УДК 004.056.53

Камилов М.Ф.
студент
1 курса, факультета «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Москва; Россия.
Kamilov M.F.
1st-year student,
Faculty of Comprehensive Security of the Fuel and Energy Complex,
Gubkin Russian State University of Oil and Gas (National Research University),
Moscow; Russia.

ОСОБЕННОСТИ КОНФИГУРИРОВАНИЯ И ЗАЩИТЫ PRIVATE VLAN НА ОБОРУДОВАНИИ CISCO, MIKROTIK И ELTEX

Аннотация: *Исследование посвящено особенностям конфигурации и защиты сетей с использованием технологии Private VLAN (PVLAN) на коммутаторах различных производителей. Рассматриваются принципы сегментации на уровнях Isolated, Community и Promiscuous, а также механизмы ограничения взаимодействия между портами внутри одной подсети. Эксперименты проведены в гетерогенной среде с использованием оборудования Cisco Catalyst 3750, Eltex MES1428 и MikroTik CRS326-24G-2S+R. Проанализированы различия в реализации PVLAN, определена эффективность изоляции трафика и выявлены потенциальные уязвимости конфигурации. Представлены практические рекомендации по повышению уровня безопасности и совместимости при межвендорной настройке PVLAN.*

Ключевые слова: *Private VLAN, PVLAN, VLAN, Cisco, MikroTik, Eltex, изоляция портов, сетевая безопасность, сегментация сети, межвендорная совместимость, тестирование.*

Abstract: *The study focuses on the configuration and protection features of networks using Private VLAN (PVLAN) technology on switches from different*

manufacturers. The principles of segmentation at the Isolated, Community, and Promiscuous levels, as well as mechanisms for restricting interaction between ports within a single subnet, are examined. Experiments were conducted in a heterogeneous environment using Cisco Catalyst 3750, Eltex MES1428, and MikroTik CRS326-24G-2S+R equipment. Differences in PVLAN implementation were analyzed, the effectiveness of traffic isolation was evaluated, and potential configuration vulnerabilities were identified. Practical recommendations are presented to enhance the level of security and interoperability in multi-vendor PVLAN configurations.

Keywords: *Private VLAN, PVLAN, VLAN, Cisco, MikroTik, Eltex, port isolation, network security, network segmentation, interoperability, testing.*

Современные корпоративные и операторские сети предъявляют высокие требования к безопасности, особенно когда множество устройств объединены в одну VLAN. Private VLAN (PVLAN) позволяет изолировать порты внутри одной VLAN и контролировать взаимодействие между ними, снижая риски несанкционированного обмена данными.

Настройка и защита PVLAN становится особенно актуальной при использовании оборудования разных производителей, так как реализации могут отличаться [1-4], создавая сложности при проектировании и эксплуатации таких сетей.

В этой статье рассматриваются особенности конфигурирования и обеспечения безопасности PVLAN на примере оборудования Cisco, MikroTik и Eltex.

Объект исследования: технологии канального уровня для сегментации сетей.

Предмет исследования: реализация и защита PVLAN на оборудовании разных вендоров.

Цель исследования: выявить общие принципы и отличия в настройке PVLAN на Cisco, MikroTik и Eltex, а также разработать рекомендации по безопасной эксплуатации данной технологии.

Private VLAN (PVLAN) — это механизм, расширяющий традиционные VLAN путём деления их на подтипы:

- **Primary VLAN** — основная VLAN, к которой относятся все подчинённые.
- **Isolated VLAN** — порты не могут взаимодействовать друг с другом.
- **Community VLAN** — порты могут взаимодействовать внутри своей группы, но не с другими Community.

Private VLAN (PVLAN) — расширение VLAN, которое позволяет разбить один VLAN на поддомены с изоляцией трафика между портами.

На практике PVLAN используется у провайдеров и в дата-центрах для изоляции клиентов в одном IP-подсети без взаимного доступа, сохраняя при этом связь с маршрутизатором через promiscuous-порт.

Среди исследований безопасности отмечают, что эффективность PVLAN зависит от корректной настройки (mapping, trunk) и от того, как оборудование обрабатывает теги и каскадные транковые соединения.

Таким образом, PVLAN уже признан проверенным инструментом сегментации L2, но требует внимание к деталям реализации на разных вендорах и учёта возможных уязвимостей при неверных конфигурациях.

Основные гипотезы исследования:

- Конфигурации PVLAN на Cisco, MikroTik и Eltex отличаются по синтаксису, но обеспечивают сопоставимый уровень сегментации и безопасности при корректной настройке.
- В мультивендорной сети корректная совместная работа PVLAN возможна при строгом соблюдении правил тегирования и настройки trunk-портов.
- Реализация PVLAN на разных вендорах имеет различную степень защиты по умолчанию, что влияет на общую устойчивость сети к ошибкам конфигурации.

Тип исследования: Анализ уязвимости с элементами экспериментального тестирования в лабораторной среде.

Характеристика среды исследования: Лабораторная сетевая инфраструктура, включающая физические коммутаторы Cisco Catalyst 3750,

MIKROTIK CRS326-24G-2S+R и Eltex MES1428 [1-4], а также два персональных компьютера. На обоих ПК установлена операционная система Alt Linux (используются для генерации атакного трафика и сбора данных).

Методы сбора данных:

- Консольный доступ и конфигурирование устройств через PuTTY (последовательное подключение к каждому коммутатору).
- Получение и сохранение выходных данных команд конфигурации и состояния, снимки конфигураций.
- Функциональные проверки целостности и доступности сети с помощью ping между тестовыми хостами и шлюзами (IP-адреса хостов вручную настроены).

Процедура проведения исследования:

1. Подключение по консоли (PuTTY) к каждому устройству и загрузка базовых конфигураций.
2. Настройка trunk/port-access и PVLAN-mapping на коммутаторах в соответствии с тестовым сценарием.
3. Назначение IP-адресов на тестовых ПК и проверка локальной конфигурации.
4. Верификация конфигураций через команды show / print — фиксация текущих настроек (vlan, trunk, bridge, port-isolation и т.п.).
5. Проверка сетевой связности и изоляции: серия ping между PC и между PC с VLAN-интерфейсам на Cisco (фиксируется успешность/провал).

Методы обработки данных:

- Сравнение выводов show/print с ожидаемой конфигурацией (trunk, untagged/tagged, роли портов).
- Учёт результатов ping (успех/неудача) для проверки доступности между узлами.
- Анализ расхождений: выявление настроек, при которых нарушается изоляция или появляется нежелательная связность.

Для теста использовалась упрощённая топология: один uplink-порт и четыре клиентских порта (2 Isolated, 2 Community). Она состоит из трех коммутаторов и четырех хостов:

- Cisco выполняет роль центрального коммутатора с promiscuous-портом для uplink и trunk-портами к другим коммутаторам. На нём настроены VLAN 101 (Isolated), VLAN 102 (Community) и VLAN 200 (для тестирования) [1].
- MikroTik обслуживает Isolated VLAN (VLAN 101) с двумя ПК (PC1 и PC2), используя bridge с фильтрацией VLAN и портовую изоляцию [2, 3, 8, 9].
- Eltex обслуживает Community VLAN (VLAN 102) и подключает к нему два ПК (PC3 и PC4).

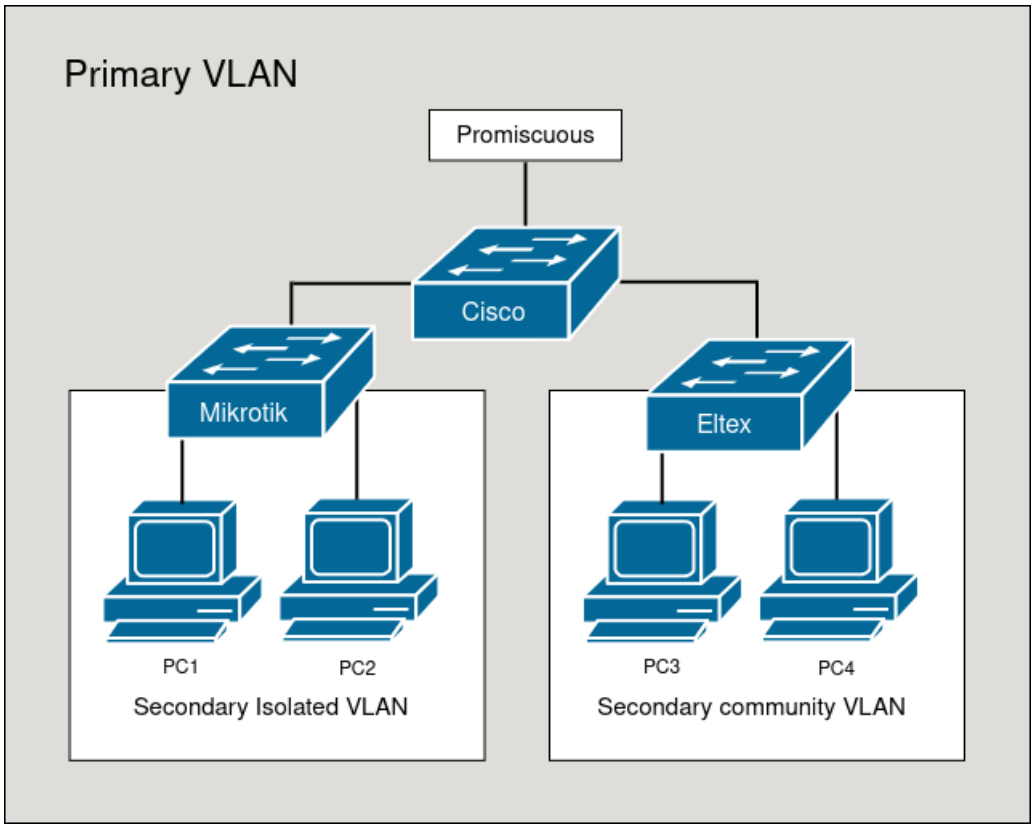

Рисунок 1. Топология сети для эксперимента

Физически соединены коммутаторы и ПК по схеме; доступ к каждому коммутатору — через консоли (PuTTY). На ПК вручную заданы IP-адреса в соответствующих подсетях. Перед тестами проверялось: кабели, видимость интерфейсов и базовая адресация (команды show interfaces / print и ip addr на хостах). Цель — обеспечить рабочее физическое состояние.

На Cisco созданы три VLAN (Isolated, Community, Uplink test), настроены trunk-порты к Eltex и MikroTik с явным списком разрешённых VLAN и SVI (интерфейсы VLAN) с IP-адресами в каждой подсети. Promiscuous-порт реализован как trunk и служит выходом/шлюзом для всех вторичных сегментов.

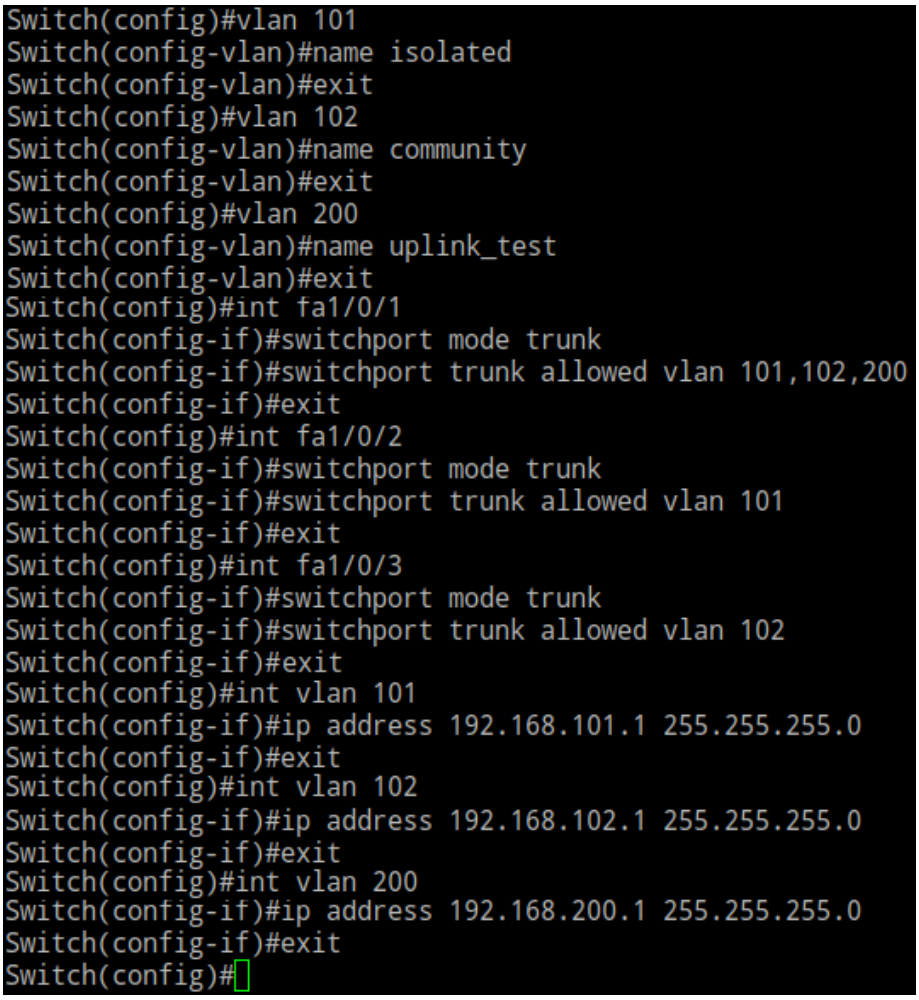

Рисунок 2. Конфигурация Cisco

На MikroTik настроен bridge с vlan-filtering — uplink порт помечен как tagged (trunk), локальные порты — untagged (access) для VLAN 101. Дополнительно включена портовая изоляция (forwarding-override) так, чтобы хосты в isolated-VLAN не могли напрямую обмениваться трафиком между собой.

```
[admin@MikroTik] >
[admin@MikroTik] > interface bridge
[admin@MikroTik] /interface bridge> add name=br-pvlan vlan-filtering=yes
[admin@MikroTik] /interface bridge> port
[admin@MikroTik] /interface bridge port> add bridge=br-pvlan interface=ether1
[admin@MikroTik] /interface bridge port> add bridge=br-pvlan interface=ether2
[admin@MikroTik] /interface bridge port> add bridge=br-pvlan interface=ether3
[admin@MikroTik] /interface bridge port> ..
[admin@MikroTik] /interface bridge> vlan
[admin@MikroTik] /interface bridge vlan> add bridge=br-pvlan tagged=ether1 untag
ged=ether2,ether3 vlan-ids=101
[admin@MikroTik] /interface bridge vlan> .. ..
[admin@MikroTik] /interface> ethernet switch port-isolation
[admin@MikroTik] /interface ethernet switch port-isolation> set ether2 forwardin
g-override=ether1
[admin@MikroTik] /interface ethernet switch port-isolation> set ether3 forwardin
g-override=ether1
[admin@MikroTik] /interface ethernet switch port-isolation>
```

Рисунок 3. Конфигурация Mikrotik

На Eltex создан community-VLAN; два порта переведены в access-режим [4, 5, 7] и привязаны к этому VLAN для PC3/PC4. Порт к Cisco сделан trunk, пропускающий только Fcommunity-VLAN. Логика — обеспечить локальную связь хостов внутри community и передавать трафик наружу через Cisco.

```
console#configure terminal
console(config)#vlan 102
console(config-vlan)#exit
console(config)#int fastethernet 0/1
console(config-if)#switchport mode trunk
console(config-if)#exit
console(config)#int fastethernet 0/2
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 102
console(config-if)#exit
console(config)#int fastethernet 0/3
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 102
console(config-if)#exit
console(config)#
```

Рисунок 4. Конфигурация Eltex

Для проверки корректности конфигурации выполнялись команды show и print на каждом коммутаторе для просмотра текущих параметров VLAN, trunk и портов. После этого проверялась связность между устройствами с помощью команды ping с подключённых ПК.

Проверка осуществлялась следующим образом:

1. ПК2 на ПК1 — внутри VLAN 101 (должен быть не доступен).

```
[root@ALT ~]# ping 192.168.101.10
PING 192.168.101.10 (192.168.101.10) 56(84) bytes of data.
From 192.168.101.10 icmp_seq=1 Destination Host Unreachable
From 192.168.101.10 icmp_seq=2 Destination Host Unreachable
From 192.168.101.10 icmp_seq=3 Destination Host Unreachable
^V^C
--- 192.168.101.10 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5159ms
pipe 3
```

Рисунок 5. Проверка отсутствия связанности PC1 с PC2

2. ПК1 на ПК4 — между VLAN 101 и 102 (доступ быть не должен).

```
[root@ALT ~]# ping 192.168.102.11
PING 192.168.102.11 (192.168.102.11) 56(84) bytes of data.
From 192.168.102.11 icmp_seq=9 Destination Host Unreachable
From 192.168.102.11 icmp_seq=10 Destination Host Unreachable
From 192.168.102.11 icmp_seq=11 Destination Host Unreachable
^C
--- 192.168.102.11 ping statistics ---
13 packets transmitted, 0 received, +3 errors, 100% packet loss, time 12303ms
pipe 4
```

Рисунок 6. Проверка отсутствия связанности PC1 с PC4

3. ПК3 на ПК4 — внутри VLAN 102 (должен быть доступ).

```
[root@ALT ~]# ping 192.168.102.11
PING 192.168.102.11 (192.168.102.11) 56(84) bytes of data.
64 bytes from 192.168.102.11: icmp_seq=1 ttl=64 time=0.889 ms
64 bytes from 192.168.102.11: icmp_seq=2 ttl=64 time=0.532 ms
^C
--- 192.168.102.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.532/0.710/0.889/0.178 ms
```

Рисунок 7. Проверка связанности PC3 с PC4

4. ПК1 на promiscuous (192.168.200.1) — проверка связи с управляющим интерфейсом Cisco.

```
[root@ALT ~]# ping 192.168.200.1
PING 192.168.200.1 (192.168.200.1) 56(84) bytes of data.
64 bytes from 192.168.200.1: icmp_seq=1 ttl=64 time=1.63 ms
64 bytes from 192.168.200.1: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.200.1: icmp_seq=3 ttl=64 time=1.84 ms
^C
--- 192.168.200.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.164/1.545/1.841/0.282 ms
```

Рисунок 8. Проверка связанности PC1 с Promiscuous

5. ПК3 на promiscuous (192.168.200.1) — проверка доступности шлюза из изолированной VLAN.

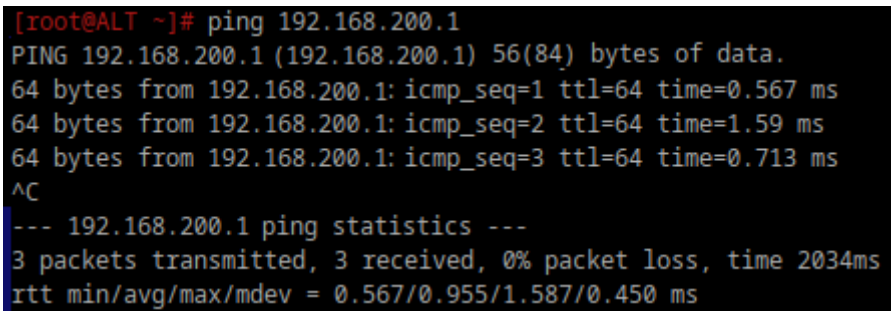

Рисунок 9. Проверка связанности PC3 с Promiscuous

В таблице приведены результаты этих проверок, включая успешность связи и комментарии о соблюдении изоляции и корректной работе механизмов PVLAN.

Таблица 1.

Результаты проверки связи между ПК и доступ к Promiscuous-порту на разных коммутаторах

Тест	**Cisco (VLAN 101, 102, 200)**	**MikroTik (VLAN 101)**	**Eltex (VLAN 102)**	**Ожидаемый результат**
Ping PC1 на PC2 (Isolated VLAN 101)	Неуспешно (изоляция работает)	Неуспешно (портовая изоляция)	Не применимо	Отсутствие связи (изоляция)
Ping PC1 на PC4 (VLAN 101 на VLAN 102)	Неуспешно	Не применимо	Неуспешно	Изоляция между VLAN
Ping PC3 на PC4 (Community VLAN 102)	Успешно	Не применимо	Успешно	Связь внутри Community VLAN
Ping PC1 на Promiscuous (192.168.200.1)	Успешно	Успешно	Успешно	Доступ к шлюзу с VLAN
Влияние настроек trunk и port mapping	Корректная настройка обеспечивает сегментацию	Forwarding-override включён	Используются switchport protected	Сопоставимый уровень сегментации и безопасности

На основе проведённого эксперимента можно сформулировать рекомендации по обеспечению безопасности при настройке PVLAN на коммутаторах Cisco, MikroTik и Eltex.

1. Cisco:

- Тщательно проектировать структуру VLAN до внедрения PVLAN, заранее определяя роли портов: promiscuous, isolated и community.
- Ограничивать распространение VLAN на trunk-портах через switchport trunk allowed vlan и явно задавать режим работы порта (switchport mode trunk).
- На клиентских портах использовать switchport mode private-vlan host с явным указанием первичной и вторичной VLAN для корректной изоляции.
- Для изоляции VLAN на нескольких коммутаторах использовать отдельные VLAN или ACL (например, ip access-group ISOLATED_FILTER in) для ограничения меж-VLAN-трафика.
- Не делить порты одной VLAN на разные подсети; лучше создавать отдельные VLAN для каждой подсети.
- Административный доступ (SSH, Telnet, SNMP) следует выделять отдельным интерфейсом или VLAN, не используемым для PVLAN.
- Регулярно проверять состояние PVLAN через show vlan private-vlan и show interfaces switchport.

2. MikroTik:

- Использовать forwarding-override вместо устаревшего horizon для явного контроля взаимодействия портов.
- Отключить default-vlan-id и явно указывать PVID для каждого access-порта, чтобы исключить попадание трафика в неправильный VLAN.
- Запретить приём неизвестных VLAN и кадров без тегов, включив vlan-filtering=yes и закрыв доступ для неописанных VLAN.
- Включить ingress-filtering=yes на всех портах, кроме trunk, чтобы блокировать трафик с чужими VLAN.
- Для управления выделять отдельный VLAN или физический интерфейс, не использовать мост для Winbox, SSH или WebFig.

3. Eltex

- На trunk-портах ограничивать список разрешённых VLAN (allowed vlan) и явно указывать режим работы (switchport mode trunk).
- На access-портах всегда явно задавать VLAN (switchport access vlan) для корректной сегментации.
- Для изоляции портов предпочтительнее использовать switchport protected; port-isolation можно применять для гибких групп портов, но требует аккуратной настройки.
- Документировать назначение портов, регулярно сохранять конфигурацию и проверять, что изолированные порты не имеют связи между собой.

Результаты проверки гипотез:

1. Конфигурации PVLAN на Cisco, MikroTik и Eltex различаются по синтаксису [1-9], но при правильной настройке обеспечивают сопоставимый уровень сегментации и изоляции трафика.
2. В мультивендорной сети корректная совместная работа PVLAN возможна при строгом соблюдении правил тегирования и ограничений trunk-портов.
3. Разные вендоры обеспечивают различный уровень защиты PVLAN по умолчанию, что влияет на устойчивость сети к ошибкам конфигурации и потенциальным нарушениям изоляции.

Научная новизна работы заключается в сравнительном анализе особенностей реализации PVLAN у трёх производителей, что позволило выявить различия в механизмах портовой изоляции и определить оптимальные практики конфигурирования для повышения безопасности мультивендорных сетей.

Практические рекомендации:

- Cisco: жёстко задавать trunk/host-порты, ограничивать allowed-vlan, использовать ACL для изоляции VLAN на нескольких коммутаторах, не делить порты одной VLAN на разные подсети, выделять отдельный VLAN/порт для управления.
- MikroTik: включать forwarding-override, явно указывать PVID на access-портах, запрещать неизвестные VLAN (vlan-filtering=yes), включать ingress-filtering, выделять отдельный интерфейс для управления.

- Eltex: ограничивать allowed VLAN на trunk, явно задавать access-VLAN на портах, предпочитать switchport protected для изоляции, документировать порты и регулярно проверять конфигурацию.

Направления дальнейшего исследования:

1. Проверка работы PVLAN на других моделях и версиях ПО для оценки масштабируемости и особенностей реализации.
2. Исследование комбинированных атак и их влияние на защиту.
3. Анализ эффективности существующих механизмов защиты в условиях нагрузочного тестирования и интеграции с системами мониторинга.

Использованные источники:

1. Cisco. *Catalyst 3750 Switch Software Configuration Guide – Configuring Private VLANs* [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_50_se/configuration/guide/scg/swpvlan.pdf (дата обращения: 03.10.2025).
2. MikroTik. *Switch Chip Features — Port Isolation (RouterOS)* [Электронный ресурс]. — Режим доступа: https://help.mikrotik.com/docs/spaces/ROS/pages/15302988/Switch+Chip+Features (дата обращения: 03.10.2025).
3. MikroTik. *CRS3xx / CRS5xx / Switch Chip Features* [Электронный ресурс]. — Режим доступа: https://help.mikrotik.com/docs/spaces/ROS/pages/30474317/CRS3xx%2BCRS5xx%2BCCR2116%2BCCR2216%2Bswitch%2Bchip%2Bfeatures (дата обращения: 03.10.2025).
4. Eltex. *MES Series User Manual* [Электронный ресурс]. — Режим доступа: https://old.eltex-co.com/upload/iblock/1dd/3ovqyknd95b2akcx5yhd04ege21okl15/MES_Series_user_manual_4.0.22_en.pdf (дата обращения: 03.10.2025).
5. Eltex. *Securing Client's Ports* [Электронный ресурс]. — Режим доступа: https://webinars.eltex-

co.com/upload/iblock/1b1/xp8qc088tdbs2voj19ddkmpmrbj7v33u/Eltex_%28web%2015.05%29%20Security%20Client_s%20Ports.pdf (дата обращения: 03.10.2025).

6. Уймин, А. Г. *Компьютерные сети. L2-технологии: Практикум.* — Москва : Ай Пи Ар Медиа, 2024. — 191 с. — ISBN 978-5-4497-2539-4.
7. Optokon Group. *Описание MES1428, MES24xx: функции VLAN и L2* [Электронный ресурс]. — Режим доступа: https://www.optokon.com/files/newsletter/2021-02/ELT_03-21_EN-MES1428%2C%20MES2428.pdf (дата обращения: 03.10.2025).
8. NetworkTik. *Configure Private VLAN on the MikroTik Switch for Port Isolation* [Электронный ресурс]. — Режим доступа: https://networktik.com/configure-private-vlan-on-the-mikrotik-switch-for-port-isolation/ (дата обращения: 03.10.2025).
9. MikroTik Community Forum. *VLAN or Port Isolation?* [Электронный ресурс]. — Режим доступа: https://forum.mikrotik.com/t/vlan-or-port-isolation/132305 (дата обращения: 03.10.2025).