01:00:00 [NSEC3][RsaSha256][23208]
[hostname truncated in screenshot] RRSIG 46 0 01:00:00 [NSEC3][RsaSha256][23208]
www              RRSIG      46    0          01:00:00  [A][RsaSha256]
[23208]
```

PS C:\Users\Administrator>

### Проверка типа зоны на SRV-B

На втором сервере выполнена проверка списка зон с использованием команды Get-DnsServerZone. В выводе отображается, что зона lab.test имеет тип Forwarder, что подтверждает её настройку в режиме переадресации, а не как первичной (Primary) зоны.

### Листинг 3 – Проверка типа зоны на SRV-B

```
PS C:\Users\Administrator> Get-DnsServerZone | Select-Object ZoneName, ZoneType
>>
ZoneName      ZoneType
-----
0.in-addr.arpa Primary
127.in-addr.arpa Primary
255.in-addr.arpa Primary
lab.test      Forwarder
```

### Получение DNSSEC-данных на SRV-B

На SRV-B выполнен Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk. Вывод содержит A и RRSIG: сервер вернул DNSSEC-данные по этому запросу. Параметр -DnssecOk запрашивает такие данные, но показанный вывод не сообщает результат криптографической проверки подписи или всей цепочки доверия.

### Листинг 4 – Успешный DNSSEC-ответ на SRV-B

```
Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
```

```
Name      Type TTL  Section IPAddress
----
www.lab.test A    3600 Answer  10.10.10.10
```

```
Name      : www.lab.test
QueryType  : RRSIG
TTL        : 3600
Section    : Answer
TypeCovered : A
Algorithm  : 8
LabelCount : 3
OriginalTtl : 3600
Expiration : 2/22/2026 2:28:16 PM
Signed     : 2/12/2026 1:28:16 PM
Signer     : lab.test
Signature  : {49, 82, 246, 205, ...}
```

```
Name      : .
QueryType  : OPT
TTL        : 32768
Section    : Additional
Data       : {}
```

```
PS C:\Users\Administrator>
```

### **Повторное подписание зоны lab.test**

На авторитативном сервере выполнены снятие DNSSEC-подписей и повторное подписание lab.test. Вывод команды содержит параметры новых KSK и ZSK, периоды ротации и параметры NSEC3.

### **Листинг 5 – Переподписание зоны lab.test на SRV-A**

```
PS C:\Users\Administrator> Invoke-DnsServerZoneUnsign -ZoneName "lab.test"
-Force
>> Invoke-DnsServerZoneSign -ZoneName "lab.test" -SignWithDefault -PassThru
-Verbose
>>
VERBOSE: This will reset the DNSSEC settings for the zone to defaults and sign
it.
The following parameters will be configured:
One KeySigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 2048
  Rollover Period: 755.00:00:00
One ZoneSigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 1024
  Rollover Period: 90.00:00:00
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.

Confirm
This will reset the DNSSEC settings for the zone to defaults and sign it.
The following parameters will be configured:
One KeySigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 2048
  Rollover Period: 755.00:00:00
One ZoneSigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 1024
  Rollover Period: 90.00:00:00
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.
Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

ZoneName ZoneType IsAutoCreated IsDsIntegrated IsReverseLookupZone IsSigned
-----
lab.test Primary False False False True
```

### **Проверка разрешения имени после смены ключей**

После переподписания зоны на авторитативном сервере выполнены очистка кэша и повторный запрос www.lab.test на SRV-B с параметром -DnssecOk. Получена ошибка DNS server failure (SERVFAIL). По одному этому выводу нельзя однозначно установить причину ошибки.

### **Листинг 6 – Ошибка разрешения имени на SRV-B после смены ключей**

```
PS C:\Users\Administrator> Clear-DnsServerCache -Force
>> Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
>>
Resolve-DnsName : www.lab.test : DNS server failure
```

```
At line:2 char:1
+ Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (www.lab.test:String)
[Resolve-DnsName], Win32Exception
+ FullyQualifiedErrorId :
RCODE_SERVER_FAILURE,Microsoft.DnsClient.Commands.ResolveDnsName

PS C:\Users\Administrator>
```

### Просмотр экспортированного ключа

После показанного SERVFAIL представлен файл keyset-lab.test в каталоге C:\DNSSEC. Наличие файла само по себе не подтверждает импорт trust anchor на SRV-B; команда импорта и успешный запрос после неё в доступных листингах отсутствуют.

### Листинг 7 – Проверка экспортированного файла ключа

```
PS C:\Users\Administrator> dir C:\DNSSEC
>>
Directory: C:\DNSSEC

Mode                LastWriteTime         Length Name
----                -
-a---- 2/12/2026 1:02 PM           805    keyset-lab.test
```

```
PS C:\Users\Administrator>
```

### Создание неподписанной зоны plain.test

### Анализ DNS-ответов в Wireshark

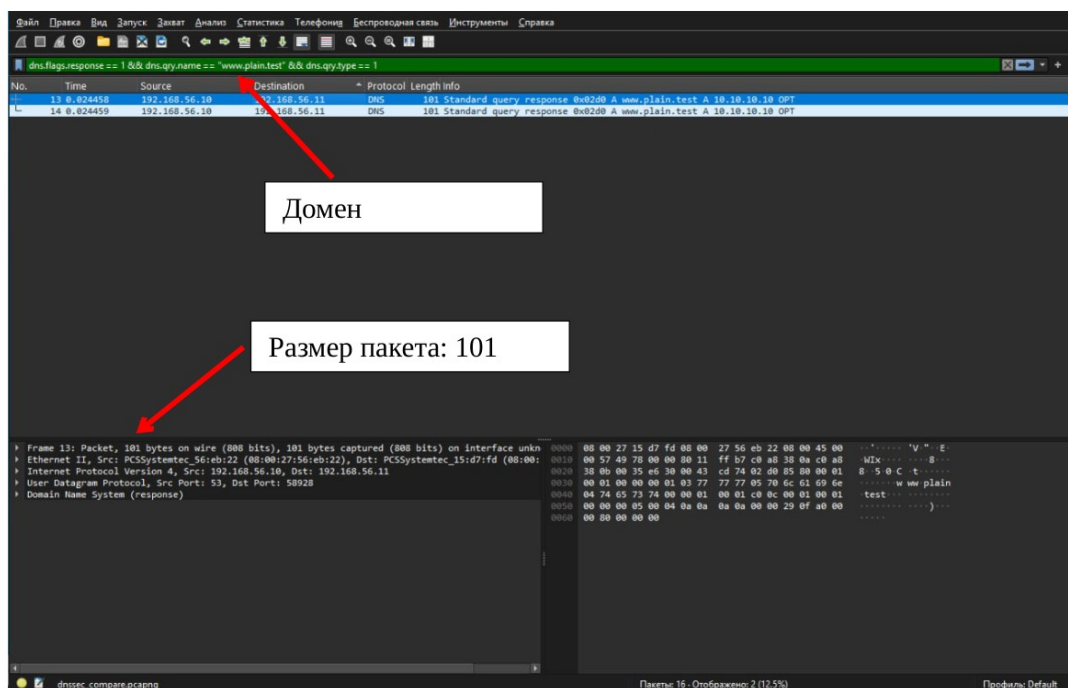


Рис. 2. DNS-ответ для www.plain.test без DNSSEC (101 байт)

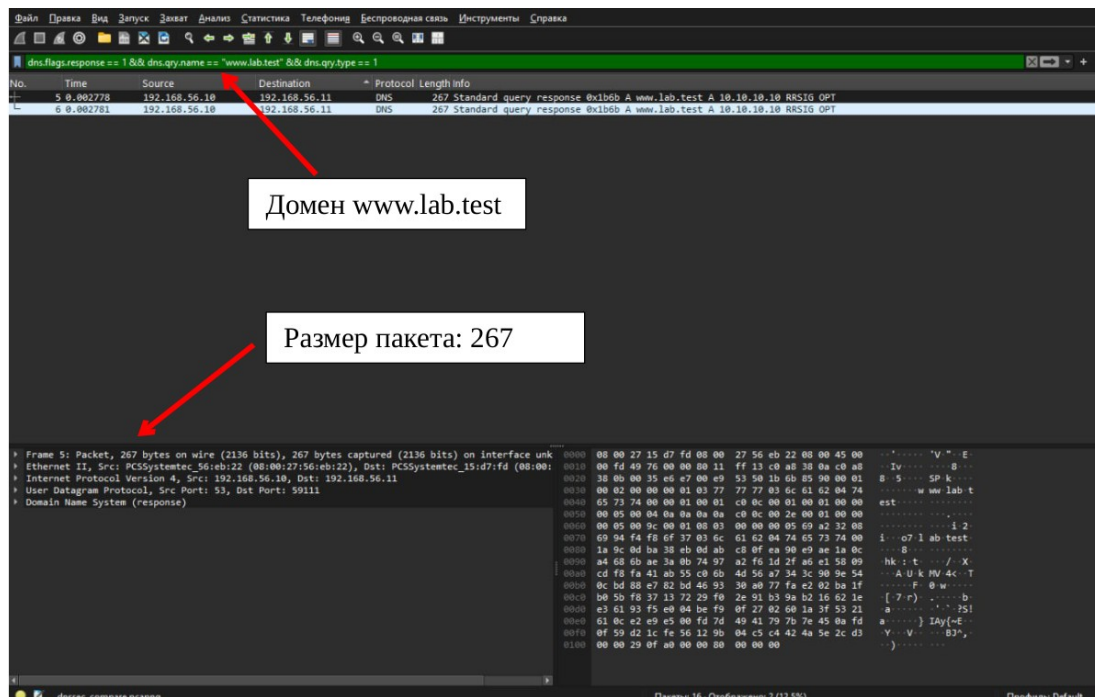


Рис. 3. DNS-ответ для www.lab.test с DNSSEC (267 байт)

## Результаты исследования

Представленные команды и ответы иллюстрируют настройку DNSSEC на двух узлах. Они не являются самостоятельной проверкой успешной валидации, эффективности защиты от атак или доступности DNS-сервиса.

В показанной конфигурации создана зона lab.test с A-записью www, разрешаемой в адрес 10.10.10.10. Отдельный вывод запроса до подписания зоны в рукописи не приведён.

После подписания зоны средствами DNSSEC произошло появление записей типов DNSKEY и RRSIG в структуре зоны. Это говорит о генерации криптографических ключей и цифровых подписей.

На SRV-B показан ответ А вместе с RRSIG по запросу с -DnssecOk. Это подтверждает получение DNSSEC-данных, но не сообщает статус проверки подписи и цепочки доверия; наличие forwarder-зоны не является самостоятельным доказательством роли валидатора.

После повторного подписания зоны и очистки кэша показан SERVFAIL. Затем приведено наличие файла экспортированного ключа. По этим листингам нельзя подтвердить импорт обновлённого trust anchor, восстановление разрешения имени или причину ошибки именно в несоответствии доверенного ключа.

В промышленной эксплуатации ключами DNSSEC часто управляют по регламентированным процедурам с поддержкой автоматической ротации при наличии соответствующей функциональности и конфигурации сервера. Успешность такой ротации в данном стенде не проверялась.

Стандарт RFC 5011 описывает механизм автоматического обновления trust anchor при соблюдении предусмотренных условий. В представленных листингах не показано, что механизм был задействован или корректно обновил доверенный ключ на SRV-B.

Показанный SERVFAIL демонстрирует отказ разрешения имени в этой последовательности команд. Без отдельного статуса валидации и сравнения ключей причина отказа не установлена; результат не оценивает снижение риска атак или все реализации DNSSEC.

Стандарты DNSSEC задают механизмы проверки подписанных DNS-данных; перечисленные ниже ограничения и сценарии не проверялись в эксперименте на lab.test и приводятся как свойства технологии по нормативным источникам:

- подмену DNS-ответов (spoofing);
- отравление кэша резолвера (cache poisoning);

- внедрение ложных ресурсных записей при перехвате трафика;
- подмену данных на промежуточных узлах сети.

Защита достигается за счёт криптографической подписи наборов записей и построения цепочки доверия от доверенного ключа верхнего уровня (trust anchor) до авторитативной зоны [1, 2, 3].

В то же время проведённый анализ показывает, что DNSSEC не обеспечивает комплексную защиту DNS-инфраструктуры и имеет ряд принципиальных ограничений.

Для иллюстрации состава DNS-ответов использованы отдельные захваты сетевого обмена в лабораторном стенде.

#### ***Анализ сетевого трафика***

В отдельных кадрах Wireshark на рисунках 2 и 3 показаны размеры двух ответов для lab.test и plain.test. Это отдельные наблюдения, а не серия измерений; по ним нельзя делать вывод о среднем времени разрешения или сравнительной производительности зон.

Следует отметить, что в реальных сетевых инфраструктурах размер DNSSEC-ответов может быть значительно больше, чем в условиях лабораторного эксперимента. Особенно это касается ответов, содержащих записи DNSKEY и полный набор криптографических подписей зоны.

Классический DNS по UDP ограничивал размер сообщения 512 байтами без EDNS. Расширение EDNS(0) позволяет объявлять больший размер полезных данных UDP; при превышении допустимого размера ответа или невозможности его передачи может использоваться TCP. Автоматический переход зависит от реализации и условий обмена.

При внедрении DNSSEC в производственных сетях необходимо учитывать возможные проблемы, связанные с фрагментацией крупных UDP-пакетов и их фильтрацией сетевыми экранами и NAT-устройствами, что может приводить к задержкам или сбоям в разрешении доменных имён.

Приведённые захваты иллюстрируют отдельные DNS-ответы в данном стенде. Оценка сравнительной производительности требует воспроизводимых повторных измерений с согласованными условиями и сохранёнными исходными данными.

Во-первых, DNSSEC не обеспечивает конфиденциальность DNS-запросов: их содержимое может быть доступно наблюдателю сетевого трафика. Это ограничение рассматривается в RFC 7626 [6]; оно не является результатом специального эксперимента на данном стенде.

Во-вторых, использование механизма authenticated denial of existence на основе записей NSEC может приводить к возможности перечисления имён зоны (zone walking), поскольку NSEC раскрывает информацию о соседних записях [3]. Для снижения данного риска применяется механизм NSEC3, основанный на хешировании имён [5], однако он не исключает полностью возможность перебора при слабых параметрах хеширования.

Authenticated denial of existence с NSEC3 рассматривается в источнике [5]. В данной рукописи не приведён вывод запроса fake.lab.test с NXDOMAIN и NSEC3, поэтому такая проверка не включена в перечень подтверждённых практических результатов.

В-третьих, DNSSEC не защищает от компрометации криптографических ключей. В случае утечки закрытого ключа KSK злоумышленник получает возможность формировать корректно подписанные, но недостоверные данные. Практики безопасного управления ключами и процедуры их ротации регламентируются отдельными рекомендациями [4], что подчёркивает необходимость организационных и технических мер защиты инфраструктуры управления ключами.

DNSSEC предназначен для проверки подлинности и целостности DNS-данных и не обеспечивает конфиденциальность запросов [2, 6]. Практическая часть этой статьи иллюстрирует конфигурацию и ответы; успешность криптографической проверки и причинная связь SERVFAIL с trust anchor отдельно не установлены.

## Заключение

На учебном стенде показаны создание и подписание зоны lab.test, настройка перенаправления DNS-запросов, повторное подписание и последующие запросы. Показанные команды и иллюстрации описывают конфигурационный сценарий, но не подтверждают полный цикл обновления trust anchor.

Криптографическая проверка DNSSEC основывается на подписях и цепочке доверия, описанных в стандартах [1–3]. Возвращённая RRSIG показывает наличие подписанных данных, но не заменяет подтверждение успешной валидации.

После повторного подписания зоны и очистки кэша показан ответ DNS server failure. Последующий листинг показывает файл экспортированного ключа, но не его импорт и не успешное разрешение имени после импорта. Поэтому восстановление DNS-разрешения и причинная атрибуция ошибки именно нарушению цепочки доверия не считаются подтверждёнными результатами.

Выводы ограничены показанными командами, конфигурацией и ответами двух виртуальных машин. Производительность, устойчивость к атакам и успешность всех криптографических проверок не оценивались. Материал может использоваться для учебного разбора настройки DNSSEC и планирования дальнейших проверок.

## Библиографический список

45. Arends R., Austein R., Larson M., Massey D., Rose S. Protocol Modifications for the DNS Security Extensions // RFC 4035. – IETF, 2005. – 52 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4035>.
46. Arends R., Austein R., Larson M., Massey D., Rose S. DNS Security Introduction and Requirements // RFC 4033. – Internet Engineering Task Force (IETF), 2005. – 21 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4033>.
47. Arends R., Austein R., Larson M., Massey D., Rose S. Resource Records for the DNS Security Extensions // RFC 4034. – IETF, 2005. – 37 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4034>.
48. Kolkman O., Mekking W. DNSSEC Operational Practices, Version 2 // RFC 6781. – IETF, 2012. – 53 с. – URL: <https://datatracker.ietf.org/doc/html/rfc6781>.
49. Laurie B., Sisson G., Arends R., Blacka D. DNSSEC Hashed Authenticated Denial of Existence (NSEC3) // RFC 5155. – IETF, 2008. – 32 с. – URL: <https://datatracker.ietf.org/doc/html/rfc5155>.
50. Bortzmeyer S. DNS Privacy Considerations // RFC 7626. – IETF, 2015. – 17 с. – URL: <https://datatracker.ietf.org/doc/html/rfc7626>.
51. Hu Z. и др. Specification for DNS over Transport Layer Security (TLS) // RFC 7858. – IETF, 2016. – URL: <https://datatracker.ietf.org/doc/html/rfc7858> (дата обращения: 17.02.2026).
52. Hoffman P., McManus P. DNS Queries over HTTPS (DoH) // RFC 8484. – IETF, 2018. – URL: <https://datatracker.ietf.org/doc/html/rfc8484> (дата обращения: 17.02.2026).

## References

53. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). Protocol modifications for the DNS Security Extensions (RFC 4035). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4035>
54. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). DNS security introduction and requirements (RFC 4033). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4033>
55. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). Resource records for the DNS Security Extensions (RFC 4034). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4034>
56. Kolkman, O., & Mekking, W. (2012). DNSSEC operational practices, version 2 (RFC 6781). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc6781>

57. Laurie, B., Sisson, G., Arends, R., & Blacka, D. (2008). DNSSEC hashed authenticated denial of existence (NSEC3) (RFC 5155). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc5155>
58. Bortzmeyer, S. (2015). DNS privacy considerations (RFC 7626). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc7626>
59. Hu, Z., et al. (2016). Specification for DNS over Transport Layer Security (TLS) (RFC 7858). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc7858>
60. Hoffman, P., & McManus, P. (2018). DNS queries over HTTPS (DoH) (RFC 8484). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc8484>

**Информация об авторах**

Колоколов С. А. — РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: kolokolovstepa@gmail.com.

Белый К. С. — РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; для корреспонденции через соавтора С. А. Колоколова: kolokolovstepa@gmail.com.

**DNSSEC CONFIGURATION AND KEY MANAGEMENT ON A WINDOWS SERVER TEACHING TESTBED**

**Kolokolov S. A., Bely K. S.**

*Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia*

**Abstract.** *This paper describes DNSSEC configuration and key management on a teaching testbed with two Windows Server virtual machines. One node hosts the authoritative lab.test zone, while the other processes queries using configured forwarding. The article presents zone creation, signing parameters, keys and signatures, trust-anchor configuration steps, and PowerShell responses. A query using DnssecOk returns A and RRSIG data after signing. This output demonstrates receipt of DNSSEC records but does not establish successful cryptographic verification of the signature or complete trust chain. A DNS server failure is displayed after re-signing and clearing the cache. The next listing shows an exported key file; importing that trust anchor and obtaining a successful query after import are not documented in the available material. Accordingly, neither the precise cause of the failure nor restored name resolution is treated as a verified result. Individual Wireshark frames illustrate response sizes for signed and unsigned zones, rather than average performance or a measurement series. Cited sources support discussion of KSK and ZSK rollover, RFC 5011, NSEC3, and the lack of DNS-query confidentiality. The practical scope is limited to the displayed commands, configurations, and responses. The material supports teaching and planning further trust-validation checks. It does not assess attack resistance, production availability, or successful operation of all validation mechanisms.*

**Keywords:** *DNSSEC; DNS security; trust anchor; Windows Server; digital signatures; chain of trust; key management.*

**Information about the authors**

Stepan A. Kolokolov — Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: kolokolovstepa@gmail.com.

Kirill S. Bely — Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence through co-author Stepan A. Kolokolov: kolokolovstepa@gmail.com.

А. А. Кудимов<sup>1</sup>, А. Д. Исаков<sup>1</sup>

<sup>1</sup> ФГАОУ ВО «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И. М. Губкина», Москва, Россия

## РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ DHCP SPOOFING (MITRE ATT&CK T1557.003) НА УРОВНЕ СЕТЕВЫХ КОММУТАТОРОВ

**Аннотация.** Представлены результаты экспериментального сравнения встроенных и доступных механизмов защиты от атаки DHCP Spoofing (MITRE ATT&CK T1557.003) на трёх управляемых коммутаторах: Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM. Атака воспроизводилась с ноутбука под управлением Kali Linux при помощи инструмента Yersinia; клиентская машина работала под управлением ALT Linux, контроль трафика выполнялся через tcpdump. Для каждой платформы применялась единая четырёхшаговая методика: базовая настройка, атака без защиты, включение штатного механизма и повторная атака. На Cisco Catalyst 2960 после включения DHCP Snooping поддельные ответы в перехвате отсутствовали, а приведённый вывод показывает статус DHCP Snooping и недоверенные порты. Отдельные значения счётчиков отброшенных пакетов в этом фрагменте не представлены. На Eltex MES1428 в использованной конфигурации и версии прошивки поддельные ответы продолжали достигать клиента, а счётчики функции оставались нулевыми; этот результат трактуется как свойство конкретной лабораторной конфигурации, а не как подтверждённый дефект устройства, и требует проверки на полной рекомендованной вендором настройке и обновлённой прошивке. На MikroTik CRS326 поддельный трафик блокировался правилом bridge filter — ручным механизмом канального уровня, отличным от нативного DHCP Snooping. Поскольку метрики платформ измерялись в разных единицах, единый числовой показатель эффективности не вводится. Предложена методика пошаговой верификации для ввода оборудования в эксплуатацию; регуляторные выводы ограничены ролью технической проверки, а не доказательства соответствия нормативным требованиям.

**Ключевые слова:** DHCP Spoofing; DHCP Snooping; MITRE ATT&CK; защита локальной сети; rogue DHCP; Yersinia.

### Введение

Протокол динамической настройки хостов (DHCP, RFC 2131 [1]) — фундаментальный элемент современных IP-сетей. Широковещательная природа обмена сообщениями Discover/Offer/Request/Ack делает его уязвимым к атаке DHCP Spoofing: злоумышленник разворачивает в сегменте поддельный DHCP-сервер (rogue server) и, отвечая быстрее легитимного, навязывает клиентам вредоносные сетевые параметры — шлюз и DNS. В результате трафик жертвы может проходить через узел атакующего, реализуя атаку «противник посередине» (AiTM). В классификации MITRE ATT&CK данная техника обозначена как T1557.003 [2]; механизм эксплуатации, включая DHCP Starvation и использование Option 121 для перенаправления VPN-трафика, рассмотрен в работах [3, 4]. Смежные угрозы канального уровня — ARP-spoofing и ARP Cache Poisoning — исследованы в [5, 6].

Угроза актуальна для российских корпоративных сетей. Нормативные документы ФСТЭК России (Приказ № 117 [7], пришедший на смену Приказу № 17, и Приказ № 239 [8]) предусматривают принятие мер по защите информации, в том числе от сетевых атак канального уровня. Свободно распространяемый инструмент Yersinia [9] позволяет воспроизвести атаку DHCP Spoofing за несколько минут.

Выбор платформ обусловлен структурой российского рынка. Cisco Catalyst 2960 широко представлен в унаследованных корпоративных инфраструктурах. Eltex MES1428 — отечественный управляемый коммутатор, применяемый в рамках политики импортозамещения [10]; закупки иностранного телекоммуникационного оборудования для ряда заказчиков ограничены. MikroTik CRS326-24G-2S+RM — доступная платформа, распространённая в сетях малого и среднего бизнеса. Вопросы конфигурации оборудования различных вендоров рассмотрены в [11]. Таким образом, исследование охватывает три характерных класса оборудования.

Актуальность L2-сегмента как недооценённого вектора угроз подтверждают работы по переполнению CAM-таблицы [12], VLAN ID Enumeration [13] и ARP Cache Poisoning [6].

**Объект, предмет, цель и задачи исследования**

Объект исследования: коммутируемая сетевая инфраструктура предприятия на базе оборудования различных производителей (зарубежного, отечественного и платформенного класса).

Предмет исследования: эффективность доступных механизмов защиты от DHCP Spoofing на уровне управляемых L2-коммутаторов.

Цель исследования: оценить в единой стендовой среде поведение встроенных и доступных механизмов защиты от атаки DHCP Spoofing на коммутаторах Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM путём натурного эксперимента.

Задачи исследования:

- настроить тестовый стенд: создать VLAN 10 на каждом коммутаторе, подключить клиентскую и атакующую машины;
- воспроизвести атаку DHCP Spoofing и зафиксировать поведение клиента и перехваченный трафик;
- активировать доступный механизм защиты (DHCP Snooping на Cisco и Eltex; Bridge Filter на MikroTik) и повторить атаку;
- провести сравнительный анализ наблюдаемых результатов и сформулировать рекомендации.

Научная новизна. Впервые в единой стендовой среде выполнено сравнительное экспериментальное наблюдение поведения доступных механизмов защиты от DHCP Spoofing на оборудовании трёх классов: зарубежного вендора (Cisco), отечественного производителя в контексте импортозамещения (Eltex) и доступной программно-аппаратной платформы (MikroTik). Для одной из конфигураций Eltex зафиксировано расхождение между статусом включённой функции и её наблюдаемым действием, что обосновывает необходимость обязательной практической верификации.

Практическая значимость. Результаты адресованы администраторам корпоративных сетей и специалистам по информационной безопасности, в том числе при переходе на отечественное оборудование. Предложенная четырёхшаговая методика верификации применима при вводе коммутаторов в эксплуатацию и при аудите; её результаты следует рассматривать как элемент технической проверки, а не как доказательство соответствия нормативным требованиям.

**Методы исследования**

В работе применены следующие методы.

Экспериментально-исследовательский метод — воспроизведение атаки DHCP Spoofing на реальном оборудовании по единому протоколу для каждой платформы; контроль трафика через tcpdump; фиксация поддельных пакетов и диагностических счётчиков до и после включения защиты.

Аналитический метод — изучение технической документации [14, 15, 16], классификатора MITRE ATT&CK [2], нормативных документов ФСТЭК [7, 8] и академических публикаций [3, 4, 17].

Метод сравнительного анализа — сопоставление трёх платформ по единому набору качественных критериев: класс механизма защиты, наличие поддельного ответа в перехвате до и после защиты, состояние диагностики, итоговый адрес клиента. Поведение фиксировалось качественно — по наличию или отсутствию поддельного ответа (DHCP Offer/ACK от постороннего сервера) в перехвате; единый числовой показатель эффективности не рассчитывался.

**Литературный обзор**

Защита локальных сетей от атак канального уровня широко освещена в литературе. В [2] техника DHCP Spoofing классифицируется по матрице MITRE ATT&CK как T1557.003, а в [3] систематически рассматриваются DHCP Starvation, rogue-серверы, атаки воспроизведения и

эксплойт TunnelVision в контексте нарушения триады CIA. Традиционным механизмом противодействия является DHCP Snooping, принцип работы которого отражён в документации вендоров [14, 15, 16]; при этом исследования [17] указывают, что наличия функции недостаточно без корректного разделения доверенных и недоверенных портов и дополнения механизмом Port Security. Смежные угрозы — ARP-spoofing и ARP Cache Poisoning — рассматриваются в [5, 6]: в [5] предложен метод обнаружения на основе анализа ARP-таблиц, в [6] — моделирование методов защиты. Технике CAM table overflow посвящена работа [12], VLAN ID Enumeration — [13]. Актуальность CVE-2024-3661 (TunnelVision [4]) подтверждает, что угроза DHCP Spoofing продолжает эволюционировать. В отличие от перечисленных работ, настоящее исследование сосредоточено на сравнении доступных механизмов защиты в реальном стенде без применения IDS/IPS.

## Методика эксперимента

### Тестовый стенд

Экспериментальная база включала:

- три управляемых коммутатора: Cisco Catalyst 2960 (IOS 15.0(2)SE9), Eltex MES1428 (SW 10.4.3), MikroTik CRS326-24G-2S+RM (RouterOS 7.22 stable);
- компьютер-клиент на ALT Linux (интерфейс enp1s0, DHCP-клиент NetworkManager);
- ноутбук-атакующий на Kali Linux с инструментом Yersinia (режим DHCP) [9];
- легитимный DHCP-сервер — лабораторный маршрутизатор 10.19.103.1, пул 10.19.103.0/24.

Клиентская и атакующая машины подключались к разным портам одного коммутатора в составе VLAN 10. Контроль трафика выполнялся командой tcpdump -i enp1s0 -n -v port 67 or port 68 на клиентской машине; поддельные ответы идентифицировались по сообщениям DHCP Offer/ACK с адреса-источника 192.168.10.99.

### Протокол тестирования

На каждом коммутаторе последовательно выполнялись четыре шага (рис. 1):

- базовая настройка: создание VLAN 10, назначение портов клиента и атакующего в режим access;
- атака без защиты: запуск атаки, переподключение клиента, фиксация полученного адреса и поддельных пакетов в tcpdump;
- активация защиты: включение DHCP Snooping (Cisco, Eltex) или настройка Bridge Filter (MikroTik);
- повторная атака: переподключение клиента, анализ tcpdump и счётчиков диагностики.

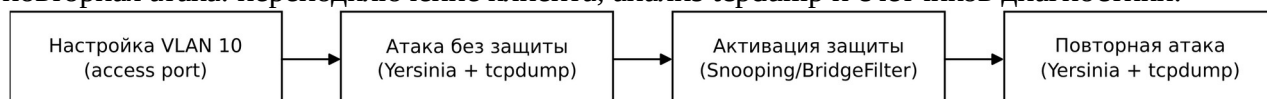


Рис. 1. Блок-схема методики тестирования (единый протокол для каждой платформы)

## Результаты исследования

### Cisco Catalyst 2960

Базовая настройка VLAN 10 и портов доступа приведена в листинге 1.

#### Листинг 1 – Настройка VLAN 10 и портов на Cisco Catalyst 2960

```
C-2960(config)# vlan 10
C-2960(config-vlan)# name TEST_VLAN
C-2960(config-vlan)# exit
C-2960(config)# interface range FastEthernet0/5-6
C-2960(config-if-range)# switchport mode access
C-2960(config-if-range)# switchport access vlan 10
C-2960(config-if-range)# no shutdown
```

При атаке без защиты клиент получил адрес 192.168.10.100 от поддельного сервера. В перехвате tcpdump за цикл подключения наряду с ответом легитимного сервера виден поддельный ответ (DHCP ACK) от источника 192.168.10.99, навязывающий адрес 192.168.10.100, шлюз 192.168.10.99 и домен test.lab (листинг 2).

**Листинг 2 – Перехват tcpdump при атаке без защиты на Cisco (фрагмент)**

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  Server-IP 192.168.10.99
  DHCP-Message (53): ACK
  Default-Gateway (3): 192.168.10.99
  Domain-Name (15): "test.lab"
```

После включения DHCP Snooping (листинг 3) все порты по умолчанию являются недоверенными; порт восходящей связи к легитимному DHCP-серверу переведён в доверенный режим командой `ip dhcp snooping trust`, что обеспечивает прохождение легитимных ответов.

**Листинг 3 – Включение DHCP Snooping и назначение доверенного uplink-порта на Cisco Catalyst 2960**

```
C-2960(config)# ip dhcp snooping
C-2960(config)# ip dhcp snooping vlan 10
C-2960(config)# interface GigabitEthernet0/1
C-2960(config-if)# ip dhcp snooping trust
```

При повторной атаке поддельный ответ в перехвате отсутствовал: клиент получил корректный адрес 10.19.103.222 из легитимного пула (листинг 4). В листинге 4 показаны недоверенные порты FastEthernet0/5 и FastEthernet0/6, но не приведено значение счётчика отброшенных DHCP-пакетов. Поэтому отсутствие поддельного ответа подтверждается приведённым фрагментом перехвата, а не отдельным измерением числа отброшенных сообщений.

**Листинг 4 – Состояние DHCP Snooping и перехват после включения защиты на Cisco (фрагмент)**

```
C-2960# show ip dhcp snooping
DHCP snooping is operational on following VLANs: 10
Insertion of option 82 is enabled
Interface      Trusted    Allow option    Rate limit (pps)
FastEthernet0/5  no        no              15
FastEthernet0/6  no        no              15
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
```

**Eltex MES1428**

Базовая настройка VLAN 10 и порта доступа приведена в листинге 5.

**Листинг 5 – Настройка VLAN 10 на Eltex MES1428**

```
console(config)# vlan 10
console(config-vlan)# name TEST_VLAN
console(config-vlan)# exit
console(config)# interface gigabitethernet 1/0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# no shutdown
```

При атаке без защиты клиент принял вредоносные параметры (адрес 192.168.10.100, шлюз 192.168.10.99); в перехвате за цикл подключения присутствует поддельный ответ от 192.168.10.99 (листинг 6).

### Листинг 6 – Перехват tcpdump при атаке без защиты на Eltex (фрагмент)

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  DHCP-Message (53): ACK
  Default-Gateway (3): 192.168.10.99
  Domain-Name (15): "test.lab"
```

После включения DHCP Snooping (листинг 7) команда `show ip dhcp snooping` отображала для VLAN 10 статус Enabled.

### Листинг 7 – Включение DHCP Snooping на Eltex MES1428

```
console(config)# ip dhcp snooping
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
```

Однако при повторной атаке поддельный ответ от 192.168.10.99 по-прежнему достигал клиента, а все счётчики функции (Number of Incoming Discovers, Requests, Transmitted Offers, Acks, Total Number Of Discards и другие) оставались нулевыми (листинг 8). Это означает, что в использованной конфигурации и версии прошивки механизм не обрабатывал DHCP-трафик.

### Листинг 8 – Диагностика DHCP Snooping и перехват после включения защиты на Eltex (фрагмент)

```
console# show ip dhcp snooping
DHCP Snooping Vlan information
VLAN                               : 10
Snooping status                    : Enabled
Number of Incoming Discovers       : 0
Number of Incoming Requests        : 0
Number of Transmitted Offers       : 0
Number of Transmitted Acks         : 0
Total Number Of Discards           : 0
Number of MAC Discards             : 0
Number of Server Discards          : 0
Number of Option Discards          : 0
# tcpdump -i enp1s0 -n -v port 67 or port 68
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  Server-ID (54): 192.168.10.99
  Domain-Name (15): "test.lab"
```

Важно отметить ограниченность вывода. Процедура настройки для серии MES14xx/24xx дополнительно предполагает активацию VLAN (`vlan active`) и явное назначение порта к легитимному серверу доверенным (`port-security-state trusted, set port uplink`); в данном запуске полный рекомендованный вендором набор команд не применялся. Нулевые счётчики согласуются как с гипотезой о неполной конфигурации, так и с гипотезой об отсутствии обработки функции в данной версии прошивки. Поэтому результат ограничивается наблюдаемым поведением конкретной лабораторной конфигурации и не является подтверждением дефекта устройства; для окончательного вывода необходима проверка на полной рекомендованной конфигурации, обновлённой прошивке и в нескольких циклах DHCP.

### *MikroTik CRS326-24G-2S+RM*

Базовая настройка VLAN 10 на программном мосте приведена в листинге 9.

### Листинг 9 – Настройка VLAN 10 на MikroTik CRS326

```
/interface bridge add name=bridge-local
/interface bridge vlan add bridge=bridge-local vlan-ids=10
/interface bridge port add interface=ether3 bridge=bridge-local pvid=10 \
  frame-types=admit-only-untagged-and-priority-tagged
/interface bridge port add interface=ether5 bridge=bridge-local pvid=10 \
```

```
frame-types=admit-only-untagged-and-priority-tagged
```

Без явной защиты подмена также возможна: поддельный сервер отвечает наравне с легитимным, и клиент может принять его параметры. Наличие в сети быстрого легитимного сервера не является надёжной защитой и не гарантирует корректную конфигурацию клиента.

Важно подчеркнуть класс применённого механизма. В отличие от Cisco и Eltex, где использован встроенный DHCP Snooping, на MikroTik применено правило bridge filter — ручная фильтрация канального уровня (листинг 10), отличная от нативного DHCP Snooping RouterOS.

#### Листинг 10 – Настройка Bridge Filter на MikroTik CRS326

```
/interface bridge filter add chain=forward action=drop \
mac-protocol=ip ip-protocol=udp src-port=67 in-interface=ether3
```

После применения правила в перехвате наблюдались только легитимные серверы (в разных циклах — 10.19.103.1 и 10.19.103.27), поддельные ответы отсутствовали, клиент получал корректные настройки, а таблица маршрутизации указывала шлюз 10.19.103.1 (листинг 11).

#### Листинг 11 – Перехват tcpdump и маршрут клиента после включения защиты на MikroTik (фрагмент)

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
# ip route show
default via 10.19.103.1 dev enp1s0 proto dhcp src 10.19.103.222 metric 100
10.19.103.0/24 dev enp1s0 proto kernel scope link src 10.19.103.222 metric 100
```

Следует учитывать, что в использованном сценарии поддельные ответы передавались широкоэвентально и не появлялись в представленном захвате после применения bridge filter. Фактический путь обработки пакетов через CPU отдельно не измерялся; для одноадресного трафика между аппаратно-ускоренными (offload) портами CRS326 правило bridge filter может не применяться. Нативный DHCP Snooping RouterOS (доступен начиная с версии 6.43, с аппаратной поддержкой на коммутаторах серии CRS3xx) в данной работе не исследовался.

#### Сравнительный анализ

Таблица 1 – Сравнительная характеристика наблюдаемого поведения механизмов защиты от DHCP Spoofing

| Критерий                                     | Cisco Catalyst 2960                                        | Eltex MES1428                | MikroTik CRS326                                    | Примечание                                                |
|----------------------------------------------|------------------------------------------------------------|------------------------------|----------------------------------------------------|-----------------------------------------------------------|
| Версия ПО                                    | IOS 15.0(2)SE9                                             | SW 10.4.3                    | RouterOS 7.22                                      | —                                                         |
| Класс механизма защиты                       | DHCP Snooping (встроенный)                                 | DHCP Snooping (встроенный)   | Bridge Filter (ручной L2-фильтр)                   | MikroTik — иной класс механизма                           |
| Поддельные ответы в tcpdump после защиты     | Отсутствуют                                                | Присутствуют                 | Отсутствуют                                        | —                                                         |
| Блокировка поддельного трафика (качественно) | Поддельные ответы не выявлены в показанном захвате         | Не наблюдалась               | Поддельные ответы не выявлены в показанном захвате | Единый числовой показатель не вводится                    |
| Счётчики диагностики                         | Показаны недоверенные порты; чисел отброшенных пакетов нет | Все счётчики = 0             | Н/д (иной механизм)                                | Нулевые счётчики Eltex требуют проверки полноты настройки |
| Итоговый адрес клиента                       | Легитимный 10.19.103.x                                     | Легитимный или rogue (гонка) | Легитимный 10.19.103.x                             | —                                                         |

| Критерий             | Cisco Catalyst 2960                     | Eltex MES1428                                                        | MikroTik CRS326                                            | Примечание                                 |
|----------------------|-----------------------------------------|----------------------------------------------------------------------|------------------------------------------------------------|--------------------------------------------|
| Поведение без защиты | Поддельный АСК присутствует             | Поддельный АСК присутствует                                          | Подмена возможна                                           | Фиксация качественная, за цикл подключения |
| Рекомендация         | DHCP Snooping; trusted только на uplink | Проверить полную конфигурацию (vlan active, trusted-порт) и прошивку | Bridge Filter или нативный DHCP Snooping (RouterOS ≥ 6.43) | —                                          |

Ключевое наблюдение касается Eltex MES1428: при статусе Enabled и активной конфигурации ip dhcp snooping поддельные ответы продолжали достигать клиента, а счётчики диагностики оставались нулевыми. Как отмечено выше, этот результат ограничивается конкретной конфигурацией и прошивкой и не переносится на устройство в целом.

Для MikroTik без явной защиты подмена возможна — поддельный сервер отвечает наравне с легитимным; наличие быстрого легитимного сервера не является надёжным механизмом защиты. После применения bridge filter поддельные ответы в перехвате отсутствовали. При этом применённое правило bridge filter относится к иному классу механизмов, чем DHCP Snooping, что необходимо учитывать при сопоставлении.

Сопоставление в таблице 1 выполнено по качественным критериям (наличие поддельного ответа в перехвате, состояние диагностики, итоговый адрес клиента); единый числовой показатель эффективности не вводится, поскольку поведение фиксировалось качественно, а сравниваемые механизмы относятся к разным классам. Введение унифицированных количественных метрик вынесено в направления дальнейших исследований.

### Обсуждение и ограничения работы

Версионная и конфигурационная зависимость. Эксперимент проведён на конкретных версиях прошивок и в ограниченных конфигурациях. Результат по Eltex, в частности, может измениться при полной рекомендованной вендором настройке и в более новых версиях ПО. Рекомендуется повторять проверку после каждого обновления.

Единственная модель каждого вендора. Cisco Catalyst 2960 представляет платформу IOS; более новые Cisco IOS-XE или серии CBS могут иметь иное поведение. Другие модели Eltex (MES23xx, MES33xx) требуют отдельной проверки.

Изолированный стенд. В реальных сетях на результаты влияют протоколы spanning tree, режимы транкинга, взаимодействие DHCP Snooping с DAI и IP Source Guard.

Единичные наблюдения. Приведённые перехваты соответствуют единичным циклам подключения; поведение фиксировалось качественно — по наличию или отсутствию поддельного ответа. Дисперсия по сериям запусков не изучалась. Для статистически значимых и количественно сопоставимых результатов рекомендуется единый протокол и не менее 30 независимых попыток на каждой платформе с едиными метриками: доля заблокированных Offer/АСК, доля защищённых сессий, время получения легитимного адреса и число ложных срабатываний.

Разные классы механизмов. Cisco и Eltex используют встроенный DHCP Snooping, MikroTik — ручной bridge filter; прямое ранжирование платформ по «эффективности» некорректно без приведения к единому механизму и единой метрике.

### Заключение

Проведённое исследование позволяет сформулировать следующие обобщающие выводы.

- Атака DHCP Spoofing (T1557.003) воспроизводима на всех трёх платформах при отсутствии явной защиты: поддельный сервер отвечает наравне с легитимным. В том числе для MikroTik это опровергает предположение о его «естественной» защищённости.

- Наличие функции в документации и её статус «включено» не являются достаточным основанием считать устройство защищённым: на Eltex MES1428 в использованной конфигурации при статусе Enabled поддельные ответы не блокировались, а счётчики оставались нулевыми; этот результат ограничен конкретной конфигурацией и прошивкой и требует верификации на полной рекомендованной настройке.
- Cisco Catalyst 2960 заблокировал поддельные ответы штатным DHCP Snooping; MikroTik CRS326 заблокировал их правилом bridge filter — механизмом иного класса. Любое решение необходимо проверять практически: анализом tcpdump и диагностических счётчиков.
- Предложенная четырёхшаговая методика с фиксацией поддельного трафика и счётчиков до и после включения защиты применима как чек-лист технической верификации при вводе коммутационного оборудования в эксплуатацию; её результаты не заменяют аудит соответствия нормативным требованиям.

Направления дальнейших исследований: проверка Eltex на полной рекомендованной конфигурации и обновлённых прошивках; статистически значимые серии ( $N \geq 30$ ) с едиными метриками на всех платформах; исследование нативного DHCP Snooping RouterOS на чипах серии CRS3xx; оценка совместной работы DHCP Snooping и DAI; защита от DHCP Starvation и ARP Spoofing.

#### **Библиографический список**

1. RFC 2131. Dynamic Host Configuration Protocol / R. Droms. – IETF, 1997. – URL: <https://datatracker.ietf.org/doc/html/rfc2131> (дата обращения: 15.05.2026). – Текст : электронный.
2. Adversary-in-the-Middle: DHCP Spoofing, Sub-technique T1557.003 / MITRE ATT&CK. – URL: <https://attack.mitre.org/techniques/T1557/003/> (дата обращения: 15.05.2026). – Текст : электронный.
3. Dilworth, R. Dark Deceptions in DHCP: Dismantling Network Defenses / R. Dilworth. – Mississippi State University, 2025. – (Препринт arXiv:2502.10646). – URL: <https://arxiv.org/abs/2502.10646> (дата обращения: 15.05.2026). – Текст : электронный.
4. Moratti, L. TunnelVision (CVE-2024-3661): How Attackers Can Decloak Routing-Based VPNs / L. Moratti, D. Crouce. – Leviathan Security Group, 2024. – URL: <https://www.leviathansecurity.com/blog/tunnelvision> (дата обращения: 15.05.2026). – Текст : электронный.
5. Разработка и экспериментальная апробация метода обнаружения ARP-spoofing атак на основе анализа сетевого трафика и ARP-таблиц / Г. Рамазанова [и др.]. – 2025. – URL: <https://cyberleninka.ru/article/n/razrabotka-i-eksperimentalnaya-aprobatziya-metoda-obnaruzheniya-arp-spoofing-atak-na-osnove-analiza-setevogo-trafika-i-arp-tablits> (дата обращения: 15.05.2026). – Текст : электронный.
6. ARP Cache Poisoning. Методы защиты. – 2024. – URL: <https://cyberleninka.ru/article/n/arp-cache-poisoning-metody-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
7. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий и государственных учреждений : Приказ ФСТЭК России от 11.04.2025 № 117 : зарегистрирован в Минюсте России 16.06.2025, рег. № 82619 : вступил в силу 01.03.2026. – Москва : ФСТЭК России, 2025. – Текст : непосредственный.
8. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25.12.2017 № 239. – Москва : ФСТЭК России, 2017. – Текст : непосредственный.
9. Berrueta, D. Yersinia: A Framework for Layer 2 Attacks / D. Berrueta, J. Andres. – Black Hat Europe, 2005. – URL: [https://www.blackhat.com/presentations/bh-europe-05/BH\\_EU\\_05-Berrueta\\_Andres/BH\\_EU\\_05-Berrueta\\_Andres.pdf](https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05-Berrueta_Andres.pdf) (дата обращения: 15.05.2026). – Текст : электронный.

10. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EсоRouter 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. – Текст : непосредственный.
11. Сравнение процесса конфигурации маршрутизации между локальными сетями VLAN с использованием оборудования различных вендоров. – 2024. – URL: <https://cyberleninka.ru/article/n/sravnenie-protssessa-konfiguratsii-marshrutizatsii-mezhdu-lokalnymi-setyami-vlan-s-ispolzovaniem-oborudovaniya-razlichnyh-vendorov> (дата обращения: 15.05.2026). – Текст : электронный.
12. Ермолин, Ф. С. Атака CAM-table overflow. Методы защиты / Ф. С. Ермолин, Д. М. Монтрель, А. Р. Саблин. – 2025. – URL: <https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
13. Стрельцов, Д. С. VLAN ID Enumeration. Методы защиты / Д. С. Стрельцов, Е. А. Бутенко. – 2024. – URL: <https://cyberleninka.ru/article/n/vlan-id-enumeration-metody-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
14. Configuring DHCP Features : Catalyst 2960 Software Configuration Guide, 12.2(55)SE / Cisco Systems. – URL: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swdhcp82.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swdhcp82.html) (дата обращения: 15.05.2026). – Текст : электронный.
15. MES Series User Manual 10.4.2.1 / Eltex Enterprise. – URL: [https://api.prod.eltex-co.ru/storage/upload\\_center/files/54/MES\\_Series\\_user\\_manual\\_10.4.2.1\\_en.pdf](https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf) (дата обращения: 15.05.2026). – Текст : электронный.
16. Bridging and Switching: DHCP Snooping : RouterOS Documentation / MikroTik. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching> (дата обращения: 15.05.2026). – Текст : электронный.
17. AbdulGhaffar, A. An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures / A. AbdulGhaffar, S. K. Paul, A. Matrawy // 2023 Biennial Symposium on Communications (BSC). – IEEE, 2023. – P. 119–124. – URL: <https://ieeexplore.ieee.org/document/10201458> (дата обращения: 15.05.2026). – Текст : электронный.

## References

1. Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. IETF. <https://datatracker.ietf.org/doc/html/rfc2131>
2. MITRE ATT&CK. (n.d.). Adversary-in-the-middle: DHCP spoofing (Sub-technique T1557.003). Retrieved May 15, 2026, from <https://attack.mitre.org/techniques/T1557/003/>
3. Dilworth, R. (2025). Dark deceptions in DHCP: Dismantling network defenses (arXiv:2502.10646). arXiv. <https://arxiv.org/abs/2502.10646>
4. Moratti, L., & Crouce, D. (2024). TunnelVision (CVE-2024-3661): How attackers can decloak routing-based VPNs. Leviathan Security Group. <https://www.leviathansecurity.com/blog/tunnelvision>
5. Ramazanova, G., et al. (2025). Razrabotka i eksperimentalnaya aprobatsiya metoda obnaruzheniya ARP-spoofing atak na osnove analiza setevogo trafika i ARP-tablits [Development and experimental validation of an ARP-spoofing detection method based on network traffic and ARP table analysis]. KiberLeninka. <https://cyberleninka.ru/article/n/razrabotka-i-eksperimentalnaya-aprobatsiya-metoda-obnaruzheniya-arp-spoofing-atak-na-osnove-analiza-setevogo-trafika-i-arp-tablits>
6. ARP cache poisoning. Metody zashchity [ARP cache poisoning: Protection methods]. (2024). KiberLeninka. <https://cyberleninka.ru/article/n/arp-cache-poisoning-metody-zaschity>
7. Federal Service for Technical and Export Control. (2025). Ob utverzhdenii Trebovaniy o zashchite informatsii, sodержashcheysya v gosudarstvennykh informatsionnykh sistemakh [On approval

- of the requirements for information protection in state information systems] (Order No. 117, April 11, 2025; in force March 1, 2026). FSTEC of Russia.
8. Federal Service for Technical and Export Control. (2017). Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob'yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii [On approval of the requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation] (Order No. 239, December 25, 2017). FSTEC of Russia.
  9. Berrueta, D., & Andres, J. (2005). Yersinia: A framework for Layer 2 attacks [Conference presentation]. Black Hat Europe. [https://www.blackhat.com/presentations/bh-europe-05/BH\\_EU\\_05-Berrueta\\_Andres/BH\\_EU\\_05-Berrueta\\_Andres.pdf](https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05-Berrueta_Andres.pdf)
  10. Uymin, A. G., & Tolmachev, I. M. (2025). Primenenie otechestvennogo setevogo oborudovaniya Eltex i EcoRouter v ramkakh spetsialnosti 09.02.06 «Setevoe i sistemnoe administrirovanie». Voprosy importozameshcheniya i podgotovki kvalifitsirovannykh kadrov v setevom oborudovanii [Application of domestic Eltex and EcoRouter network equipment within specialty 09.02.06 “Network and system administration”: Import substitution and training of qualified personnel]. Avtomatizatsiya i informatizatsiya TEK, (11), 58–62.
  11. Sravnenie protsessa konfiguratsii marshrutizatsii mezhdu lokalnymi setyami VLAN s ispolzovaniem oborudovaniya razlichnykh vendorov [Comparison of inter-VLAN routing configuration using equipment from different vendors]. (2024). KiberLeninka. <https://cyberleninka.ru/article/n/sravnenie-protsessa-konfiguratsii-marshrutizatsii-mezhdu-lokalnymi-setyami-vlan-s-ispolzovaniem-oborudovaniya-razlichnykh-vendorov>
  12. Ermolin, F. S., Montrel, D. M., & Sablin, A. R. (2025). Ataka CAM-table overflow. Metody zashchity [CAM-table overflow attack: Protection methods]. KiberLeninka. <https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zashchity>
  13. Streltsov, D. S., & Butenko, E. A. (2024). VLAN ID enumeration. Metody zashchity [VLAN ID enumeration: Protection methods]. KiberLeninka. <https://cyberleninka.ru/article/n/vlan-id-enumeration-metody-zashchity>
  14. Cisco Systems. (n.d.). Configuring DHCP features: Catalyst 2960 software configuration guide, 12.2(55)SE. Retrieved May 15, 2026, from [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swdhcp82.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swdhcp82.html)
  15. Eltex Enterprise. (n.d.). MES series user manual 10.4.2.1. Retrieved May 15, 2026, from [https://api.prod.eltex-co.ru/storage/upload\\_center/files/54/MES\\_Series\\_user\\_manual\\_10.4.2.1\\_en.pdf](https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf)
  16. MikroTik. (n.d.). Bridging and switching: DHCP snooping. RouterOS documentation. Retrieved May 15, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>
  17. AbdulGhaffar, A., Paul, S. K., & Matrawy, A. (2023). An analysis of DHCP vulnerabilities, attacks, and countermeasures. In 2023 Biennial Symposium on Communications (BSC) (pp. 119–124). IEEE. <https://ieeexplore.ieee.org/document/10201458>

#### **Информация об авторах**

Кудимов Артём Андреевич — студент группы КИ-25-01, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия, e-mail: kudimov95@yandex.ru.

Искаков Артём Денисович — студент группы КИ-25-01, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия, e-mail: artemiskakov25@gmail.com.

# IMPLEMENTATION AND EFFECTIVENESS ANALYSIS OF DHCP SPOOFING PROTECTION (MITRE ATT&CK T1557.003) AT THE NETWORK SWITCH LEVEL

Kudimov A. A.<sup>1</sup>, Iskakov A. D.<sup>1</sup>

<sup>1</sup> Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

**Abstract.** The paper reports an experimental comparison of the built-in and available mechanisms for protection against the DHCP Spoofing attack (MITRE ATT&CK T1557.003) on three managed switches: Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326-24G-2S+RM. The attack was reproduced from a Kali Linux laptop using the Yersinia tool; the client ran ALT Linux, and traffic was monitored with tcpdump. A uniform four-step procedure was applied to each platform: baseline configuration, attack without protection, enabling the available protection, and a repeated attack. On the Cisco Catalyst 2960, after DHCP Snooping was enabled, rogue replies were absent from the capture and the displayed diagnostics identified untrusted ports; separate discard-counter values were not shown. On the Eltex MES1428, in the configuration and firmware used, rogue replies kept reaching the client while the feature counters remained zero; this result is interpreted as a property of the specific laboratory configuration rather than a confirmed device defect, and it requires verification on the full vendor-recommended configuration and updated firmware. On the MikroTik CRS326, rogue traffic was blocked by a bridge filter rule, a manual link-layer mechanism distinct from native DHCP Snooping. Because the platform metrics were measured in different units, no single efficiency figure is introduced. A step-by-step verification procedure for commissioning is proposed; regulatory conclusions are limited to the role of technical verification rather than proof of regulatory compliance.

**Keywords:** DHCP spoofing; DHCP snooping; MITRE ATT&CK; LAN security; rogue DHCP; Yersinia.

## Information about the authors

Kudimov Artem Andreevich — student, group KI-25-01, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia, e-mail: kudimov95@yandex.ru.

Iskakov Artem Denisovich — student, group KI-25-01, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia, e-mail: artemiskakov25@gmail.com.

А. А. Кязымов<sup>1</sup>, А. А. Терешонок<sup>1</sup><sup>1</sup> ФГАОУ ВО «Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия**ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ IGMPV2 И СРАВНИТЕЛЬНАЯ ОЦЕНКА МЕТОДОВ ЗАЩИТЫ НА L2+ КОММУТАТОРАХ РАЗЛИЧНЫХ ВЕНДОРОВ**

**Аннотация.** Работа посвящена экспериментальному анализу атаки поддельным сообщением IGMP Leave и способов защиты multicast-групп на коммутаторах Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. В статье описаны базовые принципы IGMPv2 и IGMP snooping, которые позволяют коммутатору поддерживать сведения о подписчиках и направлять multicast-трафик на нужные порты. В эксперименте измерялось время удаления порта клиента из таблицы группы после получения Leave-сообщения: для Cisco указано около 2–3 с, для Eltex — менее 1 с, для MikroTik — около 10 с. Далее авторы рассматривают статическую привязку multicast-группы к порту, ограничение числа групп, фильтрацию IGMP ACL и настройку Last Member Query Interval и Count. В таблице приведены наблюдаемые интервалы реакции для нескольких сочетаний таймера и количества запросов; эти данные показывают компромисс между скоростью удаления подписчика и устойчивостью к ложным сообщениям. Статья отдельно отмечает эксплуатационные ограничения статических привязок и обсуждает переход к IGMPv3. Результаты относятся к трем проверенным моделям и указанным параметрам стенда, поэтому не описывают все реализации протокола. Материал формулирует практические варианты снижения риска потери multicast-доставки и подчеркивает необходимость проверять настройки на используемой модели коммутатора. Оценка отражает описанный стенд и выбранные значения таймеров, а не полный набор реализаций IGMP snooping. Результаты ограничены описанной лабораторной конфигурацией. Адреса группы в статической команде и иллюстрирующем выводе различаются, поэтому показанный вывод не подтверждает результат именно этой команды.

**Ключевые слова:** IGMPv2, IGMP snooping, multicast, L2+ коммутаторы, сетевая безопасность, атака, защита.

**Введение**

С развитием технологий групповой передачи данных, таких как IP-телевидение, видеоконференции, онлайн-трансляции и системы оповещения, возрастают требования к эффективности и безопасности доставки трафика множеству получателей. Протокол IGMP версии 2, описанный в RFC 2236 [1], является основным протоколом управления членством в multicast-группах в сетях IPv4. Однако его архитектура, разработанная в эпоху доверительных сетей, содержит ряд уязвимостей, позволяющих злоумышленнику нарушать доступность сервисов или перехватывать трафик. Особую актуальность вопросы защиты IGMPv2 приобретают на L2+ устройствах – коммутаторах, поддерживающих функции уровня 2 и расширенные возможности уровня 3, такие как IGMP snooping. IGMP snooping позволяет коммутатору анализировать IGMP-сообщения и оптимизировать рассылку multicast-трафика только на те порты, где есть подписчики, что снижает нагрузку на сеть. Однако само наличие механизма анализа создаёт поверхность для атак: злоумышленник в том же широковещательном домене может отправлять поддельные IGMP-пакеты, заставляя коммутатор исключать легитимных получателей из группы и тем самым нарушая доставку данных.

Проблема защиты IGMPv2 на L2+ устройствах становится особенно важной в корпоративных и провайдерских сетях, где multicast-сервисы играют критическую роль, а безопасность должна обеспечиваться без существенного усложнения конфигурации и потери производительности. Несмотря на наличие версии IGMPv3 с поддержкой фильтрации multicast-источников, значительная часть оборудования до сих пор эксплуатируется с поддержкой IGMPv2, а многие приложения ориентированы именно на эту версию протокола. Поэтому исследование уязвимостей и разработка методов защиты актуальны как для теоретического изучения, так и для практического применения в реальных условиях, что подтверждается современными разработками в области передачи multicast-трафика [2] и обзорами атак на канальном уровне [3].

**Объект исследования:** сетевые инфраструктуры, использующие multicast-трафик и L2+

коммутаторы с поддержкой IGMP snooping.

**Предмет исследования:** методы защиты от атак, основанных на подделке управляющих сообщений IGMPv2, включая подмену IGMP Leave и IGMP Report.

**Цель исследования:** анализ уязвимостей протокола IGMPv2 на L2+ устройствах, экспериментальная демонстрация атаки и разработка рекомендаций по обеспечению безопасности multicast-трафика.

### **Теоретические основы IGMPv2 и IGMP snooping**

#### ***RFC 2236 (IGMPv2)***

Стандарт RFC 2236 [1] определяет версию 2 протокола IGMP, используемую для управления групповой рассылкой в IPv4-сетях. Он описывает три типа сообщений: Membership Query, Membership Report и Leave Group. Уязвимость протокола заключается в отсутствии механизмов аутентификации и проверки подлинности источника: любой узел в сегменте L2 может отправить поддельное сообщение от имени другого узла, что приводит к несанкционированному изменению состояния multicast-подписок.

#### ***RFC 4541 (IGMP Snooping)***

Документ RFC 4541 [4] описывает рекомендации по реализации IGMP snooping в коммутаторах. Эта технология позволяет L2-устройствам перехватывать IGMP-пакеты между хостами и маршрутизаторами и на их основе строить таблицы, чтобы multicast-трафик доставлялся только заинтересованным портам. В RFC 4541 также рассматриваются вопросы безопасности, в частности, необходимость защиты от поддельных сообщений, однако конкретные механизмы защиты оставлены на усмотрение производителей. Это приводит к различиям в реализации и потенциальным уязвимостям.

#### ***Механизмы защиты на L2+ устройствах***

Современные L2+ коммутаторы поддерживают различные настройки управления multicast-трафиком. В руководствах Cisco [5], Eltex [6] и MikroTik [7] описаны статические привязки multicast-групп к портам, параметры IGMP snooping, Immediate-leave и фильтрация групп. IGMPv3 поддерживает фильтрацию по источникам, включая Source-Specific Multicast, но не обеспечивает самостоятельную аутентификацию отправителя IGMP-сообщения [8]. Эффективность перечисленных мер зависит от модели и конфигурации; в данной статье экспериментально проверялась атака поддельным IGMP Leave в сценарии IGMPv2.

#### ***Multicast-группы и IGMP-технологии***

Multicast-группой называется логическое объединение сетевых узлов, заинтересованных в получении одного и того же потока данных. Трафик, направляемый на групповой адрес, доставляется только тем устройствам, которые явно выразили желание его получать с помощью протокола IGMP. В отличие от широковещательной рассылки, multicast позволяет экономить пропускную способность и ресурсы конечных узлов, так как пакеты копируются только на те порты коммутатора, за которыми есть подписчики. Это достигается благодаря технологии IGMP snooping, реализуемой на L2+ коммутаторах. Коммутатор анализирует IGMP-сообщения, перехватывая их между хостом и маршрутизатором, и на основе этой информации строит таблицу пересылки multicast-трафика. Таким образом, кадры для определённой группы направляются только в порты, где имеются активные получатели, что существенно снижает нагрузку на сеть и повышает её производительность.

#### **Применение IGMP snooping даёт следующие преимущества:**

1. Гибкость развёртывания multicast-сервисов — получатели могут находиться в любом месте сети, независимо от физического расположения, и получать необходимый трафик без необходимости статической настройки.
2. Оптимизация трафика — multicast-пакеты не рассылаются во все порты, а доставляются только подписчикам, что экономит полосу пропускания и уменьшает нагрузку на оборудование.
3. Ограничение распространения трафика — IGMP snooping направляет multicast-поток на порты, где зарегистрированы подписчики. Сам по себе этот механизм не аутентифицирует отправителей IGMP-сообщений; для контроля доступа требуются

дополнительные средства защиты.

### **Диапазоны multicast-адресов**

Адресное пространство IPv4 для multicast определено в диапазоне 224.0.0.0/4. Внутри него выделяются несколько поддиапазонов:

1. Локальные адреса используются для протоколов маршрутизации и управления сетью. Пакеты с такими адресами не должны пересылаться за пределы локального сегмента.
2. Глобальные адреса могут использоваться для любых multicast-приложений в масштабах сети или интернета.
3. Административно-ограниченные предназначены для использования внутри домена или организации, аналогично частным IP-адресам. Именно из этого диапазона часто выбираются адреса для корпоративных multicast-сервисов.

### **Порты коммутатора в контексте IGMP snooping**

В зависимости от роли в multicast-рассылке порты L2+ коммутатора можно классифицировать следующим образом:

1. Порты, подключенные к multicast-маршрутизаторам — на них коммутатор ожидает IGMP-запросы и пересылает multicast-трафик от источников. Такие порты могут быть определены статически администратором или динамически обнаружены при получении IGMP-запросов.
2. Порты, подключенные к получателям — на них подключены хосты, отправившие IGMP-отчёты о присоединении к группе. Коммутатор пересылает трафик группы только на эти порты.
3. Порты с включённым IGMP filtering — административно ограничивается максимальное количество групп, к которым может присоединиться узел за портом, или блокируются определённые группы. Это эффективный фактор защиты от атак исчерпания ресурсов.
4. Статические multicast-группы — администратор может вручную привязать multicast-группу к порту, что гарантирует доставку трафика даже при отсутствии IGMP-отчётов и исключает влияние поддельных Leave-сообщений.

### **Поведение по умолчанию (без IGMP snooping)**

Если на коммутаторе не включён IGMP snooping, multicast-трафик обрабатывается как широковещательный: кадры, направленные на групповой MAC-адрес, рассылаются во все порты VLAN, за исключением порта, с которого они пришли. Это приводит к неоправданной загрузке сети и создаёт угрозу перехвата данных — любой узел в том же VLAN может принимать multicast-потoki, даже не подписываясь на них. Включение IGMP snooping переводит коммутатор в режим интеллектуальной фильтрации, что не только повышает эффективность, но и создаёт основу для внедрения политик безопасности.

### **Атаки на протокол IGMPv2**

1. Подделка IGMP Leave. Данная атака заключается в отправке поддельного сообщения о выходе из группы от имени легитимного клиента. Коммутатор с включённым IGMP snooping, получив такой пакет, может исключить порт жертвы из списка получателей multicast-трафика, что приведёт к прекращению доставки потока. Успех атаки зависит от наличия активного IGMP Querier и настроек таймеров. При использовании функции Immediate-leave порт удаляется немедленно, что делает атаку особенно эффективной.
2. Подделка IGMP Report. Злоумышленник может отправлять ложные отчёты о присоединении к группе, заставляя коммутатор пересылать multicast-трафик на свой порт. Это позволяет несанкционированно получать данные, а также создавать нагрузку на сеть, имитируя множество подписчиков. В некоторых случаях можно подменить Report таким образом, чтобы "перехватить" поток, заставив коммутатор исключить других получателей.
3. Атака на IGMP Querier. Если в сети отсутствует легитимный Querier или его роль может быть перехвачена, злоумышленник может начать отправлять свои Query-пакеты, становясь фактически управляющим устройством. Это позволяет манипулировать процессом опроса и, например, преждевременно удалять клиентов из групп. На

большинстве L2+ коммутаторов выбор Queriera осуществляется на основе наименьшего IP-адреса, что создаёт возможность для перехвата роли при наличии доступа к сети.

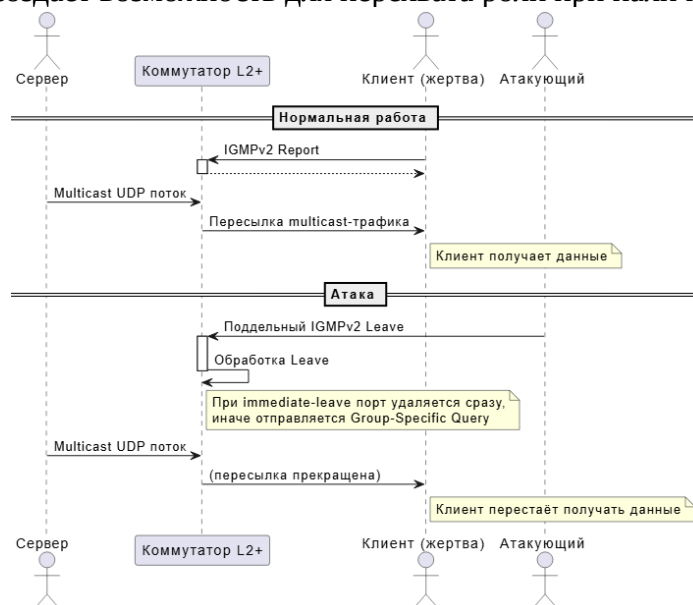


Рис. 1. Схема атаки с поддельным сообщением IGMP Leave

## Материалы и методы

### Проверка поддельного IGMP Leave на Cisco Catalyst 2960

#### Гипотеза эксперимента

Если на L2+ коммутаторе с включённым IGMP snooping не применены дополнительные факторы защиты, злоумышленник, находящийся в том же VLAN, может отправить поддельное IGMP Leave-сообщение от имени легитимного клиента и временно или полностью прекратить доставку multicast-трафика этому клиенту.

#### Условия проведения эксперимента:

Все эксперименты проводились в изолированном лабораторном стенде, исключая влияние фонового трафика. Коммутатор и устройства (сервер, клиент, атакующий) были соединены напрямую патч-кордами, без использования промежуточных коммутаторов или маршрутизаторов. Электропитание оборудования осуществлялось через стабилизаторы напряжения для исключения сбоев, связанных с нестабильностью питания. Дополнительный сетевой трафик отсутствовал, все неиспользуемые порты коммутатора были отключены.

#### Методика эксперимента:

1. К коммутатору подключаются три ПК: сервер, клиент и атакующий.
2. На коммутаторе включается IGMP snooping, настраивается IGMP Querier и статический mrouter-порт для сервера. Клиент подписывается на группу динамически.
3. Запускается multicast-поток с сервера, клиент подписывается на группу с помощью IGMP-отчёта.
4. На клиенте наблюдалось непрерывное воспроизведение видео, подтверждающее успешную подписку на multicast-группу.
5. Производится захват трафика с помощью Wireshark на ПК атакующего.
6. Атакующий запускает Python-скрипт, отправляющий IGMP Leave-пакет от имени клиента.
7. Сразу после отправки поддельного IGMP Leave-пакета воспроизведение видео на клиенте прервалось, что свидетельствует о нарушении доставки трафика.
8. Анализируется изменение состояния multicast-подписки на коммутаторе и прекращение приёма потока на клиенте.

#### Порядок эксперимента:

Используется коммутатор Cisco Catalyst 2960 Series с заводскими настройками, на котором предварительно активирован IGMP snooping для VLAN 1, назначен IP-адрес

интерфейсу VLAN 1 для выполнения роли IGMP Querier, а порт сервера статически определён как mrouter-порт (руководство по настройке [5]). ПК сервера имеет IP-адрес 10.10.10.1, клиента – 10.10.10.2, атакующего – 10.10.10.3. Все ПК подключены к портам коммутатора Fa0/11, Fa0/15 и Fa0/17 соответственно.

Перед началом атаки проверяется наличие динамической подписки клиента. Для этого на клиенте запускается скрипт-приёмник multicast, который отправляет IGMPv2 Report и начинает принимать поток. На коммутаторе команда show ip igmp snooping groups отображает группу 239.255.255.250 с портами Fa0/11 и Fa0/15. Захват трафика в Wireshark на атакующем ПК показывает IGMP-отчёты и UDP-пакеты потока.

#### Листинг 1 – Таблица IGMP-групп на коммутаторе до начала атаки

| Vlan | Group           | Type | Version | Port List      |
|------|-----------------|------|---------|----------------|
| ---- | -----           | ---- | -----   | -----          |
| 1    | 239.255.255.250 | igmp | v2      | Fa0/11, Fa0/15 |

Далее атакующий запускает скрипт igmp\_attack\_work.py, который отправляет IGMP Leave-пакет от имени клиента.

Сразу после отправки пакета на коммутаторе выполняется повторная проверка таблицы групп. Порт клиента Fa0/15 исчезает из списка получателей, что подтверждает успешную обработку Leave-сообщения.

| No.   | Time          | Source         | Destination            | Protocol | Length | Info                                   |
|-------|---------------|----------------|------------------------|----------|--------|----------------------------------------|
| 27471 | 294.215979675 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27472 | 296.216506093 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27473 | 297.489492599 | 10.10.10.2     | 224.0.0.2              | IGMPv2   | 42     | Leave Group 239.255.255.250            |
| 27474 | 298.222149100 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27475 | 300.230010447 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27476 | 302.235248360 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27477 | 303.912730131 | Cisco_35:57:83 | Cisco_35:57:83         | LOOP     | 60     | Reply                                  |
| 27478 | 304.240242947 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27479 | 306.247558761 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27480 | 308.253024463 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27481 | 310.262260146 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27482 | 312.268011193 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |
| 27483 | 313.925664884 | Cisco_35:57:83 | Cisco_35:57:83         | LOOP     | 60     | Reply                                  |
| 27484 | 315.000000000 | Cisco_35:57:83 | Nearest-Customer-Br... | STP      | 68     | Conf. Root = 32768/10/24:01:c7:35:5... |

| No.   | Time          | Source     | Destination | Protocol | Length | Info                        |
|-------|---------------|------------|-------------|----------|--------|-----------------------------|
| 27473 | 297.489492599 | 10.10.10.2 | 224.0.0.2   | IGMPv2   | 42     | Leave Group 239.255.255.250 |

| No.   | Time          | Source     | Destination | Protocol | Length | Info                        |
|-------|---------------|------------|-------------|----------|--------|-----------------------------|
| 27473 | 297.489492599 | 10.10.10.2 | 224.0.0.2   | IGMPv2   | 42     | Leave Group 239.255.255.250 |

Рис. 2. Захват пакета IGMPv2 в Wireshark

#### Листинг 2 – Таблица IGMP-групп после атаки

```
Switch#show ip igmp snooping groups
```

| Vlan | Group           | Type | Version | Port List |
|------|-----------------|------|---------|-----------|
| ---- | -----           | ---- | -----   | -----     |
| 1    | 239.255.255.250 | igmp | v2      | Fa0/11    |

Switch#

На стороне клиента приём UDP-пакетов, имитирующих видеопоток, прекращается, что свидетельствует о нарушении доставки multicast-трафика. Через некоторое время подписка может восстановиться, однако сам факт успешного временного отключения демонстрирует уязвимость протокола.

В испытанном стенде с IGMP snooping и активным Querier отправка поддельного IGMPv2 Leave приводила к нарушению multicast-связности. IGMPv2 не предусматривает встроенной аутентификации сообщений [1], поэтому узел в сегменте может влиять на состояние подписок. Статические привязки групп и ограничения по портам могут использоваться как меры снижения риска, но их действие проверялось только в указанной конфигурации. IGMPv3 позволяет фильтровать multicast-источники, однако не аутентифицирует отправителя Leave-сообщения; для защиты управления сообщениями нужен отдельный механизм. Испытания IGMPv3 в этой работе не проводились [8].

#### Валидация факторов защиты

Для эмпирической проверки эффективности предложенных в теоретической части методов защиты был проведён дополнительный эксперимент на том же лабораторном стенде с использованием коммутатора Cisco Catalyst 2960. После успешной демонстрации атаки поддельным IGMP Leave на незащищённой конфигурации была применена и протестирована

статическая привязка multicast-группы.

В тексте приведена команда `ip igmp snooping vlan 1 static 239.255.255.250 interface FastEthernet0/15` для статической привязки порта. В следующем листинге показана запись `type user` для другой группы — 239.255.1.1. Эти адреса различаются, поэтому показанный вывод не подтверждает результат именно приведённой команды; он иллюстрирует статическую запись в таблице IGMP-групп.

### Листинг 3 – Таблица IGMP-групп после применения факторов защиты

Building configuration...

[OK]

Switch#show ip igmp snooping groups

| Vlan | Group       | Type | Version | Port List      |
|------|-------------|------|---------|----------------|
| ---- | -----       | ---- | -----   | -----          |
| 1    | 239.255.1.1 | user | v2      | Fa0/11, Fa0/15 |

Switch#

Авторы сообщают, что при повторной отправке поддельного IGMPv2 Leave порт Fa0/15 остался в таблице и видеопоток не прервался. Это наблюдение относится к показанной Cisco-конфигурации. Различие адресов группы в команде и выводе ограничивает воспроизводимость этого эпизода; из него нельзя заключить о полном предотвращении таких атак во всех конфигурациях.

Статическая привязка рассматривается как вариант сохранения членства порта независимо от динамических сообщений. Её применимость к конкретному multicast-потoku следует проверять на используемой модели и с согласованными адресами группы; универсальная эффективность в этой работе не установлена.

### Сопоставление реакции Cisco, Eltex и MikroTik на поддельное IGMP Leave

#### Описание эксперимента:

Целью эксперимента являлась практическая демонстрация уязвимости протокола IGMPv2 к атаке поддельным Leave-сообщением, а также сравнительный анализ реакции на эту атаку коммутаторов трёх различных производителей: Cisco Systems (модель Catalyst 2960), MikroTik (модель CRS326-24G-2S+RM) и Eltex (модель MES1428). [5–7] Все устройства относятся к классу L2+ и поддерживают функционал IGMP snooping, что позволяет им анализировать IGMP-трафик и оптимизировать multicast-рассылку.

#### Гипотеза эксперимента:

Предполагалось, что при идентичных базовых настройках реакция на поддельное IGMP Leave-сообщение будет различаться в зависимости от производителя из-за особенностей реализации протокола, используемых таймеров и наличия дополнительных защитных механизмов.

#### Условия проведения эксперимента:

Все эксперименты проводились в изолированном лабораторном стенде, исключаяющем влияние фонового трафика. Коммутаторы и устройства (сервер, клиент, атакующий) были соединены напрямую патч-кордами, без использования промежуточных коммутаторов или маршрутизаторов. Электропитание оборудования осуществлялось через стабилизаторы напряжения для исключения сбоев, связанных с нестабильностью питания. Дополнительный сетевой трафик отсутствовал, все неиспользуемые порты коммутатора были отключены.

#### Методика эксперимента:

Для каждого коммутатора стенд собирался независимо по единой схеме:

1. К коммутатору подключались три устройства: сервер – источник multicast-потока, клиент – легитимный получатель; атакующий – источник поддельных сообщений.
2. На коммутаторе выполнялась минимально необходимая конфигурация: активировался IGMP snooping для VLAN 1, интерфейсу VLAN 1 назначался IP-адрес, включался IGMP Querier, порт сервера статически обозначался как mrouter-порт.
3. На сервере запускался скрипт, генерирующий UDP-пакеты в multicast-группу 239.255.255.250:1234.
4. На клиенте наблюдалось непрерывное воспроизведение видео, подтверждающее

успешную подписку на multicast-группу.

5. На атакующем устройстве запускался Python-скрипт, использующий библиотеку Scapy для отправки IGMPv2 Leave-пакета от имени клиента на адрес всех маршрутизаторов 224.0.0.2.
6. Сразу после отправки поддельного IGMP Leave-пакета воспроизведение видео на клиенте прервалось, что свидетельствует о нарушении доставки трафика.
7. Для каждого коммутатора замерялось время от отправки первого Leave-пакета до исчезновения порта клиента из таблицы IGMP-групп и до фактического прекращения приёма данных клиентом.

#### Контрольные замеры:

Авторы сообщают о контрольных наблюдениях легитимного Leave и интервалах истечения членства без Leave в пределах 260–300 с. Первичные журналы этих прогонов в статье не представлены. Поэтому заявленное совпадение с реакцией на поддельный Leave рассматривается как авторское наблюдение, а не доказательство отсутствия аномалий или соответствия всем настройкам по умолчанию.

#### Порядок эксперимента:

Для каждого исследуемого коммутатора собирался идентичный стенд: к устройству подключались три ПК – сервер-источник multicast-потока, клиент-получатель и атакующий. На коммутаторе активировался IGMP snooping для VLAN 1, интерфейсу VLAN 1 назначался IP-адрес 10.10.10.254, включался IGMP Querier, а порт сервера статически определялся как mrouter-порт. Сервер генерировал UDP-пакеты в группу 239.255.255.250:1234, клиент запускал скрипт-приёмник, отправляющий IGMPv2 Report и выводящий полученные данные. Корректность подписки проверялась командой show ip igmp snooping groups. Атакующий с помощью Python-скрипта на базе библиотеки Scapy отправлял IGMPv2 Leave-пакет с подменённым IP-адресом источника на адрес всех маршрутизаторов 224.0.0.2. Для захвата трафика использовался Wireshark, запущенный на атакующем ПК с предварительно настроенным зеркалированием порта клиента. Целью являлась фиксация момента отправки поддельного Leave-пакета и наблюдение за прекращением приёма multicast-трафика на клиенте, а также сравнение времени реакции исследуемых коммутаторов.

Таблица 1 – Время реакции на поддельное сообщение IGMP Leave

| Производитель | Модель        | Время реакции    |
|---------------|---------------|------------------|
| Cisco         | Catalyst 2960 | около 2-3 секунд |
| Eltex         | MES1428       | меньше 1 секунды |
| MikroTik      | CRS326        | около 10 секунд  |

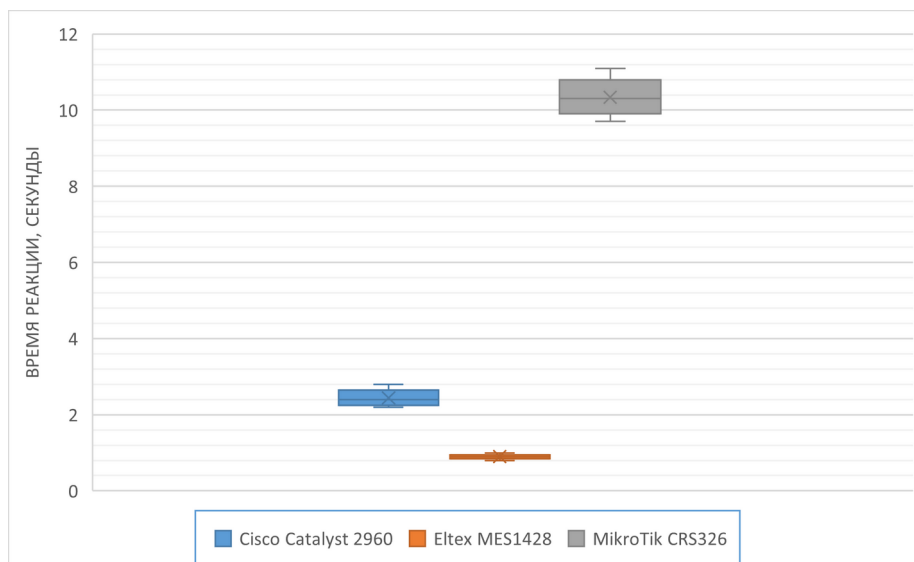


Рис. 3. Авторские наблюдения времени реакции коммутаторов на IGMP Leave

## Результаты и обсуждение

### Анализ наблюдаемых интервалов реакции

Ниже рассматриваются возможные объяснения различий авторских сводных интервалов. Путь аппаратной и программной обработки, загрузка CPU и фактические значения всех таймеров отдельно не измерялись, поэтому причинная интерпретация остаётся гипотезой.

61. Для Eltex MES1428 авторы указали реакцию менее 1 с. Это значение относится к выбранному стенду. Настройки IGMP snooping рассматриваются в документации [6], но данное наблюдение не устанавливает включение Immediate-leave по умолчанию, роль ASIC или сравнительную уязвимость платформы.
62. Для MikroTik CRS326 указано около 10 с. Настройки IGMP snooping описаны в источнике [7]. Из показанного интервала нельзя определить долю программной обработки, значения таймеров по умолчанию или строгое соответствие конкретной реализации всем рекомендациям RFC 4541.
63. Для Cisco Catalyst 2960 указано около 2–3 с. Документация [5] может использоваться при проверке параметров группы и запросов. В статье не показано отдельное измерение аппаратного ускорения; поэтому оно не считается установленной причиной отличия от других моделей.

### Масштабируемость атаки

В работе не проводились нагрузочные испытания с множественными поддельными сообщениями. Поэтому реакцию устройств на интенсивный поток IGMP-пакетов, загрузку CPU и пределы масштабирования по этим результатам оценить нельзя; это требует отдельного контролируемого эксперимента.

Следует отметить, что данное исследование было сфокусировано исключительно на атаке подделкой IGMP Leave, как на наиболее наглядном способе нарушения multicast-связности. Однако, протокол IGMPv2 уязвим и для других векторов, в частности подделки IGMP Report и атаки на IGMP Querier. Проведение экспериментов с этими типами атак требует отдельной методики и выходит за рамки данной работы, но их важность подчёркивает необходимость комплексного подхода к защите.

### Зависимость времени реакции от параметров IGMP snooping

В таблице 2 приведён авторский пример изменения last-member-query-interval и last-member-query-count на Cisco Catalyst 2960. Он не является сравнительным анализом всех возможностей регулирования таймеров на трёх платформах. Настройки других моделей и версий следует проверять по соответствующей документации; уникальная гибкость Cisco и фиксированность параметров Eltex в этой работе не установлены.

Таблица 2 – Наблюдаемое время реакции при изменении параметров опроса

| last-member-query-interval<br>(миллисекунды) | last-member-query-count<br>(количество) | Время реакции<br>(секунды) |
|----------------------------------------------|-----------------------------------------|----------------------------|
| 500                                          | 2                                       | 1,0-1,5                    |
| 1000                                         | 2                                       | 2,0-3,0                    |
| 2000                                         | 2                                       | 4,0-5,0                    |
| 1000                                         | 3                                       | 3,0-4,0                    |
| 500                                          | 3                                       | 1,5-2,0                    |

Для приведённых значений в таблице 2 авторы предлагают приближённую зависимость времени реакции от интервала и числа запросов (формула 1). В формуле  $t$  — время реакции (с);  $I$  — интервал Last Member Query (с);  $C$  — число запросов. Поправка 0,5 входит в авторское приближение; его точность за пределами приведённых комбинаций отдельно не оценивалась.

$$t \approx I \times (C + 0.5) \quad (1)$$

В испытаниях на Cisco Catalyst 2960 наблюдаемое время реакции изменялось вместе с настроенными параметрами таймеров. Эти результаты относятся только к Cisco и не подтверждают линейную зависимость на других платформах:

#### **Варианты настройки защиты IGMPv2 для трёх платформ**

Ниже представлена таблица, сравнивающая основные команды для конфигурации механизмов защиты IGMPv2 на трёх исследуемых платформах: Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. [5–7]

Таблица 3 – Примеры настройки защитных функций IGMPv2 на коммутаторах

| Действие                                         | CISCO                                                                           | ELTEX                                                                          | MIKROTIK                                                                                                                    |
|--------------------------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Включение IGMP snooping глобально                | ip igmp snooping                                                                | ip igmp snooping                                                               | /interface bridge set [find name=bridge1] igmp-snooping=yes                                                                 |
| Включение IGMP snooping для конкретного VLAN     | ip igmp snooping vlan 1                                                         | ip igmp snooping vlan 1                                                        | Настраивается через bridge VLAN; snooping работает для всех VLAN, включённых в bridge                                       |
| Настройка IGMP Querier                           | ip igmp snooping querier vlan 1                                                 | ip igmp snooping querier vlan 1                                                | /interface bridge set [find] igmp-querier=yes                                                                               |
| Назначение IP-адреса интерфейсу VLAN для Querier | interface vlan 1<br>ip address 10.10.10.254<br>255.255.255.0<br>no shutdown     | interface vlan 1<br>ip address 10.10.10.254<br>255.255.255.0                   | /interface vlan add interface=bridge1<br>name=vlan1 vlan-id=1<br>/ip address add address=10.10.10.254/24<br>interface=vlan1 |
| Включение Immediate-Leave                        | ip igmp snooping vlan 1 immediate-leave                                         | ip igmp snooping vlan 1 immediate-leave                                        | /interface bridge set [find] igmp-fast-leave=yes                                                                            |
| Статическая привязка multicast-группы к порту    | ip igmp snooping vlan 1 static<br>239.255.255.250<br>interface FastEthernet0/15 | ip igmp snooping vlan 1 static<br>239.255.255.250<br>interface ethernet 1/0/15 | /interface bridge mdb add bridge=bridge1<br>group=239.255.255.250 interface=ether1                                          |

| Действие                                           | CISCO                                                                                                                                 | ELTEX                                                                                                                                | MIKROTIK                                                                                                               |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Ограничение максимального количества групп на порт | interface<br>FastEthernet0/15<br>ip igmp limit 5                                                                                      | interface ethernet<br>1/0/15<br>ip igmp max-groups 5                                                                                 | /interface bridge port set [find<br>interface=ether1] igmp-group-limit=5                                               |
| Фильтрация IGMP-пакета с помощью ACL               | access-list 10 deny<br>239.255.255.250<br>access-list 10 permit<br>any<br>interface<br>FastEthernet0/15<br>ip igmp access-group<br>10 | access-list 10 deny<br>239.255.255.250<br>access-list 10 permit<br>any<br>interface ethernet<br>1/0/15<br>ip igmp access-group<br>10 | /ip firewall filter add chain=forward<br>action=drop protocol=igmp dst-<br>address=239.255.255.250 in-interface=ether1 |
| Настройка таймера Last Member Query Interval       | ip igmp snooping vlan 1<br>last-member-query-<br>interval 500                                                                         | ip igmp snooping vlan<br>1 last-member-query-<br>interval 500                                                                        | /interface bridge set [find] igmp-last-<br>member-query-interval=500ms                                                 |
| Настройка количества Last Member Query Count       | ip igmp snooping vlan<br>1 last-member-query-<br>count 2                                                                              | ip igmp snooping vlan<br>1 last-member-query-<br>count 2                                                                             | igmp-last-member-query-interval                                                                                        |
| Настройка Robustness Variable                      | ip igmp snooping vlan<br>1 robustness-variable 3                                                                                      | ip igmp snooping vlan<br>1 robustness-variable 3                                                                                     | /interface bridge set [find] igmp-<br>robustness=3                                                                     |
| Сохранение конфигурации                            | write memory или<br>copy running-config<br>startup-config                                                                             | write startup-config                                                                                                                 | /export file=config                                                                                                    |

Таблица 3 содержит приведённые авторами варианты настройки для планирования защиты multicast-доставки. Синтаксис и применимость команд необходимо сверять с документацией конкретной модели, версии ПО и операционной системы коммутатора. Совокупная эффективность перечисленных настроек на всех трёх платформах в работе не проверялась. Для MikroTik в таблице использован синтаксис RouterOS, тогда как источник [7] описывает SwOS. Возможность применения отдельных команд и полнота их синтаксиса по представленным материалам не подтверждены.

### Заключение

В статье описан лабораторный эпизод с поддельным IGMPv2 Leave-сообщением на Cisco Catalyst 2960 и приведены наблюдения времени реакции для Cisco, Eltex и MikroTik. Выбранные сценарии и таймеры демонстрируют риск изменения членства порта, но не устанавливают одинаковую уязвимость всех L2+ коммутаторов. Статические записи и настройки запросов рассмотрены как варианты снижения риска; выводы ограничены

представленными конфигурациями и иллюстрациями.

В качестве направления дальнейшей работы можно проверить фильтрацию multicast-источников, предусмотренную IGMPv3 [8]. Сам IGMPv3 не добавляет аутентификацию участников; защита сообщений требует отдельного механизма, например IPsec в соответствующем окружении. Экспериментальная проверка IGMPv3 в данной работе не проводилась.

Вместе с тем важно подчеркнуть, что статическая привязка multicast-групп, будучи высокоэффективным защитным механизмом, обладает существенными эксплуатационными недостатками. Ручное конфигурирование каждой группы лишает сеть гибкости динамического управления подписками, что критично в условиях часто меняющегося состава получателей. Административные издержки на поддержание статических записей в крупных инфраструктурах могут стать неприемлемыми.

#### **Библиографический список**

1. Fenner W. Internet Group Management Protocol, Version 2 : RFC 2236. — IETF, 1997. — URL: <https://datatracker.ietf.org/doc/html/rfc2236> (дата обращения: 15.02.2026).
2. Способ и устройство передачи трафика с групповой адресацией с множеством линий связи : пат. 2804753 Российская Федерация, МПК H04W 4/06, H04W 72/04 / М. Гань, Д. Лян, И. Ли, Ю. Го, Ю. Ли, Ц. Юй, С. Ян ; патентообладатель Хуавэй Текнолоджиз Ко., Лтд. — № 2022133288 ; заявл. 04.06.2021 ; опубл. 05.10.2023. — 30 с. : ил.
3. Обзор сетевых атак и методов их предотвращения на канальном уровне / Казанский национальный исследовательский технический университет имени А. Н. Туполева — КАИ. — Казань, 2024. — 6 с.
4. Christensen M., Kimball K., Solensky F. Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches : RFC 4541. — IETF, 2006. — URL: <https://datatracker.ietf.org/doc/html/rfc4541> (дата обращения: 15.02.2026).
5. Cisco Systems. Configuring IGMP Snooping for Cisco Catalyst 2960 Series Switches [Электронный ресурс]. — URL: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swigmp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swigmp.html) (дата обращения: 16.02.2026).
6. Eltex. Ethernet Switches MES14xx, MES24xx : Operation Manual, Firmware Version 10.1.8.2 [Электронный ресурс]. — URL: [https://eltexalatau.kz/upload/iblock/60f/mes14xx\\_-mes24xx\\_user-manual\\_10.2.1.1.pdf](https://eltexalatau.kz/upload/iblock/60f/mes14xx_-mes24xx_user-manual_10.2.1.1.pdf) (дата обращения: 10.12.2025).
7. MikroTik. CRS3xx and CSS3xx Series Manual [Электронный ресурс]. — URL: <https://help.mikrotik.com/docs/spaces/SWOS/pages/76415036/CRS3xx+and+CSS3xx+series+Manual> (дата обращения: 10.12.2025).
8. Cain B., Deering S., Kouvelas I., Fenner B., Thyagarajan A. Internet Group Management Protocol, Version 3 : RFC 3376. — IETF, 2002. — URL: <https://datatracker.ietf.org/doc/html/rfc3376>.

#### **References**

1. Fenner, W. (1997). *Internet Group Management Protocol, Version 2 (RFC 2236)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc2236>
2. Gan, M., Liang, D., Li, Y., Guo, Y., Li, Y., Yu, J., & Yang, S. (2023). *Sposob i ustroistvo peredachi trafika s gruppovoi adresatsiei s mnozhestvom linii svyazi [Method and device for transmitting multicast traffic over multiple communication lines] (Patent RU 2804753 C1)*. Huawei Technologies Co., Ltd.
3. Kazanskii natsionalnyi issledovatel'skii tekhnicheskii universitet imeni A. N. Tupoleva—KAI. (2024). *Obzor setevykh atak i metodov ikh predotvrashcheniya na kanalnom urovne [Overview of network attacks and methods of preventing them at the data link layer]*.
4. Christensen, M., Kimball, K., & Solensky, F. (2006). *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches (RFC 4541)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4541>

5. Cisco Systems. (n.d.). *Configuring IGMP Snooping for Cisco Catalyst 2960 Series Switches*. [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swigmp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swigmp.html)
6. Eltex. (n.d.). *Ethernet Switches MES14xx, MES24xx: Operation Manual, Firmware Version 10.1.8.2*. [https://eltexalatau.kz/upload/iblock/60f/mes14xx\\_-mes24xx\\_user-manual\\_10.2.1.1.pdf](https://eltexalatau.kz/upload/iblock/60f/mes14xx_-mes24xx_user-manual_10.2.1.1.pdf)
7. MikroTik. (n.d.). *CRS3xx and CSS3xx Series Manual*. <https://help.mikrotik.com/docs/spaces/SWOS/pages/76415036/CRS3xx+and+CSS3xx+series+Manual>
8. Cain, B., Deering, S., Kouvelas, I., Fenner, B., & Thyagarajan, A. (2002). *Internet Group Management Protocol, Version 3 (RFC 3376)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc3376>

### Информация об авторах

Кязымов Адалат Адалатович — студент факультета комплексной безопасности ТЭК ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: [adalat.kiazymov@mail.ru](mailto:adalat.kiazymov@mail.ru).

Терешонок Артём Алексеевич — студент факультета комплексной безопасности ТЭК ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: [kr3nver@yandex.ru](mailto:kr3nver@yandex.ru).

## EXPERIMENTAL ANALYSIS OF IGMPV2 VULNERABILITIES AND COMPARATIVE EVALUATION OF PROTECTION METHODS ON L2+ SWITCHES FROM DIFFERENT VENDORS

Kyazimov A. A.<sup>1</sup>, Tereshonok A. A.<sup>1</sup>

<sup>1</sup> Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

**Abstract.** This paper describes a laboratory example involving a spoofed IGMP Leave message and discusses ways to protect multicast group membership on Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326 switches. It outlines IGMPv2 and IGMP snooping, which maintain subscriber information and direct multicast traffic to selected ports. The article reports approximate client-port removal intervals of two to three seconds for Cisco, less than one second for Eltex, and about ten seconds for MikroTik. These observations concern the stated models and test settings. The main attack and static-entry example concerns the Cisco configuration. Static multicast binding, group-count limits, IGMP access lists, and Last Member Query Interval and Count settings are considered as possible controls. Reported timer combinations illustrate the trade-off between faster membership removal and tolerance of false messages. The illustrated static command and displayed group table contain different multicast addresses, so the displayed result cannot verify that exact command. The authors report uninterrupted delivery during one repeated attempt, but this does not establish universal protection. Operational limitations of static entries and IGMPv3 are discussed rather than independently tested across all platforms. The results support local configuration checks and distinguish observed behavior from proposed protective settings.

**Keywords:** IGMPv2, IGMP snooping, multicast, L2+ switches, network security, attack, protection.

### Information about the authors

Kyazimov Adalat Adalatovich — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: [adalat.kiazymov@mail.ru](mailto:adalat.kiazymov@mail.ru).

Tereshonok Artem Alekseevich — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: [kr3nver@yandex.ru](mailto:kr3nver@yandex.ru).

Ляхова М. В., Сеникова Н. Г.

Российский государственный университет нефти и газа (национальный исследовательский университет)  
имени И. М. Губкина, Москва, Россия

## ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ RSTP С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА ROOT GUARD НА L2+ УСТРОЙСТВАХ

**Аннотация.** В статье рассматривается учебный сценарий изменения корневого моста в коммутируемой сети и применение Root Guard для ограничения такого изменения. Цель работы состоит в разборе наблюдений лабораторного стенда и формулировании проверяемого порядка настройки защиты, а не в сравнении производительности оборудования. Исходный стенд включает рабочие станции, коммутаторы Cisco 2960 SI, Eltex MES1428 и устройство MikroTik; для генерации управляющих кадров используется Yersinia. В работе сохранены схемы трех подключений, адресные части идентификаторов корня до и после воздействия, отдельные ответы ring и фрагменты служебного вывода. Эти материалы показывают состояния конкретных узлов и позволяют обсудить изменение выбора корня, но не устанавливают единую временную последовательность всех событий. Авторы также приводят таблицу наблюдений при включенной защите, в которой адресные части идентификаторов остаются неизменными. Такой результат рассматривается как ограниченное наблюдение стенда, поскольку полный журнал настроек и переходов портов не представлен. Документированное поведение Root Guard отделено от наблюдаемых результатов; приведены примеры настройки и диагностики для Cisco IOS и RouterOS с явными условиями применимости. Время восстановления, загрузка процессора, длительность разрыва связи и потери во время защитного блокирования не измерялись и не используются в выводах. Практическая ценность материала заключается в последовательном разделении исходного состояния, воздействия, проверки идентификатора корня и проверки состояния защищенного порта. Полученные выводы относятся к учебному сценарию и не подтверждают универсальную защиту от всех атак канального уровня.

**Ключевые слова:** RSTP; Root Guard; корневой мост; BPDU; коммутируемая сеть; учебный стенд.

### Введение

Протоколы семейства Spanning Tree формируют беспетлевую активную топологию сети Ethernet. RSTP возник как расширение с ускоренной реконфигурацией дерева; назначение стандарта описано IEEE [1]. Базовые состояния порта — discarding, learning и forwarding; выбор корня зависит от сравнения идентификаторов мостов и параметров пути [2]. Возможность передачи более предпочтительного BPDU делает выбор корня зависимым от доверия к подключенному сегменту. Само получение роли корня не доказывает перехват всего пользовательского трафика: путь передачи определяется топологией и ролями портов.

Root Guard позволяет задать административную границу, через которую не должен появляться более предпочтительный корень. В реализации Cisco прием superior BPDU на защищенном порту вызывает root-inconsistent и блокирование передачи через этот порт; после прекращения таких BPDU восстановление происходит автоматически [3]. Поэтому сохранение положения корня и непрерывная доступность всех узлов — разные свойства. Цель статьи — разобрать имеющийся учебный пример и показать, какие наблюдения необходимы для корректной интерпретации защиты.

### Материалы и методы

Использованный лабораторный стенд включает рабочие станции PC1, PC2 и PCA и коммутаторы Cisco 2960 SI, Eltex MES1428 и MikroTik. Модель MikroTik и версии программного обеспечения не указаны. Схемы стенда приведены на рис. 1–4. На отдельных схемах для рабочей станции используются обозначения PC3 и PCA; далее PCA означает атакующий узел, однако тождество этих обозначений во всех конфигурациях не подтверждено. Показанные IP-адреса 192.168.1.1–192.168.1.3 относятся к одному диапазону адресации; исходное описание отдельных подсетей не подтверждено приведёнными настройками.

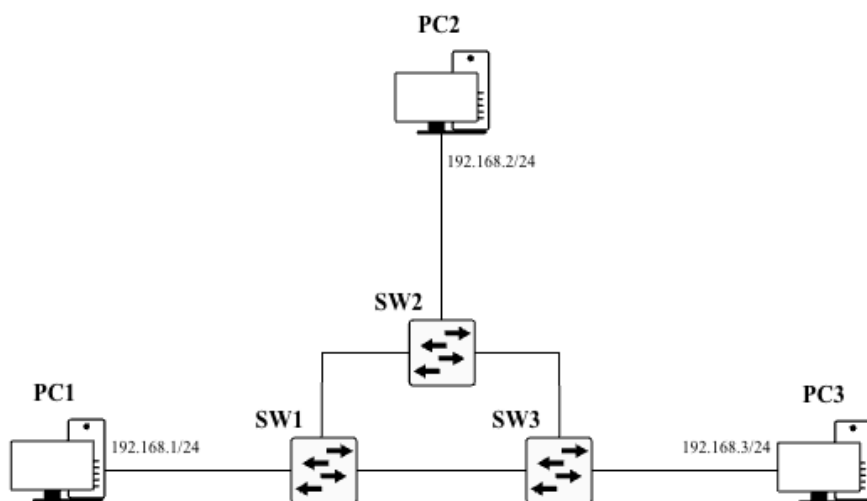


Рис. 1. Общая схема стенда: рабочие станции PC1–PC3 и коммутаторы SW1–SW3

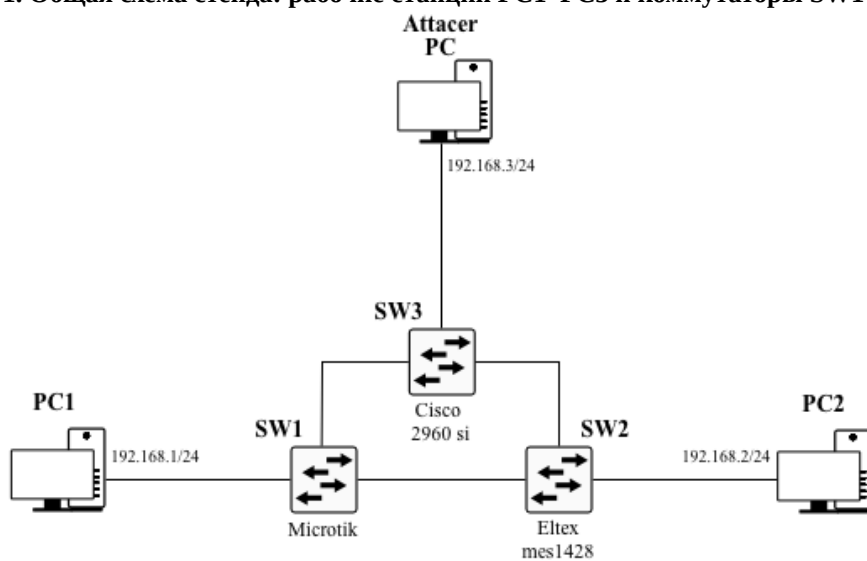


Рис. 2. Первый вариант соединения коммутаторов MikroTik, Eltex и Cisco

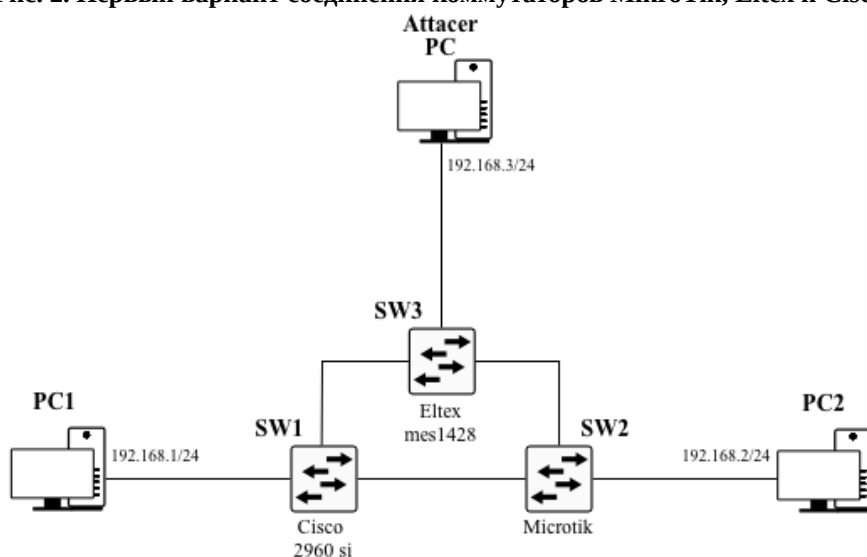


Рис. 3. Второй вариант соединения коммутаторов Cisco, MikroTik и Eltex

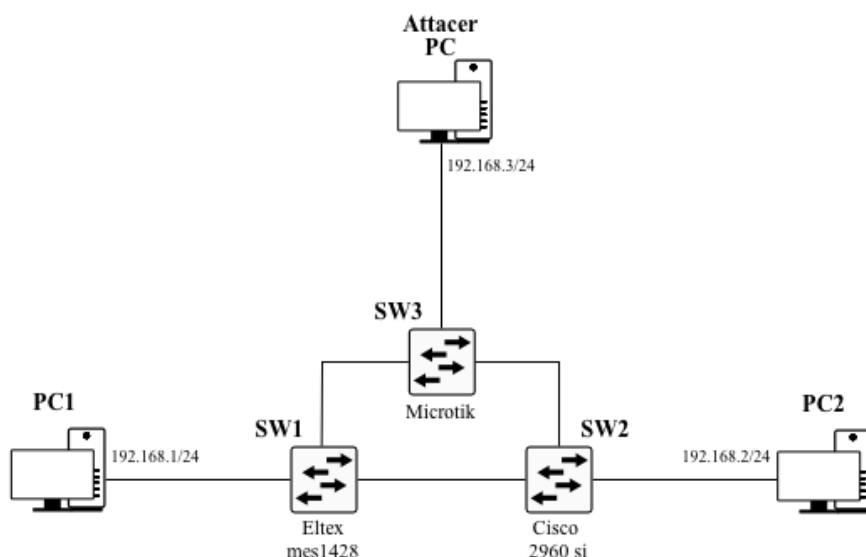


**Рис. 4. Третий вариант соединения коммутаторов Eltex, Cisco и MikroTik**

Для формирования управляющего трафика применялась утилита Yersinia. Реализованные в ней протокольные сценарии описаны в репозитории разработчиков [4], а способ запуска и перечень поддерживаемых протоколов — в справочнике Kali Linux [5]. Версия программы, параметры генерируемых BPDU и данные о повторных запусках не приведены. Поэтому ниже сопоставляются только наблюдаемые состояния устройств и сообщённые значения; причинное сравнение производителей и статистическая оценка эффективности не выполняются.

Перед воздействием были выполнены короткие проверки ping. В листингах 1–3 сохранены количество пакетов и время ответа. Один или два ответа не позволяют оценить долговременную доступность сети и не отражают потери во время воздействия.

#### **Листинг 1 – Исходная проверка адреса 192.168.1.1**

```

ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.843 ms
^C
--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.843/0.843/0.843/0.000 ms
  
```

#### **Листинг 2 – Исходная проверка адреса 192.168.1.2**

```

ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.046 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.046/0.049/0.052/0.003 ms
  
```

#### **Листинг 3 – Исходная проверка адреса 192.168.1.3**

```

ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=2.97 ms
^C
--- 192.168.1.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.974/2.974/2.974/0.000 ms
  
```

#### **Результаты**

В таблице 1 представлены адресные части Root ID до и после воздействия при отключённой защите. Приоритет моста не приведён, поэтому полный Bridge ID по этим значениям восстановить нельзя. Три наблюдения не следует трактовать как синхронные состояния одной инстанции дерева: в отдельных выводах устройства независимо показывают

себя корнем. Без временных меток и полного протокольного журнала можно установить лишь сообщённое изменение адресной части идентификатора, но нельзя однозначно связать его с определённым поддельным BPDU.

**Таблица 1 – Адресные части идентификатора корня до и после воздействия без защиты**

| Наблюдение | До воздействия    | После воздействия |
|------------|-------------------|-------------------|
| 1          | 2401.c735.5780    | e4:5a:d4:9a:40:40 |
| 2          | e4:5a:d4:9a:40:40 | C4:AD:34:03:6F:2A |
| 3          | C4:AD:34:03:6F:2A | 2401.c735.5780    |

В листингах 4–6 приведены фрагменты консольного вывода коммутаторов. Сообщения This bridge is the root и root-bridge: yes характеризуют состояние соответствующего устройства, но не подтверждают получение атакующей станцией роли корня. В выводе Eltex указан MSTP, что дополнительно ограничивает трактовку всех эпизодов как работы в едином режиме RSTP.

#### **Листинг 4 – Фрагмент состояния дерева STP на Cisco**

```
Spanning tree enabled protocol rstp
Root ID      Priority      32868
              Address      2401.c735.5780
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID    Priority      32868 (priority 32768 sys-id-ext 100)
              Address      2401.c735.5780
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300 sec
Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/7        Desg FWD 19         128.7    P2p
Fa0/13       Desg FWD 19         128.13   P2p
Fa0/17       Desg FWD 19         128.17   P2p
```

#### **Листинг 5 – Фрагмент состояния дерева STP на Eltex**

```
console#show spanning-tree
Root Id      Priority      32768
              Address      e4:5a:d4:9a:40:40
              Cost          0
              Port          0 [0]
              This bridge is the root
              Max age 0 sec Forward delay 0 sec Hello time 0 sec
              Hello Time 2 sec 0 cs

MST00
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id    Priority      32768
              Address      e4:5a:d4:9a:40:40
              Max age 0 sec Forward delay 0 sec Hello time 0 sec
              Hello Time 2 sec 0 cs
```

#### **Листинг 6 – Фрагмент состояния моста на MikroTik**

```
[admin@MikroTik] /interface bridge port> /interface bridge monitor bridge
;;; defconf
state: enabled
current-mac-address: C4:AD:34:03:6F:2A
root-bridge: yes
root-bridge-id: 0x8000.C4:AD:34:03:6F:2A
root-path-cost: 0
root-port: none
port-count: 26
designated-port-count: 1
fast-forward: no
```

В листинге 7 представлены сообщения Destination Host Unreachable. Они фиксируют недоступность узла в отдельный момент времени, однако продолжительность и непосредственная причина отказа на основании этого фрагмента не устанавливаются.

#### **Листинг 7 – Фрагмент сообщений о недоступности узла**

```
From 192.168.1.2 icmp_seq=1 Destination Host Unreachable
From 192.168.1.2 icmp_seq=2 Destination Host Unreachable
```

From 192.168.1.2 icmp\_seq=3 Destination Host Unreachable

В таблице 2 приведены значения идентификатора корня при включённой защите: адресная часть остаётся неизменной. Для этих наблюдений отсутствуют полные команды настройки Root Guard и журнал переходов защищённых портов. Поэтому неизменность идентификатора не доказывает переход всех устройств в root-inconsistent и не подтверждает непрерывность пользовательского обмена.

Таблица 2 – Адресные части идентификатора корня до и после воздействия при защите

| Наблюдение | До воздействия    | После воздействия |
|------------|-------------------|-------------------|
| 1          | 2401.c735.5780    | 2401.c735.5780    |
| 2          | e4:5a:d4:9a:40:40 | e4:5a:d4:9a:40:40 |
| 3          | C4:AD:34:03:6F:2A | C4:AD:34:03:6F:2A |

### Обсуждение и порядок настройки

Дальнейшие команды приведены по документации производителей как примеры для повторной проверки, а не как журнал команд, выполненных в описанном эксперименте. В Cisco IOS Root Guard задаётся на интерфейсе, за которым согласно проекту не должен появляться корневой мост [3]. Порт должен выбираться по фактической схеме: включение Root Guard на ожидаемом восходящем root port способно нарушить связность. Root Guard отличается от BPDU Guard: первая функция ограничивает выбор корня, тогда как вторая может отключать граничный порт при получении BPDU [6].

### Листинг 8 – Пример включения Root Guard и проверки портов Cisco IOS

```
configure terminal
interface fastethernet 0/8
spanning-tree guard root
end
show spanning-tree inconsistentports
```

Синтаксис зависит от версии Cisco IOS. Для отдельных старых платформ в документации приведена команда spanning-tree rootguard [3]. Без версии ПО исследованного коммутатора нельзя считать листинг 8 дословной записью настроек стенда.

В RouterOS ограничение возможной роли корня на порту задаётся параметром restricted-role. Для STP/RSTP документация указывает поддержку начиная с RouterOS 7.14: при приёме superior BPDU порт переходит в роль alternate-port и состояние discarding, а не обязательно получает диагностическую метку Cisco root-inconsistent [7]. Листинг 9 применим к уже созданному мосту и интерфейсу на поддерживаемой версии RouterOS; его выполнение на использованном стенде не подтверждено.

### Листинг 9 – Пример ограничения роли порта в RouterOS

```
/interface bridge port
set [find where interface=ether1] restricted-role=yes
/interface bridge port monitor [find where interface=ether1] once
```

Для Eltex показано состояние дерева, но не указаны версия ПО и применённая команда защиты. Поэтому команды других моделей Eltex не выдаются за проведённую настройку. Для воспроизводимой проверки следует фиксировать модель и версию, конфигурацию порта, режим и инстанцию STP, затем — исходный Root ID, параметры полученного BPDU, роль и состояние защищённого порта и восстановление после прекращения воздействия. Эти данные позволяют отличить ограничение выбора корня от случайного изменения связности.

Представленные материалы не содержат временных рядов загрузки процессора, скорости передачи, длительности восстановления либо серии контролируемых испытаний с одинаковой топологией. Эти показатели не оценивались. Неизменный Root ID не подтверждает непрерывную передачу через блокируемый порт. Root Guard не аутентифицирует отправителя BPDU и не заменяет остальные меры защиты сети: его применение зависит от допустимого направления появления более предпочтительного корневого моста.

### Заключение

Учебные наблюдения демонстрируют необходимость контролировать выбор корня и корректно интерпретировать вывод команд Spanning Tree. В таблицах приведены адресные

части идентификаторов корня до и после воздействия, а в листингах — состояния устройств и отдельные ответы ring. Материалы не доказывают универсальную эффективность Root Guard на всех моделях, перехват пользовательского трафика или рост производительности. Документированная функция Root Guard ограничивает появление superior BPDU со стороны выбранного порта и может блокировать передачу через него. Следовательно, такое поведение следует учитывать при проектировании. Для сравнительного экспериментального исследования потребовались бы одинаковые протокольные настройки, версии ПО, параметры кадров и полные журналы, которые в данном опыте отсутствуют.

Благодарности. Научный руководитель — Павловский В. В., старший преподаватель кафедры безопасности информационных технологий РГУ нефти и газа (НИУ) имени И. М. Губкина.

### **Библиографический список**

64. IEEE 802.1 Working Group. 802.1w — Rapid Reconfiguration of Spanning Tree [Электронный ресурс]. — URL: <https://www.ieee802.org/1/pages/802.1w.html>. — Текст : электронный.
65. Cisco Systems. Understand Rapid Spanning Tree Protocol (802.1w) [Электронный ресурс]. — 2023. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>. — Текст : электронный.
66. Cisco Systems. Enhance STP with Root Guard [Электронный ресурс]. — 2026. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>. — Текст : электронный.
67. Yersinia developers. Yersinia: A framework for layer 2 attacks [Электронный ресурс]. — URL: <https://github.com/tomac/yersinia>. — Текст : электронный.
68. Kali Linux. Yersinia [Электронный ресурс]. — URL: <https://www.kali.org/tools/yersinia/>. — Текст : электронный.
69. Cisco Systems. Understand STP Loop Guard and UDLD Features [Электронный ресурс]. — 2022. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol-stp-8021d/218321-configure-stp-with-loop-guard-and-bpdu-s.html>. — Текст : электронный.
70. MikroTik. Bridging and Switching [Электронный ресурс]. — URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>. — Текст : электронный.

### **References**

71. IEEE 802.1 Working Group. (n.d.). 802.1w — *Rapid Reconfiguration of Spanning Tree*. <https://www.ieee802.org/1/pages/802.1w.html>
72. Cisco Systems. (2023). *Understand Rapid Spanning Tree Protocol (802.1w)*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>
73. Cisco Systems. (2026). *Enhance STP with Root Guard*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>
74. Yersinia developers. (n.d.). *Yersinia: A framework for layer 2 attacks*. <https://github.com/tomac/yersinia>
75. Kali Linux. (n.d.). *Yersinia*. <https://www.kali.org/tools/yersinia/>
76. Cisco Systems. (2022). *Understand STP Loop Guard and UDLD Features*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol-stp-8021d/218321-configure-stp-with-loop-guard-and-bpdu-s.html>
77. MikroTik. (n.d.). *Bridging and Switching*. <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>

### **Информация об авторах**

Ляхова Мария Владимировна — студентка Российского государственного университета нефти и газа (национального исследовательского университета) имени И. М. Губкина, Москва, Россия; e-mail: [mariahlyahova@yandex.ru](mailto:mariahlyahova@yandex.ru).

Сеникова Наталья Григорьевна — студентка Российского государственного университета нефти и газа (национального исследовательского университета) имени И. М. Губкина, Москва, Россия; адрес для корреспонденции через соавтора М. В. Ляхову: [mariahlyahova@yandex.ru](mailto:mariahlyahova@yandex.ru).

Lyakhova M. V., Senikova N. G.

Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

**Abstract.** The article examines an educational scenario involving a change of the root bridge in a switched network and the use of Root Guard to restrict that change. The aim is to interpret the available laboratory observations and describe a verifiable configuration procedure rather than compare equipment performance. The test setup includes workstations, Cisco 2960 SI and Eltex MES1428 switches, and a MikroTik device. Yersinia is used to generate control traffic. The paper preserves connection diagrams, address components of root identifiers before and after the reported intervention, individual ping responses, and console fragments. These materials describe particular node states, but do not establish a synchronized sequence for all events. A second table reports unchanged root addresses when protection was enabled. This is treated as a limited observation because the available evidence does not include complete configuration logs or protected port state transitions. Documented Root Guard behavior is distinguished from experimental observations. Cisco IOS and RouterOS configuration examples are accompanied by explicit applicability conditions and are not presented as commands executed in the reported trial. Recovery time, processor utilization, interruption duration, and packet loss during protective blocking were not measured. The practical contribution is a structured distinction between the baseline state, intervention, root identifier check, and protected port state check. The conclusions apply to the educational case and do not establish universal protection against Layer 2 attacks.

**Keywords:** RSTP; Root Guard; root bridge; BPDU; switched network; educational setup.

### Information about the authors

Maria V. Lyakhova — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: mariahyahova@yandex.ru.

Natalia G. Senikova — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence through co-author M. V. Lyakhova: mariahyahova@yandex.ru.

## **УСЛОВИЯ И ПОРЯДОК НАПРАВЛЕНИЯ МАТЕРИАЛОВ**

Редакция научного журнала «ПРОФЕССИОНАЛИТЕТ» принимает к рассмотрению статьи, исправленные версии рукописей, ответы на замечания редакции и рецензентов, а также сопроводительную переписку по конкретной статье. Направление материалов осуществляется в электронной форме в соответствии с внутренним регламентом редакции.

Каждое письмо должно содержать информативную тему и заполненный сопроводительный текст. Переписка ведется в официально-деловом стиле. В теме письма указываются тип обращения, фамилия автора, краткое название статьи и, при необходимости, номер итерации исправления.

В тексте письма обязательно приводятся полное название статьи, сведения обо всех авторах, дисциплина (если применимо), номер итерации исправления и контактные данные ответственного автора. Для исправленных версий дополнительно рекомендуется указывать, на какое письмо редакции или рецензии дается ответ, и кратко обозначать внесенные исправления.

Файл рукописи направляется в формате .docx, на кириллице, по установленной форме наименования. Исправленные версии направляются исключительно ответом на письмо редакции с обязательным указанием номера итерации в теме письма, тексте письма и имени файла.

Материалы, оформленные с нарушением установленных требований, могут быть возвращены без рассмотрения до устранения технических замечаний.

### **Контактные данные редакционной коллегии**

Почта России · Москва, Ленинский пр-кт, 65/1 Отделение почтовой связи № 119296

ДО ВОСТРЕБОВАНИЯ

Получатель Павловский Владимир Владимирович

Тел. +7(950) 632-04-38

e-mail: organizers@au-team.ru

главный редактор – Уймин Антон Григорьевич;

ответственный секретарь - Уймина Ольга Ивановна;

технический редактор - Козлов Глеб Васильевич.

### **ПРОФЕССИОНАЛИТЕТ, 2026, № 3 (011)**

Научное электронное издание.

Сведения о программном обеспечении: шаблон Microsoft Word (DOTM); автоматизированная сборка и контроль структуры — Python (OOXML); контрольный просмотр макета — LibreOffice.

Техническая обработка и подготовка материалов выполнены авторами.

Подписано к использованию: [ДАТА ПОСЛЕ УТВЕРЖДЕНИЯ РЕДАКЦИЕЙ]

Объем издания: [РАЗМЕР ИТОГОВОГО PDF ПОСЛЕ СБОРКИ]

Комплектация издания: pdf.

Запись на физический носитель: Уймин А. Г., тел. +7 (950) 632-04-38.

Издатель — редакция научного журнала «ПРОФЕССИОНАЛИТЕТ».

Место издания: Москва.

Электронная версия подготовлена редакцией журнала для распространения в локальной и сетевой форме.

Носитель электронного издания: URALOLIMP.WEBSITE

