

Э. Б. Бекнеев<sup>1</sup>, М. В. Марченко<sup>1</sup>

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

## КОМБИНИРОВАННЫЙ ШАБЛОН БЕЗОПАСНОЙ НАСТРОЙКИ МЕЖСЕТЕВОГО ЭКРАНА ELTEX ESR-15R НА ОСНОВЕ CIS BENCHMARK И ПРОФИЛЕЙ ЗАЩИТЫ ФСТЭК: АДАПТАЦИЯ И ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА

**Аннотация.** Рассматривается единый комбинированный шаблон безопасной настройки отечественного межсетевого экрана Eltex ESR-15R, построенный на основе рекомендаций CIS Benchmark и профилей защиты межсетевых экранов ФСТЭК России. Актуальность связана с переходом корпоративных сетей на отечественное оборудование при отсутствии официальных профилей CIS Benchmark для платформ Eltex, из-за чего контролю приходится переносить вручную. Цель работы состоит в адаптации отобранных требований к синтаксису ESR-15R, систематизации мер в таблице по тематическим направлениям CIS и профиля ИТ.МЭ.А4.ПЗ, применении шаблона на лабораторном стенде и проверке наблюдаемых показателей. Методика включает сопоставление рамок, настройку зон безопасности, запрет по умолчанию и ограничение административного доступа, а также проверки сканированием Nmap, генерацией трафика средствами hping3 и scapy, разбором журналов и серией неудачных входов SSH. После применения шаблона порты 22, 23, 80, 443 перестали отвечать на зондирование из недоверенной сети, управляющий адрес стал недоступен из пользовательской сети, в авторской сводке представлены сообщения о запретах и блокировке после неудачных попыток SSH. Раздельные сценарии только CIS и только ФСТЭК не выполнялись, поэтому выводы ограничены проверкой комбинированного шаблона. Материал может служить основой для адаптации и локальной проверки настроек в филиалах перед включением в корпоративный стандарт. Полная воспроизводимость ограничена отсутствием ряда команд и несогласованной адресацией сегмента управления.

**Ключевые слова:** межсетевой экран, CIS Benchmark, профиль защиты, Eltex ESR, фильтрация трафика, hardening, Nmap.

### Введение

Безопасная настройка межсетевых экранов (МЭ) корпоративного периметра стандартизируется проверяемыми чек-листами CIS Benchmark [1] и профилями защиты ФСТЭК России, применимыми с учётом назначения и условий эксплуатации оборудования [2], детализирующими требования приказа ФСТЭК от 09.02.2016 №9 [3]. Ненастроенный экран создает ложное ощущение защищенности при открытой поверхности атаки.

Подходы к построению политик экранирования систематизированы в руководстве NIST, где закреплён запрет по умолчанию и управление жизненным циклом правил [4]. Разведка открытых сервисов как подготовительная техника нарушителя описана в матрице MITRE ATT&CK [5]. Методика построения правил фильтрации с опорой на NIST SP 800-41 и минимизацией ошибок настройки предложена в работе [6]. Ограничения классических методов фильтрации при туннелировании и шифрованном трафике показаны в исследовании [7]; сравнение программных экранов с генерацией трафика и моделированием атак выполнено в работе [8].

Для отечественных платформ задача обостряется импортозамещением: практика внедрения Eltex и EcoRouter описана в работе [9], подход к выбору отечественных платформ по критериям «стоимость-функционал» предложен в исследовании [10], приемы первичной настройки ESR, включая консоль и двухэтапное применение конфигурации, отражены в руководстве [11]. Как показано для коммутаторов Eltex, отсутствие профильного CIS Benchmark для рассматриваемого устройства требует адаптации общих рекомендаций с проверкой их применимости [12]. Настоящая работа переносит эту постановку на класс межсетевых экранов: вместо доказательства преимуществ совместного применения двух рамок проверяется единый комбинированный шаблон с тематическим сопоставлением правил и контрольных направлений CIS и ФСТЭК.

Под CIS Benchmark понимаются консенсусные рекомендации Center for Internet Security с проверками и исправлениями [1]. Под профилем защиты понимается методический документ

## Рубрика 2. Методы и системы защиты информации, информационная безопасность

ФСТЭК с требованиями к МЭ [2–3]. Под hardening понимается отключение лишнего и ужесточение оставшегося. Под поверхностью атаки понимается совокупность доступных нарушителю интерфейсов и сервисов.

Цель работы – проверить единый комбинированный шаблон безопасной настройки ESR-15R, построенный на основе CIS Benchmark и профилей защиты ФСТЭК. Методическое ограничение фиксируется сразу: отдельные сценарии только CIS и только ФСТЭК не выполнялись, количественное сравнение вклада каждой рамки не проводится; сопоставление рамок дано на уровне требований, а измерен только эффект комбинированного шаблона. Задачи работы состоят в следующем:

- сопоставить требования CIS Benchmark и профилей защиты ФСТЭК применительно к функциям МЭ;
- формализовать меры ESR-15R в таблице по направлениям рекомендаций CIS и требованиям профиля ИТ.МЭ.А4.ПЗ, не приписывая им неподтвержденные номера конкретных пунктов;
- применить шаблон на стенде: зоны, запрет по умолчанию, ограничение административного доступа;
- проверить наблюдаемые показатели сканированием Nmap, генерацией трафика, журналами и серией входов SSH.

### Материалы и методы

#### Стенд и протокол эксперимента

Стенд включает МЭ Eltex ESR-15R (сетевая операционная система ветки 1.x, версия руководства по эксплуатации 1.18 [13]), рабочую станцию Windows 11 с PuTTY, Nmap 7.94 с Zenmap, генераторы hping3 и Scapy на узле диагностики, сервер syslog и NTP. Топология: внутренняя сеть 192.168.1.0/24 на br1 (адрес экрана 192.168.1.1/24, узел пользователя 192.168.1.10), управляющий сегмент 10.19.103.0/24 (в материалах одновременно указаны адрес экрана 10.0.0.1/24 на gigabitethernet 1/0/1 и узел администратора 10.19.103.50; эти адреса относятся к разным подсетям и требуют уточнения маршрутизации либо исправления схемы). Исходное состояние – заводская конфигурация без зон и правил фильтрации. Методика сканирования Nmap соответствует руководству проекта [14]; архитектура SSH стандартизирована в RFC 4251 [15]; термины используются по ГОСТ 34.003-90 [16] и ГОСТ Р 57580.1-2017 [17].

Критерии успешности заданы до эксперимента: зондирование портов 22, 23, 80, 443 из недоверенной сети не получает ответа; SSH и HTTPS отвечают только узлу из разрешенной management-сети; запрещающие срабатывания фиксируются в syslog с корректными метками времени; пять последовательных неудачных входов SSH вызывают временную блокировку источника. Протокол проверок приведен в таблице 1.

Таблица 1 – Протокол экспериментальных проверок комбинированного шаблона

| Тест                  | Источник → цель, команда                                            | Ожидание                                   | Факт и подтверждение                                                               |
|-----------------------|---------------------------------------------------------------------|--------------------------------------------|------------------------------------------------------------------------------------|
| T1. Nmap до           | 192.168.1.10 → 192.168.1.1: nmap -sS -p 22,23,80,443 -Pn            | базовые статусы                            | все open; листинг 2                                                                |
| T2. Ping до           | 192.168.1.10 → 192.168.1.1: ping                                    | ответы без ограничений                     | 0% потерь                                                                          |
| T3. Nmap после        | 192.168.1.10 → 192.168.1.1: та же команда                           | ответа нет                                 | все filtered; листинг 6                                                            |
| T4. Изоляция и доступ | 192.168.1.10 → 10.0.0.1 ping; SSH из 192.168.1.10 и из 10.19.103.50 | из LAN ответа нет; SSH только из mgmt      | 100% потерь; SSH из LAN без ответа, из mgmt успешен                                |
| T5. Фильтрация        | hping3 и Scapy: Telnet/HTTP из Untrust; established из Trust        | нелегитимный отброшен, легитимный проходит | 50 отправлено, ответов нет; пример deny в сводке, объем отброшенного не установлен |

| Тест                   | Источник → цель, команда                     | Ожидание                        | Факт и подтверждение                                                     |
|------------------------|----------------------------------------------|---------------------------------|--------------------------------------------------------------------------|
| Т6.<br>Журналы и время | show logging; разбор syslog;<br>сверка NTP   | deny и входы связаны по времени | Примеры deny/login; полный журнал и сверка NTP не приложены              |
| Т7. Перебор SSH        | 5 неудачных входов подряд с одного источника | временная блокировка            | В сводке указана блокировка после 5 попыток; исходный журнал отсутствует |

### Комбинированный шаблон и формализованные правила

Базой служит зональная модель: доверенная зона Trust (внутренняя сеть) и недоверенная зона Untrust (внешняя сеть); весь межзонный трафик по умолчанию блокируется [1–4, 6]. Зоны и пара зон создаются командами security zone (листинг 3). Для пары UNTRUST-TRUST показано правило deny; включение журналирования в представленном фрагменте команд явно не продемонстрировано; конфигурация применяется двухэтапно commit/confirm с окном отката (листинг 4) [11, 13]. Доступ к управлению ограничивается расширенным списком MGMT-ACCESS и объектной группой MGMT\_ACCESS, привязываемой к SSH-серверу, чтобы ограничить SSH выбранной сетью (проверяемый результат приведён в авторской сводке) (листинг 5). Отключение Telnet и HTTP, ограничение HTTPS, настройка паролей, внешнего syslog, NTP и защиты от перебора перечислены в авторской сводке, однако полные конфигурации этих параметров в приведённых листингах отсутствуют [1–3, 15].

Правила сведены в таблицу 2: номер и приоритет, зоны и адреса, сервис, действие и журнал, сопоставление с направлениями CIS и профиля ФСТЭК. Таблица не содержит идентификаторов конкретных пунктов CIS или оценочных компонентов профиля; поэтому это тематическая матрица, а не проверенная постатейная трассировка. Комбинация слоев такова: зональные политики определяют существование межзонного трафика; ACL задает разрешенные источники обращений к демонам; object-group выносит адреса в именованный объект для привязки к SSH. Без слоя MGMT правило deny закрывает транзит, но не ограничивает доступ к самому устройству.

**Таблица 2 – Меры настройки ESR-15R и их тематическое сопоставление с CIS и ФСТЭК**

| №, приоритет | Зоны и адреса                     | Сервис             | Действие, журнал                                          | Тематическая связь с CIS / ФСТЭК               |
|--------------|-----------------------------------|--------------------|-----------------------------------------------------------|------------------------------------------------|
| 10, deny     | UNTRUST → TRUST; любые            | all                | deny; журналирование заявлено, команда не показана        | CIS: deny by default; ФСТЭК: фильтрация        |
| 20, mgmt     | any → self; только 10.19.103.0/24 | SSH 22/TCP         | allow из группы; прочие без ответа                        | CIS: ограничение SSH; ФСТЭК: контур управления |
| 21, web      | any → self; только 10.19.103.0/24 | HTTPS 443/TCP      | allow; HTTP 80 запрещен                                   | CIS: только HTTPS; ФСТЭК: защита управления    |
| 22, службы   | UNTRUST → self; любые             | Telnet 23, HTTP 80 | Рекомендуется ограничить; команда не приведена            | CIS: лишние службы; ФСТЭК: минимизация         |
| 30, ICMP     | UNTRUST → self                    | ICMP               | Недоступность ICMP сообщена; полная политика не приведена | CIS: скрывание; ФСТЭК: скрывание топологии     |
| 40, возврат  | TRUST → UNTRUST established       | обратные сессии    | Разрешение established заявлено, команда не приведена     | CIS и NIST: состояние; ФСТЭК: соединения       |
| 50, аудит    | self → syslog, NTP                | syslog, NTP        | Журналирование и NTP заявлены, команды не приведены       | CIS: syslog и время; ФСТЭК: регистрация        |

### Выбор профиля ФСТЭК и границы соответствия

Для привязки выбран профиль ИТ.МЭ.А4.ПЗ: ESR-15R стоит на границе сегментов и работает на сетевом уровне, что соответствует типу «А»; четвертый класс принят как ориентир

## Рубрика 2. Методы и системы защиты информации, информационная безопасность

для типовой корпоративной инфраструктуры [2–3]. В таблице 2 указаны категории рекомендаций CIS и группы мер профиля (фильтрация, управление, аудит), но отсутствует подтверждённая привязка к номерам конкретных проверок и компонентов требований. Работа не претендует на оценку соответствия и сертификацию; формулировки о соответствии заменены инженерной ориентацией на требования: покрыты базовые механизмы фильтрации, управления и регистрации, вне шаблона остались классовые процедуры жизненного цикла и документирования, требуемые при сертификации.

### **Фрагменты конфигурации и диагностического вывода**

#### **Листинг 1 – Исходное состояние интерфейсов**

```
esr-15r# show ip interfaces
br1 192.168.1.1/24 Up
br2 dhcp Up
```

Проверка связности до настройки показала отсутствие ограничений ICMP: ответы получены со 0% потерь.

#### **Листинг 2 – Nmap до применения шаблона**

```
nmap -sS -p 22,23,80,443 -Pn 192.168.1.1
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
443/tcp open https
```

Все четыре порта отвечали на установление соединения; Telnet передаёт данные сеанса без защиты канала; его отключение соответствует подходу минимизации доступных небезопасных служб [1–3, 15].

#### **Листинг 3 – Зоны и пара зон**

```
config
security zone Trust
description ICN
exit
security zone UNTRUST
description EN
exit
interface bridge 1
security-zone UNTRUST
exit
security zone-pair UNTRUST-TRUST
exit
```

#### **Листинг 4 – Запрещающее правило и применение**

```
security zone-pair UNTRUST-TRUST
rule 10
action deny
enable
exit
exit
do commit
do confirm
```

#### **Листинг 5 – ACL, группа и привязка к SSH**

```
ip access-list extended MGMT-ACCESS
permit ip 10.19.103.0/24 any
deny ip any any
exit
object-group network MGMT_ACCESS
10.19.103.0/24
exit
ip ssh access-addresses MGMT_ACCESS
do commit
do confirm
```

**Результаты**

После применения шаблона повторное сканирование той же командой показало отсутствие ответов: все порты перешли в состояние `filtered`, то есть сканер не может установить, открыт порт или закрыт, поскольку фильтрация препятствует ответу (листинг 6). Такая формулировка сознательно ограничена: `filtered` подтверждает фильтрацию в выбранном сценарии, а отключение служб отдельно заявлено в авторской таблице, но команды выключения Telnet и HTTP в доступных листингах не приведены.

**Листинг 6 – Nmap и ping после применения шаблона**

```
nmap -sS -p 22,23,80,443 -Pn 192.168.1.1
22/tcp filtered
23/tcp filtered
80/tcp filtered
443/tcp filtered
ping 10.0.0.1 (from 192.168.1.0/24)
Request timed out (100% loss)
```

Проверка изоляции дала 100% потерь до 10.0.0.1 из пользовательской сети при успешном SSH из разрешенной management-сети 10.19.103.50 и отсутствии ответа из пользовательской сети. Сообщённый авторами положительный тест из разрешённой сети указывает на сохранение административного доступа при указанной ими адресации; без описания маршрута между 10.19.103.0/24 и 10.0.0.0/24 этот эпизод нельзя воспроизвести однозначно.

Листинг 7 представляет укрупнённую авторскую сводку команд и сообщений (не полный непрерывный вывод терминала или оригинальный журнал). По фразе «50 sent, 0 replies» нельзя доказать, что именно 50 пакетов были отброшены межсетевым экраном; для этого нужны счётчики, запись об отбрасывании каждого пакета либо согласованный захват на обеих сторонах.

**Листинг 7 – Генерация трафика, журнал и перебор**

```
hping3 -S -p 23 192.168.1.1 -c 50 -> 50 sent, 0 replies, deny logged
scapy: TCP(dport=80)/HTTP from Untrust -> dropped, deny logged
syslog: %FW-DENY: UNTRUST-TRUST rule 10 TCP 23 denied
syslog: login failed for admin from 192.168.1.10 (5) -> source blocked
ssh admin@10.0.0.1 from 10.19.103.50 -> established, session logged
```

Сводка наблюдаемых показателей дана в таблице 3. Подчеркивается: сравниваются состояния до и после единого шаблона; отдельные варианты только CIS и только ФСТЭК отсутствуют.

**Таблица 3 – Наблюдаемые показатели до и после применения шаблона**

| Показатель                   | До                        | После                                                           |
|------------------------------|---------------------------|-----------------------------------------------------------------|
| Порты 22, 23, 80, 443 (Nmap) | open                      | filtered из недоверенной сети                                   |
| Telnet и HTTP                | службы включены           | Выключение служб заявлено; команды не показаны                  |
| SSH и HTTPS                  | без ограничений источника | Ограничение управления заявлено; полный набор команд не показан |
| Зоны и политика              | отсутствуют; permit any   | Trust/Untrust; deny any, правило 10                             |
| Ping 10.0.0.1 из LAN         | ответы, 0% потерь         | Нет ответа (100% потерь), путь маршрутизации не описан          |
| Нелегитимный трафик          | проходил                  | 50 послано, 0 ответов; сколько отброшено — не подтверждено      |
| Журналы и время              | локальные, не сверены     | Примеры журнала; синхронизация часов не подтверждена            |
| Перебор SSH (5 попыток)      | без блокировки            | Сообщение о временной блокировке в сводке                       |

## Рубрика 2. Методы и системы защиты информации, информационная безопасность

### Обсуждение

Наблюдаемый переход open → filtered означает, что нарушитель из недоверенной сети лишается подтверждаемых сервисов для разведки; отключение Telnet устраняет один из небезопасных каналов удалённого администрирования [1–3, 15]. Отличие синтаксиса ESR-15R (пары зон, object-group для SSH и commit/confirm) подтверждает необходимость адаптации CIS, ранее показанную для коммутаторов Eltex [12], и согласуется с практикой настройки ESR [11, 13]. Классические методы фильтрации без инспекции содержимого имеют известные слепые зоны [7–8]; данный шаблон их не устраняет, а закрывает базовый уровень.

Ограничения фиксируются явно. Стенд лабораторный: без сложной маршрутизации, граничной нагрузки и VPN-концентрации. Раздельные сценарии не выполнялись, поэтому вывод о совместном применении ограничен проверкой комбинированного шаблона. Производительность при предельной доле мелких пакетов не измерялась; подходы к таким измерениям описаны в работах с генерацией трафика [7–8]. Без регламента backup и периодического reaudit конфигурация деградирует временными разрешениями, поэтому шаблон внедряется циклом «применение – проверка – разбор – обновление» [2–4].

Практический смысл для импортозамещения: представленная модель контроля позволяет сформировать локальный чек-лист настройки и проверки отечественного межсетевого экрана; её результативность за пределами стенда требует отдельной проверки [9–11].

### Заключение

Предложен и проверен единый комбинированный шаблон безопасной настройки ESR-15R: адаптация CIS и требований профиля ИТ.МЭ.А4.ПЗ к синтаксису устройства, описание семи контрольных направлений в тематической матрице, применение части настроек на стенде и анализ авторских результатов. Основные итоги состоят в следующем:

- до применения шаблона порты 22, 23, 80, 443 отвечали на зондирование, управление не ограничивалось;
- после применения зондирование из недоверенной сети осталось без ответа, управляющий сегмент недоступен из пользовательской сети при сохранённом доступе из разрешённой сети;
- таблица мер сопоставляет направления CIS и ФСТЭК, но не заменяет проверку конкретных нормативных и методических пунктов;
- в сводке отражены отсутствие ответов на часть тестовых соединений и отдельные сообщения журнала; количественный показатель доли отброшенных пакетов не подтверждён;
- в авторском примере приведено сообщение о временной блокировке после пяти неудачных попыток входа.

Инженерам рекомендуются следующие шаги:

- фиксировать running-config, версии ПО и перечень служб до изменений;
- применять шаблон блоками с backup и проверкой после каждого блока;
- отключать Telnet, HTTP и нешифрованный SNMP глобально, разрешать SSHv2 и HTTPS точно из management-сети;
- задавать сложность паролей, таймауты и блокировку перебора;
- включать внешний syslog не ниже informational и NTP до ввода в эксплуатацию;
- закреплять reaudit не реже раза в квартал и при смене прошивки или топологии [2–4].

Перспективы – раздельные сценарии только CIS и только ФСТЭК с таблицей различий, сверка полных конфигураций, счётчиков и журналов с чек-листом, тесты при включённых IPSec и граничной нагрузке.

### Библиографический список

1. Center for Internet Security. CIS Benchmarks. – East Greenbush : Center for Internet Security, 2024. – URL: <https://www.cisecurity.org/cis-benchmarks> (дата обращения: 01.06.2026). – Текст : электронный.

2. Профили защиты межсетевых экранов : методический документ : утв. ФСТЭК России 12.09.2016 №240/24/4278. – Москва : ФСТЭК России, 2016. – URL: <https://fstec.ru> (дата обращения: 01.06.2026). – Текст : электронный.
3. Требования к межсетевым экранам : утв. приказом ФСТЭК России от 09.02.2016 №9. – Москва : ФСТЭК России, 2016. – URL: <https://fstec.ru> (дата обращения: 01.06.2026). – Текст : электронный.
4. Scarfone, K. Guidelines on Firewalls and Firewall Policy : NIST Special Publication 800-41 Rev. 1 / K. Scarfone, P. Hoffman. – Gaithersburg : National Institute of Standards and Technology, 2009. – 48 p.
5. MITRE ATT&CK: Enterprise Matrix. – McLean : The MITRE Corporation, 2024. – URL: <https://attack.mitre.org> (дата обращения: 01.06.2026). – Текст : электронный.
6. Старков, Д. И. Методика построения политики безопасности межсетевых экранов / Д. И. Старков ; науч. рук. В. Г. Жуков // КиберЛенинка. – URL: <https://cyberleninka.ru/article/n/metodika-postroeniya-politiki-bezopasnosti-mezhsetevyh-ekranov> (дата обращения: 01.06.2026). – Текст : электронный.
7. Степанова, Е. Ю. Анализ эффективности классических методов фильтрации сетевого трафика в условиях современных киберугроз / Е. Ю. Степанова, Е. В. Расеева // КиберЛенинка. – URL: <https://cyberleninka.ru/article/n/analiz-effektivnosti-klassicheskikh-metodov-filtratsii-setevogo-trafika-v-usloviyah-sovremennyh-kiberugroz> (дата обращения: 01.06.2026). – Текст : электронный.
8. Филоненко, Д. Ю. Анализ методов фильтрации в программных межсетевых экранах / Д. Ю. Филоненко, Д. А. Болдырев, В. А. Пыхтин // Электронный архив УрФУ. – Екатеринбург, 2025. – URL: <https://elar.urfu.ru/handle/10995/143603> (дата обращения: 01.06.2026). – Текст : электронный.
9. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EсоRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – Текст : непосредственный.
10. Носкова, В. А. Разработка сетевой инфраструктуры для IT-компании на отечественном сетевом оборудовании / В. А. Носкова // Вестник науки. – 2026. – № 5(98), Т. 2. – С. 1065–1070. – Текст : непосредственный.
11. Алтунин, В. В. Первоначальная настройка Eltex ESR-200 FSTEC / В. В. Алтунин // Блог AltuninVV. – URL: <https://blog.altuninvv.ru> (дата обращения: 01.06.2026). – Текст : электронный.
12. Еремина, Е. А. Сравнительный анализ эффективности применения CIS Benchmark для коммутаторов Eltex в корпоративной инфраструктуре / Е. А. Еремина, А. Н. Простова // Профессионалитет. – 2025. – № 1(005). – С. 41–59. – Текст : непосредственный.
13. ESR-15R. Руководство по эксплуатации. – Новосибирск : Предприятие «Элтекс», 2024. – URL: <https://docs.eltex-co.ru> (дата обращения: 01.06.2026). – Текст : электронный.
14. Lyon, G. F. Nmap Network Scanning : Official Nmap Project Guide / G. F. Lyon. – Sunnyvale : Insecure.Com LLC, 2009. – 468 p. – URL: <https://nmap.org/docs.html> (дата обращения: 01.06.2026). – Текст : электронный.
15. Ylonen, T. The Secure Shell (SSH) Protocol Architecture : RFC 4251 / T. Ylonen, C. Lonvick. – Fremont : IETF, 2006. – 30 p. – URL: <https://www.rfc-editor.org/rfc/rfc4251> (дата обращения: 01.06.2026). – Текст : электронный.
16. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. – Москва : Изд-во стандартов, 1991. – 24 с.
17. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – Москва : Стандартинформ, 2017. – 54 с.

**References**

1. Center for Internet Security. (2024). CIS Benchmarks. <https://www.cisecurity.org/cis-benchmarks>
2. Federal Service for Technical and Export Control of Russia. (2016). Profili zashchity mezhsetevykh ekranov [Firewall protection profiles] (Methodological Document No. 240/24/4278 of September 12, 2016). <https://fstec.ru>
3. Federal Service for Technical and Export Control of Russia. (2016). Trebovaniya k mezhsetevym ekranam [Firewall requirements] (Order No. 9 of February 9, 2016). <https://fstec.ru>
4. Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy (NIST Special Publication 800-41 Rev. 1). National Institute of Standards and Technology.
5. The MITRE Corporation. (2024). MITRE ATT&CK: Enterprise matrix. <https://attack.mitre.org>
6. Starkov, D. I. (n.d.). Metodika postroeniya politiki bezopasnosti mezhsetevykh ekranov [Firewall security policy methodology]. CyberLeninka. <https://cyberleninka.ru/article/n/metodika-postroeniya-politiki-bezopasnosti-mezhsetevykh-ekranov>
7. Stepanova, E. Y., & Raseeva, E. V. (n.d.). Analiz effektivnosti klassicheskikh metodov filtratsii setevogo trafika v usloviyakh sovremennykh kiberugroz [Analysis of classical network traffic filtering methods under modern cyber threats]. CyberLeninka. <https://cyberleninka.ru/article/n/analiz-effektivnosti-klassicheskikh-metodov-filtratsii-setevogo-trafika-v-usloviyakh-sovremennykh-kiberugroz>
8. Filonenko, D. Y., Boldyrev, D. A., & Pykhtin, V. A. (2025). Analiz metodov filtratsii v programmnykh mezhsetevykh ekranakh [Analysis of filtering methods in software firewalls]. Ural Federal University Electronic Archive. <https://elar.ufu.ru/handle/10995/143603>
9. Uymin, A. G., & Tolmachev, I. M. (2025). Primenenie otechestvennogo setevogo oborudovaniya Eltex i EcoRouter v ramkakh spetsialnosti 09.02.06 “Setevoe i sistemnoe administrirovanie”. Voprosy importozameshcheniya i podgotovki kvalifitsirovannykh kadrov v setevom oborudovanii [Application of domestic Eltex and EcoRouter network equipment within specialty 09.02.06 “Network and system administration”: Import substitution and training of qualified network equipment personnel]. Avtomatizatsiya i informatizatsiya TEK, (11), 58–62.
10. Noskova, V. A. (2026). Razrabotka setevoy infrastruktury dlya IT-kompanii na otechestvennom setevom oborudovanii [Development of network infrastructure for an IT company using domestic network equipment]. Vestnik nauki, 5(98, Vol. 2), 1065–1070.
11. Altunin, V. V. (n.d.). Pervonachalnaya nastroyka Eltex ESR-200 FSTEC [Initial setup of Eltex ESR-200 FSTEC]. AltuninVV Blog. <https://blog.altuninvv.ru>
12. Eremina, E. A., & Prostova, A. N. (2025). Sravnitelnyy analiz effektivnosti primeneniya CIS Benchmark dlya kommutatorov Eltex v korporativnoy infrastrukture [Comparative analysis of CIS Benchmark effectiveness for Eltex switches in corporate infrastructure]. Professionalitet, 1(005), 41–59.
13. Eltex. (2024). ESR-15R. Rukovodstvo po ekspluatatsii [ESR-15R operation manual]. <https://docs.eltex-co.ru>
14. Lyon, G. F. (2009). Nmap network scanning: Official Nmap project guide. Insecure.Com LLC. <https://nmap.org/docs.html>
15. Ylonen, T., & Lonvick, C. (2006). The Secure Shell (SSH) protocol architecture (RFC 4251). Internet Engineering Task Force. <https://www.rfc-editor.org/rfc/rfc4251>
16. USSR State Committee for Standards. (1991). GOST 34.003-90: Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Terminy i opredeleniya [Information technology. Automated systems. Terms and definitions] (24 p.). Standards Publishing.
17. Federal Agency on Technical Regulating and Metrology. (2017). GOST R 57580.1-2017: Bezopasnost finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy [Security of banking operations. Information protection of financial organizations] (54 p.). Standartinform.

### Информация об авторах

Бекнеев Эркен Бааторович — студент 4-го курса специалитета по направлению «Информационно-аналитические системы безопасности», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: bekneev.erken.olymp@gmail.com

Марченко Мария Владиславовна — студентка 4-го курса специалитета по направлению «Информационно-аналитические системы безопасности», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mari.nikiforrovaaa@mail.ru

## COMBINED HARDENING TEMPLATE FOR THE ELTEX ESR-15R FIREWALL BASED ON CIS BENCHMARK AND FSTEC PROTECTION PROFILES: ADAPTATION AND EXPERIMENTAL VERIFICATION

E. B. Bekneev<sup>1</sup>, M. V. Marchenko<sup>1</sup>

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

**Abstract.** This article examines a combined hardening template for the Eltex ESR-15R firewall, informed by CIS Benchmarks and Russian FSTEC firewall protection profiles. The objective is to adapt selected security measures to the ESR-15R interface, organize them by relevant control areas, and evaluate the laboratory observations reported by the authors. The test procedure includes segmentation into security zones, default-deny filtering, restrictions on management access, Nmap probes, hping3 and Scapy traffic generation, inspection of abbreviated log excerpts, and unsuccessful SSH login attempts. In the reported testbed, TCP ports 22, 23, 80, and 443 changed from open to filtered when probed from the user network; the summary also describes the loss of access to a management address and a temporary block after repeated login failures. However, the tables map measures to broad CIS and FSTEC categories rather than to verifiable numbered requirements. Several service and audit settings are not shown in the configuration listings, and the management addresses belong to different IP subnets without an explained routing path. Therefore, the evidence supports a limited assessment of the combined configuration, not a certification or a quantitative measure of the contribution of either framework. Separate CIS-only and FSTEC-only configurations were not tested. The proposed checklist requires complete configuration records and repeatable logs before operational deployment.

**Keywords:** firewall, CIS Benchmark, protection profile, Eltex ESR, traffic filtering, hardening, Nmap.

### Information about the authors

Bekneev Erken Baatorovich — 4th-year specialist's degree student in the direction “Information-Analytical Security Systems”, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: bekneev.erken.olymp@gmail.com

Marchenko Maria Vladislavovna — 4th-year specialist's degree student in the direction “Information-Analytical Security Systems”, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: mari.nikiforrovaaa@mail.ru