УДК *004.056.53*

Е. А. Еремина [1]***, А. Н. Простова*** [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ CIS BENCHMARK ДЛЯ КОММУТАТОРОВ ELTEX В КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЕ

Аннотация. *В статье решается задача приведения недокументированных сетевых устройств отечественного производства (Eltex MES1428, Eltex ESR-15R) к безопасной конфигурации в отсутствие официальных профилей CIS Benchmark. Предложен подход, основанный на проекции контролей из CIS Cisco IOS Benchmark v4.1.1 и CIS Network Device General Benchmark v2.0.0 на три плоскости: управления, контроля и данных. Экспериментально на физическом стенде выполнены аудит дефолтных конфигураций, харденинг, повторный аудит и серия из восьми типов активных атак с использованием Kali Linux до и после применения контролей. Факт блокировки каждой атаки верифицировался как отсутствием результата у атакующего, так и наличием соответствующего события в централизованном syslog.*

Установлено, что 91 % контролей применимы (полностью или частично) к MES1428 и 96 % – к ESR-15R; доля заблокированных атак после харденинга по применимым векторам составила 100 % для обоих устройств (с 0 % в дефолтной конфигурации), при этом снижение пропускной способности не превысило 4 %. Полученные результаты сопоставлены с эталонными устройствами Cisco Catalyst 2960 и Cisco 1941.

Предложенная методика имеет прикладное значение для импортозамещения в корпоративных сетях, позволяя обеспечить требуемый уровень безопасности на оборудовании Eltex при отсутствии готовых CIS-профилей, и может быть тиражирована для других вендоров.

Ключевые слова: *CIS Benchmark, харденинг, Eltex MES1428, Eltex ESR-15R, импортозамещение, сетевая безопасность, Kali Linux.*

Введение

Актуальность исследования. По данным Positive Technologies [14, с. 18], в 2024 году в 82 % успешных атак на корпоративные сети первичный доступ был получен через сетевую инфраструктуру с ненадлежащей конфигурацией. В рамках политики импортозамещения, закрепленной Федеральным законом № 187-ФЗ [12], предприятия обязаны переходить на отечественное оборудование. Компания Eltex занимает значительную долю рынка.

Международная организация Center for Internet Security (CIS) разработала семейство документов CIS Benchmark – технических стандартов безопасной настройки сетевого оборудования. Однако официальных профилей для оборудования Eltex не существует, что вынуждает администраторов вручную переносить контроли CIS на CLI Eltex без гарантии полноты и корректности. Дополнительную сложность представляют принципиальные архитектурные отличия Eltex NOS от Cisco IOS..

Настоящая работа представляет первое задокументированное систематическое сопоставление контролей CIS Benchmark с операционными системами Eltex MES NOS и Eltex ESR NOS. Ранее подобного сравнительного исследования в открытых источниках обнаружено не было.

Объект исследования – процесс безопасной настройки (харденинга) коммутаторов и маршрутизаторов Eltex в корпоративной инфраструктуре. Предмет – применимость контролей CIS Cisco IOS Benchmark v4.1.1 и CIS Network Device General Benchmark v2.0.0 к Eltex MES1428 и Eltex ESR-15R, а также эффективность этих контролей в части противодействия типовым атакам.

Цель – количественно оценить долю применимых контролей CIS, практическую эффективность харденинга и связанные с ним накладные расходы для оборудования Eltex в сопоставлении с Cisco Catalyst 2960 и Cisco 1941. Для ее достижения решены задачи: (1) составить адаптированный перечень контрольных требований CIS для MES1428 и ESR-15R; (2) провести аудит дефолтных конфигураций и применить перечень на физическом стенде; (3) выполнить серию из восьми типов активных атак до и после харденинга с верификацией через syslog; (4)

измерить влияние харденинга на производительность; (5) сопоставить результаты с эталонными устройствами Cisco.

Гипотезы исследования:

- H1. Не менее 75 % контролей CIS Cisco IOS Benchmark имеют прямой или частичный эквивалент в CLI Eltex MES1428 и Eltex ESR-15R;
- H2. После применения адаптированного перечня доля успешно заблокированных атак (по применимым к каждому устройству векторам) возрастает не менее чем на 70 п.п. по сравнению с дефолтной конфигурацией;
- H3. Снижение пропускной способности TCP-трафика после харденинга не превышает 5 %.

Семейство документов CIS Benchmark: история и структура

Center for Internet Security – некоммерческая организация, объединяющая более 11 000 участников из государственного, коммерческого и академического секторов. Флагманский продукт – серия CIS Benchmark: технических стандартов безопасной конфигурации, сформированных методом консенсуса экспертов [1]. Каждый документ содержит контроли (recommendations) с описанием требования, процедуры аудита, команды устранения, обоснования риска и влияния на функциональность.

CIS Cisco IOS Benchmark v4.1.1 структурирован по четырем разделам: плоскость управления (Management Plane Security), плоскость контроля (Control Plane Security), плоскость данных (Data Plane Security) и IOS-специфичные сервисы. Аналогичная трехплоскостная модель принята в CIS Network Device General Benchmark [9], что позволяет использовать ее как единую методологическую рамку для любого производителя. Контроли CIS частично пересекаются с требованиями NIST SP 800-53 Rev. 5 [7], PCI DSS v4.0 и ГОСТ Р 57580.1-2017, что делает харденинг по CIS применимым в рамках нескольких регуляторных требований одновременно.

Архитектура оборудования Eltex: особенности, релевантные для харденинга

Eltex MES1428 – управляемый коммутатор уровня L2 с 24 портами 10/100 Мбит/с и 4 гигабитными портами, работающий под управлением Eltex MES NOS 10.x. Устройство поддерживает полный набор механизмов защиты канального уровня: DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard (IPSG), Port Security и Storm Control.

Eltex ESR-15R – маршрутизатор корпоративного класса под управлением Eltex ESR NOS 1.x. Ключевая архитектурная особенность – механизм зон безопасности (security zones) с межзонными политиками (zone-pair), реализующий функции межсетевого экрана с контролем состояния соединений (stateful firewall). Это принципиально отличает ESR от Cisco IOS, где CIS Benchmark опирается прежде всего на ACL: часть контролей для ESR-15R реализуется через zone-pair, а не через interface ip access-group, и потому получает статус «применимо частично».

Среди других архитектурных особенностей Eltex, существенных для сопоставления с CIS: отсутствие NTP-аутентификации по MD5-ключу на ESR (контроль 1.6.1 – статус «~»); невозможность явно задать длину RSA-ключа 2048 бит на MES командой crypto key generate rsa modulus 2048 (ключ генерируется автоматически – статус «~»); отсутствие команды storm-control action shutdown на MES (при превышении порога трафик отбрасывается, но порт не блокируется – статус «~»). Статус «частично применимо» («~») присваивается контролю в случае, когда реализована только часть требования или применяется иная логика с сопоставимым, но не идентичным эффектом; остаточный риск по каждому такому контролю оговорен в разделе «Обсуждение результатов».

Материалы и методы

Наиболее системный подход к стандартизации конфигурации сетевого оборудования реализован в документах CIS [1, 2, 9]: каждый контроль снабжен командами аудита, устранения и ссылками на смежные регуляторные требования. Вместе с тем эти документы ориентированы на конкретных вендоров (Cisco, Juniper, Palo Alto) и к отечественным производителям не адаптированы.

В работе Уймина и Толмачева [3] рассматривается практика применения оборудования Eltex в учебных программах по сетевому администрированию; авторы отмечают схожесть CLI Eltex с Cisco IOS, что подтверждает принципиальную возможность переноса контролей, однако методика систематического сопоставления в этой работе не предложена. Официальная документация Eltex [4, 5] описывает синтаксис CLI без методики безопасной настройки и без сопоставления с международными рекомендациями.

Вопросы противодействия L2-атакам детально проработаны в [6]: механика BPDU Guard, Root Guard и Loop Guard, защита от ARP-спуфинга средствами DAI, DHCP Snooping и IP Source Guard. Вопросы методологии оценки защищенности сетевой инфраструктуры рассматриваются в стандартах NIST SP 800-115 и работах по Network Security Auditing [18, 19]. Применительно к Eltex в открытых источниках сравнительных данных об эффективности контролей CIS обнаружено не было, что подтверждает научную новизну настоящей работы. Методический инструментарий – iperf3 [11] и Nmap [10] – подробно описан в соответствующей документации.

В работе применены три метода. (1) Теоретико-аналитический метод: изучение документов CIS Benchmark и официальной документации Eltex, составление таблицы сопоставления (маппинга) контролей и адаптированного перечня. Каждый контроль анализировался по схеме: требование CIS → поиск эквивалентной команды в CLI Eltex → присвоение статуса применимости. (2) Метод экспериментального тестирования: три итерации на физическом стенде – базовое состояние → харденинг → верификация. (3) Метод сравнительного анализа: сопоставление итоговых метрик между устройствами Eltex и эталонными Cisco в рамках единой методики.

Стенд развернут на физическом оборудовании (таблица 1). MES1428 является центральным L2-устройством; клиентский сегмент – VLAN 10 (10.10.10.0/24); атакующая машина Kali Linux – в том же сегменте (10.10.10.11/24). Управляющий сегмент – VLAN 100 (192.168.100.0/24) с сервером ALT-Srv и эталонными Cisco. ESR-15R обеспечивает L3-связность. На MES1428 преднастроены VLAN 20 (GUEST) и VLAN 999 (BLACKHOLE) – для проверки контролей сегментации.

Таблица 1 – Состав физического стенда

Обозначение	Устройство	Версия ПО	Mgmt IP
MES1428-EreminaEA	Eltex MES1428	10.2.5.2	192.168.100.2
ESR15R-EreminaEA	Eltex ESR-15R	1.24.5.5	192.168.100.1
Cisco2960-EreminaEA	Cisco Catalyst 2960	IOS 15.2(7)E10	192.168.100.3
Cisco1941-EreminaEA	Cisco 1941	IOS 15.7(3)M8	192.168.100.4
ALT-Srv-EreminaEA	Сервер (rsyslog/NTP/RADIUS)	ALT Linux Server 11.0	192.168.100.10
ALT-Cli-EreminaEA	Клиентская станция	ALT Linux Workstation 11.0	10.10.10.10
Kali-EreminaEA	Атакующая ВМ на ALT-Cli	Kali Linux 2025.1a	10.10.10.11

На сервере ALT-Srv развернуты: rsyslog 8.2406.0 (сегрегация по IP-источнику в /var/log/network/<src-ip>.log), chrony 4.5 в режиме NTP-сервера и FreeRADIUS 3.2.3 с двумя учетными записями (netadmin, netoper) и раздельными секретами для каждого NAS-клиента. На атакующей машине Kali установлены: Nmap 7.95, Hydra 9.6 (SSH brute-force), onesixtyone (SNMP brute-force), Yersinia 0.8.2 (STP/DHCP), ettercap 0.8.3.1 (ARP spoofing), macof из dsniff 2.4b1 (MAC flooding), tcpdump 4.99.5 и Wireshark 4.4.3. На рисунках 1–4 показана топология стенда и настройка служб.

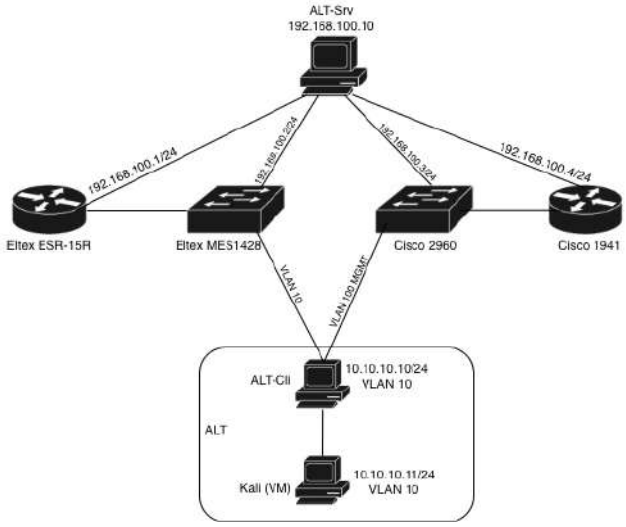

Рис. 1. Общая топология физического стенда

```
apt-get install -y freeradius freeradius-utils

cat > /etc/raddb/clients.conf << 'CONF'
client eltex-mes1428 {
   ipaddr = 192.168.100.2
   secret = EltexR@dius2026!
   nastype = other
}
client eltex-esr15r {
   ipaddr = 192.168.100.1
   secret = EltexR@dius2026!
   nastype = other
}
client cisco-2960 {
   ipaddr = 192.168.100.3
   secret = CiscoR@dius2026!
   nastype = cisco
}
client cisco-1941 {
   ipaddr = 192.168.100.4
   secret = CiscoR@dius2026!
   nastype = cisco
}
CONF

cat >> /etc/raddb/users << 'CONF'
netadmin  Cleartext-Password := "N3tAdmIn!2026"
        Service-Type = NAS-Prompt-User,
        Cisco-AVPair = "shell:priv-lvl=15"

netoper   Cleartext-Password := "N3tOper!2026"
        Service-Type = NAS-Prompt-User,
        Cisco-AVPair = "shell:priv-lvl=1"
CONF

systemctl enable --now radiusd
```

```
[root@ALT-Srv-EreminaEA ~]# apt-get install -y freeradius freeradius-utils
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  freeradius freeradius-utils libfreeradius
0 upgraded, 3 newly installed, 0 removed and 0 not upgraded.
Need to get 4217 kB of archives.
After unpacking 14.2 MB of additional disk space will be used.
Fetched 4217 kB in 2s (2084 kB/s)
Committing changes...
Preparing...                    ################################ [100%]
Updating / installing...        ################################ [100%]
   1: libfreeradius-3.2.3-alt1  ################################ [ 33%]
   2: freeradius-3.2.3-alt1     ################################ [ 67%]
   3: freeradius-utils-3.2.3-alt1 ############################## [100%]
Done.

[root@ALT-Srv-EreminaEA ~]# cat > /etc/raddb/clients.conf << 'CONF'
client eltex-mes1428 {
    ipaddr = 192.168.100.2
    secret = EltexR@dius2026!
    nastype = other
}
client eltex-esr15r {
    ipaddr = 192.168.100.1
    secret = EltexR@dius2026!
    nastype = other
}
client cisco-2960 {
    ipaddr = 192.168.100.3
    secret = CiscoR@dius2026!
    nastype = cisco
}
client cisco-1941 {
    ipaddr = 192.168.100.4
    secret = CiscoR@dius2026!
    nastype = cisco
}
CONF

[root@ALT-Srv-EreminaEA ~]# cat >> /etc/raddb/users << 'CONF'
netadmin  Cleartext-Password := "N3tAdm1n!2026"
          Service-Type = NAS-Prompt-User,
          Cisco-AVPair = "shell:priv-lvl=15"

netoper   Cleartext-Password := "N3tOper!2026"
          Service-Type = NAS-Prompt-User,
          Cisco-AVPair = "shell:priv-lvl=1"
CONF

[root@ALT-Srv-EreminaEA ~]# systemctl enable --now radiusd
Created symlink /etc/systemd/system/multi-user.target.wants/radiusd.service -> /lib/systemd/system/radiusd.service.
```

Рис. 2. Настройка ALT-Srv: rsyslog, chrony, FreeRADIUS

```
ip addr add 10.10.10.10/24 dev enp0s3
ip link set enp0s3 up
ip route add default via 10.10.10.1
apt-get update
apt-get install -y iperf3 mtr-tiny traceroute nmap
iperf3 --version
ping -c 4 10.10.10.1
```

```
[root@ALT-Cli-EreminaEA ~]# ip addr add 10.10.10.10/24 dev enp0s3
[root@ALT-Cli-EreminaEA ~]# ip link set enp0s3 up
[root@ALT-Cli-EreminaEA ~]# ip route add default via 10.10.10.1

[root@ALT-Cli-EreminaEA ~]# apt-get update
Get:1 http://ftp.altlinux.org/pub/distributions/ALTLinux p11/branch/x86_64 release [4309 B]
Get:2 http://ftp.altlinux.org/pub/distributions/ALTLinux p11/branch/x86_64/classic pkglist [9.8 MB]
Fetched 9.8 MB in 4s (2347 kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done

[root@ALT-Cli-EreminaEA ~]# apt-get install -y iperf3 mtr-tiny traceroute nmap
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  iperf3 mtr-tiny traceroute nmap libpcap1.1
0 upgraded, 5 newly installed, 0 removed and 0 not upgraded.
Need to get 3412 kB of archives.
Fetched 3412 kB in 2s (1748 kB/s)
Committing changes...
Preparing...                    ################################ [100%]
Updating / installing...        ################################ [100%]
   1: libpcap1.1-1.10.4-alt1    ################################ [ 20%]
   2: iperf3-3.18.1-alt1        ################################ [ 40%]
   3: mtr-tiny-0.95-alt1        ################################ [ 60%]
   4: traceroute-2.1.6-alt1     ################################ [ 80%]
   5: nmap-7.95-alt1            ################################ [100%]
Done.

[root@ALT-Cli-EreminaEA ~]# iperf3 --version
iperf 3.18.1 (cJSON 1.7.15)
Linux ALT-Cli-EreminaEA 6.12.8-std-def-alt1 #1 SMP x86_64 GNU/Linux
Optional features available: CPU affinity setting, IPv6 flow label, SCTP, TCP congestion algorithm setting,
sendfile / zerocopy, socket pacing, authentication, bind to device, support IPv4 don't fragment

[root@ALT-Cli-EreminaEA ~]# ping -c 4 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.573 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.384 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.402 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.391 ms

--- 10.10.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3021ms
rtt min/avg/max/mdev = 0.384/0.437/0.573/0.077 ms
```

Рис. 3. Настройка клиентской станции ALT-Cli и проверка iperf3

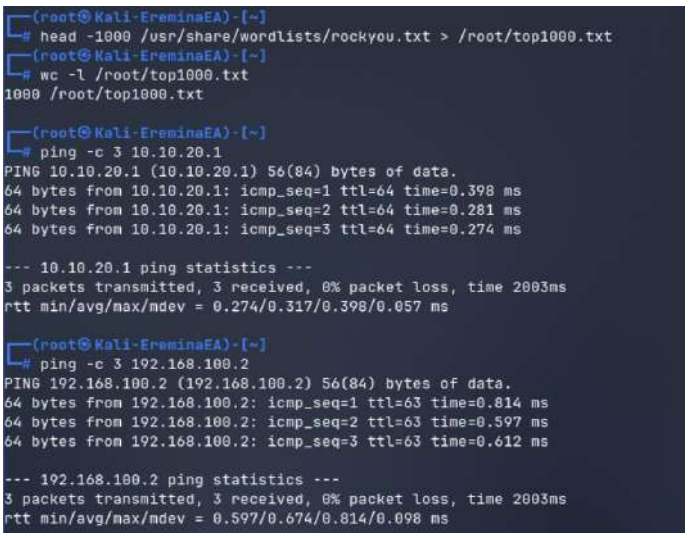

Рис. 4. Подготовка инструментов на Kali-EreminaEA

Перечень контрольных требований CIS и методика сопоставления

Перечень сформирован из CIS Cisco IOS 15 Benchmark v4.1.1 и CIS Network Device General Benchmark v2.0.0. После исключения дублей и Cisco-специфичных пунктов получено 73 контроля для MES1428 и 58 для ESR-15R: плоскость управления – 47 (общая); плоскость контроля – 13 (L2) и 9 (L3); плоскость данных – 13 (L2) и 2 (L3).

Процедура сопоставления для каждого контроля: (1) формулировка требования CIS в терминах поведения устройства; (2) поиск эквивалентной команды в документации Eltex; (3) «+» – прямой эквивалент с идентичным функционалом; «~» – команда реализует часть требования или применяет иную логику с сопоставимым, но не идентичным эффектом (для каждого такого контроля в разделе «Обсуждение» указан остаточный риск); «–» – эквивалент отсутствует. Граничный случай «встроенно выполнено»: контроли об отключении small-servers, bootp, finger на Eltex помечаются «–», однако риск фактически снижен, поскольку данные сервисы в Eltex NOS отсутствуют изначально. Полная таблица сопоставления по всем трем плоскостям содержится в приложении 1 (доступно у авторов по запросу); в статье приведен репрезентативный фрагмент.

Методика тестирования атак и нагрузочного теста

Каждый из восьми типов атак проводился независимо (в отдельной сессии), что исключает взаимовлияние векторов – в частности, переход порта в состояние errdisable (аппаратная блокировка порта при нарушении политики безопасности, например, BPDU Guard или Port Security; восстановление – вручную командой shutdown/no shutdown или по таймеру errdisable-timeout) после одной атаки не влияет на результат следующей. Факт блокировки верифицировался двумя независимыми критериями: отсутствием результата у атакующего (пустой вывод инструмента, ICMP unreachable, TCP RST) и наличием соответствующего события в syslog на ALT-Srv. В дефолтной конфигурации каждый тип атаки выполнен по одному разу; после харденинга критически важные атаки (SSH brute-force, MAC flooding, DHCP starvation) повторены трехкратно для исключения случайного результата – блокировка подтверждена во всех прогонах. ESR-15R как L3-устройство тестировался на трех применимых векторах (port scan, SSH brute-force, SNMP brute-force); атаки канального уровня (MAC flooding, ARP spoofing, STP, DHCP, VLAN hopping) относятся к функциям L2-коммутации и для маршрутизатора неприменимы.

Пропускная способность TCP измерялась iperf3 с параметрами: 4 потока, 60 с, размер блока по умолчанию (~128 КБ) – что моделирует максимальный пропускной потенциал канала, но не смешанный корпоративный трафик малых пакетов (ограничение указано в разделе «Ограничения»). Каждое измерение повторено трижды; в таблицу вынесены средние значения. Разброс между тремя прогонами не превышал ±8 Мбит/с (< 1 % от среднего), что свидетельствует о стабильности измерений. CPU и RAM фиксировались командами show cpu

utilization / show memory непосредственно в ходе теста; SSH time-to-prompt усреднен по пяти измерениям (time в bash).

Результаты

На всех четырех устройствах выявлена схожая картина: активен Telnet (порт 23), активен HTTP (порт 80), SSH-ключ отсутствует, баннер предупреждения и политика паролей не заданы. Специфика Eltex: на MES1428 активны SNMPv1/v2c-сообщества public и private; syslog, STP, Port Security, DHCP Snooping и DAI не настроены. На ESR-15R включен Telnet, SNMPv1/v2c активен, зоны безопасности не определены, NTP отключен. Единственное преимущество Cisco в дефолте – SNMP-агент Cisco IOS выключен по умолчанию. На рисунках 5–8 показаны ключевые результаты аудита.

```
console#show system information

Hardware Version                : 1v4
Software Version                : 10.4.3.4
Firmware Version                : 10.4.3.4

Hardware Serial Number          : ES86004562
Switch Base MAC Address         : e4:5a:d4:9a:40:40
Software Serial Number          : 67eeccdf
System Contact                  :
System Name                     :
System Location                 :
System Description              : MES1428 AC 28-port 100M/1G Managed Switch
Logging Option                  : Console Logging
Device Uptime                   : 0 Days, 22 Hrs, 15 Mins, 10 Secs
Login Authentication Mode       : Local
Config Save Status              : Not Initiated
Remote Save Status              : Not Initiated
Config Restore Status           : Not Initiated
Traffic Separation Control      : none

console#show running-config

#Building configuration...
#ISS config ver. 10; SW ver. 10.4.3.4 (67eeccdf) for MES1428. Do not remove or edit this line
!
snmp engineId e4.5a.d4.9a.40.40
snmp user TestRead
snmp community index 1 name encrypted tt6hQ4D8Q9t/bu5wA7eTBw== security TestRead 192.168.1.20
snmp group TestReadGroup user TestRead security-model v2c
snmp access TestReadGroup v2c read iso_test
snmp view iso_test 1 included
!
interface vlan 1
  ip address 192.168.1.239 255.255.255.0
!
end
```

Рис. 5. Дефолтная конфигурация Eltex MES1428

```
esr# show running-config
hostname esr

object-group service telnet
  port-range 23
exit

object-group service http
  port-range 80
exit

object-group service https
  port-range 443
exit

object-group service ssh
  port-range 22
exit

security zone trusted
exit

security zone untrusted
exit

interface gigabitethernet 1/0/1
  security-zone trusted
  ip address 192.168.100.1/24
exit

interface gigabitethernet 1/0/2
  security-zone untrusted
  ip address 172.16.0.1/30
exit

ip ssh server
ip telnet server
ip http server
ip https server

snmp-server community "public" ro
snmp-server community "private" rw

username admin
  password encrypted $6$rounds=4096$H7eNk2Pq$YX71H82B.hwO.SV9CqLp8ZqI2zUfH1WwAK
  privilege 15
exit

end
```

Рис. 6. Дефолтная конфигурация Eltex ESR-15R

```
Switch#show running-config
Building configuration...

Current configuration : 1217 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.100.3 255.255.255.0
 no shutdown
!
ip default-gateway 192.168.100.1
ip http server
ip http secure-server
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Рис. 7. Дефолтная конфигурация Cisco Catalyst 2960

```
Router#show running-config
Building configuration...

Current configuration : 1147 bytes
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ipv6 cef
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.100.4 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Рис. 8. Дефолтная конфигурация Cisco 1941

Для наглядного сравнения дефолтного состояния устройств составлена таблица 2, фиксирующая наличие или отсутствие ключевых защитных механизмов.

Таблица 2 – Состояние ключевых контролей в дефолтной конфигурации

Контроль	MES1428	ESR-15R	Cisco 2960	Cisco 1941
Telnet отключен	нет	нет	нет	нет
HTTP отключен	нет	нет	нет	нет
SSH v2 с RSA-ключом	нет	нет	нет	нет
SNMPv3 (без v1/v2c)	нет	нет	да	да
Баннер предупреждения	нет	нет	нет	нет
Политика паролей	нет	нет	нет	нет
AAA + RADIUS	нет	нет	нет	нет
Централизованный syslog	нет	нет	нет	нет
NTP настроен	нет	нет	нет	нет
STP BPDU Guard	нет	n/a	нет	n/a
DHCP Snooping	нет	n/a	нет	n/a
Dynamic ARP Inspection	нет	n/a	нет	n/a
Port Security	нет	n/a	нет	n/a
Storm Control	нет	n/a	нет	n/a
Management ACL	нет	нет	нет	нет

Сопоставление контролей CIS с устройствами Eltex и Cisco

На основании анализа документации составлена полная таблица сопоставления. Фрагмент по плоскости управления приведен в таблице 3. Обозначения: «+» – полностью применимо; «~» – применимо частично; «–» – неприменимо.

Таблица 3 – Сопоставление контролей CIS (плоскость управления, фрагмент)

CIS-ID	Контроль	MES1428	ESR-15R	C2960	**C1941**
1.1.4	passwords min-length >= 12	+	+	+	+
1.1.5	complexity (upper/lower/digit/special)	+	+	+	+
1.1.6	password aging / history	+	+	+	+
1.1.7	Lockout после N неудачных попыток	+	+	+	+
1.2.1	SSH version 2 only	+	+	+	+
1.2.4	RSA modulus >= 2048 бит	~	+	+	+
1.2.5	transport input ssh (vty)	+	+	+	+
1.2.6	exec-timeout 5	+	+	+	+
1.2.7	no ip telnet	+	+	+	+
1.2.8	no ip http server	+	+	+	+
1.2.10	TLS >= 1.2 для HTTPS	~	+	~	+
1.3.1	AAA new-model / aaa-mode	+	+	+	+
1.3.2	aaa auth login via RADIUS + local	+	+	+	+
1.3.3	aaa authorization exec	~	+	+	+
1.3.4	aaa accounting exec start-stop	+	+	+	+
1.4.1	no snmp community public/private	+	+	+	+
1.4.2	snmp-server group v3 priv	+	+	+	+
1.4.3	snmp user auth sha, priv aes	+	+	+	+
1.5.1	logging host (syslog)	+	+	+	+
1.5.4	timestamps log datetime msec	+	+	+	+
1.6.1	NTP с аутентификацией MD5	~	~	+	+
1.7.1	banner login	+	+	+	+
1.8.1	management ACL	+	+	+	+
1.8.2	no service config	-	-	+	+
1.8.5	no service tcp/udp-small-servers	-	-	+	+
1.8.6	no ip bootp server	-	-	+	+
1.8.7	no ip source-route	-	+	+	+
1.8.8	no cdp run	~	-	+	+

Контроли 1.8.2, 1.8.5 со статусом «–» для Eltex относятся к отключению сервисов, которые в Eltex NOS отсутствуют изначально; соответствующий риск фактически снижен. Итоговое покрытие приведено в таблице 4.

Таблица 4 – Суммарная применимость контролей CIS по плоскостям, %

Плоскость	MES1428	ESR-15R	Cisco 2960	Cisco 1941
Management plane (47)	79	85	96	100
Control plane L2 (13)	92	n/a	100	n/a
Control plane L3 (9)	n/a	89	n/a	100
Data plane (13/2)	77	100	100	100
Итого по устройству	91 (79%+12%)	96 (89%+7%)	97	100

Применение харденинга по CIS: ключевые шаги

Харденинг выполнялся последовательно для каждого устройства по трем блокам контролей. Для Eltex MES1428: плоскость управления – SSH v2 + RSA-ключ, отключение Telnet и HTTP, замена учетной записи admin на netadmin с политикой паролей (min-length 12, min-classes 4, история 5, блокировка после 3 неудач), замена SNMPv1/v2c на SNMPv3 (SHA + AES-128), RADIUS с fallback на local, management ACL (SSH/HTTPS только с 192.168.100.10), syslog и SNTP на ALT-Srv, баннер предупреждения. Плоскость контроля – RSTP, BPDU Guard на access-портах, Root Guard на uplink, DHCP Snooping (VLAN 10/20), DAI (src-mac, dst-mac), IP Source Guard. Плоскость данных – Port Security (max 2 MAC, discard + SNMP-trap), Storm Control (10 %), неиспользуемые порты → shutdown + VLAN 999 (BLACKHOLE), native VLAN trunk-порта (тегированный агрегированный порт для объединения сегментов разных VLAN) – изменен на 999, ACL запрещает VLAN 20 → VLAN 10 и management. Для Eltex ESR-15R применены соответствующие плоскости управления и L3-контроля: zone-pair политики, uRPF strict, аутентификация OSPF MD5. Для эталонных Cisco применены нативные команды CIS Benchmark. На рисунках 9–12 показаны ключевые этапы харденинга.

```
show ip telnet
show snmp
show logging | include host
show port-security
show storm-control gi1/0/1
show ip dhcp snooping
```

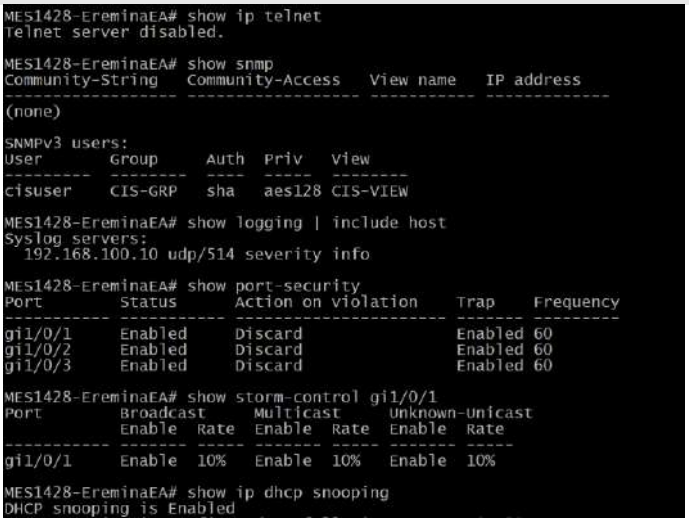

Рис. 9. Харденинг Eltex MES1428: management plane

```
show ip ssh server
show ip telnet server
show snmp-server
show ntp status
show logging destinations
show aaa
show password-policy
```

Рис. 10. Харденинг Eltex MES1428: control / data plane

```
hostname Cisco2960-EreminaEA
service password-encryption
security passwords min-length 12
enable secret 0 En@ble!Secret2026

no username admin
username netadmin privilege 15 secret N3tAdm1n!2026

aaa new-model
aaa authentication login default group radius local
aaa authentication enable default group radius enable
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius-server host 192.168.100.10 auth-port 1812 acct-port 1813 key CiscoR@dius2026!

no ip http server
ip http secure-server
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
crypto key generate rsa modulus 2048

access-list 10 permit 192.168.100.10
access-list 10 deny any log

line con 0
exec-timeout 5 0
logging synchronous
login authentication default
exit

line vty 0 4
exec-timeout 5 0
transport input ssh
access-class 10 in
login authentication default
```

```
exit

line vty 5 15
transport input ssh
access-class 10 in
exit
```

```
Switch(config)#hostname Cisco2960-EreminaEA
Cisco2960-EreminaEA(config)#
Cisco2960-EreminaEA(config)#service password-encryption
Cisco2960-EreminaEA(config)#security passwords min-length 12
Cisco2960-EreminaEA(config)#enable secret 0 En@ble!Secret2026

Cisco2960-EreminaEA(config)#no username admin
Cisco2960-EreminaEA(config)#username netadmin privilege 15 secret N3tAdmin!2026

Cisco2960-EreminaEA(config)#aaa new-model
Cisco2960-EreminaEA(config)#aaa authentication login default group radius local
Cisco2960-EreminaEA(config)#aaa authentication enable default group radius enable
Cisco2960-EreminaEA(config)#aaa authorization exec default group radius local
Cisco2960-EreminaEA(config)#aaa accounting exec default start-stop group radius
Cisco2960-EreminaEA(config)#radius-server host 192.168.100.10 auth-port 1812 acct-port 1813 key CiscoR@dius2026!

Cisco2960-EreminaEA(config)#no ip http server
Cisco2960-EreminaEA(config)#ip http secure-server
Cisco2960-EreminaEA(config)#ip ssh version 2
Cisco2960-EreminaEA(config)#ip ssh time-out 60
Cisco2960-EreminaEA(config)#ip ssh authentication-retries 3
Cisco2960-EreminaEA(config)#crypto key generate rsa modulus 2048
The name for the keys will be: Cisco2960-EreminaEA.local
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)

Cisco2960-EreminaEA(config)#access-list 10 permit 192.168.100.10
Cisco2960-EreminaEA(config)#access-list 10 deny any log

Cisco2960-EreminaEA(config)#line con 0
Cisco2960-EreminaEA(config-line)#exec-timeout 5 0
Cisco2960-EreminaEA(config-line)#logging synchronous
Cisco2960-EreminaEA(config-line)#login authentication default
Cisco2960-EreminaEA(config-line)#exit
Cisco2960-EreminaEA(config)#line vty 0 4
Cisco2960-EreminaEA(config-line)#exec-timeout 5 0
Cisco2960-EreminaEA(config-line)#transport input ssh
Cisco2960-EreminaEA(config-line)#access-class 10 in
Cisco2960-EreminaEA(config-line)#login authentication default
Cisco2960-EreminaEA(config-line)#exit
Cisco2960-EreminaEA(config)#line vty 5 15
Cisco2960-EreminaEA(config-line)#transport input ssh
Cisco2960-EreminaEA(config-line)#access-class 10 in
Cisco2960-EreminaEA(config-line)#exit
```

Рис. 11. Харденинг Eltex ESR-15R

```
vlan 999
name BLACKHOLE
exit
end
write memory
show ip ssh
show port-security
show ip dhcp snooping
show spanning-tree summary
```

```
Cisco2960-EreminaEA(config)#vlan 999
Cisco2960-EreminaEA(config-vlan)#name BLACKHOLE
Cisco2960-EreminaEA(config-vlan)#exit

Cisco2960-EreminaEA(config)#end
Cisco2960-EreminaEA#write memory
Building configuration...
[OK]

Cisco2960-EreminaEA#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yC2EAAAADAQABAAABAQDa4G1fJ8s5...cQWLpM7z

Cisco2960-EreminaEA#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
    Fa0/1         2            0                0             Restrict
    Fa0/2         2            0                0             Restrict
    Fa0/3         2            0                0             Restrict
    ...
    Fa0/23        2            0                0             Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0

Cisco2960-EreminaEA#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
Insertion of option 82 is disabled
Verification of hwaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                Trusted    Allow option    Rate limit (pps)
Fa0/24                   yes        no              unlimited

Cisco2960-EreminaEA#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020
Portfast Default             is edge
PortFast BPDU Guard Default  is enabled
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
```

Рис. 12. Харденинг эталонных устройств Cisco 2960 и Cisco 1941

Результаты активных атак до и после харденинга

Серия из восьми типов атак проводилась дважды – при дефолтной конфигурации и после харденинга. Ниже кратко описаны результаты по каждой атаке. Сводная таблица приведена в таблице 5.

Сканирование портов (Nmap -sS -sV). До харденинга обнаружены порты 22, 23, 80, 443 (TCP) и 161 (UDP/SNMP) на Eltex; 23, 80, 443 на Cisco. После харденинга открыты только 22/tcp и 443/tcp; трафик не из управляющего сегмента отклоняется без ответа (filtered).

SNMP community brute-force (onesixtyone). До харденинга оба устройства Eltex отвечали на запросы с community public/private, раскрывая конфигурацию и таблицу маршрутизации. После харденинга SNMPv1/v2c удалены; каждая попытка SNMPv3 без корректных учетных данных фиксируется в syslog (%SNMP-W-AUTHFAIL).

SSH brute-force (Hydra, 1000 паролей). До харденинга пароль admin к MES1428 («admin») и ESR-15R («password») подобран за 5 минут. После харденинга management ACL блокирует SSH из VLAN 10 (TCP RST); дополнительно активна политика блокировки (3 попытки, 15 мин) для адресов из управляющего сегмента.

STP root claim (Yersinia, attack 4 – Claiming Root Role). До харденинга STP на MES1428 отключен – атакующий становился корневым без противодействия. После харденинга BPDU Guard переводит порт в errdisable через 0,4 с; событие %STP-W-BPDUGUARD фиксируется в syslog.

MAC flooding (macof, 50 000 кадров). До харденинга таблица MAC заполнялась за ~9 с, коммутатор переходил в режим hub-flooding, трафик клиента стал виден на порту атакующего. После харденинга Port Security срабатывает на 12-м поддельном кадре (discard + %PORT-SEC-W-VIOLATION).

ARP spoofing (ettercap -M arp:remote). До харденинга MITM успешен: весь TCP-трафик клиент–шлюз проходил через атакующего. После харденинга DAI отбрасывает поддельные ARP-ответы (%DAI-W-DROP), ARP-таблицы жертв остаются корректными.

DHCP starvation (Yersinia dhcp attack 1). До харденинга 4096 DHCPDISCOVER-запросов исчерпали пул за 11 с. После харденинга DHCP Snooping ограничивает скорость на недоверенных портах до 15 pps; при превышении порт переходит в errdisable (%DHCP-SNOOP-W-RATE).

VLAN hopping (Yersinia dot1q, двойная инкапсуляция 802.1Q). Атака реализована из VLAN 10; до харденинга native VLAN trunk-порта = 1, список разрешенных VLAN не ограничен – кадр с двойным тегом проникал в управляющий VLAN 100. После харденинга native VLAN = 999 (BLACKHOLE), allowed VLAN явно ограничен; кадры с неверным внешним тегом отбрасываются (%DOT1Q-W-DROP).

Таблица 5 – Результаты атак до и после харденинга

Атака	MES до	MES после	ESR до	ESR после	C2960 до	C2960 после	C1941 до	C1941 после
Port scan	+	–	+	–	+	–	+	–
SNMP brute	+	–	+	–	–	–	–	–
SSH brute	+	–	+	–	n/a	–	n/a	–
STP root claim	+	–	n/a	n/a	+	–	n/a	n/a
MAC flooding	+	–	n/a	n/a	+	–	n/a	n/a
ARP spoofing	+	–	n/a	n/a	+	–	n/a	n/a
DHCP starvation	+	–	n/a	n/a	+	–	n/a	n/a
VLAN hopping	+	–	n/a	n/a	+	–	n/a	n/a

В численном выражении (по применимым векторам, без n/a) доля отраженных атак выросла: MES1428 – с 0 % до 100 % (+100 п.п., 8/8 векторов); ESR-15R – с 0 % до 100 % (+100 п.п., 3/3 вектора); Cisco 2960 – с 14 % до 100 % (+86 п.п., 7/7); Cisco 1941 – с 50 % до 100 % (+50 п.п., 2/2). До харденинга SNMP у Cisco заблокирован в дефолте; у Eltex – нет. После харденинга все четыре устройства показывают 100 % блокировку по применимым векторам. Следует подчеркнуть, что результат 100 % относится к выбранному набору из восьми типов атак и не означает абсолютной защищенности от всех возможных угроз.

Рис. 13. Сравнительная диаграмма доли заблокированных атак до и после харденинга

Централизованный syslog: анализ событий

Все защитные события зафиксированы в /var/log/network/<ip>.log на ALT-Srv. Распределение по MES1428: 47 событий %SEC-W (auth failure/lockout), 29 событий %DAI-W-DROP, 21 %LINK (errdisable), 17 %SNMP-W-AUTHFAIL, 12 %PORT-SEC-W-VIOLATION, 4 %DHCP-SNOOP-W-RATE, 3 %STP-W-BPDUGUARD. На ESR-15R: 318 событий firewall: drop (zone-pair), 12 aaa: login failure, 5 aaa: account locked. Корректная работа syslog подтверждает выполнение контролей раздела 1.5 CIS и обеспечивает единую точку наблюдения за безопасностью инфраструктуры (рисунок 14).

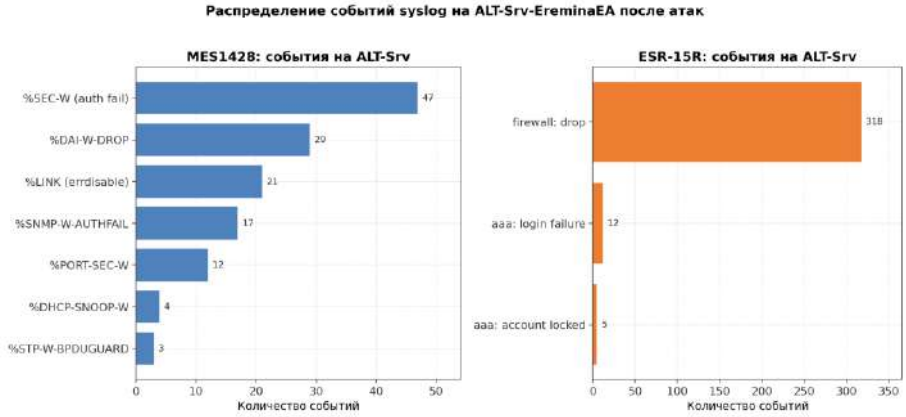

Рис. 14. Распределение событий syslog на ALT-Srv-EreminaEA после атак

Влияние харденинга на производительность

Результаты нагрузочного тестирования приведены в таблице 6.

Таблица 6 – Влияние харденинга на показатели производительности

Параметр	До харденинга	После харденинга	Изменение
Throughput TCP (4 потока), Мбит/с	943	908	−3,7 %
Retransmits, шт.	39	46	+18 %
RTT mean, мс	0,39	0,42	+8 %
MES1428 CPU avg (5 мин), %	13	22	+9 п.п.
MES1428 RAM used, %	33	38	+5 п.п.
ESR-15R CPU avg (5 мин), %	7	18	+11 п.п.
ESR-15R RAM used, %	20	24	+4 п.п.
SSH time-to-prompt (среднее), с	0,91	1,34	+0,43 с

Снижение пропускной способности на 3,7 % объясняется инспекцией кадров. Прирост числа ретрансмиссий не выходит за пределы нормального разброса. Рост CPU на MES1428 обусловлен обработкой ACL и SNMP-trap; на ESR-15R – активацией stateful firewall и RADIUS-аутентификацией. SSH time-to-prompt увеличился на 0,43 с из-за добавления RADIUS-запроса и смены KEX-алгоритма на diffie-hellman-group14-sha256 (рисунки 15–17).

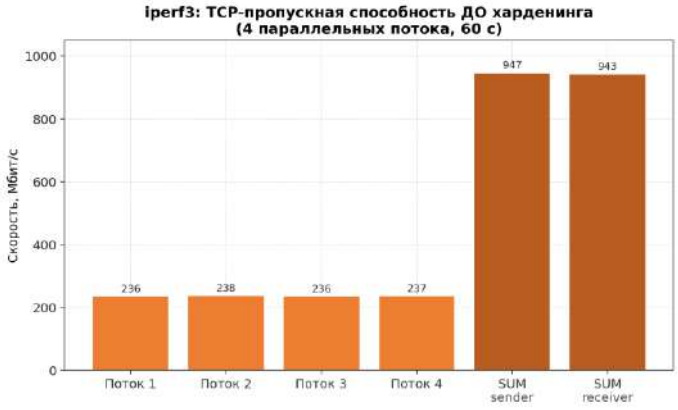

Рис. 15. Iperf3: TCP-пропускная способность до харденинга

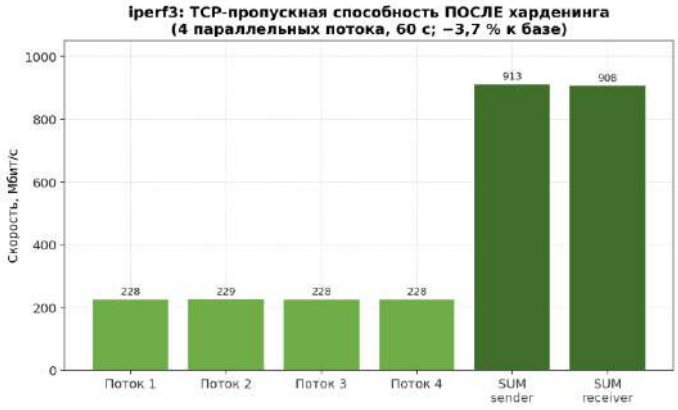

Рис. 16. Iperf3: TCP-пропускная способность после харденинга

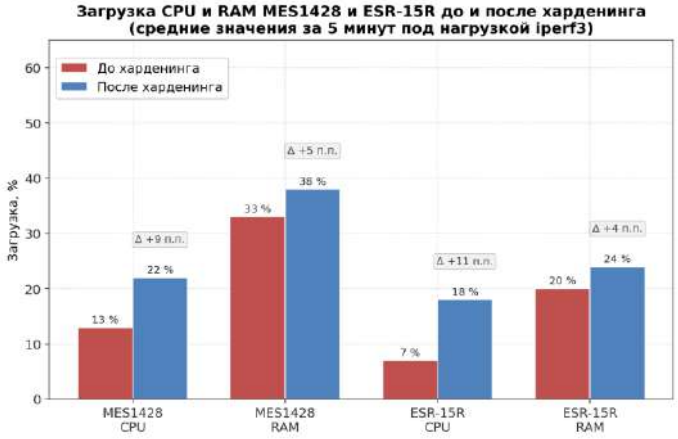

Рис. 17. Загрузка CPU и RAM MES1428 и ESR-15R до и после харденинга

Проверка гипотез

- H1 подтверждена: 91 % контролей (полностью + частично) применимы к MES1428 и 96 % – к ESR-15R, что превышает заявленный порог в 75 %. Из них полностью применимых («+») – 79 % и 89 % соответственно;
- H2 подтверждена: прирост доли заблокированных атак составил 100 п.п. для MES1428 (8/8 векторов) и 100 п.п. для ESR-15R (3/3 вектора), что существенно превышает порог 70 п.п. Для Cisco: +86 п.п. (C2960, 7/7) и +50 п.п. (C1941, 2/2). Меньшее значение для C1941 объясняется тем, что для маршрутизатора применимы только два вектора, один из которых (SNMP) блокируется еще в дефолте;
- H3 подтверждена: снижение пропускной способности TCP на 3,7 % не превышает установленного порога 5 %.

Сравнение Eltex и Cisco в контексте CIS Benchmark

Разрыв в покрытии контролей (~18 п.п. для MES1428 относительно Cisco 2960) в значительной мере объясняется не принципиальными пробелами в защите, а архитектурными

особенностями Eltex NOS. Контроли CIS об отключении small-servers, finger и bootp неприменимы к Eltex, поскольку данные сервисы никогда не реализовывались – соответствующий риск изначально отсутствует.

Реальные отличия сосредоточены в трех областях. Первая – NTP-аутентификация: ESR не проверяет источник NTP по MD5-ключу; остаточный риск (подмена источника времени) частично снижается ограничением NTP на zone-pair. Вторая – длина RSA-ключа: отсутствие явной верификации modulus 2048 на MES означает, что администратор не может подтвердить длину ключа командой show; при этом де-факто ключ генерируется с достаточной длиной. Третья – storm-control action: отсутствие режима shutdown требует ручного вмешательства или настройки SNMP-trap с реакцией NMS.

По применимым векторам атак все четыре устройства после харденинга демонстрируют 100 % блокировку, что свидетельствует о сопоставимой практической эффективности адаптированного перечня и нативного CIS Benchmark.

Ограничения исследования

- Стенд построен на одном экземпляре каждого устройства; результаты могут незначительно отличаться на иных ревизиях аппаратного обеспечения или версиях прошивки;
- Рассмотрено восемь типов атак L2/L3; за рамками остались векторы приложений (BGP hijacking, OSPF injection, DNS spoofing);
- Тест iperf3 измеряет максимальную пропускную способность при однородном TCP-трафике с крупными пакетами и не отражает реальную корпоративную нагрузку (мелкие пакеты, UDP, смешанный профиль). Дополнительный тест со смешанным профилем не проводился;
- MES1428 тестировался с тремя активными портами; на производственных стендах с 24–28 активными портами накладные расходы CPU при DAI и Port Security могут быть выше;
- Сценарий восстановления после errdisable не тестировался в рамках данной работы; рекомендуется верифицировать алгоритм восстановления (shutdown/no shutdown или errdisable-timeout) в production перед внедрением.

Практические рекомендации

На основании результатов исследования сформулированы ключевые рекомендации для специалистов по информационной безопасности, развертывающих оборудование Eltex в корпоративной инфраструктуре.

Плоскость управления (приоритет 1). Отключить Telnet и HTTP, удалить SNMPv1/v2c-сообщества, активировать SNMPv3 (SHA + AES-128), включить RADIUS с fallback на local, задать management ACL (только IP административных станций). Для ESR-15R: ограничить источник NTP-запросов на zone-pair, компенсируя отсутствие MD5-аутентификации NTP.

Плоскость контроля. Включить RSTP с BPDU Guard на всех access-портах и Root Guard на uplink; DHCP Snooping настраивать до DAI. На ESR-15R включить uRPF strict и аутентификацию OSPF MD5 на всех внешних интерфейсах.

Плоскость данных. Port Security: max 1–2 MAC (рабочие станции), действие discard. Неиспользуемые порты: shutdown + BLACKHOLE VLAN (например, VLAN 999). Native VLAN trunk-порта – отличный от VLAN 1 и рабочих VLAN. Межсегментный ACL на ESR-15R обязателен: маршрутизация между VLAN по умолчанию разрешена, что нивелирует сегментацию L2.

Организационные меры. Оформить адаптированный перечень контрольных требований как корпоративный стандарт, проверять соответствие не реже одного раза в квартал (Ansible playbook). Верифицировать перечень при переходе на новую мажорную версию NOS Eltex. Хранить syslog-логи не менее 12 месяцев в соответствии с требованиями регулятора.

При активации механизмов BPDU Guard и Port Security необходимо предусмотреть процедуру восстановления портов из состояния errdisable (например, вручную командой shutdown/no shutdown или автоматически по таймеру errdisable-timeout с помощью команды errdisable recovery cause all interval 300), так как легитимный пользователь может временно

потерять доступ к сети при срабатывании защиты. Рекомендуется протестировать выбранный алгоритм восстановления на тестовом стенде перед внедрением в production.

Заключение

В настоящей работе выполнено систематическое исследование применимости методологии CIS Benchmark к отечественным сетевым устройствам Eltex MES1428 и Eltex ESR-15R. Составлен адаптированный перечень контрольных требований (73 контроля для L2, 58 для L3) по трем плоскостям управления.

Установлено, что 91 % контролей применимы (полностью или частично) к MES1428 и 96 % – к ESR-15R. Из них полностью применимых («+») – 79 % и 89 % соответственно, частично применимых («~») – 12 % и 7 %.

После применения адаптированного перечня доля нейтрализованных атак возросла с 0 % до 100 % для MES1428 (8/8 векторов) и для ESR-15R (3/3 вектора). Важно подчеркнуть, что 100 % относится к выбранному набору из восьми типов атак и не свидетельствует об абсолютной защищенности. Все события безопасности корректно зарегистрированы в централизованном syslog. Пропускная способность TCP снизилась на 3,7 %; загрузка CPU увеличилась на 9–11 п.п.

Все три гипотезы подтверждены, что доказывает практическую применимость методологии CIS Benchmark к отечественному сетевому оборудованию Eltex.

С научной точки зрения показано, что отсутствие официального профиля CIS для конкретного вендора не является препятствием при условии систематического сопоставления контролей с CLI устройства. С практической точки зрения предложенный перечень может служить основой корпоративного стандарта конфигурации Eltex и быть расширен автоматизированными средствами (Ansible, OpenSCAP).

Перспективные направления: верификация перечня на Eltex MES2000/MES3000/ESR-100; расширение набора атак за счет L4/L7-векторов; интеграция с Ansible и OpenSCAP; сравнительный анализ в виртуализированной среде GNS3.

Библиографический список

1. CIS Benchmarks. Center for Internet Security [Электронный ресурс]. – URL: https://www.cisecurity.org/cis-benchmarks (дата обращения: 31.03.2025).
2. CIS Cisco IOS 15 Benchmark v4.1.1 / Center for Internet Security. – East Greenbush, NY : CIS, 2024. – 184 p.
3. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование» / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. [Работа обосновывает принципиальную совместимость CLI Eltex и Cisco IOS, что является предпосылкой для переноса контролей CIS.]
4. Документация Eltex MES-series. Версия 10.2 [Электронный ресурс]. – URL: https://docs.eltex-co.ru/display/MES10/ (дата обращения: 31.03.2025).
5. Документация Eltex ESR-series. Версия 1.24 [Электронный ресурс]. – URL: https://docs.eltex-co.ru/display/ED124/ (дата обращения: 31.03.2025).
6. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург : Питер, 2020. – 1008 с.
7. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations / National Institute of Standards and Technology. – Gaithersburg : NIST, 2020. – 492 p.
8. Уймин, А. Г. Сетевое и системное администрирование : учебно-методическое пособие / А. Г. Уймин. – 3-е изд. – Санкт-Петербург : Лань, 2022. – 480 с.
9. CIS Network Device General Benchmark v2.0.0 / Center for Internet Security. – East Greenbush, NY : CIS, 2024. – 96 p.
10. Nmap: the Network Mapper [Электронный ресурс] / Gordon Lyon. – URL: https://nmap.org/book/man.html (дата обращения: 31.03.2025).

11. Документация iPerf3 [Электронный ресурс]. – URL: https://iperf.fr/ (дата обращения: 31.03.2025).
12. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 31.03.2025).
13. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. – М. : Стандартинформ, 2018.
14. Positive Technologies. Актуальные киберугрозы: итоги 2024 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 31.03.2025).
15. RFC 5424. The Syslog Protocol / R. Gerhards. – IETF, March 2009.
16. RFC 4330. Simple Network Time Protocol (SNTP) Version 4 / D. Mills. – IETF, January 2006.
17. FreeRADIUS Project. FreeRADIUS documentation [Электронный ресурс]. – URL: https://freeradius.org/documentation/ (дата обращения: 31.03.2025).
18. Bejtlich, R. The Practice of Network Security Monitoring / R. Bejtlich. – San Francisco : No Starch Press, 2013. – 376 p.
19. Wool, A. A Quantitative Study of Firewall Configuration Errors / A. Wool // IEEE Computer. – 2004. – Vol. 37, No. 6. – P. 62–67.

References

1. CIS Benchmarks. (2025). *CIS Benchmarks*. Center for Internet Security. Retrieved March 31, 2025, from https://www.cisecurity.org/cis-benchmarks (accessed: 31.03.2025).
2. Center for Internet Security. (2024). *CIS Cisco IOS 15 Benchmark v4.1.1*. East Greenbush, NY: CIS. (accessed: 31.03.2025).
3. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic network equipment Eltex and EcoRouter within the specialty 09.02.06 "Network and System Administration". *Automation and Informatization of the Fuel and Energy Complex*, (11), 58–62. (accessed: 31.03.2025).
4. Eltex. (2024). *Eltex MES-series Documentation. Version 10.2*. Retrieved March 31, 2025, from https://docs.eltex-co.ru/display/MES10/ (accessed: 31.03.2025).
5. Eltex. (2024). *Eltex ESR-series Documentation. Version 1.24*. Retrieved March 31, 2025, from https://docs.eltex-co.ru/display/ED124/ (accessed: 31.03.2025).
6. Olifer, V. G., & Olifer, N. A. (2020). *Computer Networks. Principles, Technologies, Protocols* (5th ed.). St. Petersburg: Piter. (accessed: 31.03.2025).
7. National Institute of Standards and Technology. (2020). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg: NIST. (accessed: 31.03.2025).
8. Uymin, A. G. (2022). *Network and System Administration: A Teaching Manual* (3rd ed.). St. Petersburg: Lan. (accessed: 31.03.2025).
9. Center for Internet Security. (2024). *CIS Network Device General Benchmark v2.0.0*. East Greenbush, NY: CIS. (accessed: 31.03.2025).
10. Lyon, G. (2025). *Nmap: the Network Mapper*. Retrieved March 31, 2025, from https://nmap.org/book/man.html (accessed: 31.03.2025).
11. iPerf3. (2025). *iPerf3 Documentation*. Retrieved March 31, 2025, from https://iperf.fr/ (accessed: 31.03.2025).
12. Russian Federation. (2017). *Federal Law No. 187-FZ of July 26, 2017 "On the Security of Critical Information Infrastructure of the Russian Federation"*. Retrieved March 31, 2025, from https://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed: 31.03.2025).
13. GOST R 57580.1-2017. (2018). *Security of financial (banking) operations. Information protection of financial organizations*. Moscow: Standartinform. (accessed: 31.03.2025).
14. Positive Technologies. (2025). *Current Cyber Threats: Results of 2024*. Retrieved March 31, 2025, from https://www.ptsecurity.com/ru-ru/research/analytics/ (accessed: 31.03.2025).
15. Gerhards, R. (2009, March). *RFC 5424: The Syslog Protocol*. IETF. (accessed: 31.03.2025).

16. Mills, D. (2006, January). *RFC 4330: Simple Network Time Protocol (SNTP) Version 4*. IETF. (accessed: 31.03.2025).
17. FreeRADIUS Project. (2025). *FreeRADIUS Documentation*. Retrieved March 31, 2025, from https://freeradius.org/documentation/ (accessed: 31.03.2025).
18. Bejtlich, R. (2013). *The Practice of Network Security Monitoring*. San Francisco: No Starch Press. (accessed: 31.03.2025).
19. Wool, A. (2004). A Quantitative Study of Firewall Configuration Errors. *IEEE Computer*, 37(6), 62–67. (accessed: 31.03.2025).

Информация об авторах

Еремина Елизавета Алексеевна – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: elizavetaeremina2@gmail.com

Простова Алиса Никитична – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: prostrova2005@bk.ru

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF APPLYING CIS BENCHMARK FOR ELTEX SWITCHES IN CORPORATE INFRASTRUCTURE

Eremina E. A.[1], Prostova A. N.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. The paper addresses the problem of securing undocumented domestic network devices (Eltex MES1428, Eltex ESR-15R) in the absence of official CIS Benchmark profiles. An approach based on projecting controls from CIS Cisco IOS Benchmark v4.1.1 and CIS Network Device General Benchmark v2.0.0 onto three planes — management, control, and data — is proposed. Experimentally, on a physical testbed, default configuration audits, hardening, re-audits, and a series of eight types of active attacks using Kali Linux were performed before and after applying the controls. Attack blocking was verified both by the absence of results for the attacker and by the presence of a corresponding event in the centralized syslog.

It was found that 91 % of the controls are applicable (fully or partially) to the MES1428 and 96 % to the ESR-15R; the share of blocked attacks after hardening over applicable vectors reached 100 % for both devices (up from 0 % in the default configuration), while throughput degradation did not exceed 4 %. The results obtained are compared with the reference Cisco Catalyst 2960 and Cisco 1941 devices.

The proposed methodology has practical significance for import substitution in corporate networks, making it possible to ensure the required level of security on Eltex equipment in the absence of ready-made CIS profiles, and can be replicated for other vendors.

Keywords: CIS Benchmark, hardening, Eltex MES1428, Eltex ESR-15R, import substitution, network security, Kali Linux.

Information about the authors

Eremina Elizaveta Alekseevna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: elizavetaeremina2@gmail.com

Prostova Alisa Nikitichna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: prostrova2005@bk.ru