

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 разрешенные 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 защищенные 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. Использованы 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.

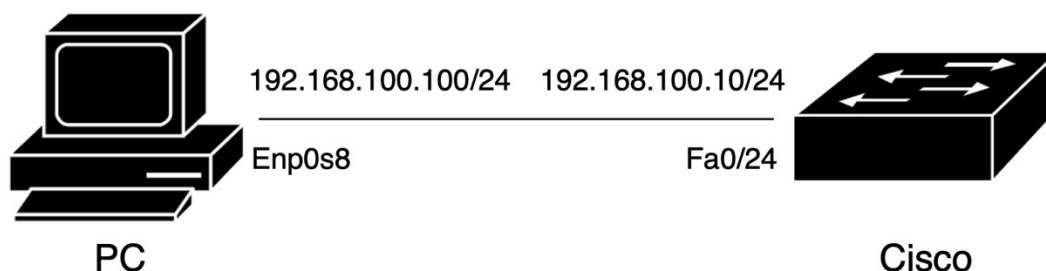


Рис. 1. Схема соединения ПК и коммутатора Cisco 3550

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

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

Таблица 6 – Команды внутреннего аудита MikroTik

Команда	Значение
/system identity print /system resource print /system routerboard print	Базовая информация.
/user print /user group print /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 /ip ssh print detail	SSH настройки, какие алгоритмы поддерживаются
/ip firewall filter print /ip firewall nat print /ip firewall address-list print	Безопасность доступа. Firewall правила, NAT правила и списки доступа
/ip service print where port=80 or port=443 /ip service disable www,www-ssl	Настройки веб-доступа. HTTP/HTTPS доступ.
/system package update print /system package update check /system package update print	Обновления и версии. Доступные обновления.

Таблица 7 – Команды внутреннего аудита Eltex

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

Команда	Значение
show vlan brief show vlan show port-security show running-config include port-security show running-config interface	Настройки VLAN и портов. Безопасность портов и настройки интерфейсов
show clock show ntp status show running-config include ntp show logging show running-config include logging show snmp 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 (требуется проверка)	Слабые: diffie-hellman-group1-sha1, CBC-шифры	В приведённых выводах Nmap не показаны
POODLE / состояние TLS (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.