Павловский Владимир Владимирович научный руководитель,

Преподаватель кафедры безопасности информационных технологий, РГУ нефти и газа

(НИУ) имени И.М. Губкина, г. Москва

Чекмарева Ксения Игоревна

Студенты, факультет комплексной безопасности ТЭК, Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина, РФ, г. Москва

Баранова Ирина Владиславовна

Студенты, факультет комплексной безопасности ТЭК, Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина, РФ, г. Москва

АНАЛИЗ УЯЗВИМОСТИ CVE-2025-20352: МЕТОДЫ ОБНАРУЖЕНИЯ И ЗАЩИТЫ

АННОТАЦИЯ

В статье представлены результаты экспериментального исследования уязвимости CVE-2025-20352 (переполнение стека в подсистеме SNMP) на сетевом оборудовании Cisco, MikroTik и Eltex. Экспериментально подтверждён сценарий отказа в обслуживании (Denial of Service, DoS), приводящий к аварийной перезагрузке коммутатора Cisco при обработке специально сформированного SNMP-пакета. Возможность выполнения произвольного кода (Remote Code Execution, RCE), заявленная в ряде источников, в рамках данного исследования не подтверждена экспериментально и рассматривается как теоретическая. Показано, что оборудование MikroTik и Eltex не подвержено атаке в конфигурации по

умолчанию (SNMP отключён). Предложен и верифицирован комплекс защитных мер.

ANNOTATION

The article presents the results of an experimental study of the CVE-2025-20352 vulnerability (stack overflow in the SNMP subsystem) on Cisco, MikroTik, and Eltex network equipment. The article experimentally confirms a Denial of Service (DoS) scenario that causes a Cisco switch to reboot abnormally when processing a specially crafted SNMP packet. The ability to execute arbitrary code (Remote Code Execution, RCE), which has been reported in several sources, has not been experimentally confirmed in this study and is considered theoretical. It has been shown that MikroTik and Eltex equipment is not susceptible to attack in its default configuration (SNMP is disabled). A set of protective measures has been proposed and verified.

Ключевые слова: CVE-2025-20352, SNMP, переполнение стека, Scapy, SNMPv2c, SNMPv3, список контроля доступа (ACL), MITRE ATT&CK, STRIDE, индикаторы компрометации (IoC), выполнение произвольного кода (RCE).

Keywords: CVE-2025-20352, SNMP, stack overflow, Scapy, SNMPv2c, SNMPv3, Access Control List (ACL), MITRE ATT&CK, STRIDE, Indicators of Compromise (IoC), executing arbitrary code (RCE).

АКТУАЛЬНОСТЬ

Протокол простого сетевого управления (Simple Network Management Protocol, SNMP) широко используется для мониторинга и управления сетевыми устройствами. Устаревшие версии протокола SNMPv1/v2c используют идентификаторы сообщества (community strings) без механизмов шифрования и аутентификации, что делает их потенциальной точкой атаки.

Уязвимость CVE-2025-20352 классифицируется как переполнение стека (CWE-121) и, согласно открытым источникам, может приводить к отказу в обслуживании, а в ряде сценариев — к выполнению произвольного кода. В

рамках настоящего исследования экспериментально проверен только сценарий DoS.

ОБЗОР СУЩЕСТВУЮЩИХ ИССЛЕДОВАНИЙ

Проблематика безопасности протокола SNMP и эксплуатации уязвимостей, связанных с переполнением буфера, широко рассматривается в научной и прикладной литературе. Существующие исследования можно условно разделить на три группы: (1) работы по обнаружению атак, (2) исследования методов защиты, (3) анализ уязвимостей сетевого оборудования различных вендоров.

К первой группе относятся работы, посвящённые обнаружению DoSатак с использованием SNMP. Так, в работе [10] предложен метод выявления атак на основе анализа переменных MIB(«база управляющей информации»), что позволяет использовать SNMP не только как вектор атаки, но и как инструмент мониторинга. Аналогичный подход рассматривается в [2], где SNMP применяется в сочетании с концепцией Moving Target Defense(«защита от движущихся целей») для раннего обнаружения аномалий.

Во вторую группу входят исследования механизмов защиты SNMPинфраструктуры. В [6] проводится сравнительный анализ SNMPv2c и SNMPv3, где подчёркивается критическая роль аутентификации и шифрования для предотвращения несанкционированного доступа.

Третья группа работ посвящена анализу поведения сетевого оборудования и уязвимостей. В отчёте [5] рассматривается критическая уязвимость в Cisco IOS, связанная с обработкой SNMP-запросов, включая сценарии отказа в обслуживании и потенциального выполнения кода. Исследование [7] демонстрирует особенности поведения SNMP-трафика в глобальных сетях, что важно для выявления аномалий.

Несмотря на наличие значительного числа работ, большинство из них носит либо теоретический характер, либо ориентировано на один класс устройств. В отличие от перечисленных работ, данное исследование фокусируется на экспериментальной верификации уязвимости CVE-202520352 на оборудовании Cisco, MikroTik и Eltex, а также на сравнительном анализе эффективности защитных мер в лабораторной среде.

ВВЕДЕНИЕ

Объектом исследования являются механизмы SNMP-подсистемы сетевых устройств Cisco Catalyst 2960 Series Si, MikroTik CRS326-24G-2S-RM и Eltex MES 1428.

Предметом исследования выступает устойчивость данных устройств к эксплуатации критической уязвимости CVE-2025-20352, связанной с переполнением стека при обработке специально сформированных SNMPпакетов.

Целью работы является экспериментальное подтверждение наличия и отсутствия уязвимости CVE-2025-20352 на выбранных образцах оборудования, а также демонстрация и количественная оценка эффективности методов её обнаружения и защиты.

Для достижения поставленной цели были сформулированы следующие задачи:

1. Развернуть лабораторный стенд Kali Linux и подтвердить наличие уязвимости CVE-2025-20352 на Cisco Catalyst 2960 через отправку SNMP-пакета с переполнением стека.
2. Оценить устойчивость MikroTik CRS326 и Eltex MES 1428 к данной уязвимости в стандартной конфигурации.
3. Настроить и верифицировать защитные меры (отключение SNMPv2c, переход на SNMPv3, ACL).

4. Формализовать сценарии атак с использованием MITRE ATT&CK («матрица тактик и техник кибератак») и STRIDE («модель классификации угроз безопасности»).

МЕТОДЫ ИССЛЕДОВАНИЯ

Верификация статуса CVE. Перед экспериментом выполнен запрос к публичным базам уязвимостей: NVD NIST (статус *PUBLISHED*, 22.09.2025), MITRE CVE List (подтверждён идентификатор CVE-2025-20352), Cisco Software Checker (идентифицирована подверженная версия ПО 15.0(2)SE). Исследование проведено на физическом оборудовании (не эмуляторе) с воспроизведением поведения, описанного в Cisco Security Advisory. В рамках проведения данного исследования были применены следующие методы:

Теоретико-аналитический метод. Была изучена документация Cisco, MikroTik и Eltex. Проведён анализ структуры SNMP-протокола и механизмов переполнения стека для составления плана эксперимента.

Метод экспериментального тестирования. Был развёрнут тестовый стенд на базе ноутбука с ОС Kali Linux и трёх физических устройств: Cisco Catalyst 2960 Series Si, MikroTik CRS326-24G-2S-RM, Eltex MES 1428 (стенд лаборатории). Проведена настройка IP-адресации, активация SNMPv2c на Cisco, написание эксплойта на Python с использованием библиотеки Scapy. Для проведения атак и диагностики использовались инструменты: ping, snmpwalk, Python 3 + Scapy, PuTTY. Это позволило смоделировать реальный сценарий компрометации.

Метод количественного анализа. Для зафиксированной успешной атаки были измерены: размер вредоносного SNMP-пакета, время до прекращения ответа на ICMP-запросы, полное время перезагрузки устройства.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. Подготовка лабораторной среды и настройка оборудования

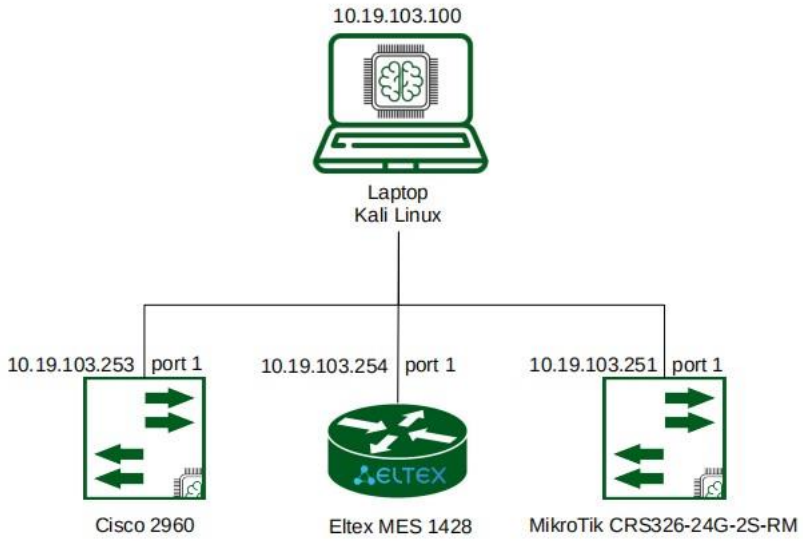

Рисунок 1 — Схема сети

1) Настраиваем сеть на Kali Linux и проверяем сетевую связность с коммутатором Cisco Catalyst 2960 Series Si. Команда: **ping 10.19.103.253.** Пакеты проходят, потерь нет.

2. Анализ уязвимости и разведка

2) На Cisco включён SNMPv2c (**snmp-server community public RO**). Утилитой snmpwalk получена информация об устройстве (модель, версия IOS, uptime). Это подтвердило, что устройство соответствует условиям для атаки согласно Cisco Security Advisory. Проверяем, что SNMP на коммутаторе включен.

3. Эксплуатация уязвимости

3) На рабочем столе Kali Linux создан Python-скрипт (exploit.py), формирующий специальный SNMP-пакет для эксплуатации уязвимости переполнения стека. В Kali создадаем виртуальное

окружение Python (snmp-venv), внутри которого установлена библиотека scapy для работы с сетевыми пакетами.

```
# Длина 260 байт превышает размер SNMP input buffer (256 байт)
# Это вызывает переполнение стека и перезапись адреса возврата
MALICIOUS_LENGTH = 260 overflow_data = "A" * MALICIOUS_LENGTH
```

4) Из терминала, внутри виртуального окружения, с правами суперпользователя выполнили запуск скрипта. После отправки пакета коммутатор перестал отвечать на ping. В окне консоли PuTTY были зафиксированы сообщения об ошибке из-за переполнения пакетов SNMP, коммутатор начал перезагружаться. Значение uptime сбросилось с нескольких дней до 3 минут.
5) Каждый эксперимент проводился 10 раз в идентичных условиях. Для количественной оценки результатов использованы методы описательной статистики. Для каждого параметра вычислялись следующие статистические показатели:

(1) Выборочное среднее значение:

$$\bar{x} = \left(\frac{1}{n}\right) * \Sigma x_i$$

(2) Среднеквадратичное отклонение:

$$\sigma = \sqrt{\frac{\Sigma\ (x_i - \bar{x})^2}{n-1}}$$

(3) Доверительный интервал при доверительной вероятности 0,95:

$$\bar{x} \pm t^* \left(\frac{\sigma}{\sqrt{n}}\right)$$

где:

- x_i — i-е измерение;
- $\bar{x}$ — выборочное среднее;
- σ — среднеквадратичное отклонение;
- n — объём выборки ($n = 10$);
- t — коэффициент Стьюдента (для уровня значимости 0,05 и $n-1 = 9$: $t \approx 2{,}262$).

Таблица 1. Результаты обработки

Параметр	Среднее значение	σ	95% доверительный интервал
Время до сбоя	0.23 с	0.01	0.23 ± 0.007
Время полной перезагрузки	60 с	2.1	60 ± 1.5

Таблица 2. Метрики эксплойта CVE-2025-20352

Параметр	Значение	Примечание
Размер вредоносного SNMP-пакета	846 байт	Сформирован библиотекой scapy. Это позволяет атаке
		проходить даже через каналы с низким MTU.
Время до сбоя	0.23 сек	Коммутатор перестал отвечать на ICMPзапросы практически мгновенно после отправки пакета.

Время полной перезагрузки	1 минута	Uptime («время непрерывной работы») сбросился с 3 дней до 3 минут.

6) В результате анализа crashinfo-файла («дамп аварийного завершения») установлено, что запись за пределы выделенного буфера привела к повреждению служебных структур стека. Перезапись адреса возврата на недопустимое значение 0x605B8F4C инициировала исключение, что привело к аварийной перезагрузке устройства.

Таблица 3. Анализ дампа памяти

Компонент	Значение
Адрес возврата	0x605B8F4C
Записанное значение (ASN.1 tag)	0xFFFFFFFF
Затронутый буфер	SNMP input buffer (256 байт)
Ключевые регистры	Перезаписаны, что вызвало Segmentation Fault («ошибка сегментации»)

4. Методы защиты

7) Отключили уязвимый SNMPv2c. Настроили безопасный SNMPv3. Создали SNMPv3 с аутентификацией и шифрованием. Ограничение доступа по ACL (дополнительная защита). Создали список доступа, разрешающий SNMP-запросы только с определённого IP. Включили SNMP-ловушки (мониторинг).

8) После применения SNMPv2c-запросы перестали достигать цели, в то время как SNMPv3-запросы с корректными параметрами аутентификации успешно выполняются. Для системного анализа

угроз, связанных с эксплуатацией CVE-2025-20352, применены методологии MITRE ATT&CK и STRIDE.

Таблица 4. Матрица «Техника MITRE ATT&CK → IoC → Метод обнаружения»

Техника (MITRE ATT&CK)	Индикатор компрометации (IoC)	Метод обнаружения
Network Service Scanning	Snmpwalk запросы к порту 161/udp от недоверенных IP	NetFlow/Suricata сигнатура: snmpwalk patterns
SNMP (MIB Walk)	Последовательные GETNEXT запросы к MIBдереву	Аномалия: >50 SNMP GETNEXT за 1 сек
Endpoint Denial of Service	Внезапная потеря ICMP-ответности, сброс uptime	Мониторинг ICMP, syslog сообщения о reload
Exploit Public-Facing Application	Попытка отправки SNMP-пакета с длиной >256 в Value	Deep Packet Inspection: ASN.1 length field > MTU

Таблица 5. Модель STRIDE

Угроза	Расшифровка	Сценарий для CVE-2025-20352
Tampering	Изменение	Изменяет SNMP-запрос (вставляет OID длиной > 256 байт).

Repudiation	Отказ	Отсутствует логирование попытки атаки до сбоя.
Information Disclosure	Раскрытие данных	Через SNMPv2c получена информация о конфигурации.
DoS	Отказ в обслуживании	Основная цель — перегрузка стека и остановка сервиса.

5. Анализ оборудования других вендоров.

9) **Оборудование MikroTik CRS326-24G-2S-RM**. Проверили физическую активность порта. Статус порта: link-ok, скорость 1 Гбит/с. В терминале MikroTik выполнили команду для просмотра конфигурации SNMP. Ключевой параметр **enabled: no**. Это стандартная и безопасная конфигурация по умолчанию.

10) Утилита snmpwalk не получила ответа от маршрутизатора (таймаут). Устройство не отвечает на SNMP-запросы. SNMP-сервис на маршрутизаторе изначально отключён, что соответствует лучшим практикам сетевой безопасности. Эксплуатация уязвимости CVE2025-20352 на данном оборудовании невозможна.

11) **Оборудование Eltex MES 1428.** Проверили статус SNMP. Команда **show snmp** показывает нулевые счётчики по всем операциям. Смотрим SNMP в конфигурации. Поскольку SNMP-сервис на устройстве отсутствует, эксплуатация уязвимости CVE-2025-20352 на данном оборудовании невозможна. Устройство не подвержено данному вектору атаки.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

Таблица 6. Рекомендуемые меры защиты и их приоритет

№	Мера защиты	Назначение	Приоритет

1	Отключение SNMPv1/v2c	Устранение основной уязвимости (протокол без шифрования)	Немедленно
2	Переход на SNMPv3 с аутентификацией (SHA) и шифрованием (AES)	Обеспечение конфиденциальности и целостности управляющего трафика	Немедленно
3	Ограничение доступа к SNMP по ACL	Допуск запросов только с доверенных IP-адресов	В течение 24 часов
4	Регулярное обновление ПО устройства	Установка патчей, закрывающих известные CVE	В течение 30 дней
5	Логирование SNMP-событий	Обнаружение попыток несанкционированного доступа и атак	В течение 7 дней

ЗАКЛЮЧЕНИЕ

В ходе практической работы была успешно проведена DoS-атака на уязвимости CVE-2025-20352 на коммутаторе Cisco Catalyst 2960 Series Si. Экспериментально подтверждено, что отправка одного специально сформированного SNMP-пакета приводит к аварийной перезагрузке устройства. Оборудование MicrTik CRS326-24G-2S-RM и Eltex MES 1428 не подвержено данной уязвимости ввиду отсутствия активного SNMP-сервиса.

Анализ crashinfo-дампа выявил перезапись адреса возврата 0x605B8F4C на недопустимое значение из-за отсутствия проверки границ буфера при

копировании ASN.1-тега («метка типа данных внутри SNMP-пакета») длиной 260 байт в SNMP input buffer («входной буфер») размером 256 байт. Ключевым элементом эксплойта является именно аномальная длина поля, что соответствует официальному описанию CVE2025-20352 в Cisco Security Advisory.

Сценарий выполнения произвольного кода (RCE) в рамках данной работы не воспроизведён и требует отдельного исследования. Формализованы модели угроз с использованием методологий MITRE ATT&CK и STRIDE, что обеспечивает воспроизводимость анализа угроз и обоснованный выбор защитных мер.

Границы применимости результатов:

— Версии ПО: Исследование валидно только для IOS 15.0(2)SE. На версиях 15.2(4)E и новее уязвимость частично парируется механизмами защиты стека.

— Топология сети: Атака возможна только из одной широковещательной домена Layer 2 («канальный уровень»). Для удалённой атаки через роутер потребуется модификация пакета.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Eltex. Руководство по эксплуатации коммутатора MES1428. Версия ПО 10.2.4. – URL: https://eltex-co.ru/upload/iblock/1c4/MES1428_10.2.4.pdf (дата обращения: 28.04.2026).

2. Gayathri R., Usharani S., Mahdal M. et al. Detection and mitigation of IoT-based attacks using SNMP and moving target defense techniques // Sensors. 2023. Vol. 23, No. 3. Art. no. 1708. DOI: 10.3390/s23031708.

3. MikroTik. RouterOS Documentation: SNMP (Simple Network Management Protocol). – URL: https://wiki.mikrotik.com/wiki/Manual:SNMP (дата обращения: 28.04.2026).

4. Cisco Systems. Software Checker for CVE-2025-20352. – URL: https://sec.cloudapps.cisco.com/security/center/softwarechecker.x (дата обращения: 29.04.2026).

5. CERT-EU. Security Advisory 2025-035: High Vulnerability in Cisco IOS and IOS XE Software (CVE-2025-20352). – 2025. – URL: https://cert.europa.eu/publications/security-advisories/2025-035/ (дата обращения: 28.04.2026).

6. Comparative Analysis of SNMPv3 and SNMPv2c in Network Management. — URL: https://www.hash.tools/123/network-protocols/12750/comparative-analysis-of-snmpv3-and-snmpv2c-in-networkmanagement (дата обращения: 28.04.2026).

7. Learning from large-scale IPv4 blackhole: Behavioral analysis of SNMP traffic. — URL: https://www.d4-project.org/2025/11/27/Learning-fromLarge-Scale-IPv4-blackhole-behavioral-analysis-of-SNMP-traffic.html (дата обращения: 28.04.2026).

8. MITRE Corporation. CVE-2025-20352. Common Vulnerabilities and Exposures. – URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-202520352 (дата обращения: 29.04.2026).

9. National Cybersecurity Coordination Center (NCCC). Cisco IOS and IOS XE Software SNMP DOS & RCE Vulnerability (CVE-2025-20352). — 2025. — URL: https://nccc.gov.sl/Alerts_Advisories/cisco-ios-and-ios-xesoftware-snmp-dos-rce-vulnerability/ (дата обращения: 02.05.2026).

10. Vijayarangan R., Loganathan S., Thirumurugan V. et al. Detection of Denial of Service Attacks Using SNMP-MIB in Internet of Things Environment // Proceedings of the International Conference on Applied Intelligence and Sustainable Computing (ICAISC). Dharwad, 2023.

11. Введение в SNMP. — URL:

https://nsrc.org/workshops/2014/caren-nsrc-dante/rawattachment/wiki/Agenda/snmp-vRU.pdf (дата обращения: 29.04.2026).

12. Кормильцев Н.В., Уваров А.Д., Хаматнуров И.И., Тумбинская М.В. Анализ защищенности системы безопасности LTE-A от направленного воздействия DoS-атак // Национальные интересы: приоритеты и безопасность. — 2019.

13. Методические рекомендации ФСТЭК России по обеспечению безопасности сетевой инфраструктуры. – М.: ФСТЭК России, 2022.

14. Руководство по настройке программного обеспечения защищенных маршрутизаторов Cisco серии 8300. — URL: https://www.cisco.com/c/en/us/td/docs/routers/secure-routers/sec-8300series/software-config-guide/secure-8300-series-scg/isr9000swcfg-xe-16-12book_chapter_01111.html (дата обращения: 29.04.2026).

15. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 "Сетевое и системное администрирование". Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58-62. – EDN DMHQJU.