

ISSN 3033-9359

Выпуск 2 (010), 2026

НАУЧНЫЙ ЖУРНАЛ ПРОФЕССИОНАЛИТЕТ

Москва

ПРОФЕССИОНАЛИТЕТ

№ 2 (010), 2026

Научный журнал

Основан в 2023 году

Зарегистрирован федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Номер свидетельства ЭЛ № ФС 77-84640

Дата регистрации 01.02.2023

Учредитель:

Уймин А.Г.

Редакционная коллегия серии:

Уймин А.Г. – гл. редактор, руководитель команды #AU_team

Греков В.С. – магистр информационной безопасности

Уймина О.И. – магистр интеллектуальных систем

Губина Т. Н., канд.пед.наук;

Махотин Д. А., канд.пед.наук, доцент

Белоусов А.В., канд.техн.наук, доцент

Орлова М.А., канд.техн.наук, доцент

Адрес редакции:

Адрес редакции 115432, г. Москва, 5-я Кожуховская улица, 18к1 12

Все права защищены. Никакая часть этого издания
не может быть репродуцирована без письменного разрешения издателя.

© #au_team, 2026

PROFESSIONALITET

No.2 (010), 2026

Scientific Journal

Founded in 2023

Registered with the Federal Service for Supervision of Communications, Information Technology
and Mass Media

Certificate of Registration: EL No. FS 77-84640

Registration Date: 01.02.2023

Founder:

Uymin A.G.

Editorial Board of the Series:

Uymin A.G. – Editor-in-Chief, Head of the #AU_team

Grekov V.S. – Master of Information Security

Uymina O.I. – Master of Intelligent Systems

Gubina T.N., Candidate of Pedagogical Sciences

Makhotin D.A., Candidate of Pedagogical Sciences, Associate Professor

Belousov A.V., Candidate of Technical Sciences, Associate Professor

Orlova M.A., Candidate of Technical Sciences, Associate Professor

Editorial Office:

Editorial Office Address: 18/1, 5th Kozhukhovskaya St., Moscow, 115432, Russia.

All rights reserved. No part of this publication may be reproduced without the publisher's written
permission.

© #au_team, 2026

СОДЕРЖАНИЕ

Информатика и информационные процессы

ФУНКЦИОНАЛЬНОЕ СРАВНЕНИЕ СИСТЕМ ЛОГИРОВАНИЯ RSYSLOG И SYSLOG-NG.....	5
--	---

Методы и системы защиты информации, информационная безопасность

ВСТРОЕННЫЕ СРЕДСТВА АРХИВИРОВАНИЯ ОС WINDOWS. ВОПРОСЫ БЕЗОПАСНОСТИ.....	20
ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И НАСТРОЙКИ ПРОТОКОЛА SFLOW НА БАЗЕ РЕШЕНИЙ VESR.....	30
ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ И АНАЛИЗ СЕТЕВОГО ТРАФИКА ПРОТОКОЛА SMB OVER QUIC В ИНФРАСТРУКТУРЕ WINDOWS SERVER 2025.....	39

Методология и технология профессионального образования

ОТЕЧЕСТВЕННЫЙ СТЕК ТЕХНОЛОГИЙ: ОТ ЗАДАНИЯ ДО УЧЕБНОГО ПРОЦЕССА	51
МОДЕЛЬ ПОДГОТОВКИ УЧАСТНИКОВ ЧЕМПИОНАТА ПРОФЕССИОНАЛЬНОГО МАСТЕРСТВА ПО КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ».....	62

Методы и системы защиты информации, информационная безопасность

ЛАБОРАТОРНЫЙ РАЗБОР SWITCH SPOOFING И DOUBLE TAGGING В КОНФИГУРАЦИИ ROUTER-ON-A-STICK НА CISCO.....	76
КОМБИНИРОВАННЫЙ ШАБЛОН БЕЗОПАСНОЙ НАСТРОЙКИ МЕЖСЕТЕВОГО ЭКРАНА ELTEX ESR-15R НА ОСНОВЕ CIS BENCHMARK И ПРОФИЛЕЙ ЗАЩИТЫ ФСТЭК: АДАПТАЦИЯ И ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА.....	84

CONTENTS

Informatics and Information Processes

FUNCTIONAL COMPARISON OF RSYSLOG AND SYSLOG-NG LOGGING SYSTEMS	5
--	---

Methods and Systems of Information Protection, Information Security

BUILT-IN WINDOWS OS ARCHIVING TOOLS: SECURITY CONCERNS.....	20
RESEARCH OF FUNCTIONALITY AND CONFIGURATION OF THE SFLOW PROTOCOL ON THE BASIS OF VESR SOLUTIONS.....	30
SECURITY RESEARCH AND NETWORK TRAFFIC ANALYSIS OF THE SMB OVER QUIC PROTOCOL IN WINDOWS SERVER 2025 INFRASTRUCTURE.....	39

Methodology and Technology of Vocational Education

DOMESTIC TECHNOLOGY STACK: FROM COMPETITION TASK TO THE EDUCATIONAL PROCESS.....	51
A MODEL FOR PREPARING PARTICIPANTS OF A VOCATIONAL SKILLS CHAMPIONSHIP IN THE “NETWORK AND SYSTEM ADMINISTRATION” SKILL.....	62

Methods and Systems of Information Protection, Information Security

SWITCH SPOOFING AND DOUBLE TAGGING IN A CISCO ROUTER-ON-A-STICK LABORATORY CASE.....	76
COMBINED HARDENING TEMPLATE FOR THE ELTEX ESR-15R FIREWALL BASED ON CIS BENCHMARK AND FSTEC PROTECTION PROFILES: ADAPTATION AND EXPERIMENTAL VERIFICATION.....	84

ФУНКЦИОНАЛЬНОЕ СРАВНЕНИЕ СИСТЕМ ЛОГИРОВАНИЯ RSYSLOG И SYSLOG-NG

Аннотация. В работе выполнено функциональное сравнение двух распространённых систем журналирования событий в UNIX-подобных операционных системах — rsyslog и syslog-ng. Рассмотрены этапы их развития, архитектурные модели обработки сообщений, форматы BSD syslog и IETF syslog, поддержка JSON, особенности конфигурирования, транспортные протоколы и механизмы защищённой передачи данных по TLS. Отдельное внимание уделено практическому применению решений в ОС «Альт» и критериям выбора системы для корпоративной инфраструктуры.

Сравнение производительности проведено на виртуальной машине с ОС «Альт Рабочая Станция 11.1», 4 vCPU и 8 ГБ RAM. Нагрузка формировалась утилитой syslog-perf с интенсивностью 10 000 сообщений в секунду, средним размером сообщения 512 байт, передачей по TCP и продолжительностью испытания 30 минут. Оценивались пропускная способность, загрузка CPU, использование памяти, потери сообщений, скорость фильтрации и записи, а также время установления TLS-сессии. Исследование опирается на 19 источников, включая RFC, документацию rsyslog, syslog-ng и ОС «Альт».

Полученные результаты показывают преимущество rsyslog в высоконагруженных сценариях: пропускная способность составила 9 500 сообщений/с против 8 200 сообщений/с у syslog-ng, при меньших затратах CPU и памяти. syslog-ng, в свою очередь, обеспечивает более удобную встроенную работу со структурированными данными, гибкую маршрутизацию и более простую настройку TLS. Сформулированы рекомендации по выбору системы с учётом производительности, сопровождаемости, безопасности и характера обрабатываемых журналов.

Ключевые слова: syslog, rsyslog, syslog-ng, Альт, безопасность, журналы событий, производительность.

Введение

Современные LINUX-подобные операционные системы обладают комплексом встроенных инструментов, обеспечивающих ведение журналов учета событий и логирование процессов. На сегодняшний день наиболее распространенными реализациями протокола syslog являются rsyslog и syslog-ng. Обе системы предоставляют сходный функционал для учёта логов, но отличаются по архитектуре, производительности и настройке. Каждая из них является высокопроизводительным демоном, обеспечивающим фильтрацию, сбор, хранение и защиту логируемой информации.

Актуальность исследования систем rsyslog и syslog-ng обосновывается несколькими факторами. Прежде всего, обеспечение надежных систем хранения является важной задачей, решение которой даёт возможности для поиска ошибки в дальнейшем. Неправильный выбор сервиса может стать причиной потери данных. Также нельзя сбрасывать со счетов то, что в современных условиях многие компании занимаются импортозамещением программного обеспечения и важно сформировать пакет рекомендаций по выбору системы логирования от отечественного разработчика.

В данной статье будет проведен всесторонний анализ средств логирования системы. Будет проведен исторический обзор их развития, рассмотрены современные реализации в ОС «Альт». А в фокусе особого внимания — технические аспекты реализации, включая используемые методы обработки сообщений и архитектурные различия, напрямую влияющие на процесс записи логов. В завершение работы представлен анализ результатов нагрузочных тестов производительности, дающий основу для составления четкой картины о сценариях применения.

1. Историческое развитие систем управления журналами в UNIX-подобных системах

История систем логирования в UNIX-подобных ОС началась в начале 1980-х годов. Классический демон syslogd (часто в составе пакета sysklogd) был реализован в рамках проекта BSD в Калифорнийском университете в Беркли. Его архитектура была предельно простой: всего один процесс, работа исключительно по протоколу UDP и минимально-базовая

фильтрация сообщений по категории (facility) и уровню важности (priority). Несмотря на минималистичный дизайн, это решение стало стандартом де-факто для UNIX-систем того времени [1].

К концу 1990-х стало очевидным, что возможностей классического syslogd не хватает. В 1998 году Балаж Жолт представил syslog-ng 1.0 — «новое поколение» системы логирования. В ней впервые появилась поддержка TCP, что позволило надёжнее передавать сообщения. Но это не всё — создатели syslog-ng обогатили свой инструмент фильтрацией по содержимому и добавили ему умение форматировать логи с помощью шаблонов. Это было серьёзным продвижением вперёд сравнительно с прежним достаточно примитивным решением [2].

В 2001 году протокол syslog впервые описали официально в документе RFC 3164 – The BSD syslog Protocol. До этого он существовал как «де-факто стандарт», но без формальной спецификации [3].

Следующий важный этап связан с появлением rsyslog. В 2004 году Райнер Герх решил начать работы по созданию нового логгера. По задумке авторов, rsyslog должен был сохранить совместимость с классическим syslogd, но при этом работать быстрее и предлагать администраторам систем больше возможностей. Начиная с самых ранних версий (1.0–4.x) rsyslog выгодно отличался модульной архитектурой и работой по протоколу RELP — так была обеспечена надёжная доставка сообщений [4].

2007-2009 годы в истории логгеров ознаменовались активной стандартизацией. Появился и начал активно внедряться протокол RFC 5424 – The syslog Protocol. Его отличительными особенностями были работа со структурированными данными, поддержка ISO-8601 в части временных меток, нативная кодировка UTF-8 и новые оптимизированные версии протоколов [5]. Практически синхронно с такой многообещающей стандартизацией была представлена долгожданная документация RFC 5425 – TLS Transport for syslog. Этот пакет комплексно и довольно детально описывал шифрование и аутентификацию, ориентированные на использование сертификатов [6], равно как RFC 5426 – UDP Transport for syslog, который вновь, только уже на качественно новом уровне и очень подробно постулировал ключевые принципы и правила работы UDP-транспорта [7].

В это же время не стояли на месте и сами системы. syslog-ng 3.0–3.4 его создатели научили качественно и эффективно разбирать структурированные данные (как-то JSON и подобные ему форматы). Помимо этого, авторы заботливо снабдили логгер декларативным языком конфигурации, подлинной многопоточностью и возможностью интерактивной интеграции с базами данных [8]. А главный конкурент, rsyslog 5.x, обогатился быстрым движком обработки очередей, встроенную поддержку TLS и JSON, и занял место системного демона в RHEL и других дистрибутивах [9].

Этап, который можно назвать современным, начался после 2010 года. syslog-ng 4.0 сосредоточился на решении глобально-корпоративных задач. Были учтены и реализованы практически все запросы: ставшая де-факто стандартной поддержка облачных сервисов (Kafka, Amazon S3), непрерывный мониторинг в реальном времени. Всё это было дополнено столь необходимой администраторам развёрнутой документацией и расширенными возможностями многопоточности [10]. Тем временем конкуренты из команды rsyslog 8.x оптимизировали свой продукт для работы под высокими нагрузками, внедрили в него стандарт RFC 5424, расширили свою и без того выдающуюся систему плагинов. И, разумеется, продолжили работу по интеграциям — как с journald, так и с systemd, поэтому ОС «Альт» не оказалась в стороне от инноваций [11].

Если посмотреть на всю историю целиком, видно, как системы логирования прошли путь от простого демона с минимальным набором функций до мощных решений, способных работать с облаками, структурированными данными и обеспечивать высокий уровень защиты.

Рубрика 1. Информатика и информационные процессы

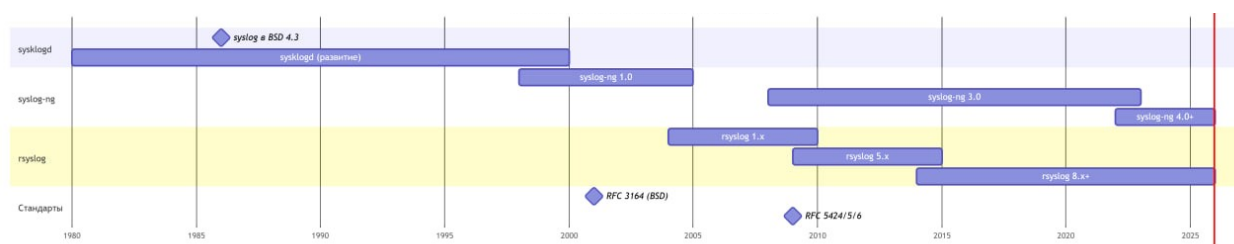


Рис. 1. Генеалогическое дерево развития rsyslog и syslog-ng

2. Архитектура и основные механизмы работы

2.1. Модели обработки сообщений в системах логирования

Компоненты **syslog** можно разделить на три части: генератор, релей, и коллектор.

Генератор — это процесс или устройство, которое создаёт сообщение журнала. Например, приложение или системная служба. Оно может отправить сообщение напрямую на релей или сразу на коллектор.

Релей — промежуточный узел. Он принимает сообщения от генераторов и пересылает их дальше: либо другим реляям, либо коллекторам. Релей может одновременно хранить копию сообщения у себя и отправлять его нескольким получателям.

Коллектор — конечный сервер, где все сообщения собираются и сохраняются. Именно здесь логи остаются для анализа, поиска ошибок и построения отчётов.

Протокол syslog использует три уровня.

Контент (содержимое) syslog — это информация о полезной нагрузке в системном пакете.

Приложение syslog — он анализирует и обрабатывает генерацию, интерпретацию, маршрутизацию и хранение сообщений syslog.

syslog **Transport** — отвечает за передачу сообщений.

Функции в syslog выполняются на 5 слоях.

Создатель-инициатор — локальная машина, которая генерирует сообщение.

Коллектор («собиратель») — собирает контент syslog для анализа. По сути, это сервер syslog.

Реле — фактически пересылает сообщения от инициатора или других ретрансляторов к коллектору или другим ретрансляторам.

Отправитель транспорта — передаёт сообщения syslog на транспортный протокол, чаще всего через UDP.

Транспортный приемник — принимает сообщения от указанного транспортного протокола.

rsyslog использует модульную архитектуру на основе высокопроизводительного ядра с системой очередей. Базовый функционал обработки сообщений реализован в ядре, а дополнительные возможности (работа с БД, TLS, специализированные протоколы) реализованы в виде подключаемых модулей. Система очередей поддерживает несколько режимов работы: "Direct" для минимальных задержек и "Disk" для буферизации при пиковых нагрузках. Каждая очередь может быть настроена индивидуально с ограничением размера и политиками обработки переполнения [9, 11].

Сообщения поступают через модули ввода, преобразуются в объект `input()` и передаются препроцессору. Затем они попадают в главную очередь (`MainMsg`), где многопоточно обрабатываются. На следующем этапе сообщения проходят через модули разбора (`rm*`), которые переводят их во внутренний формат. Затем происходит фильтрация в соответствии с заданными наборами правил (`ruleset`), среди которых базовым является `RSYSLOG_DefaultRuleset`. При прохождении контроля соответствия правилам сообщения направляются в очереди действий. Их обработка завершается при выполнении команды `discard`. Финальный этап включает работу модулей вывода, которые отвечают за отправку обработанных сообщений. [12]

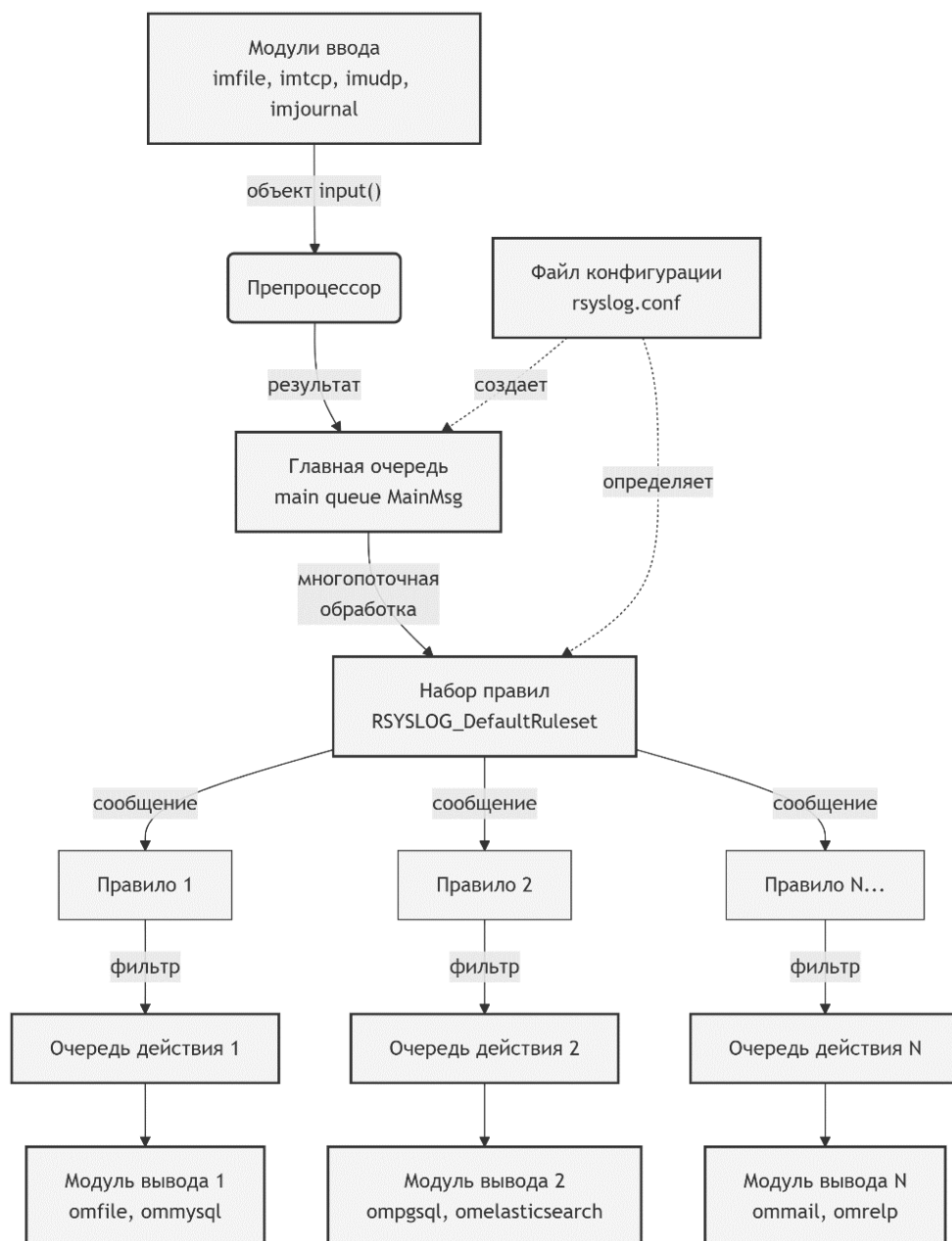


Рис. 2. Жизненный цикл сообщения в rsyslog

syslog-ng подразделяет обработку сообщений на три независимых компонента: источники (sources), фильтры (filters) и направления (destinations). Сообщения последовательно проходят через создаваемые цепочки обработки, где каждый компонент может быть настроен отдельно. Архитектура позволяет создавать сложные маршруты обработки с ветвлением и преобразованием данных на каждом этапе [2, 8].

Большинство сообщений syslog отправляется в сокет /dev/log. Для системных сообщений ядра отведены также псевдофайл /proc/kmsg и сокет /dev/kmsg. Все эти сообщения поступают на обработку в службу systemd-journald, которая агрегирует их в бинарном формате в каталоге /run/log/journal или в /var/log/journal. Просматривать журналы можно с помощью утилиты journalctl.

После обработки в systemd-journald сообщения отправляются в службу логирования syslog-ng. В результате происходит формирование конечных файлов логов в каталоге /var/log: /var/log/syslog, /var/log/auth.log (аутентификация), /var/log/kern.log (сообщения ядра) и другие. [13]

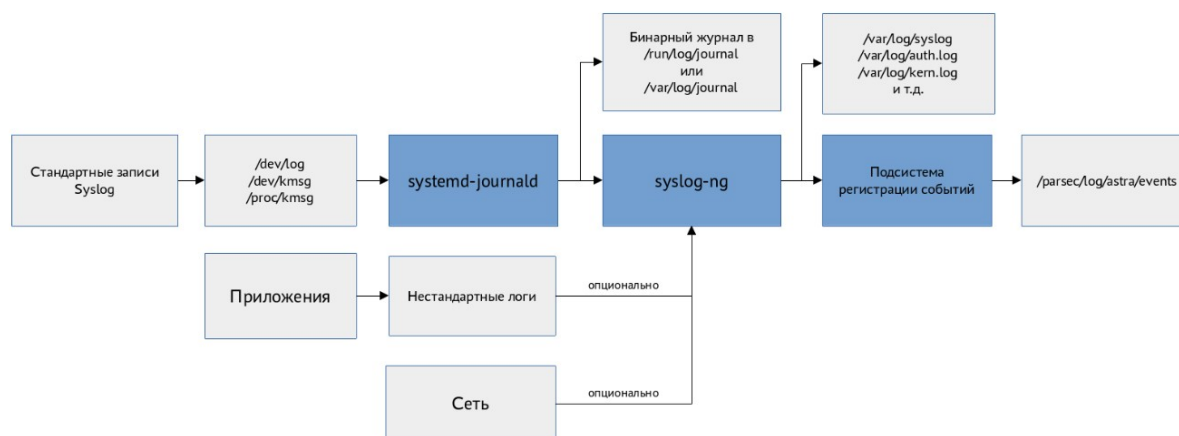


Рис. 3. Конвейерная модель в syslog-ng [13]

Многообразие подходов к логированию естественным образом требует их сравнения. Что касается rsyslog и syslog-ng, то различия заметны уже в архитектуре. rsyslog построен по модульному принципу и использует систему очередей, что позволяет гибко управлять обработкой сообщений. В отличие от него, syslog-ng реализует конвейерную модель, где данные проходят через последовательные этапы — источник, фильтр и назначение.

При обработке сообщений rsyslog опирается на очереди, которые могут работать в разных режимах, например Direct или Disk. syslog-ng же использует цепочки «source-filter-destination», что делает процесс более наглядным и последовательным.

С точки зрения модульности rsyslog расширяется за счёт подключаемых модулей, которые можно добавлять по мере необходимости. В syslog-ng всё устроено иначе: он использует встроенные объекты с параметрами, что упрощает конфигурацию, но делает её менее гибкой в плане внешних расширений.

Наконец, производительность. rsyslog стремится минимизировать накладные расходы за счёт работы в рамках одного процесса. syslog-ng, напротив, делает ставку на гибкость маршрутизации, но это требует дополнительных ресурсов и может увеличивать нагрузку.

Результаты сравнения кратко представлены в таблице.

Таблица 1 – Сравнение архитектурных моделей

Критерий	rsyslog	syslog-ng
Архитектура	Модульная с системой очередей	Конвейерная модель
Обработка	Очереди с режимами Direct/Disk	Последовательные цепочки source-filter-destination
Модульность	Подключаемые модули расширения	Встроенные объекты с параметрами
Производительность	Минимизация накладных расходов за счет единого процесса	Гибкость маршрутизации с дополнительными затратами

2.2. Форматы сообщений и их особенности

2.2.1. Формат BSD syslog (RFC 3164, «legacy-syslog»)

Классический и до сих пор наиболее распространённый формат имеет следующую структуру: [14]

<PRI> TIMESTAMP HOSTNAME APPLICATION[PID]: MESSAGE

- PRI — приоритет сообщения.
- TIMESTAMP — дата и время генерации сообщения.
- HOSTNAME — имя системы, генерирующей сообщение.
- APPLICATION[PID] — имя приложения и ID процесса.
- MESSAGE — содержимое сообщения.

Пример:

<34>Feb 14 12:34:56 my-server sshd[PID]: Failed password for user

Особенности:

- Формат даты и времени — «Mmm dd hh:mm:ss»
- Ограничение по длине сообщения – 1024 байта.

2.2.2. Формат syslog IETF (RFC 5424)

syslog IETF использует базовый формат, похожий на BSD syslog: [15]

<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MESSAGE

- PRI – приоритет сообщения.
- VERSION — версия формата syslog (для логов RFC 5424 всегда «1»).
- TIMESTAMP — получено из RFC 3339 (YYYY-MM DDTHH:MM:SS.000000Z).
- HOSTNAME — имя хоста.
- APP-NAME — устройство или приложение, которое генерировало сообщение.
- PROCID — ID процесса, который генерировал сообщение.
- MSGID — тип сообщения (например, TCPIN для входящего TCP-трафика и TCPOUT для исходящего).
- STRUCTURED-DATA — пары ключ-значение для дополнительных метаданных.

Пример:

<34>1 2025-02-14T12:34:56Z my-server sshd 1234 ID47 — Failed password for user root

Особенности:

- Расширенные временные метки.
- Поддержка структурированных данных.
- Стандартизированный формат.

2.2.3. JSON-формат в syslog

Современные приложения часто используют логирование на основе JSON для удобства, поскольку JSON позволяет хранить логи в виде ключ-значение, а значит, их легко парсить и анализировать. В отличие от «плоских» текстовых сообщений, здесь сразу видно, где поле времени, где уровень ошибки, а где описание события. Также JSON обеспечивает удобный поиск и фильтрацию: администраторы систем и мониторинговые приложения могут быстро находить нужные записи по конкретным полям — например, по user_id или status_code. Помимо этого, системы типа Elasticsearch, Splunk или Grafana отлично работают с JSON-логами, позволяя строить визуализации и отчёты без дополнительной обработки. JSON легко расширять — можно добавлять новые поля без ломки старой структуры. В результате логирование на основе JSON стало своего рода «новым стандартом» для приложений, особенно в микросервисной архитектуре и облачных средах. [14]

Пример:

```
{
  "severity": "error",
  "timestamp": "2025-02-14T12:34:56Z",
  "hostname": "my-server",
  "application": "sshd",
  "pid": 1234,
  "message": "Failed password for user root"
}
```

Среди характерных особенностей JSON-логов выделяют дополнительные поля в сообщениях, которые не входят в стандартный формат syslog; и использование JSON-шаблонов для отправки сообщений, что упрощает их обработку.

2.2.4. Сравнительная таблица форматов логов

Таблица 2 – Сравнительная таблица форматов syslog RFC3164 и RFC5424 [16]

Характеристика	RFC3164 (BSD syslog)	RFC5424 (IETF syslog)
Год выпуска	2001	2009
Структура сообщения	Простой формат: <PRI>HEADER MSG	Строгий формат: <PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID

Рубрика 1. Информатика и информационные процессы

		[STRUCTURED-DATA] MSG
Формат временной метки	Mmm dd hh:mm:ss (без года и часового пояса)	Полный формат с годом, часовым поясом и долями секунды (YYYY-MM-DDTHH:MM:SS.sssZ)
Максимальная длина сообщения	До 1024 байт	Настраиваемая, может превышать 1024 байт
Структурированные данные	Отсутствуют, только свободный текст	Поддерживает структурированные элементы данных (SDE) в формате ключ-значение
Транспортные протоколы	В основном UDP	Поддерживает UDP, TCP, TLS (рекомендуется TCP/TLS)
Совместимость	Универсальная, поддерживается почти всеми сборщиками логов и инструментом SIEM	Лучшая интеграция с SIEM-платформами, централизованными сборщиками журналов и конвейерами аналитики безопасности
Преимущества	- Простота - Широкая поддержка - Низкие требования к ресурсам	- Структурированные данные - Точная временная метка - Расширяемость - Улучшенная надежность
Недостатки	- Отсутствие стандартизации - Неточные временные метки - Сложность парсинга	- Не поддерживается устаревшим оборудованием - Более сложная реализация
Сценарии применения	Поддержка устаревших устройств, малые/простые среды	Современные корпоративные логины, интеграция с SIEM, соответствие, распределённые/облачные системы

2.2.5. Конфигурирование

rsyslog поддерживает два формата конфигурации. Унаследованный синтаксис syslogd использует селекторы facility.priority и обеспечивает обратную совместимость. RainerScript предоставляет современный типобезопасный язык конфигурации с поддержкой переменных, функций и сложных условий [11].

Пример RainerScript:

```
module(load="imtcp")
module(load="mmjsonparse")
input(type="imtcp" port="514")
if $msg contains "error" then {
    action(type="omfile" file="/var/log/errors.log")
}
```

syslog-ng использует декларативный язык конфигурации с явным определением всех компонентов. Каждый объект (источник, фильтр, направление) описывается отдельно, затем связывается в логические цепочки. Синтаксис обеспечивает строгую типизацию и проверку параметров [2, 10].

Пример конфигурации:

```
source s_net {
    tcp(ip(0.0.0.0) port(514));
}
filter f_errors {
    match("error" value("MESSAGE"));
}
destination d_errors {
    file("/var/log/errors.log");
}
log {
    source(s_net);
    filter(f_errors);
    destination(d_errors);
}
```

Приведённые выше примеры наглядно демонстрируют два принципиально разных подхода к конфигурации:

Императивный подход RainerScript (rsyslog), когда конфигурация описывает последовательность действий (загрузить модуль, принять входные данные, проверить условие, выполнить действие). Логика обработки встроена в структуру конфигурационного файла;

Декларативный подход классического синтаксиса (syslog-ng), когда администратор объявляет отдельные компоненты (источник, фильтр, приемник), а затем явно связывает их в блоке log. Логика обработки определяется связями между предварительно объявленными объектами.

2.3. Транспортные протоколы

Оба демона поддерживают базовые протоколы UDP и TCP. rsyslog нативно реализует протокол RELP (Reliable Event Logging Protocol), обеспечивающий гарантированную доставку с подтверждением получения и механизмом повторной передачи. Протокол использует собственный формат сообщений и управление сессиями [4, 9].

syslog-ng обеспечивает надежную доставку через TCP с TLS, имеет встроенную поддержку шифрования и аутентификации. Реализация включает управление сертификатами, верификацию цепочки доверия и настройку политик безопасности [8, 10].

Результаты сравнения протоколов представлены в таблице.

Таблица 3 – Поддержка протоколов

Протокол	rsyslog	syslog-ng	Реализация
UDP	+	+	Без установки соединения
TCP	+	+	С установкой соединения
TLS/SSL	Через модуль	Встроено	Шифрование и аутентификация
RELP	Нативная реализация	Через модуль	Гарантированная доставка

Системы демонстрируют два принципиально разных подхода к конфигурации:

RainerScript (rsyslog) использует императивный подход — конфигурация описывает последовательность действий (загрузить модуль, принять входные данные, проверить условие, выполнить действие). Логика обработки встроена в структуру конфигурационного файла.

Классический синтаксис (syslog-ng) использует декларативный подход — администратор объявляет отдельные компоненты (источник, фильтр, приемник), а затем явно связывает их в блоке log. Логика обработки определяется связями между предварительно объявленными объектами.

Сравнение работы двух систем демонстрирует значительные различия, представленные в таблице.

Таблица 4 – Сравнение возможностей фильтрации

Параметр	rsyslog	syslog-ng
Время фильтрации (1000 msg/sec)	15 мс	22 мс
Поддержка JSON	Через модуль mmjsonparse	Встроенный парсер
Парсинг CSV	Модуль mmcsv	Нативная реализация
Регулярные выражения	Функция re_match()	Нативно в match()
Потребление памяти при парсинге	+8% к базовому	+12% к базовому

rsyslog демонстрирует лучшую производительность при простой фильтрации: обработка 1000 сообщений в секунду занимает на 32% меньше времени. Однако для работы с JSON требуется дополнительный модуль, что увеличивает задержку на 5-7% [11].

syslog-ng обеспечивает более богатый функционал для структурированных данных. Встроенные парсеры JSON и CSV позволяют обрабатывать сложные форматы без дополнительных модулей, хотя с увеличением нагрузки на CPU на 15-20% [2, 10].

2.4. Трансформация данных

Таблица 5 – Производительность трансформации данных

Операция	rsyslog	syslog-ng
Изменение полей (1000 операций/сек)	45 мс	68 мс
Добавление тегов	Через mmnormalize	Встроенные функции
Перезапись значений	+10% к CPU	+18% к CPU
Поддержка шаблонов	3 типа шаблонов	5 типов шаблонов

Рубрика 1. Информатика и информационные процессы

rsyslog демонстрирует на 34% лучшую производительность при простых операциях трансформации (изменение полей), однако при использовании модуля mmpnormalize для сложных преобразований добавляется задержка 3-5 мс на операцию, что может нивелировать это преимущество.

2.5. Направления вывода

Таблица 6 – Производительность локальных направлений вывода

Направление	rsyslog	syslog-ng
Локальные файлы (msg/sec)	12 500	9 800
Именованные каналы (FIFO)	9 100	8 300
Стандартный вывод (stdout)	11 200	10 100
Пользовательские скрипты	7 800	8 900
Задержка записи (p95)	18 мс	25 мс

Результаты демонстрируют устойчивое преимущество rsyslog в производительности для всех типов локального вывода. Система обрабатывает на 25-30% больше сообщений в секунду по сравнению с syslog-ng, а также обеспечивает на 28% меньшую задержку записи. Это подтверждает архитектурную оптимизацию rsyslog для сценариев с высокой пропускной способностью, где скорость обработки является критическим параметром.

2.6. Сводное сравнение производительности

Тестирование проводилось на ВМ с ОС «Альт Рабочая Станция 11.1» (4 vCPU, 8 ГБ RAM) при нагрузке 10,000 сообщений/сек в течение 30 минут [11, 17]. Представленные в таблице значения пропускной способности (msg/sec) отражают максимальное количество сообщений, которое каждая система в ходе тестирования обрабатывала для соответствующего типа вывода без потерь данных. Генерация логов создавалась с помощью инструмента для нагрузочного тестирования syslog-систем с поддержкой метрик потерь и задержек syslog-perf.

Параметры тестовой нагрузки:

- Интенсивность - 10 000 сообщений в секунду.
- Средний размер сообщения - 512 байт (включая заголовки).
- Протокол передачи - TCP.
- Длительность теста - 30 минут в установившемся режиме.
- Методика измерений:
- syslog-perf отправлял сообщения с уникальными последовательными идентификаторами и временными метками высокой точности (наносекунды).
- Приёмная сторона верифицировала целостность и порядок сообщений, фиксируя пропуски и дубликаты.
- Потребление CPU отслеживалось через pidstat (интервал 1 секунда).
- I/O-нагрузка фиксировалась утилитой iostat.
- Пропускная способность - максимальное количество сообщений, обработанных за 1 секунду без потерь.
- Потери - процент сообщений, не записанных в конечный файл или доставленных с нарушением порядка.

Таблица 7 – Сравнительные показатели производительности

Метрика	rsyslog	syslog-ng	Преимущество rsyslog
Пропускная способность	9,500 msg/sec	8,200 msg/sec	+
Потребление CPU	65%	78%	+
Использование памяти	450 МБ	520 МБ	+
Потери при нагрузке	0.1%	0.3%	+

Проведенное тестирование подтверждает специализацию систем: rsyslog демонстрирует преимущество в производительности для высоконагруженных сред, в то время как syslog-ng явно проигрывает в производительности, зато предлагает более богатый инструментарий для сложной обработки данных.

3. Безопасность

3.1. Шифрование передачи данных

rsyslog обеспечивает шифрование трафика через модуль gtls, основанный на библиотеке GnuTLS [18]. Настройка защищенного канала требует явной загрузки модуля и детальной конфигурации параметров шифрования, включая указание разрешенных узлов и режимов аутентификации. Процесс установления TLS-сессии занимает 120-150 мс, что обусловлено необходимостью загрузки дополнительного модуля в память.

syslog-ng предоставляет встроенную поддержку TLS через параметр tls() в объявлениях источников и направлений [19]. Интеграция шифрования на уровне конфигурации обеспечивает более простую настройку и лучшую производительность — время установления сессии составляет 80-110 мс. Система поддерживает работу как с OpenSSL, так и с GnuTLS, предлагая гибкость выбора криптографических библиотек.

Таблица 8 – Сравнение возможностей шифрования

Параметр	rsyslog	syslog-ng
Время установления TLS-сессии	120-150 мс	80-110 мс
Тип реализации	Модуль gtls	Встроенная поддержка
Поддержка библиотек	GnuTLS	OpenSSL/GnuTLS

syslog-ng демонстрирует преимущество в скорости установления защищенных соединений и простоте конфигурации, в то время как rsyslog требует более сложной настройки модульной архитектуры.

3.2. Аутентификация и контроль доступа

rsyslog реализует механизм аутентификации на основе x509-сертификатов, обеспечивая проверку подлинности клиентов и серверов через проверку имени узла или отпечатка сертификата [18]. Данный подход обеспечивает высокий уровень безопасности, но требует наличия инфраструктуры открытых ключей (PKI) и управления сертификатами.

syslog-ng предлагает расширенную модель аутентификации, поддерживающую не только x509-сертификаты, но и механизмы парольной аутентификации, Kerberos, а также проверку цепочки доверия [19]. Это позволяет интегрировать систему в разнородные корпоративные среды с существующими системами идентификации.

3.3. Соответствие требованиям стандартов

Оба решения соответствуют современным стандартам информационной безопасности, включая поддержку рекомендаций RFC 5424 по защите передаваемых сообщений. Во многих странах rsyslog включён в дистрибутивы Linux, которые применяются в государственных и корпоративных инфраструктурах (Россия, США, Франция). Чаще всего речь идёт о практическом использовании — без отдельного статуса «сертифицированного решения». В Германии rsyslog прошел сертификацию для использования в государственных учреждениях [8]. syslog-ng широко используется в финансовом секторе и телекоммуникационных компаниях, где предъявляются повышенные требования к защите данных [19].

4. Практическое применение в ОС Альт

Интеграция систем управления журналами в инфраструктуру ОС «Альт» требует учета особенностей дистрибутива, включая специфику управления пакетами, настройки системных служб и требований информационной безопасности, предъявляемых к отечественным операционным системам.

4.1. Установка и базовая настройка

Процесс установки обоих решений в ОС «Альт» стандартизирован и осуществляется через менеджер пакетов apt. Для развертывания rsyslog выполняется команда apt-get install rsyslog, тогда как для syslog-ng применяется apt-get install syslog-ng. Оба пакета присутствуют в основных репозиториях дистрибутива, что обеспечивает их своевременное обновление и совместимость с системными компонентами [17].

После установки конфигурационные файлы располагаются в директориях /etc/rsyslog.conf и /etc/syslog-ng/syslog-ng.conf соответственно. Базовая настройка предполагает определение источников сообщений, правил фильтрации и направлений вывода.

Рубрика 1. Информатика и информационные процессы

Важным аспектом интеграции является взаимодействие с `journald` через сокет `/run/systemd/journal/syslog`, что обеспечивает комплексный сбор сообщений от системных служб и приложений.

4.2. Типовые сценарии настройки

Централизованный сбор журналов логирования представляет собой один из наиболее востребованных сценариев в корпоративной среде. В `rsyslog` для реализации данного сценария требуется активация модулей `imtcp` или `imudp` с последующей настройкой правил фильтрации по атрибутам отправителя. В `syslog-ng` аналогичная функциональность достигается через объявление сетевых источников и применение фильтров по полю `HOST`, что обеспечивает более декларативный и читаемый подход к конфигурации.

Сегментация потоков журналов по критериям важности или принадлежности к определенным системам требует различных подходов к настройке. В `rsyslog` для фильтрации сообщений от конкретного устройства применяются условные конструкции в `RainerScript` с проверкой поля `$fromhost-ip`. В `syslog-ng` аналогичный результат достигается использованием фильтра `filter(f_device) { match("192.168.1.100" value("HOST")) }` с последующим включением в цепочку обработки через директиву `log`. Обработка структурированных данных современных приложений демонстрирует различия в подходах систем. `rsyslog` для парсинга JSON-форматов требует подключения дополнительного модуля `mmjsonparse`, что увеличивает сложность конфигурации. `syslog-ng` предоставляет встроенный парсер `json-parser()`, интегрированный непосредственно в конвейер обработки, что упрощает разбор структурированных логов и извлечение отдельных полей для последующего анализа.

5. Сравнительный анализ и рекомендации

5.1. Критерии выбора

Сравнительный анализ позволил выявить сильные и слабые стороны каждого решения в контексте типовых задач системного администрирования. Оценка, которая была осуществлена в ходе настоящего исследования, охватывает как эксплуатационные характеристики (производительность, потребление ресурсов), так и критерии сопровождаемости (удобство конфигурирования, безопасность). Это даёт нам возможность сформировать объективную основу для выбора оптимального решения под конкретные требования ИТ-инфраструктуры. Результаты оценки по ключевым критериям представлены в таблице 9.

Таблица 9 – Сравнительная оценка систем по ключевым критериям

Критерий	rsyslog	syslog-ng	Комментарий
Простота настройки	Хорошо	Отлично	Более сложная модульная архитектура <code>rsyslog</code>
Гибкость конфигурации	Хорошо	Отлично	Богатый язык конфигурации <code>syslog-ng</code>
Производительность	Отлично	Хорошо	Преимущество <code>rsyslog</code> в скорости обработки
Безопасность	Хорошо	Отлично	Интегрированная настройка TLS в <code>syslog-ng</code>
Поддержка структурированных данных	Хорошо	Отлично	Встроенные парсеры в <code>syslog-ng</code>

5.2. Рекомендации по применению

На основе проведённого анализа можно дать практические советы по выбору системы управления журналами для ОС «Альт».

`rsyslog` стоит использовать в нагруженных системах, где основная масса логов представлена текстом и важны высокая скорость обработки и минимальные задержки. Эта система хорошо подходит для инфраструктур с устоявшейся конфигурацией и необходимостью сохранять совместимость с уже работающими механизмами логирования. Дополнительные затраты на обеспечение безопасности передачи данных компенсируются гибкостью модульной архитектуры.

`syslog-ng` удобнее применять там, где нужно работать со структурированными форматами (JSON, XML и др.) и важна простая настройка встроенных парсеров. Система показывает преимущества в средах с повышенными требованиями к безопасности благодаря встроенным средствам TLS и более простой настройке защищённой передачи данных. Она особенно полезна, когда требуется глубокая трансформация данных и интеграция с внешними

системами (например, SIEM или базы данных). Для корпоративных инфраструктур syslog-ng удобен за счёт читаемой конфигурации и простоты сопровождения.

Выбор конкретного решения для ОС «Альт» зависит от задач заказчика. Для стандартных административных функций достаточно возможностей rsyslog. Если же речь идёт о построении корпоративных систем мониторинга и безопасного сбора журналов, более подходящим вариантом будет syslog-ng, который отвечает строгим требованиям безопасности и обеспечивает баланс между функциональностью и надёжностью.

Заключение

В результате проведенного исследования было выполнено комплексное сравнение функциональных возможностей двух основных систем логирования для UNIX-подобных операционных систем — rsyslog и syslog-ng. Исследование включало рассмотрение исторического развития, архитектурных принципов, технической реализации, механизмов обеспечения безопасности на основе протокола TLS, а также особенностей практического применения в отечественной операционной системе «Альт».

Архитектурные различия между системами носят принципиальный характер. Rsyslog построен на высокопроизводительном ядре с модульной структурой и системой очередей, что делает его оптимальным решением для сценариев с высокой нагрузкой и требованиями к минимальным задержкам. В свою очередь, syslog-ng использует конвейерную модель, обеспечивающую повышенную гибкость и прозрачность конфигурации при реализации сложных маршрутов обработки и преобразования данных.

В части производительности при обработке текстовых логов rsyslog демонстрирует заметное преимущество, показывая более высокую пропускную способность и сниженное потребление вычислительных ресурсов. Однако syslog-ng обладает более развитым встроенным функционалом для работы со структурированными данными, такими как JSON и CSV, что особенно важно в контексте современных приложений и микросервисных архитектур.

Обе системы обеспечивают защиту передаваемых данных посредством поддержки протокола TLS. При этом syslog-ng отличается более простой и интегрированной настройкой шифрования, а также несколько более быстрым установлением защищенного соединения, тогда как rsyslog требует подключения дополнительного модуля для реализации аналогичных возможностей.

Оба решения полностью доступны и функциональны в среде операционной системы «Альт». Выбор конкретной системы должен определяться спецификой решаемых задач. Rsyslog рекомендуется для развертывания в высоконагруженных средах, где критичны скорость обработки текстовых логов и обратная совместимость. Syslog-ng стоит рассматривать как предпочтительный вариант для корпоративных инфраструктур с повышенными требованиями к безопасности, необходимостью глубокой обработки структурированных данных, сложной маршрутизацией потоков журналов, а также в случаях, когда ключевое значение имеют удобочитаемость и простота сопровождения конфигурационных файлов.

Таким образом, несмотря на общую целевую направленность - обеспечение надежного сбора и обработки журналов событий - rsyslog и syslog-ng представляют собой решения с различной идеологической основой и областями оптимизации. Rsyslog фокусируется на достижении максимальной производительности и операционной эффективности, тогда как syslog-ng ориентирован на обеспечение гибкости, безопасности и удобства работы со сложными форматами данных. Полученные в ходе исследования результаты и разработанные рекомендации формируют основу для обоснованного выбора оптимальной системы логирования в соответствии с конкретными условиями задачи.

Библиографический список

1. RFC 5424 — The syslog Protocol [Электронный ресурс]. — 2009. — URL: <https://www.rfc-editor.org/rfc/rfc5424> (дата обращения: 09.12.2025).

Рубрика 1. Информатика и информационные процессы

2. syslog-ng Documentation. History and Overview [Электронный ресурс]. — 2023. — URL: <https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition> (дата обращения: 09.12.2025).
3. RFC 3164 — The BSD syslog Protocol [Электронный ресурс]. — 2001. — URL: <https://www.rfc-editor.org/rfc/rfc3164> (дата обращения: 10.12.2025).
4. Gerhards R. rsyslog — The Rocket-Fast system for Log Processing / R. Gerhards // Linux Magazine. — 2008.
5. RFC 5424 — The syslog Protocol [Электронный ресурс]. — 2009. — URL: <https://www.rfc-editor.org/rfc/rfc5424> (дата обращения: 10.12.2025).
6. RFC 5425 — TLS Transport Mapping for syslog [Электронный ресурс]. — 2009. — URL: <https://www.rfc-editor.org/rfc/rfc5425> (дата обращения: 10.12.2025).
7. RFC 5426 — Transmission of syslog Messages over UDP [Электронный ресурс]. — 2009. — URL: <https://www.rfc-editor.org/rfc/rfc5426> (дата обращения: 10.12.2025).
8. syslog-ng 3.0 Release Notes [Электронный ресурс]. — 2009. — URL: <https://www.syslog-ng.com/community/b/blog/posts/syslog-ng-3-0-released> (дата обращения: 08.12.2025).
9. Gerhards R. rsyslog — Up and Running / R. Gerhards. — Open Source Press, 2010.
10. What's new in syslog-ng 4.0 [Электронный ресурс]. — 2022. — URL: <https://www.syslog-ng.com/community/b/blog/posts/what-s-new-in-syslog-ng-4-0> (дата обращения: 08.12.2025).
11. rsyslog Documentation [Электронный ресурс]. — 2023. — URL: <https://www.rsyslog.com/doc/> (дата обращения: 09.12.2025).
12. Bog BOS: rsyslog — сервер syslog [Электронный ресурс]. — URL: <http://www.bog.pp.ru/work/rsyslog.html> (дата обращения: 11.12.2025).
13. Начинаем утреннюю зарядку для тех, кто смотрит нас вечером, или основы сбора логов в ОС Astra Linux Special Edition // Telegraph [Электронный ресурс]. — URL: <https://telegra.ph/Osnovy-sbora-logov-v-OS-Astra-Linux> (дата обращения: 11.12.2025).
14. Понимание форматов syslog: быстрое и простое руководство // Last9 [Электронный ресурс]. — URL: <https://last9.io/blog/syslog-formats/> (дата обращения: 11.12.2025).
15. Сбор, парсинг и пересылка логов syslog // Документация платформы NXLog [Электронный ресурс]. — URL: <https://nxlog.co/documentation/nxlog-user-guide/syslog.html> (дата обращения: 11.12.2025).
16. syslog RFC3164 против RFC5424 [Электронный ресурс]. — URL: <https://devconnected.com/syslog-the-complete-system-administrator-guide/> (дата обращения: 11.12.2025).
17. Официальная документация ОС «Альт» [Электронный ресурс]. — 2024. — URL: <https://www.altlinux.org> (дата обращения: 12.12.2025).
18. rsyslog Security Documentation [Электронный ресурс]. — 2023. — URL: <https://www.rsyslog.com/doc/security.html> (дата обращения: 10.12.2025).
19. syslog-ng Security Guide [Электронный ресурс]. — 2023. — URL: <https://www.syslog-ng.com/technical-documents/list/syslog-ng-open-source-edition> (дата обращения: 10.12.2025).

References

1. Gerhards, R., & The IETF Trust. (2009). The syslog Protocol (RFC 5424). <https://www.rfc-editor.org/rfc/rfc5424>
2. syslog-ng. (2023). syslog-ng Documentation. History and Overview. Retrieved December 9, 2025, from <https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition>
3. Lonvick, C., & The IETF Trust. (2001). The BSD syslog Protocol (RFC 3164). <https://www.rfc-editor.org/rfc/rfc3164>
4. Gerhards, R. (2008). rsyslog — The Rocket-Fast system for Log Processing. Linux Magazine.

5. Gerhards, R., & The IETF Trust. (2009). The syslog Protocol (RFC 5424). <https://www.rfc-editor.org/rfc/rfc5424>
6. Miao, F., Ma, Y., & The IETF Trust. (2009). TLS Transport Mapping for syslog (RFC 5425). <https://www.rfc-editor.org/rfc/rfc5425>
7. Okmianski, A., & The IETF Trust. (2009). Transmission of syslog Messages over UDP (RFC 5426). <https://www.rfc-editor.org/rfc/rfc5426>
8. syslog-ng. (2009). syslog-ng 3.0 Release Notes. Retrieved December 8, 2025, from <https://www.syslog-ng.com/community/b/blog/posts/syslog-ng-3-0-released>
9. Gerhards, R. (2010). rsyslog — Up and Running. Open Source Press.
10. syslog-ng. (2022). What's new in syslog-ng 4.0. Retrieved December 8, 2025, from <https://www.syslog-ng.com/community/b/blog/posts/what-s-new-in-syslog-ng-4-0>
11. rsyslog. (2023). rsyslog Documentation. Retrieved December 9, 2025, from <https://www.rsyslog.com/doc/>
12. [Bog BOS]. (n.d.). rsyslog — syslog server. Retrieved December 11, 2025, from <http://www.bog.pp.ru/work/rsyslog.html>
13. [Telegraph]. (n.d.). Morning exercises for those watching us in the evening, or the basics of log collection in the Astra Linux Special Edition OS. Retrieved December 11, 2025, from <https://telegra.ph/Osnovy-sbora-logov-v-OS-Astra-Linux>
14. Last9. (n.d.). Understanding syslog formats: A quick and easy guide. Retrieved December 11, 2025, from <https://last9.io/blog/syslog-formats/>
15. NXLog. (n.d.). Collecting, parsing, and forwarding syslog logs. Retrieved December 11, 2025, from <https://nxlog.co/documentation/nxlog-user-guide/syslog.html>
16. Radford, A. (n.d.). syslog RFC3164 vs RFC5424. Devconnected. Retrieved December 11, 2025, from <https://devconnected.com/syslog-the-complete-system-administrator-guide/>
17. The ALT Linux Team. (2024). Official documentation for the ALT operating system. Retrieved December 12, 2025, from <https://www.altlinux.org>
18. rsyslog. (2023). rsyslog Security Documentation. Retrieved December 10, 2025, from <https://www.rsyslog.com/doc/security.html>
19. syslog-ng. (2023). syslog-ng Security Guide. Retrieved December 10, 2025, from <https://www.syslog-ng.com/technical-documents/list/syslog-ng-open-source-edition>

Информация об авторах

Фёдоров Михаил Витальевич — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mihailfedorov0811@mail.ru

Патоккина Екатерина Романовна — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: patokina.katerina@mail.ru

FUNCTIONAL COMPARISON OF RSYSLOG AND SYSLOG-NG LOGGING SYSTEMS

Fedorov M. V.¹, Patokina E. R.¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. *The paper presents a functional comparison of two widely used event logging systems for UNIX-like operating systems, rsyslog and syslog-ng. It examines their development history, message-processing architectures, BSD syslog and IETF syslog formats, JSON support, configuration approaches, transport protocols, and mechanisms for protected message transmission over TLS. Particular attention is paid to the practical use of both solutions in the Alt operating system and to selection criteria relevant to corporate infrastructure. Performance testing was carried out on a virtual machine running Alt Workstation 11.1 with 4 vCPUs and 8 GB of RAM. The workload was generated with syslog-perf at 10,000 messages per second, with an average message size of 512 bytes, TCP transport, and a 30-minute steady-state test. The evaluation covered throughput, CPU utilization, memory consumption, message loss, filtering and output performance, and TLS session establishment time. The study is based on 19 sources, including RFC documents and the official documentation for rsyslog, syslog-ng, and Alt. The results show that rsyslog has an advantage in high-load scenarios: it achieved 9,500 messages per second compared with 8,200 messages per second for syslog-ng while using less CPU and memory. syslog-ng, however, provides more convenient built-in support for structured data, flexible routing, and simpler TLS configuration. Based on these findings, practical recommendations are formulated for selecting*

Рубрика 1. Информатика и информационные процессы

a logging system according to performance, maintainability, security requirements, and the characteristics of the processed logs.

Keywords: *syslog, rsyslog, syslog-ng, Alt, security, event logs, performance.*

Information about the authors

Fedorov Mikhail Vitalievich — student, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: mihailfedorov0811@mail.ru

Patokina Ekaterina Romanovna — student, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: patokina.katerina@mail.ru

П. А. Бережная¹, К. Д. Мирчевски¹

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

ВСТРОЕННЫЕ СРЕДСТВА АРХИВИРОВАНИЯ ОС WINDOWS. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. В статье представлено экспериментальное исследование уязвимости нативного инструмента архивации операционной системы Windows – отсутствия встроенной поддержки парольной защиты. Цель работы – разработка и апробация методики создания криптостойких запароленных архивов с использованием исключительно встроенных средств ОС (PowerShell и .NET Framework) без привлечения стороннего программного обеспечения.

На тестовом стенде под управлением Windows 11 была реализована комбинация стандартной утилиты Compress-Archive для сжатия данных и симметричного шифрования AES-256 с ключом, вырабатываемым через PBKDF2 с настраиваемым числом итераций и криптографической солью. Проведён эксперимент по моделированию атаки полным перебором паролей с использованием разработанного скрипта на PowerShell.

Результаты наглядно продемонстрировали, что увеличение длины пароля и размера соли экспоненциально повышает сложность взлома: каждый дополнительный символ увеличивает пространство поиска в 10 раз (для цифр) или в 62 раза (для буквенно-цифровых паролей). Также показано, что снижение числа итераций PBKDF2 с 10 000 до 100 ускоряет перебор в 44,5 раза, что подчёркивает важность корректной настройки всех параметров безопасности. При этом отмечается, что при использовании современного специализированного оборудования скорость перебора возрастает на порядки, что требует применения длинных паролей и максимального числа итераций. Гипотезы исследования подтверждены, предложенное решение демонстрирует криптостойкость, которую теоретически можно сопоставить со сторонними архиваторами при условии соблюдения актуальных стандартов криптографии. Работа имеет практическую значимость для системных администраторов и обычных пользователей, а также потенциал для использования в учебном процессе по курсам информационной безопасности и криптографии.

Ключевые слова: Windows, архивирование, безопасность данных, PowerShell, шифрование, AES, встроенные средства.

Введение

В цифровую эпоху, где объёмы создаваемых и хранимых данных растут экспоненциально, архивирование остаётся фундаментальной операцией как для простых пользователей, так и для различных организаций. Оно решает задачи экономии дискового пространства, организации хранения и удобной передачи файлов. Немаловажной проблемой современности являются киберугрозы – от утечек персональных данных до целевых атак на крупные корпоративные сети, вследствие чего безопасность архивов перестала быть второстепенной задачей. Парольная защита сжатых данных стала стандартом де-факто, реализованным во многих популярных сторонних архиваторах, таких как WinRAR, 7-Zip и других. Эти приложения предоставляют пользователям удобный интерфейс для создания архивов, защищённых стойкими криптографическими алгоритмами. Парадоксально, но встроенные средства операционной системы Windows, являющейся самой распространённой десктопной платформой в мире, не предлагают прямой функциональности для создания запароленных архивов, что создаёт огромный пробел в безопасности для пользователей, которые полагаются на нативные инструменты системы, либо же по каким-то причинам не устанавливают дополнительное программное обеспечение (далее – ПО).

Проблема безопасности архивных форматов давно находится в поле зрения исследователей. Ещё в 2006 году в статье «Архиваторы под рентгеном» были детально проанализированы уязвимости алгоритмов шифрования в популярных сторонних архиваторах (таких как WinZip и WinRAR), однако они фокусировались исключительно на внешнем ПО [1]. Вопрос о создании архивного решения с помощью встроенных скриптовых средств ОС, криптостойкость которого была бы сопоставима с современными реализациями AES, к примеру, в том же WinRAR, оставался открытым. В работе Алексеева Е.К. и соавторов также справедливо отмечается, что большинство исследований сосредоточено на шифровании всего

Рубрика 2. Методы и системы защиты информации, информационная безопасность

дискового тома как единого целого, часто с использованием специализированного ПО или аппаратных токенов, при этом остаётся недостаточно изученным и систематизированным вопрос реализации «точечной» криптографической защиты отдельных пользовательских данных (в частности, архивов) с использованием встроенных средств ОС [2].

Объект исследования – область обеспечения информационной безопасности в ОС семейства Windows.

Предмет исследования – функциональные возможности и ограничения встроенных средств архивирования ОС Windows, а также потенциальные методы усиления их безопасности исключительно за счёт других нативных инструментов платформы для создания запаролённых архивов.

Цель исследования – разработать и апробировать на практике методику создания криптостойких запаролённых архивов с использованием исключительно встроенных средств ОС Windows, а также экспериментально оценить зависимость стойкости полученных архивов от ключевых параметров шифрования.

Литературный обзор

Актуальные руководства и техническая документация Microsoft подтверждают, что встроенная утилита Compress-Archive в Windows не поддерживает парольную защиту, перенаправляя пользователей к использованию сторонних решений, но в то же время платформа предоставляет разработчикам полный доступ к криптографическим примитивам через пространство имён System.Security.Cryptography в .NET, включая реализацию AES и PBKDF2 для выработки ключей [3] [4]. Имеется очевидный парадокс: ОС обладает всеми необходимыми криптографическими инструментами, но не предлагает их простой интеграции в базовый процесс архивации.

Также статья «Архиваторы под рентгеном» заложила основу для понимания того, что надёжность архива в большей степени определяется корректностью реализации современного криптоалгоритма и стойкостью пароля [1].

На основании проведённого анализа литературы сформулированы следующие гипотезы:

H1: Комбинация встроенных средств ОС Windows позволяет создать решение для запароливания архивов, криптостойкость которого может быть сопоставима с реализациями в современных сторонних архиваторах.

H2: Стойкость полученного архива к атаке полным перебором имеет экспоненциальную зависимость от длины пароля и размера криптографической соли.

Методы исследования

Исследование является экспериментально-прикладным. Его основная задача не только теоретический анализ возможностей встроенных средств Windows, но и практическая разработка, тестирование и количественная оценка работоспособности предложенной методики в контролируемых условиях.

Характеристика выборки: программная платформа – Windows 11 со всеми актуальными обновлениями с ключевыми компонентами, такими как среда PowerShell и платформа .NET, предоставляющая доступ к пространству имён System.Security.Cryptography. Тестовые данные – синтетический тестовый файл фиксированного размера (10 МБ).

Методы сбора данных: прямое измерение, включающее в себя фиксацию времени выполнения ключевых этапов процесса, моделирование атаки с помощью самодельного скрипта, сравнительный анализ конфигураций для сопоставления результатов времени взлома для различных комбинаций параметров. При этом следует учитывать, что полученные оценки времени перебора относятся исключительно к реализации атаки средствами PowerShell на одном CPU. Использование современных GPU и специализированного ПО может сократить время взлома на несколько порядков, что необходимо учитывать при интерпретации абсолютных значений.

Описание процедуры проведения исследования:

Для генерации тестовых данных в директории D:\TestArchive был создан набор текстовых файлов минимального объёма.

Далее с помощью скриптов было реализовано два параллельных тестирования, отличающихся ключевым криптографическим параметром – количеством итераций алгоритма выработки ключа PBKDF2.

Скрипт создавал ZIP-архив из тестовых данных с помощью Compress-Archive [5]. Полученный архив шифровался алгоритмом AES-256, а ключ шифрования вырабатывался из пароля ("9"*length) с использованием PBKDF2 с количеством итераций 100 или 10000 [6]. Данное количество итераций выбрано исключительно для демонстрации разницы в производительности и не являются стандартом безопасности на 2025/2026 год. Согласно актуальным рекомендациям OWASP (Password Storage Cheat Sheet), для алгоритма PBKDF2-HMAC-SHA256 минимальное рекомендуемое количество итераций составляет 310 000 (а в последних обновлениях руководства рекомендуется не менее 600 000) для обеспечения адекватной защиты от атак с использованием GPU [8]. Далее запускался алгоритм, систематически генерирующий все возможные комбинации цифр заданной длины. Для каждой сгенерированной комбинации из заголовка зашифрованного файла извлекалась криптографическая соль и вектор инициализации, выполнялась попытка выработки ключа и последующего расшифрования, а корректность пароля проверялась по успешности дешифрования и наличию валидной сигнатуры файла. Фиксировалось общее время от начала перебора до успешного подбора пароля, подсчитывалось общее количество попыток, а также средняя скорость перебора, как отношение количества попыток ко времени.

Методы обработки данных: сравнительный и качественный анализ, а также экстраполяция, где на основе полученных данных и известной формулы сложности перебора будет построена оценочная таблица, демонстрирующая теоретическое время взлома для более широкого алфавита.

Ход исследования

Для подготовки рабочего окружения перед выполнением основных операций скрипта если не существует папка по нужному пути, то создадим её:

```
$testDataPath = "D:\TestArchive"
if (-not (Test-Path $testDataPath)) {
    New-Item -ItemType Directory -Path $testDataPath -Force
}
```

```
$alphabetDigits = "0123456789"
```

Функцией Create-SecureArchive создадим защищённый архив в два этапа. Сначала стандартное сжатие средствами Compress-Archive, затем шифрование полученного файла алгоритмом AES-256, функции для 10000:

```
function Create-SecureArchive {
    param(
        [string]$SourceFolder,
        [string]$OutputPath,
        [string]$Password
    )

    $tempZip = Join-Path $env:TEMP "temp_$(Get-Random).zip"

    try {
        Compress-Archive -Path "$SourceFolder\*" -DestinationPath $tempZip -Force

        $bytes = [System.IO.File]::ReadAllBytes($tempZip)
        $salt = New-Object byte[] 32
        (New-Object
            System.Security.Cryptography.RNGCryptoServiceProvider).GetBytes($salt)

        $key = [System.Security.Cryptography.Rfc2898DeriveBytes]::new(
            $Password, $salt, 10000,
            [System.Security.Cryptography.HashAlgorithmName]::SHA256
        ).GetBytes(32)

        $aes = [System.Security.Cryptography.Aes]::Create()
```

Рубрика 2. Методы и системы защиты информации, информационная безопасность

```
$aes.Key = $key
$aes.GenerateIV()

$ms = New-Object System.IO.MemoryStream
$cs = New-Object System.Security.Cryptography.CryptoStream(
    $ms, $aes.CreateEncryptor(),
[System.Security.Cryptography.CryptoStreamMode]::Write)

$ms.Write($salt, 0, $salt.Length)
$ms.Write($aes.IV, 0, $aes.IV.Length)
$cs.Write($bytes, 0, $bytes.Length)
$cs.Close()

[System.IO.File]::WriteAllBytes($OutputPath, $ms.ToArray())

} finally {
    if (Test-Path $tempZip) { Remove-Item $tempZip -Force }
}
}
```

Test-Password для проверки корректности пароля путём попытки расшифровки и верификации целостности архива:

```
function Test-Password {
    param(
        [string]$EncryptedFile,
        [string]$Password
    )

    try {
        $bytes = [System.IO.File]::ReadAllBytes($EncryptedFile)
        $salt = $bytes[0..31]
        $iv = $bytes[32..47]
        $encryptedData = $bytes[48..($bytes.Length - 1)]

        $key = [System.Security.Cryptography.Rfc2898DeriveBytes]::new(
            $Password, $salt, 10000,
[System.Security.Cryptography.HashAlgorithmName]::SHA256
        ).GetBytes(32)

        $aes = [System.Security.Cryptography.Aes]::Create()
        $aes.Key = $key
        $aes.IV = $iv

        $ms = New-Object System.IO.MemoryStream
        $cs = New-Object System.Security.Cryptography.CryptoStream(
            $ms, $aes.CreateDecryptor(),
[System.Security.Cryptography.CryptoStreamMode]::Write)

        $cs.Write($encryptedData, 0, $encryptedData.Length)
        $cs.Close()

        $decryptedBytes = $ms.ToArray()
        $tempFile = Join-Path $env:TEMP "test_$(Get-Random).zip"
        [System.IO.File]::WriteAllBytes($tempFile, $decryptedBytes)

        try {
            $archive = [System.IO.Compression.ZipFile]::OpenRead($tempFile)
            $archive.Dispose()
            Remove-Item $tempFile -Force
            return $true
        } catch {
            Remove-Item $tempFile -Force -ErrorAction SilentlyContinue
            return $false
        }
    }
}
```

```

    }
} catch {
    return $false
}
}

```

Crack-PasswordBruteForce необходима для моделирования атаки методом полного перебора с использованием Test-Password для 10000 итераций:

```

function Crack-PasswordBruteForce-Unlimited {
    param(
        [string]$EncryptedFile,
        [string]$Chars = "0123456789",
        [int]$MaxLength = 4
    )

    $startTime = Get-Date
    $attempts = 0
    $foundPassword = $null

    for ($len = 1; $len -le $MaxLength; $len++) {
        $indices = New-Object int[] $len
        do {
            $password = ""
            for ($i = 0; $i -lt $len; $i++) {
                $password += $Chars[$indices[$i]]
            }

            $attempts++

            if (Test-Password -EncryptedFile $EncryptedFile -Password $password)
            {
                $foundPassword = $password
                break
            }

            $carry = 1
            for ($i = $len - 1; $i -ge 0 -and $carry -gt 0; $i--) {
                $indices[$i] += $carry
                if ($indices[$i] -ge $Chars.Length) {
                    $indices[$i] = 0
                    $carry = 1
                } else {
                    $carry = 0
                }
            }

        } while ($carry -eq 1 -and -not $foundPassword)

        if ($foundPassword) { break }
    }

    $time = (Get-Date) - $startTime
    @{
        Password = $foundPassword
        Attempts = $attempts
        Time = $time
        Speed = if ($time.TotalSeconds -gt 0) { [math]::Round($attempts /
$хime.TotalSeconds, 2) } else { 0 }
    }
}

```

Для проверки меньшего количества солей в функции Create-SecureArchive заменим 10000 на 100. Также заменим функции Test-Password и Crack-PasswordBruteForce на Crack-

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Password-HighSpeed, которая является функцией для высокоскоростного перебора паролей с оптимизированной проверкой с помощью сигнатуры для 100 итераций:

```
function Crack-Password-HighSpeed {
    param(
        [string]$EncryptedFile,
        [string]$Chars = "0123456789",
        [int]$MaxLength = 4
    )

    $bytes = [System.IO.File]::ReadAllBytes($EncryptedFile)
    $salt = $bytes[0..31]
    $iv = $bytes[32..47]
    $encryptedData = $bytes[48..($bytes.Length - 1)]

    $startTime = Get-Date
    $attempts = 0
    $foundPassword = $null

    for ($len = 1; $len -le $MaxLength; $len++) {
        $indices = New-Object int[] $len
        do {
            $password = ""
            for ($i = 0; $i -lt $len; $i++) {
                $password += $Chars[$indices[$i]]
            }

            $attempts++

            try {
                $key = [System.Security.Cryptography.Rfc2898DeriveBytes]::new(
                    $password, $salt, 100,
                    [System.Security.Cryptography.HashAlgorithmName]::SHA256
                ).GetBytes(32)

                $aes = [System.Security.Cryptography.Aes]::Create()
                $aes.Key = $key
                $aes.IV = $iv

                $ms = New-Object System.IO.MemoryStream
                $cs = New-Object System.Security.Cryptography.CryptoStream(
                    $ms, $aes.CreateDecryptor(),
                    [System.Security.Cryptography.CryptoStreamMode]::Write)

                $cs.Write($encryptedData, 0, $encryptedData.Length)
                $cs.FlushFinalBlock()

                $decryptedBytes = $ms.ToArray()

                if ($decryptedBytes.Length -ge 4 -and
                    $decryptedBytes[0] -eq 0x50 -and
                    $decryptedBytes[1] -eq 0x4B -and
                    $decryptedBytes[2] -eq 0x03 -and
                    $decryptedBytes[3] -eq 0x04) {
                    $foundPassword = $password
                    break
                }
            } catch {
                # Ошибка дешифрования - неверный пароль
            }
        } while ($true)

        $carry = 1
    }
}
```

```

        for ($i = $len - 1; $i -ge 0 -and $carry -gt 0; $i--) {
            $indices[$i] += $carry
            if ($indices[$i] -ge $Chars.Length) {
                $indices[$i] = 0
                $carry = 1
            } else {
                $carry = 0
            }
        }

    } while ($carry -eq 0 -and -not $foundPassword)

    if ($foundPassword) { break }
}

$time = (Get-Date) - $startTime
$speed = if ($time.TotalSeconds -gt 0) { [math]::Round($attempts /
$time.TotalSeconds, 2) } else { 0 }

@{
    Password = $foundPassword
    Attempts = $attempts
    Time = $time
    Speed = $speed
    TotalCombinations = [math]::Pow($Chars.Length, $MaxLength)
}
}

```

Результаты исследования

В ходе исследования сравнивались две конфигурации шифрования, отличающиеся количеством итераций алгоритма выработки ключа PBKDF2, что напрямую влияет на скорость атаки методом полного перебора. Отметим, что полученное время справедливо только для атаки «скрипт против скрипта».

Длина	Алфавит	Комбинации	ВремяВзлома_сек	Попыток	Скорость	НайденныйПароль
1	Цифры (10)	10	0,01	10	909.12 попыток/сек	9
2	Цифры (10)	100	0,07	110	1511.14 попыток/сек	99
3	Цифры (10)	1000	0,55	1110	2017.82 попыток/сек	999
4	Цифры (10)	10000	5,29	11110	2098.57 попыток/сек	9999

Рис. 1. Результаты алгоритма на 100 итераций (маленькая соль)

Длина	Алфавит	Комбинации	ВремяВзлома_сек	Попыток	Скорость	НайденныйПароль
1	Цифры (10)	10	0,23	10	43.02 попыток/сек	9
2	Цифры (10)	100	2,41	110	45.69 попыток/сек	99
3	Цифры (10)	1000	23,79	1110	46.65 попыток/сек	999
4	Цифры (10)	10000	249,27	11110	44.57 попыток/сек	9999

Рис. 2. Результаты алгоритма на 10000 итераций (большая соль)

Таблица 1 – Сравнительная таблица результатов эксперимента

Длина пароля	Алфавит	Количество комбинаций	Время взлома 100 итераций PBKDF2, с	Время взлома 10000 итераций PBKDF2, с
1	цифры (10)	10	0,01	0,23
2	цифры (10)	100	0,07	2,41
3	цифры (10)	1000	0,55	23,79
4	цифры (10)	10000	5,29	249,27

Важно отметить, что полученные оценки времени перебора относятся исключительно к реализации атаки средствами PowerShell на одном центральном процессоре (CPU), и при использовании современного специализированного аппаратного обеспечения (например,

Рубрика 2. Методы и системы защиты информации, информационная безопасность

графических процессоров уровня NVIDIA RTX 4090) и оптимизированного программного обеспечения для взлома (такого как Hashcat), скорость перебора хэшей PBKDF2-НМАС-SHA256 может достигать десятков миллионов попыток в секунду. В таком сценарии время взлома 4-значного числового пароля сократится с сотен секунд до долей секунды, а для 8-значного пароля составит от нескольких секунд до минут. Это подчеркивает критическую необходимость использования длинных (от 12 символов) и сложных паролей, а также применения максимального числа итераций, рекомендованного современными стандартами.

Заключение

В работе было проведено экспериментально-прикладное исследование, направленное на решение актуальной практической задачи: преодоление функционального ограничения встроенных средств архивации ОС Windows, а именно отсутствия поддержки парольной защиты в утилите Compress-Archive. В качестве методологического подхода была предложена и реализована гибридная методика, комбинирующая стандартное средство сжатия с криптографическими возможностями платформы .NET Framework, доступными через PowerShell.

В ходе исследования был разработан, реализован и протестирован скриптовый комплекс, включающий функции создания запароленных архивов на основе алгоритма AES-256, а также инструменты для моделирования атаки методом полного перебора. Эксперимент проводился в контролируемых условиях с варьированием ключевых параметров безопасности: длины пароля и вычислительной сложности алгоритма выработки ключа PBKDF2 (100 и 10000 итераций). Собранные количественные данные позволили построить модели и провести экстраполяцию для оценки стойкости защиты в различных сценариях.

Результат проверки гипотез:

1. Гипотеза Н1 подтвердилась. Комбинация встроенных инструментов Windows (PowerShell Compress-Archive и криптографических библиотек .NET System.Security.Cryptography) действительно позволяет создать работоспособное и криптостойкое решение для защиты архивов. Стойкость системы при использовании алгоритма AES-256 с демонстрационными параметрами (длинная соль, 10 000 итераций PBKDF2) сопоставима с реализациями в современных сторонних архиваторах, основанных на тех же криптографических примитивах.

2. Гипотеза Н2 получила убедительное количественное подтверждение. Экспериментально установлена чёткая экспоненциальная зависимость времени взлома от длины пароля. Каждый дополнительный символ в пароле увеличивает сложность перебора в степени, равной мощности алфавита (в 10 раз для цифр, в 62 раза для алфавита букв и цифр) [7]. Кроме того, критическое влияние параметров криптографии продемонстрировано на примере количества итераций PBKDF2: их снижение с 10 000 до 100 привело к увеличению скорости перебора в 44,5 раза, что подчёркивает важность корректной настройки всех элементов системы безопасности, а не только выбора сложного пароля.

Данная работа открывает перспективные направления для дальнейших исследований. К примеру, можно продолжить развивать вопрос безопасности встроенных средств архивирования ОС Windows, рассмотрев его с использованием других методов. Также есть возможность для исследования этой темы для усовершенствования уже предложенного в работе эксперимента, использования различных режимов шифрования или разработка графического интерфейса для более комфортного повседневного использования.

Результаты данной работы подтверждают, что встроенные средства ОС представляют собой мощный и недостаточно используемый ресурс для построения гибких, безопасных и не зависящих от стороннего ПО решений в области защиты данных.

Библиографический список

1. Архиваторы под рентгеном. – Текст : электронный // Хакер : журнал. – 2006. – 12 дек. – URL: <https://xakep.ru/2006/12/12/35719/> (дата обращения: 01.11.2025).
2. Защищенное хранение данных и полнодисковое шифрование / Е. К. Алексеев, Л. Р. Ахметзянова, А. А. Бабуева, С. В. Смышляев. – Текст : электронный // Прикладная

- дискретная математика. – 2020. – № 4 (50). – С. 95–110. – URL: <https://cyberleninka.ru/article/n/zaschischyonnoe-hranenie-dannyh-i-polnodiskovoe-shifrovanie> (дата обращения: 02.11.2025).
3. How to password protect a zip file in Windows 11? – Текст : электронный // Microsoft Community Hub : сайт. – URL: <https://techcommunity.microsoft.com/discussions/windows11/how-to-password-protect-a-zip-file-in-windows-11/4408591> (дата обращения: 01.11.2025).
 4. How to Password Protect a Zip File on Windows 11/10 PC. – Текст : электронный // SYSGEEKER : сайт. – URL: <https://www.sysgeeker.com/blog/password-protect-a-zip-file-on-windows-pc.html> (дата обращения: 01.11.2025).
 5. Compress-Archive (Microsoft.PowerShell.Archive). – Текст : электронный // Microsoft Learn : официальная документация. – URL: <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.archive/compress-archive?view=powershell-7.5> (дата обращения: 01.11.2025).
 6. Симметричный алгоритм блочного шифрования Advanced Encryption Standard. – Текст : электронный // Хабр : портал. – URL: <https://habr.com/ru/articles/534620/> (дата обращения: 03.11.2025).
 7. Сколько времени требуется для взлома пароля в 2024 году? – Текст : электронный // Comss : портал о кибербезопасности. – URL: <https://www.comss.ru/page.php?id=13587> (дата обращения: 05.11.2025).
 8. OWASP Password Storage Cheat Sheet. – Текст : электронный // OWASP Foundation : официальная документация. – URL: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html (дата обращения: 10.11.2025).

References

1. Archivers Under the X-Ray // Hacker. URL: <https://xakep.ru/2006/12/12/35719/> (accessed: 01.11.2025).
2. Alekseev, E. K., Akhmetzyanova, L. R., Babueva, A. A., & Smyshlyaev, S. V. (2020). *Secure Data Storage and Full-Disk Encryption*. PDM, (49). URL: <https://cyberleninka.ru/article/n/zaschischyonnoe-hranenie-dannyh-i-polnodiskovoe-shifrovanie> (accessed: 02.11.2025).
3. How to password protect a zip file in Windows 11? // Microsoft Community Hub. URL: <https://techcommunity.microsoft.com/discussions/windows11/how-to-password-protect-a-zip-file-in-windows-11/4408591> (accessed: 01.11.2025).
4. How to Password Protect a Zip File on Windows 11/10 PC // SYSGEEKER. URL: <https://www.sysgeeker.com/blog/password-protect-a-zip-file-on-windows-pc.html> (accessed: 01.11.2025).
5. Compress-Archive (Microsoft.PowerShell.Archive) - PowerShell | Microsoft Learn // Microsoft Learn. URL: <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.archive/compress-archive?view=powershell-7.5> (accessed: 01.11.2025).
6. Symmetric Block Encryption Algorithm Advanced Encryption Standard // Habr. URL: <https://habr.com/ru/articles/534620/> (accessed: 03.11.2025).
7. How Long Does It Take to Crack a Password in 2024? // Comss. URL: <https://www.comss.ru/page.php?id=13587> (accessed: 05.11.2025).
8. OWASP Password Storage Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html (accessed: 05.11.2025).

Информация об авторах

Бережная Полина Александровна – студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: palinaberezhnaya047@gmail.com

Мирчевски Кристина Далиборовна – студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mirchevski23@gmail.com

BUILT-IN WINDOWS OS ARCHIVING TOOLS: SECURITY CONCERNS

Berezhnaya P. A.¹, Mirchevski K. D.¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. *The article presents an experimental study of a limitation of the native Windows archiving tools: the lack of built-in password protection. The aim is to develop and test a method for creating cryptographically strong password-protected archives using only built-in OS components (PowerShell and .NET Framework), without third-party software. On a Windows 11 test bench, the standard Compress-Archive utility was combined with AES-256 symmetric encryption. The encryption key was derived with PBKDF2 using a configurable iteration count and a cryptographic salt. A custom PowerShell script was used to simulate a brute-force password attack. The results show that increasing password length substantially expands the search space: each additional character increases it by a factor of 10 for numeric passwords or 62 for alphanumeric passwords. Reducing the PBKDF2 iteration count from 10,000 to 100 increased the brute-force rate by a factor of 44.5, demonstrating the importance of correctly configuring all security parameters. The study also notes that modern specialized hardware can accelerate brute-force attacks by orders of magnitude, so long passwords and current recommended iteration counts are required in practice. The hypotheses were confirmed. The proposed approach can provide cryptographic strength comparable in principle to third-party archivers when current cryptographic practices are followed. The method is practically relevant to system administrators, end users, and information-security education.*

Keywords: Windows, archiving, data security, PowerShell, encryption, AES, built-in tools.

Information about the authors

Berezhnaya Polina Aleksandrovna – 3rd year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: palinaberezhnaya047@gmail.com

Mirchevski Kristina Daliborovna – 3rd year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: mirchevski23@gmail.com

Е. С. Цагареева¹, Д. В. Перлова¹

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

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И НАСТРОЙКИ ПРОТОКОЛА sFlow НА БАЗЕ РЕШЕНИЙ VESR

Аннотация. В статье представлен структурный анализ протокола сетевой телеметрии sFlow и описана практическая методика его настройки и настройки зон безопасности на базе виртуального сервисного маршрутизатора vESR. Актуальность работы обусловлена потребностью в эффективном мониторинге корпоративных сетей в условиях цифровизации, роста числа подключённых устройств и ужесточения требований к информационной безопасности критической информационной инфраструктуры. Подробно рассматриваются архитектура протокола sFlow в соответствии с RFC 3176, назначение sFlow-агента и коллектора, основные механизмы статистической выборки пакетов и периодического опроса счётчиков интерфейсов, а также структура пакета данных, включающая заголовок и дискретизации типов Flow Sample и Counter Sample. На практическом примере развёртывания лабораторного стенда показано, как определить параметры конфигурации sFlow-агента, настроить экспорт телеметрических данных на приёмник UDP-датаграмм и выполнить настройку зон безопасности TRUSTED и UNTRUSTED. Правила доступа и негативные тесты в работе не проверялись. Методика ориентирована на использование бесплатного программного обеспечения и не требует приобретения коммерческих решений для базового мониторинга. Сформулированы ограничения технологии и практические рекомендации по применению sFlow в корпоративных сетях. Работа носит учебно-методический характер: демонстрируется настройка sFlow на vESR и факт поступления телеметрии на приёмник. Декодирование sFlow-датаграмм и негативные тесты защиты в рамках данного эксперимента не проводились.

Ключевые слова: sFlow, vESR, сетевая телеметрия, RFC 3176, информационная безопасность, виртуальный маршрутизатор.

Введение

Актуальность

Современные корпоративные сети характеризуются многообразием подключённых устройств, распределённой топологией и необходимостью оперативного контроля за передаваемым трафиком. Традиционные методы мониторинга на основе SNMP дают общую картину загрузки интерфейсов, но не позволяют понять, какой именно трафик создаёт нагрузку — какие протоколы используются, между какими узлами происходит обмен, кто является основным потребителем ресурсов. Для решения этих задач были разработаны протоколы экспорта потоковой информации о трафике. В условиях цифровизации предприятий и ужесточения требований к информационной безопасности особую актуальность приобретают средства телеметрии, позволяющие оперативно выявлять перегрузки сети, аномальную активность и инциденты информационной безопасности. Одним из наиболее распространённых протоколов сетевой телеметрии является sFlow, обеспечивающий сбор статистических данных посредством выборочного анализа пакетов. sFlow (RFC 3176) — это протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга [1]. sFlow (Sampled Flow) — технология, предложенная компанией InMon Corporation и стандартизированная в качестве отраслевого решения для мониторинга трафика в корпоративных сетях. В отличие от альтернативных подходов, sFlow изначально проектировался с учётом требований масштабируемости и минимального воздействия на производительность сетевого оборудования.

Объект, предмет и цель

В качестве платформы для исследования выбран виртуальный сервисный маршрутизатор vESR (разработка компании Eltex), который поддерживает функции sFlow-агента и широко используется в российских корпоративных и провайдерских сетях [2, 3]. Изучение его возможностей по настройке и эксплуатации sFlow представляет практический интерес для сетевых администраторов и инженеров. Актуальность экспериментальной проверки функциональных возможностей виртуальных маршрутизаторов vESR при внедрении новых

Рубрика 2. Методы и системы защиты информации, информационная безопасность

сетевых технологий ранее подтверждалась в исследованиях, посвящённых нагрузочному тестированию и верификации работы стека IPsec на данной платформе [4].

Объектом исследования является процесс мониторинга сетевого трафика с использованием протокола sFlow в среде виртуального маршрутизатора vESR.

Предметом исследования выступают функциональные возможности протокола sFlow, его настройка на платформе vESR, а также методы сбора и анализа статистических данных о трафике.

Цель работы заключается в изучении протокола sFlow на маршрутизаторе vESR, его функционала, демонстрации настройки экспорта телеметрии с заданными параметрами и описании подходов к настройке зон безопасности передаваемой телеметрической информации. Для достижения поставленной цели были сформулированы следующие задачи исследования:

- проанализировать архитектуру протокола sFlow в соответствии с RFC 3176, включая структуру пакета данных sFlow, механизмы формирования статистической выборки и взаимодействие агента с коллектором;
- выполнить конфигурацию sFlow-агента на платформе vESR с заданными параметрами (sampling rate = 100, poll interval = 30 c);
- обеспечить приём UDP-датаграмм sFlow на PC3 и подтвердить факт их поступления;
- проверить работоспособность sFlow-агента при заданных параметрах конфигурации;
- выполнить настройку зон безопасности TRUSTED и UNTRUSTED; правила доступа и негативные тесты в работе не проверялись;
- определить ограничения применения технологии и сформулировать рекомендации по использованию sFlow в корпоративных сетях.

Преимущества sFlow:

- стоимостная эффективность — требуется минимум компьютерных ресурсов;
- мониторинг трафика для всех сетевых портов с минимальным воздействием на производительность сети;
- постоянный мониторинг сети;
- визуальное представление сети;
- мониторинг трафика на уровнях от L2 до L7 для всех устройств, доступный как в реальном времени, так и в архиве в виде детализированного отчёта [5, 6].

Литературный обзор

Протокол sFlow (Sampled Flow) был разработан компанией InMon Corporation в начале 2000-х годов как ответ на растущую потребность в эффективном мониторинге корпоративных сетей. Первая спецификация была опубликована в 2001 году в виде информационного документа RFC 3176, авторами которого выступили Питер Фаль (Peter Phaal), Стивен Панчен (Stephen Panchen) и Нил МакКи (Neil McKee) — ключевые разработчики InMon. Идея, заложенная в основу sFlow, была революционной для своего времени: вместо анализа каждого пакета (как это делали ранние версии NetFlow) предлагалось использовать статистическую выборку, что позволило существенно снизить нагрузку на процессоры сетевых устройств и открыло путь к организации мониторинга в режиме реального времени без существенного увеличения затрат на обработку данных [7, 8].

Согласно официальной спецификации RFC 3176, система sFlow строится на взаимодействии двух основных компонентов: sFlow Agent и sFlow Collector [1].

Коллектор данных получает данные, отправленные агентом sFlow, и выполняет две функции: анализ sFlow-данных и их хранение. База управляющей информации sFlow MIB позволяет управлять агентом sFlow Agent через SNMP [9]. Агент sFlow использует технологию выборки для снятия статистики трафика и передаёт данные в стандартном формате [10].

Каждый пакет данных sFlow представляет собой UDP-пакет, содержащий:

- заголовок пакета — версия протокола, IP-адрес агента, порядковый номер пакета, количество дискретизаций;

- одну или несколько дискретизаций — каждый процесс формирования выборки может быть либо Flow Sample (информация о пакете), либо Counter Sample (статистика интерфейса) [11].

Настройка sFlow на устройстве обычно включает три ключевых параметра [10, 12]:

- sampling rate (частота выборки) — определяет, какой процент пакетов будет подвергнут анализу. Более высокие значения снижают нагрузку на оборудование, но уменьшают точность семплирования;
- poll interval (интервал опроса счётчиков) — время в секундах между отправками Counter Sample. Типичные значения — от 10 до 60 секунд;
- адрес и порт коллектора — IP-адрес и UDP-порт, на который агент будет отправлять дейтаграммы. По умолчанию используется порт 6343.

Материалы и методы

Тип исследования является экспериментальным. Для демонстрации функционала протокола sFlow и настройки зон безопасности телеметрических сегментов на базе решений vESR была настроена сетевая топология, состоящая из маршрутизатора vESR (версия 1.18.9 build 3) и трёх виртуальных машин PC1, PC2 и PC3 под управлением ОС Alpine Linux.

Сетевая топология, представленная на рис. 1, включает:

- PC1 (10.0.11.1/24) и PC2 (10.0.12.1/24) — генераторы трафика в доверенной зоне (TRUSTED);
- vESR — маршрутизатор и экспортёр sFlow-данных;
- PC3 (10.0.13.1/24) — приемник UDP-датаграмм в недоверенной зоне (UNTRUSTED).



Рис. 1. Схема лабораторного стенда: PC1 и PC2 — источники трафика, vESR — маршрутизатор и агент sFlow, PC3 — приёмник UDP-датаграмм

Ограничения методики

В рамках данной работы не проводилось: декодирование sFlow-датаграмм средствами Wireshark, sflowtool или sfcapd с анализом полей; варьирование sampling rate и poll interval; негативные тесты доступа к коллектору и проверка фильтрации UDP-порта 6343. Требования ГОСТ Р 57580.1-2017 к защите каналов передачи телеметрии в работе не рассматривались [13]. Перечисленные ограничения определяют учебно-методический характер работы.

Результаты

Критерии оценки качества сбора данных приведены в таблице 1.

Таблица 1 – Критерии оценки качества сбора данных

Критерий	Описание	Метод проверки
Факт приёма данных	Подтверждение доставки UDP-датаграмм sFlow от агента на приемник	Анализ вывода утилиты nc на PC3
Декодирование структуры sFlow	Проверка соответствия RFC 3176	В данной работе не проводилось

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Проведённое исследование показало следующие количественные результаты: в ходе эксперимента было отправлено по 20 ICMP-пакетов с PC1 и PC2 в сторону PC3. На PC3 через утилиту nc получены UDP-датаграммы на порт 6343, что подтверждает факт поступления телеметрии от sFlow-агента на vESR. Декодирование структуры sFlow-датаграмм и проверка соответствия RFC 3176 в данной работе не проводились.

Результаты исследования

Была произведена базовая настройка сетевых интерфейсов на маршрутизаторе vESR и виртуальных машинах PC1, PC2 и PC3 согласно топологии (листинги 1-4).

Листинг 1 – Настройка интерфейсов на vESR

```
vesr# config
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# ip address 10.0.11.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# ip address 10.0.12.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/3
vesr(config-if-gi)# ip address 10.0.13.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# do commit
```

Листинг 2 – Настройка интерфейсов на PC1

```
localhost:~# ip addr add 10.0.11.1/24 dev eth1
localhost:~# ip link set eth1 up
localhost:~# ip route add default via 10.0.11.2
```

Листинг 3 – Настройка интерфейсов на PC2

```
PC2:~# ip addr add 10.0.12.1/24 dev eth1
PC2:~# ip link set eth1 up
PC2:~# ip route add default via 10.0.12.2
```

Листинг 4 – Настройка интерфейсов на PC3

```
PC3:~# ip addr add 10.0.13.1/24 dev eth1
PC3:~# ip link set eth1 up
PC3:~# ip route add default via 10.0.13.2
```

Была произведена настройка протокола sFlow на маршрутизаторе vESR. В качестве приемника был указан PC3 с IP-адресом 10.0.13.1. Экспорт sFlow-данных был активирован глобально и включён на входящих интерфейсах gi1/0/1 и gi1/0/2 (листинги 5-6).

Листинг 5 – Настройка sFlow на vESR

```
vesr(config)# sflow collector 10.0.13.1
vesr(config-sflow-host)# exit
vesr(config)# sflow poll-interval 30
vesr(config)# sflow sampling-rate 100
vesr(config)# sflow enable
vesr(config)# do commit
```

Листинг 6 – Включение экспорта sFlow на интерфейсах gi1/0/1 и gi1/0/2

```
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# ip sflow export
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# ip sflow export
vesr(config-if-gi)# exit
vesr(config)# do commit
```

Для настройки зон безопасности на vESR были созданы зоны безопасности TRUSTED и UNTRUSTED. Интерфейсы gi1/0/1 и gi1/0/2, к которым подключены PC1 и PC2, были помещены в доверенную зону TRUSTED. Интерфейс gi1/0/3, к которому подключён приёмник PC3, помещён в недоверенную зону UNTRUSTED (листинг 7).

Листинг 7 – Настройка зон безопасности TRUSTED и UNTRUSTED

```

vesr(config)# security zone TRUSTED
vesr(config-zone)# exit
vesr(config)# security zone UNTRUSTED
vesr(config-zone)# exit
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# security-zone TRUSTED
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# security-zone TRUSTED
vesr(config-if-gi)# exit
vesr(config)# security zone-pair TRUSTED UNTRUSTED
vesr(config-zone-pair)# EXIT
vesr(config)# interface gi1/0/3
vesr(config-if-gi)# security-zone UNTRUSTED
vesr(config-if-gi)# exit
vesr(config)# do commit

```

В листинге 7 приведены команды создания зон безопасности и назначения интерфейсов. Правила доступа (zone-pair policies) в рамках данной работы не настраивались, поэтому листинг демонстрирует конфигурацию зон, а не действующую политику изоляции. Проверка разрешённых и запрещённых обращений не выполнялась.

Проверка связности осуществлялась с помощью ping; результат подтвердил корректную маршрутизацию между всеми узлами сети (листинги 8-9).

Листинг 8 – Связность PC1 с vESR и PC3

```

PC1:~# ping 10.0.11.2 -c 4
PING 10.0.11.2 (10.0.11.2): 56 data bytes
64 bytes from 10.0.11.2: seq=0 ttl=64 time=4.706 ms
64 bytes from 10.0.11.2: seq=1 ttl=64 time=2.149 ms
64 bytes from 10.0.11.2: seq=2 ttl=64 time=1.983 ms
64 bytes from 10.0.11.2: seq=3 ttl=64 time=2.772 ms
--- 10.0.11.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.983/2.902/4.706 ms
PC1:~# ping 10.0.13.1 -c 4
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=6.414 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=3.210 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=5.664 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=5.634 ms
--- 10.0.13.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 3.210/5.230/6.414 ms

```

Листинг 9 – Связность PC2 с vESR и PC3

```

PC2:~# ping 10.0.12.2 -c 4
PING 10.0.12.2 (10.0.12.2): 56 data bytes
64 bytes from 10.0.12.2: seq=0 ttl=64 time=8.184 ms
64 bytes from 10.0.12.2: seq=1 ttl=64 time=1.939 ms
64 bytes from 10.0.12.2: seq=2 ttl=64 time=2.084 ms
64 bytes from 10.0.12.2: seq=3 ttl=64 time=1.834 ms
--- 10.0.12.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.834/3.510/8.184 ms
PC2:~# ping 10.0.13.1 -c 4
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=6.245 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=4.726 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=4.059 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=4.230 ms
--- 10.0.13.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.059/4.815/6.245 ms

```

Рубрика 2. Методы и системы защиты информации, информационная безопасность

На PC3 была запущена утилита nc, слушающая 6343 порт для приёма UDP-датаграмм (листинг 10).

Листинг 10 – Прием UDP-датаграмм на PC3

```
PC3:~# nc -l -u -p 6343
```

Вывод утилиты nc подтверждает поступление UDP-датаграмм на порт 6343 при настроенном экспорте sFlow с vESR. Декодирование структуры датаграмм и разбор полей в работе не проводились.

Для проверки работоспособности системы с помощью ping был сгенерирован тестовый ICMP-трафик от PC1 и PC2 в сторону PC3 (листинг 11).

Листинг 11 – ICMP-трафик

```
PC1:~# ping 10.0.13.1 -c 20
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=4.608 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=2.308 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=2.632 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=2.756 ms
64 bytes from 10.0.13.1: seq=4 ttl=63 time=3.987 ms
64 bytes from 10.0.13.1: seq=5 ttl=63 time=2.317 ms
64 bytes from 10.0.13.1: seq=6 ttl=63 time=3.163 ms
64 bytes from 10.0.13.1: seq=7 ttl=63 time=1.987 ms
64 bytes from 10.0.13.1: seq=8 ttl=63 time=2.917 ms
64 bytes from 10.0.13.1: seq=9 ttl=63 time=2.953 ms
64 bytes from 10.0.13.1: seq=10 ttl=63 time=3.985 ms
64 bytes from 10.0.13.1: seq=11 ttl=63 time=2.944 ms
64 bytes from 10.0.13.1: seq=12 ttl=63 time=3.929 ms
```

В листинге 11 показан фрагмент серии; полная серия включала по 20 пакетов.

Обсуждение

Полученные результаты подтверждают, что sFlow-агент на vESR формирует и экспортирует UDP-датаграммы на приёмник. Это соответствует цели демонстрации работоспособности протокола. Однако интерпретация результатов ограничена:

- факт поступления датаграмм не подтверждает корректность их структуры и соответствие RFC 3176 без декодирования;
- настройка зон безопасности TRUSTED и UNTRUSTED выполнена, однако правила доступа не заданы, а негативные тесты не проводились, поэтому защитные свойства конфигурации не доказаны.

Заключение

Проведённое исследование функционала протокола sFlow и настройки зон безопасности телеметрических сегментов на базе решений vESR представляет собой актуальную задачу в области сетевого администрирования. Работа представляет собой учебно-методический пример настройки sFlow на виртуальном маршрутизаторе vESR: систематизирована последовательность конфигурации агента, экспорта телеметрии и настройки зон безопасности TRUSTED и UNTRUSTED. Правила доступа и негативные тесты в работе не проверялись; доказательство защитных свойств конфигурации не выполнялось. Сравнительный анализ с существующими методиками не проводился.

В ходе работы был рассмотрен протокол sFlow (Sampled Flow), его архитектура, принципы работы и технические особенности. Согласно документации и литературе [1, 7, 8], sFlow, основанный на статистической выборке пакетов и периодическом опросе счётчиков интерфейсов, относится к низконагрузочным протоколам. Нагрузка на vESR в данной работе не измерялась.

В рамках экспериментальной части работы был развёрнут лабораторный стенд на базе Oracle VirtualBox, включающий виртуальный маршрутизатор vESR и три клиентские системы (PC1, PC2, PC3) [14]. Последовательно были выполнены этапы настройки IP-адресации, маршрутизации, конфигурации sFlow-агента на vESR и приема UDP-датаграмм на PC3.

Экспериментальным путем подтверждён факт экспорта sFlow-телеметрии с vESR — при генерации тестового трафика приемник успешно принимал UDP-датаграммы.

Проведённое исследование продемонстрировало, что sFlow может применяться для мониторинга трафика на платформе vESR, а платформа предоставляет базовую поддержку данного протокола. Декодирование sFlow-датаграмм и проверка защитных свойств конфигурации требуют отдельных экспериментов. Сильными сторонами sFlow, по данным литературы, остаются низкая нагрузка на оборудование, независимость от сетевого уровня и простота настройки.

Библиографический список

1. Phaal, P. RFC 3176 – InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks / P. Phaal, S. Panchen, N. McKee. – September 2001. – URL: <https://www.rfc-editor.org/info/rfc3176> (дата обращения: 09.07.2026). – Текст : электронный.
2. Документация Eltex. – URL: <https://docs.eltex-co.ru/> (дата обращения: 27.06.2026). – Текст : электронный.
3. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11 (628). – С. 58–62. – Текст : непосредственный.
4. Скоромников, В. С. Исследование реализации IPsec IKEv2 на базе vESR / В. С. Скоромников, А. П. Андрюхина // Профессионалитет. – 2025. – № 1 (005). – С. 5–11. – Текст : непосредственный.
5. Бигаров, Р. Описание технологии : sFlow D-Link HQ / Р. Бигаров. – [Б. м. : б. и.], 2007. – Текст : непосредственный.
6. Cisco Systems. NetFlow and sFlow Key Concepts // Cisco IOS XR Netflow Configuration Guide for Cisco 8000 Series Routers, Release 26.1.1. – URL: <https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/configuration/b-netflowconfiguration-ios-xr-8000/netflow-sflow-key-concepts.pdf> (дата обращения: 09.07.2026). – Текст : электронный.
7. OpenNet. Обзор протоколов NetFlow и sFlow. – URL: <https://www.opennet.ru/docs/RUS/netflowbsd/> (дата обращения: 09.07.2026). – Текст : электронный.
8. Baeldung. Key Differences Between NetFlow and sFlow // Baeldung on Computer Science. – 2024. – URL: <https://www.baeldung.com/cs/cisco-netflow-vs-innom-sflow> (дата обращения: 09.07.2026). – Текст : электронный.
9. Eltex. Настройка Netflow, sFlow, SNMP. – URL: <https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=383648346> (дата обращения: 09.07.2026). – Текст : электронный.
10. Павленко, А. Пример настройки sFlow-сети / А. Павленко // OTUS. – 2021. – URL: <https://otus.ru/nest/post/22371> (дата обращения: 09.07.2026). – Текст : электронный.
11. sFlow Version 5 : спецификация протокола. – URL: <https://www.protokols.ru/WP/wp-content/uploads/2004/07/sFlow5.pdf> (дата обращения: 09.07.2026). – Текст : электронный.
12. OpenNix. sFlow – мониторинг сетевого трафика в VyOS. – URL: <https://opennix.org/docs/vyos/system/vyos-sflow/> (дата обращения: 09.07.2026). – Текст : электронный.
13. ГОСТ Р 57580.1-2017. Защита информации. Безопасность финансовых (банковских) операций. Защита информации при осуществлении переводов денежных средств. – Москва : Стандартинформ, 2017. – Текст : непосредственный.
14. Oracle VirtualBox : официальная документация и руководство пользователя. – URL: <https://www.virtualbox.org/wiki/Documentation> (дата обращения: 09.07.2026). – Текст : электронный.

References

1. Phaal, P., Panchen, S., & McKee, N. (2001). *RFC 3176 – InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*. <https://www.rfc-editor.org/info/rfc3176>
2. *Eltex documentation*. (n.d.). <https://docs.eltex-co.ru/>
3. 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.
4. Skoromnikov, V. S., & Andriukhina, A. P. (2025). *Issledovanie realizatsii IPsec IKEv2 na baze vESR* [Study of IPsec IKEv2 implementation on the basis of vESR]. *Professionalitet*, (1), 5–11.
5. Bigarov, R. (2007). *Opisanie tekhnologii: sFlow D-Link HQ* [Description of technology: sFlow D-Link HQ].
6. Cisco Systems. (n.d.). *NetFlow and sFlow Key Concepts*. In *Cisco IOS XR Netflow Configuration Guide for Cisco 8000 Series Routers, Release 26.1.1*. <https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/configuration/b-netflowconfiguration-ios-xr-8000/netflow-sflow-key-concepts.pdf>
7. OpenNet. (n.d.). *Obzor protokolov NetFlow i sFlow* [Overview of NetFlow and sFlow protocols]. <https://www.opennet.ru/docs/RUS/netflowbsd/>
8. Baeldung. (2024). *Key Differences Between NetFlow and sFlow*. *Baeldung on Computer Science*. <https://www.baeldung.com/cs/cisco-netflow-vs-innom-sflow>
9. Eltex. (n.d.). *Nastroyka Netflow, sFlow, SNMP* [Setup Netflow, sFlow, SNMP]. <https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=383648346>
10. Pavlenko, A. (2021). *Primer nastroyki sFlow-seti* [Example of configuration sFlow-network]. OTUS. <https://otus.ru/nest/post/22371>
11. *sFlow Version 5: spetsifikatsiya protokola* [sFlow Version 5: protocol specification]. (n.d.). <https://www.protokols.ru/WP/wp-content/uploads/2004/07/sFlow5.pdf>
12. OpenNix. (n.d.). *sFlow – monitoring setevogo trafika v VyOS* [sFlow – Network traffic monitoring in VyOS]. <https://opennix.org/docs/vyos/system/vyos-sflow/>
13. GOST R 57580.1-2017. (2017). *Zashchita informatsii. Bezopasnost finansovykh (bankovskikh) operatsiy. Zashchita informatsii pri osushchestvlenii perevodov denezhnykh sredstv* [Information protection. Security of financial (bank) transactions. Protection of information when carrying out cash transfers]. Standartinform.
14. *Oracle VirtualBox: ofitsialnaya dokumentatsiya i rukovodstvo polzovatelya* [Oracle VirtualBox: official documentation and user guide]. (n.d.). <https://www.virtualbox.org/wiki/Documentation>

Информация об авторах

Цагараева Елизавета Станиславовна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация, e-mail: tsagarati@mail.com

Перлова Диана Викторовна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация, e-mail: dianaperl0va55@gmail.com

RESEARCH OF FUNCTIONALITY AND CONFIGURATION OF THE SFlow PROTOCOL ON THE BASIS OF VESR SOLUTIONS

E. S. Tsagaraeva¹, D. V. Perlova¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article analyses the sFlow network telemetry protocol and describes its practical configuration and security zone setup on the vESR virtual service router. The relevance of the work is driven by the need for effective monitoring of corporate networks amid digitalisation, the growing number of connected devices and increasingly stringent information security requirements for critical information infrastructure. In detail, the paper examines the architecture of the sFlow protocol in accordance with RFC 3176, the roles of the sFlow agent and collector, the main mechanisms of statistical packet sampling and periodic polling of interface counters, as well as the structure of the data packet, including the header and samples of the Flow Sample and Counter Sample types. Using a practical example of deploying a laboratory testbed, the article demonstrates how to determine the sFlow agent configuration parameters, configure the export of telemetry data to a UDP datagram receiver, and set up the TRUSTED and UNTRUSTED security zones. The work is educational and methodological in nature: the configuration of sFlow on vESR and the fact of telemetry arrival at the receiver are demonstrated.

Keywords: sFlow, vESR, network telemetry, RFC 3176, information security, virtual router.

Information about the authors

Tsagaraeva Elizabeth Stanislavovna — student, National University of Oil and Gas «Gubkin University», Moscow, Russian Federation, e-mail: tsagarati@mail.com

Perlova Diana Viktorovna — student, National University of Oil and Gas «Gubkin University», Moscow, Russian Federation, e-mail: dianaperlova55@gmail.com

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ И АНАЛИЗ СЕТЕВОГО ТРАФИКА ПРОТОКОЛА SMB OVER QUIC В ИНФРАСТРУКТУРЕ WINDOWS SERVER 2025

Аннотация. В условиях роста объемов передаваемых данных и популярности удаленной работы обеспечение безопасности файловых ресурсов становится критической задачей. Традиционный протокол SMB over TCP (порт 445) уязвим к пассивному перехвату трафика и часто блокируется межсетевыми экранами. В статье рассматривается протокол SMB over QUIC, инкапсулирующий SMB-трафик в защищенный туннель QUIC поверх UDP (порт 443) с обязательным шифрованием TLS 1.3. Целью работы является практическая проверка методики развертывания данного протокола и сравнительный анализ его сетевого трафика с классическим SMB. В ходе эксперимента была развернута изолированная лабораторная среда на базе Windows Server 2025 (версия 24H2, сборка 26100.32230) и Windows 11 Pro (версия 25H2, сборка 26200.7840). С помощью анализатора Wireshark 4.6.8 был перехвачен и исследован трафик обоих протоколов. Результаты показали, что в сеансе SMB over QUIC анализатор отображает полезную нагрузку исключительно как Protected Payload, не декодируя команды протокола или имена файлов. В контрольном сеансе классического SMB over TCP (при настройках по умолчанию без принудительно включенного SMB Encryption) те же операции (Create Request, Read, Close) и имя файла test.txt (размер 1 КБ) отображаются в открытом виде. Сделан вывод, что SMB over QUIC является потенциальной альтернативой классическим VPN-решениям исключительно для защищенного файлового доступа, при условии корректной настройки инфраструктуры открытых ключей (PKI), строгой аутентификации и аудита, однако не заменяет полноценный VPN для маршрутизации всего сетевого трафика. Ограничения исследования включают использование самоподписанного сертификата и лабораторной сети без моделирования реальных условий эксплуатации.

Ключевые слова: SMB over QUIC, Windows Server 2025, сетевая безопасность, Wireshark, TLS 1.3, протокол QUIC, общий файловый ресурс.

Введение

Современные корпоративные ИТ-системы стремительно меняются: объемы данных растут, сотрудники всё чаще работают удаленно, а на периферию сетей выходят мобильные устройства. При этом информация постоянно передается по открытым глобальным каналам [1]. Для обмена файлами между клиентами и серверами по-прежнему незаменим протокол SMB, который ценят за надежность и стабильность [2]. Однако в условиях центра обработки данных (далее ЦОД) главная задача – защитить эти данные от несанкционированного доступа и перехвата [3].

Ответом на эти вызовы стал SMB over QUIC от Microsoft. В этой реализации файловый протокол инкапсулируется в QUIC (работающий поверх UDP на порту 443) и обязательно шифруется с помощью TLS 1.3. Поддержка новинки уже появилась в Windows Server 2022 (Azure Edition), Windows Server 2025 и Windows 11 [4, 5].

Что это дает на практике? Во-первых, обязательное шифрование TLS 1.3 и инкапсуляция в QUIC создают эффект защищенного туннеля. В сценариях файлового доступа администраторы могут рассмотреть SMB over QUIC как альтернативу классическим VPN-решениям, а встроенное шифрование снижает необходимость в дополнительной защите на сетевом уровне. Во-вторых, использование порта UDP 443 позволяет снизить вероятность блокировки трафика: провайдеры и межсетевые экраны часто закрывают "родной" порт SMB (TCP 445), тогда как порт UDP 443 в современных сетевых политиках зачастую имеет меньше ограничений на прохождение, при условии, что правила межсетевого экрана корректно настроены именно для UDP-трафика, а не только для классического HTTPS по TCP [4].

Такой подход отлично вписывается в современные тренды сетевых технологий. Стандартизация QUIC консорциумом IETF (RFC 9000, RFC 9001) решила проблему head-of-line blocking, свойственную TCP, а установка TLS-соединения по UDP происходит заметно быстрее [6, 7, 8]. Однако если обратиться к научной литературе, создается ощущение, что QUIC создан исключительно для веба. Большинство исследований посвящены HTTP/3 и

сравнению его производительности с классическим HTTP/1.1 и HTTP/2 (оба работают по TCP). Применению QUIC в файловых протоколах, в частности в SMB, уделено мало внимания [9, 10, 4]. Существующие материалы сводятся либо к официальной документации вендора [2, 4], которая описывает лишь общие принципы, либо к поверхностным упоминаниям без глубокого анализа механизмов защиты в реальных условиях.

В отличие от общей документации Microsoft [4, 5] и стандартов IETF [6, 7], описывающих теоретические основы протокола, вклад данного исследования заключается в практической верификации развертывания SMB over QUIC в изолированной лабораторной среде без использования доменной инфраструктуры Active Directory. Автором разработан и апробирован конкретный сценарий настройки: от генерации самоподписанного сертификата с SAN до принудительной привязки к порту UDP 443 и перехвата трафика. Полученные файлы захвата pcapng и сравнительный анализ декодируемости команд в Wireshark дополняют официальную документацию наглядным доказательством механизмов сокрытия полезной нагрузки в реальных условиях, а также выявляют специфические ограничения, требующие учета при переходе от лабораторного стенда к промышленной эксплуатации.

Объект исследования – современные сетевые файловые протоколы и инфраструктура Windows Server, обеспечивающие совместный доступ к данным в корпоративных средах.

Предмет исследования – механизмы обеспечения информационной безопасности, структура сетевого трафика и практические аспекты развертывания протокола SMB over QUIC в сравнении с классическим протоколом SMB over TCP в среде Windows Server 2025 и Windows 11.

Цель исследования – разработать и на практике проверить методику безопасного развертывания файлового сервера на базе SMB over QUIC, а также сравнить уровень защиты передаваемых данных с классическим подходом.

На практике это означает настройку инфраструктуры открытых ключей (PKI) для корректной проверки сертификатов, конфигурацию серверной и клиентской частей ОС Windows, а также перехват и детальный разбор сетевого трафика с помощью анализатора Wireshark.

Итогом работы станет готовое к использованию конфигурационное решение. В ходе эксперимента будет доказано, что полезная нагрузка трафика шифруется по стандарту TLS 1.3, и выявлены ключевые отличия нового протокола от классического SMB. Результаты исследования покажут, как с помощью SMB over QUIC можно организовать защищенный доступ к файловым ресурсам в качестве альтернативы классическим VPN-решениям (при соблюдении требований к PKI и аутентификации). Эти наработки будут полезны системным администраторам и специалистам по ИБ при модернизации корпоративной ИТ-инфраструктуры.

Литературный обзор

File share (общий файловый ресурс SMB) – это сетевой ресурс, предоставляющий пользователям доступ к файлам и каталогам, размещенным на удаленном сервере. В корпоративных информационных системах общие файловые ресурсы SMB играют ключевую роль: они обеспечивают централизованное хранение данных, совместную работу сотрудников над документами, резервное копирование и разграничение прав доступа. Типичный корпоративный общий файловый ресурс включает в себя серверную часть (файловый сервер), клиентскую часть (рабочие станции пользователей) и сетевой протокол, обеспечивающий передачу данных между ними.

В экосистеме Windows стандартом де-факто для реализации общих файловых ресурсов является протокол SMB (Server Message Block). Его история насчитывает несколько десятилетий: от первой реализации SMB1 (также известного как CIFS – Common Internet File System) до современных версий SMB2 и SMB3 [11]. Протокол SMB3, представленный в Windows 8 и Windows Server 2012, добавил поддержку шифрования данных, многоканальности и непрерывной доступности, что сделало его пригодным для использования в корпоративных средах с высокими требованиями к надежности [2].

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Появление протокола QUIC (Quick UDP Internet Connections), стандартизированного рабочей группой IETF в документе RFC 9000 в 2021 году [6], предложило новую парадигму построения защищенных соединений. Протокол был изначально разработан компанией Google в 2012 году как экспериментальная замена TCP для веб-трафика, но быстро завоевал популярность благодаря своим преимуществам: уменьшению времени установления соединения, устранению проблемы блокировки начала очереди (head-of-line blocking) за счет независимых потоков внутри одного соединения и встроенной защите от анализа трафика [9, 10].

Современные научные исследования активно изучают преимущества и особенности протокола QUIC. В работе М. М. Адживапаева [1] проводится подробный сравнительный анализ транспортных протоколов TCP, UDP и QUIC, где автор подчеркивает, что QUIC эффективно устраняет проблему блокировки начала очереди и ускоряет установление соединения. Автор отмечает, что QUIC сочетает в себе функции транспорта и криптографии, обеспечивая надёжную доставку, управление потоком и шифрование в едином протоколе. И. А. Смирнов [10] рассматривает QUIC как фундамент для HTTP/3, отмечая его высокую криптографическую стойкость и перспективы применения в высоконагруженных сервисах. В статье проводится сравнительный анализ HTTP/3 и HTTP/2, а также QUIC и TCP, обсуждаются сложности развёртывания и перспективы дальнейшего развития протоколов. Н. С. Андреев [3] в своем исследовании клиент-серверных протоколов подтверждает, что внедрение QUIC существенно повышает отказоустойчивость и безопасность сетевых соединений за счет встроенных механизмов шифрования и криптографической аутентификации. Автор подчеркивает, что каждый пакет QUIC содержит часть информации, передаваемой между клиентом и сервером, и может быть независимо обработан, что повышает надежность передачи данных.

Вопросы информационной безопасности при использовании новых протоколов требуют отдельного внимания. А. Ю. Симачев [9] исследует возможности формирования скрытых каналов в протоколе QUIC, что указывает на необходимость глубокого практического анализа его сетевого трафика с использованием специализированных анализаторов. В статье показано, что даже современные защищенные протоколы могут иметь скрытые уязвимости, требующие постоянного мониторинга и анализа. В контексте файловых систем А. В. Галимуллина [11] описывает особенности использования SMB, подчеркивая важность корректной настройки протокола для предотвращения несанкционированного доступа. Автор отмечает, что SMB-клиент-серверный протокол предназначен для получения доступа к файлам, каталогам и сетевым ресурсам, и его неправильная конфигурация может привести к серьезным проблемам безопасности.

Официальная документация Microsoft [2, 4] позиционирует SMB over QUIC как своеобразный “SMB VPN”, позволяющий безопасно передавать файлы через интернет по стандартному порту UDP 443, эффективно минуя традиционные блокировки порта TCP 445 интернет-провайдерами и межсетевыми экранами. Протокол требует наличия действительного сертификата X.509 с альтернативным именем субъекта (SAN), что обеспечивает криптографическую аутентификацию сервера. Шифрование осуществляется на базе TLS 1.3, который является последним стандартом Transport Layer Security и обеспечивает высокую скорость установления соединения благодаря механизму 0-RTT (Zero Round Trip Time) [7, 5].

Инфраструктура открытых ключей (PKI) играет важную роль в развёртывании SMB over QUIC. Сертификат сервера должен быть выпущен доверенным центром сертификации (CA) и содержать правильное альтернативное имя субъекта (SAN), соответствующее DNS-имени сервера [4]. Использование самоподписанных сертификатов возможно в тестовых средах, но требует их ручного импорта в хранилище доверенных корневых центров сертификации на клиентских устройствах. Неправильная настройка PKI является одной из наиболее частых причин проблем с подключением по SMB over QUIC.

Анализ сетевого трафика с использованием специализированных инструментов, таких как Wireshark, позволяет детально изучить механизмы работы протокола. Анализ трафика

позволяет выявить структуру пакетов Initial, Handshake и Protected Payload, а также убедиться в наличии шифрования передаваемых данных.

На основе проведенного анализа литературы и поставленной цели исследования формулируются следующие основные гипотезы:

Гипотеза 1. Развертывание файлового сервера с поддержкой SMB over QUIC в изолированной среде является технически реализуемым при условии корректной настройки инфраструктуры открытых ключей (PKI) и привязки самоподписанного сертификата к порту UDP 443.

Гипотеза 2. Анализ сетевого трафика с использованием анализатора Wireshark экспериментально демонстрирует, что в сеансе SMB over QUIC команды протокола и имена файлов не поддаются декодированию (в отличие от классического SMB over TCP), что свидетельствует о сквозном шифровании полезной нагрузки на базе TLS 1.3 (при этом сетевые метаданные, такие как IP-адреса и порты, остаются видимыми).

Гипотеза 3. Использование протокола SMB over QUIC по порту UDP 443 позволяет успешно обойти стандартные ограничения на использование порта TCP 445, что делает данный протокол потенциальной альтернативой классическим VPN-решениям для обеспечения защищенного доступа именно к файловым ресурсам (при условии корректной настройки PKI и аутентификации).

Методы исследования

Исследование носит экспериментально-сравнительный характер. Основной метод — практический эксперимент по развертыванию файлового сервера с поддержкой протокола SMB over QUIC в изолированной лабораторной среде и последующий перехват сетевого трафика с помощью анализатора Wireshark для сравнения с классическим SMB over TCP.

Для проведения исследования была развернута изолированная клиент-серверная среда. Для обеспечения воспроизводимости эксперимента ключевые параметры стенда сведены в таблицу 1.

Таблица 1 – Параметры экспериментальной среды

Компонент/Параметр	Значение/Команда
Сервер (SRV-QUIC)	ОС: Windows Server 2025 (Desktop Experience, версия 24H2 сборка 26100.32230) Роли: FS-FileServer, AD-CS-Cert-Authority IP: 192.168.10.10/24
Клиент (CLIENT-QUIC)	ОС: Windows 11 Pro (версия 25H2, сборка 26200.7840) IP: 192.168.10.20/24 Имя в hosts: 192.168.10.10 SRV-QUIC.local
Сертификат	Самоподписанный X.509, SAN: SRV-QUIC.local, RSA 2048-bit, SHA256. Команда привязки: New-SmbServerCertificateMapping -Name "SRV-QUIC.local" -ThumbPrint <Thumbprint> -Storename My
Анализатор сетевого трафика	Wireshark 4.6.8 (с поддержкой декодирования QUIC IETF)
Сценарий и файл	Подключение к \\SRV-QUIC.local\QUICShare, открытие и чтение файла test.txt (размер 1 КБ)
Критерии успеха	Успешное монтирование диска, чтение файла, наличие трафика UDP 443 (QUIC) или TCP 445 (SMB2)
Название файлов захвата pcapng	SMB over QUIC: 25u19t3.pcapng SMB over TCP: 2ieu5t3.pcapng
Параметры захвата	Фильтр QUIC: udp.port == 443 (файл 25u19t3.pcapng, ~417 пакетов, длительность ~3 сек). Фильтр TCP: tcp.port == 445 (файл 2ieu5t3.pcapng, ~26 пакетов, длительность ~2 сек).

Методы сбора данных

- анализ сетевого трафика: перехват пакетов на клиентской машине во время подключения к общему файловому ресурсу SMB \\SRV-QUIC.local\QUICShare;

Рубрика 2. Методы и системы защиты информации, информационная безопасность

- сравнение структуры пакетов: оценка видимости метаданных (имен файлов, команд протокола) и наличия шифрования (открытый текст против Protected Payload);
- анализ конфигурации: проверка состояния служб и привязки сертификата с помощью командлетов PowerShell (Get-SmbServerConfiguration, Get-NetUDPEndpoint, Get-ChildItem Cert:\LocalMachine\My).

Описание процедуры проведения исследования

Эксперимент проводился в следующей последовательности:

- подготовка ролей и сертификата. На сервере установлены роли файлового сервера и службы сертификации. С помощью PowerShell сгенерирован самоподписанный сертификат X.509 с альтернативным именем субъекта (SAN) командой: `New-SelfSignedCertificate -DnsName "SRV-QUIC.local" -CertStoreLocation "Cert:\LocalMachine\My" -KeyAlgorithm RSA -KeyLength 2048 -HashAlgorithm SHA256`;
- настройка SMB over QUIC. Сертификат привязан к порту UDP 443 командой `New-SmbServerCertificateMapping`. Поддержка протокола включена командой `Set-SmbServerConfiguration -EnableSMBQUIC $true`. Служба LanmanServer перезапущена;
- настройка клиента. Сертификат сервера импортирован в хранилище доверенных корневых центров сертификации (Cert:\LocalMachine\Root) на клиенте. В файле hosts прописано соответствие имени и IP-адреса;
- захват трафика SMB over QUIC. На клиенте запущен Wireshark с фильтром `udp.port == 443`. Подключение к ресурсу выполнено с явным указанием транспорта QUIC командой: `New-SmbMapping -LocalPath 'Z:' -RemotePath '\\SRV-QUIC.local\QUICShare' -TransportType QUIC`. Это позволило принудительно использовать QUIC вместо стандартного TCP-подключения. Произведено открытие и чтение тестового файла test.txt (размер 1 КБ);
- захват трафика классического SMB. Для чистоты эксперимента поддержка QUIC на клиенте временно отключена (`Set-SmbClientConfiguration -EnableSMBQUIC $false`). Фильтр Wireshark изменен на `tcp.port == 445`. Подключение и операции с файлом повторены;
- сравнительный анализ. Захваченный трафик (файлы 25u19t3.pcapng для SMB over QUIC и 2ieu5t3.pcapng для SMB over TCP) проанализирован на предмет декодируемости команд протокола и шифрования полезной нагрузки.

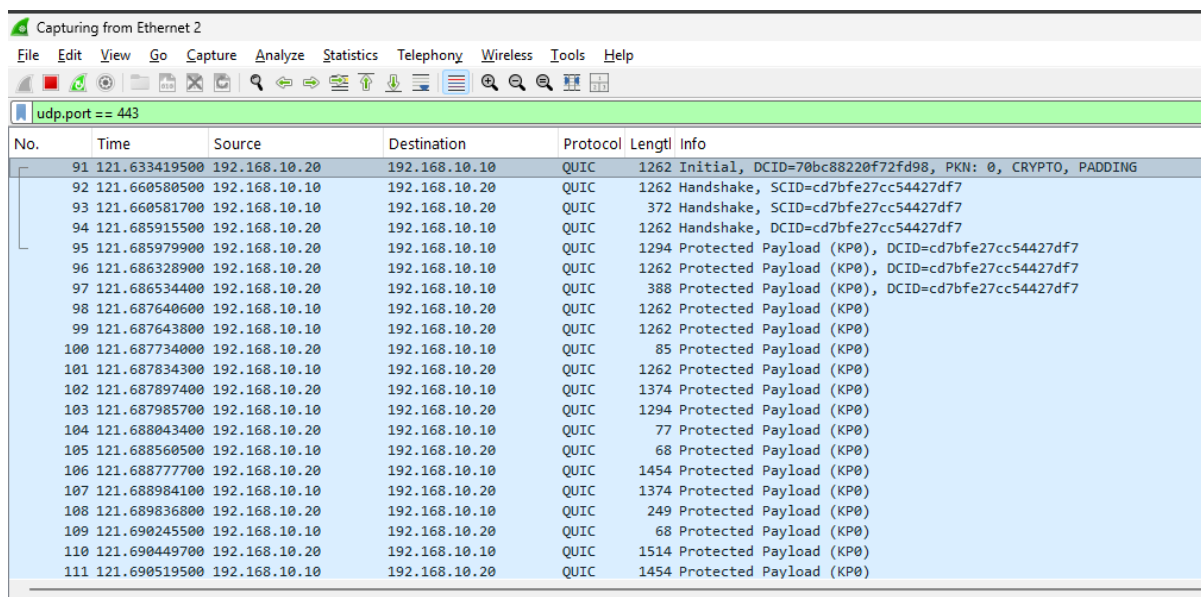
Результаты исследования

В ходе эксперимента была успешно развернута клиент-серверная инфраструктура с поддержкой SMB over QUIC. На сервере SRV-QUIC (Windows Server 2025) установлены роли файлового сервера и службы сертификации, сгенерирован самоподписанный сертификат X.509 с альтернативным именем субъекта (SAN) SRV-QUIC.local. Сертификат привязан к порту UDP 443 командой `New-SmbServerCertificateMapping`, после чего поддержка протокола активирована через `Set-SmbServerConfiguration -EnableSMBQUIC $true`.

На клиентской машине (Windows 11 Pro 25H2) сертификат импортирован в хранилище доверенных корневых центров сертификации, что обеспечило корректную валидацию при подключении. Подключение к общему файловому ресурсу `\\SRV-QUIC.local\QUICShare` прошло успешно, файлы открывались и читались без ошибок.

Следовательно, гипотеза 1 подтверждена полностью: развертывание файлового сервера с поддержкой SMB over QUIC в изолированной среде технически реализуемо при корректной настройке PKI и привязке сертификата к порту UDP 443.

Для анализа структуры сетевого трафика на клиентской машине был запущен анализатор Wireshark 4.6.8 с фильтром `udp.port == 443`. В ходе захвата были зафиксированы пакеты протокола QUIC, инкапсулирующего SMB-трафик.



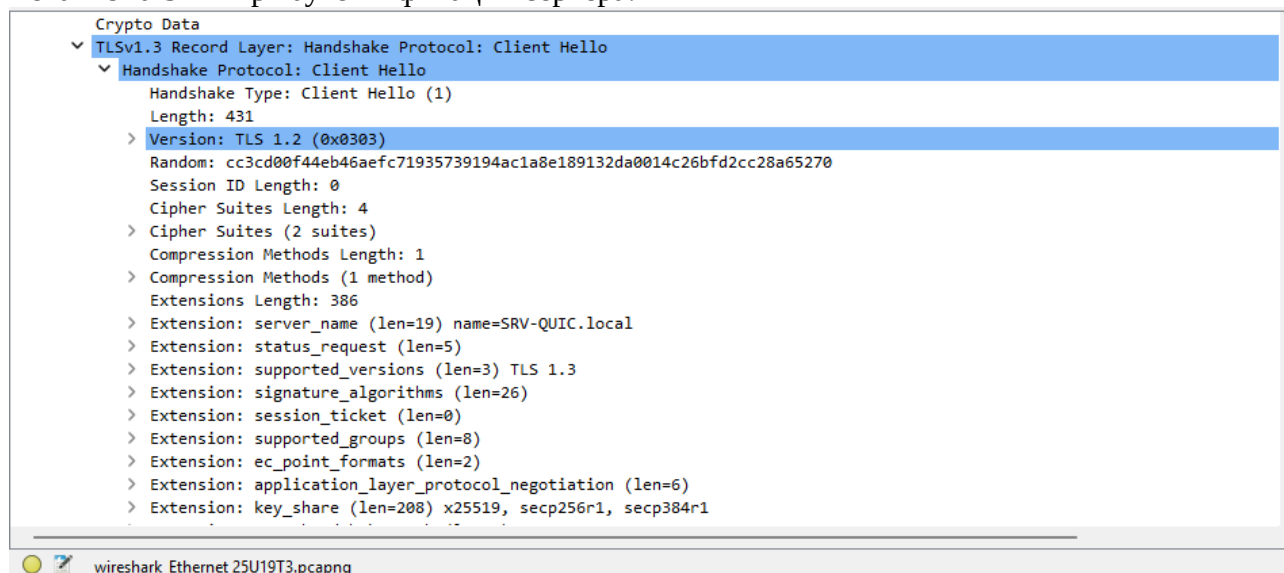
No.	Time	Source	Destination	Protocol	Length	Info
91	121.633419500	192.168.10.20	192.168.10.10	QUIC	1262	Initial, DCID=70bc88220f72fd98, PKN: 0, CRYPTO, PADDING
92	121.660580500	192.168.10.10	192.168.10.20	QUIC	1262	Handshake, SCID=cd7bfe27cc54427df7
93	121.660581700	192.168.10.10	192.168.10.20	QUIC	372	Handshake, SCID=cd7bfe27cc54427df7
94	121.685915500	192.168.10.20	192.168.10.10	QUIC	1262	Handshake, DCID=cd7bfe27cc54427df7
95	121.685979900	192.168.10.20	192.168.10.10	QUIC	1294	Protected Payload (KP0), DCID=cd7bfe27cc54427df7
96	121.686328900	192.168.10.20	192.168.10.10	QUIC	1262	Protected Payload (KP0), DCID=cd7bfe27cc54427df7
97	121.686534400	192.168.10.20	192.168.10.10	QUIC	388	Protected Payload (KP0), DCID=cd7bfe27cc54427df7
98	121.687640600	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KP0)
99	121.687643800	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KP0)
100	121.687734000	192.168.10.20	192.168.10.10	QUIC	85	Protected Payload (KP0)
101	121.687834300	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KP0)
102	121.687897400	192.168.10.20	192.168.10.10	QUIC	1374	Protected Payload (KP0)
103	121.687985700	192.168.10.10	192.168.10.20	QUIC	1294	Protected Payload (KP0)
104	121.688043400	192.168.10.20	192.168.10.10	QUIC	77	Protected Payload (KP0)
105	121.688560500	192.168.10.10	192.168.10.20	QUIC	68	Protected Payload (KP0)
106	121.688777700	192.168.10.20	192.168.10.10	QUIC	1454	Protected Payload (KP0)
107	121.688984100	192.168.10.10	192.168.10.20	QUIC	1374	Protected Payload (KP0)
108	121.689836800	192.168.10.20	192.168.10.10	QUIC	249	Protected Payload (KP0)
109	121.690245500	192.168.10.10	192.168.10.20	QUIC	68	Protected Payload (KP0)
110	121.690449700	192.168.10.20	192.168.10.10	QUIC	1514	Protected Payload (KP0)
111	121.690519500	192.168.10.10	192.168.10.20	QUIC	1454	Protected Payload (KP0)

Рис. 1. Общий вид захвата трафика SMB over QUIC в Wireshark. Файл: 25u19t3.pcapng, фильтр: udp.port == 443, диапазон пакетов 91–111. Видны пакеты QUIC Initial, Handshake и Protected Payload

На рисунке 1 отчетливо видна структура QUIC-соединения:

- QUIC Initial (пакет 91) — начальный пакет с параметрами соединения и началом TLS-рукопожатия;
- QUIC Handshake (пакеты 92–94) — обмен криптографическими параметрами и сертификатами;
- QUIC Protected Payload (пакеты 95–111 и далее) — зашифрованные данные SMB, которые Wireshark не может декодировать без ключей сессии.

Детальный разбор пакета QUIC Initial, показанный на рисунке 2, демонстрирует наличие расширения server_name со значением SRV-QUIC.local, что подтверждает корректную работу механизма SAN при аутентификации сервера.

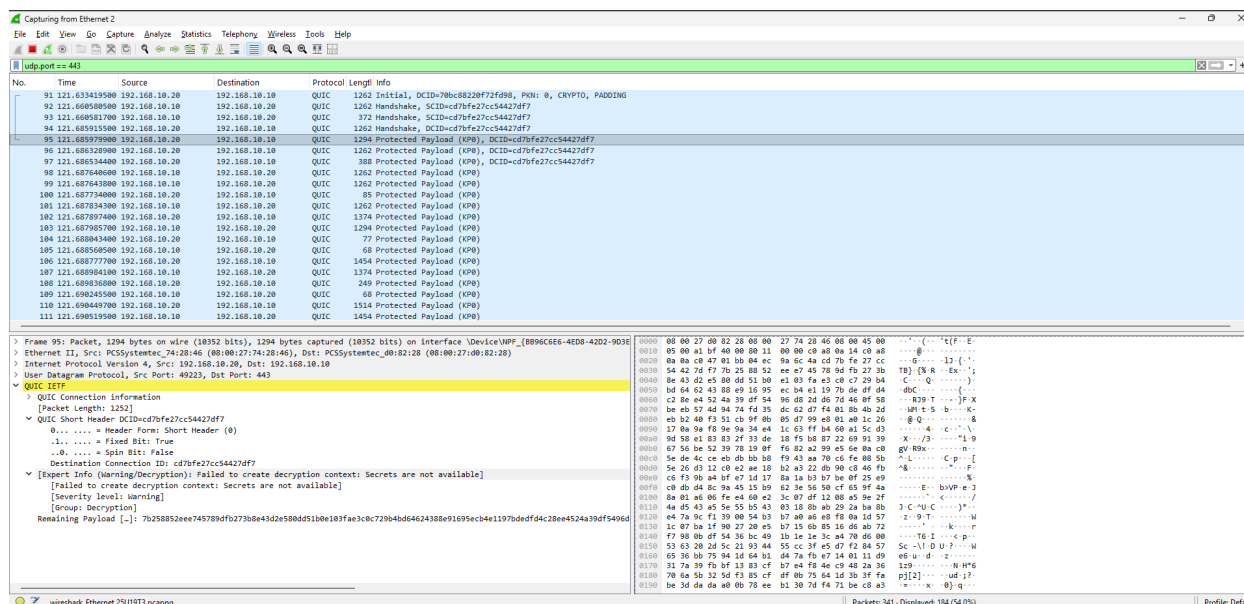


Layer	Protocol	Client Hello
Crypto Data	TLSv1.3 Record Layer: Handshake Protocol: Client Hello	
Handshake Protocol	Client Hello	
Handshake Type	Client Hello (1)	
Length	431	
Version	TLS 1.2 (0x0303)	
Random	cc3cd00f44eb4aefc71935739194ac1a8e189132da0014c26bfd2cc28a65270	
Session ID Length	0	
Cipher Suites Length	4	
Cipher Suites	(2 suites)	
Compression Methods Length	1	
Compression Methods	(1 method)	
Extensions Length	386	
Extensions	server_name (len=19) name=SRV-QUIC.local	
Extensions	status_request (len=5)	
Extensions	supported_versions (len=3) TLS 1.3	
Extensions	signature_algorithms (len=26)	
Extensions	session_ticket (len=0)	
Extensions	supported_groups (len=8)	
Extensions	ec_point_formats (len=2)	
Extensions	application_layer_protocol_negotiation (len=6)	
Extensions	key_share (len=208) x25519, secp256r1, secp384r1	

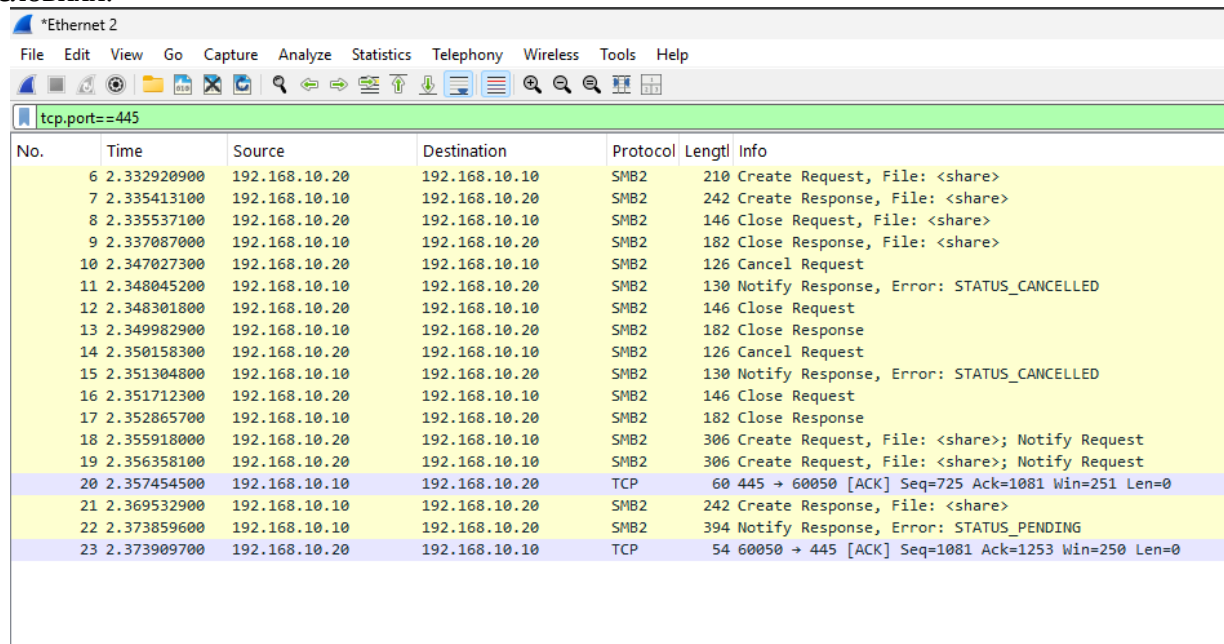
Рис. 2. Детальный разбор пакета QUIC Initial (пакет № 91, файл 25u19t3.pcapng). Видно расширение server_name = SRV-QUIC.local, подтверждающее использование SAN для аутентификации сервера

Все пакеты типа Protected Payload отображаются в Wireshark как зашифрованные, как показано на рисунке 3. Ни имена файлов, ни команды SMB (Create, Read, Write), ни содержимое файлов не поддаются декодированию. Это наглядно демонстрирует эффект сквозного шифрования TLS 1.3, встроенного в протокол QUIC.

Рубрика 2. Методы и системы защиты информации, информационная безопасность



Для сравнения был проведен повторный эксперимент с отключенной поддержкой QUIC на клиенте (Set-SmbClientConfiguration -EnableSMBQUIC \$false). Фильтр Wireshark изменен на tcp.port == 445. Важно отметить, что в данной контрольной конфигурации SMB Encryption на стороне сервера не был включён принудительно, что соответствует настройкам по умолчанию. Подключение и операции с файлом test.txt были повторены в идентичных условиях.



На рисунке 4 отчетливо видны пакеты протокола SMB2 с полностью читаемыми командами: Create Request, Close Request, Notify Request, Read Request. Wireshark успешно декодирует структуру каждого пакета, включая имена файлов и параметры операций.

Детальный разбор пакета SMB2, представленный на рисунке 5, показывает, что в открытом виде передаются:

- имя файла: test.txt;
- команды протокола: Create, Read, Close;

- параметры доступа: Read, Write, Delete;
- временные метки и атрибуты файла.

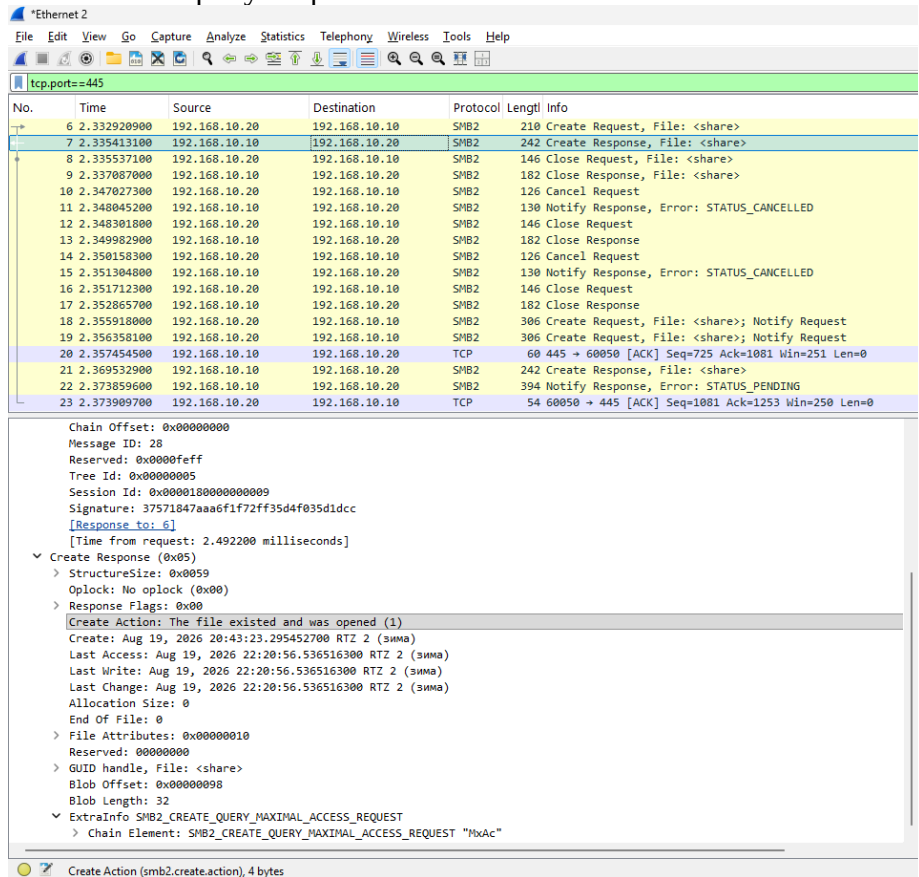


Рис. 5. Детальный разбор пакета SMB2 Create Request (пакет № 19, файл 2ieu5t3.pcapng). В открытом виде отображаются имя файла test.txt и параметры операции. Конфигурация: SMB over TCP без включённого SMB Encryption

Наиболее показательным является пакет SMB2 Read Response, как показано на рисунке 6, в котором содержимое файла передается в открытом виде. В поле данных четко читается текст "Test test test", что подтверждает отсутствие шифрования полезной нагрузки в классическом SMB over TCP при настройках по умолчанию.

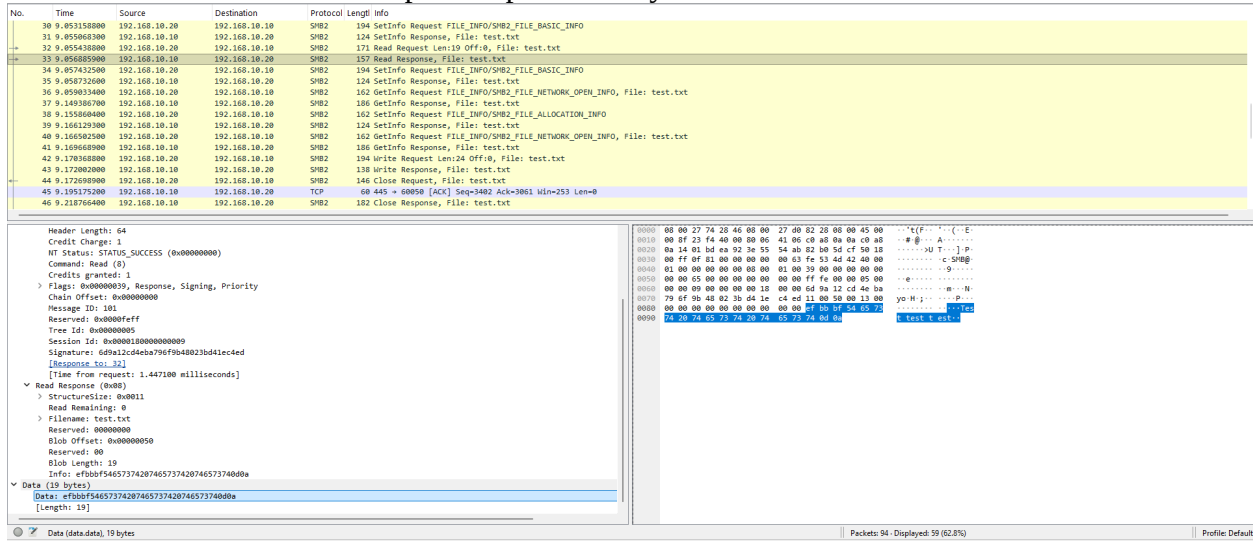


Рис. 6. Пакет SMB2 Read Response (пакет № 20, файл 2ieu5t3.pcapng). Содержимое файла test.txt ("Test test test") передается в открытом виде. Конфигурация: SMB over TCP без включённого SMB Encryption

Таким образом, гипотеза 2 подтверждена. В ходе эксперимента наблюдалось, что в сеансе SMB over QUIC анализатор Wireshark отображает полезную нагрузку исключительно как Protected Payload, не позволяя декодировать команды протокола или имена файлов. В

Рубрика 2. Методы и системы защиты информации, информационная безопасность

контрольном сеансе классического SMB over TCP (порт 445) при настройках по умолчанию (без принудительно включённого SMB Encryption) те же операции (Create Request, Read, Close) и имя файла test.txt отображаются в открытом виде. Наблюдаемое различие согласуется с документацией Microsoft [4] и стандартом RFC 9001 [7], согласно которым SMB over QUIC использует обязательное шифрование TLS 1.3. При этом сетевые метаданные (IP-адреса, порты, размеры пакетов) остаются видимыми в обоих случаях.

Для систематизации результатов исследования составлена таблица 2, отражающая ключевые различия между протоколами.

Таблица 2 – Сравнительный анализ SMB over QUIC и SMB over TCP

Критерий	SMB over QUIC	SMB over TCP
Транспортный протокол	UDP	TCP
Порт	443*	445
Шифрование	Обязательное (TLS 1.3)	Опциональное (по умолчанию отключено)**
Видимость команд SMB в Wireshark	Нет (Protected Payload)	Да (Create, Read, Write, Close)**
Видимость имен файлов	Нет	Да**
Видимость содержимого файлов	Нет	Да**
Аутентификация сервера	X.509 сертификат (SAN)	Kerberos/NTLM

*Доступность порта 443 по протоколу UDP в данной работе показана только в рамках изолированной лабораторной сети. Доступность HTTPS по TCP 443 не гарантирует прохождение UDP-трафика, необходимого для QUIC - в реальных сетях это требует отдельной проверки.

**Наблюдение относится к контрольной конфигурации SMB over TCP без принудительно включённого SMB Encryption.

Эксперимент показал, что SMB over QUIC успешно работает по порту UDP 443 в рамках изолированной лабораторной сети. Важно отметить, что работоспособность в данной работе продемонстрирована только в лабораторных условиях. Доступность HTTPS по TCP 443 не гарантирует прохождения UDP-трафика на порт 443, так как это разные транспортные протоколы, которые могут обрабатываться межсетевыми экранами по-разному, что требует отдельной проверки на конкретном сетевом оборудовании.

В лабораторных условиях было продемонстрировано, что SMB over QUIC может обеспечивать защищенный доступ к файловым ресурсам без необходимости развертывания классических VPN-решений. Однако важно отметить ограничения данного вывода:

- эксперимент проводился в изолированной среде с самоподписанным сертификатом;
- в производственной среде требуется инфраструктура PKI с доверенным центром сертификации;
- SMB over QUIC не заменяет полноценный VPN для доступа ко всем сетевым ресурсам, а только к общим файловым ресурсам SMB.

Таким образом, гипотеза 3 подтверждена частично: использование SMB over QUIC по порту UDP 443 позволяет обойти стандартные ограничения на порт TCP 445 и обеспечивает защищенный доступ к файловым ресурсам, но полная замена VPN-решений требует учета дополнительных факторов (PKI, аутентификация, политики доступа).

Заключение

В ходе исследования была разработана и экспериментально проверена методика безопасного развертывания файлового сервера с поддержкой протокола SMB over QUIC в изолированной лабораторной среде. Был проведен сравнительный анализ структуры сетевого трафика SMB over QUIC и классического SMB over TCP с использованием анализатора Wireshark.

На основе полученных результатов проведена проверка сформулированных гипотез:

Гипотеза 1 подтверждена полностью. Эксперимент доказал техническую реализуемость развертывания SMB over QUIC в изолированной среде без полноценной инфраструктуры Active Directory. Ключевым условием успешной настройки является корректная генерация самоподписанного сертификата X.509 с обязательным указанием альтернативного имени субъекта (SAN), его импорт в доверенное хранилище на клиенте и явная привязка к порту UDP.

Гипотеза 2 подтверждена. Экспериментально наблюдалось, что в сеансе SMB over QUIC анализатор Wireshark отображает полезную нагрузку как Protected Payload, не декодируя команды протокола или имена файлов. В контрольном сеансе классического SMB over TCP при настройках по умолчанию (без включенного SMB Encryption) операции Create Request, Read, Close и имя файла test.txt отображаются в открытом виде. При этом сетевые метаданные (IP-адреса, порты, размеры и временные метки пакетов) остаются видимыми в обоих случаях.

Гипотеза 3 подтверждена частично. Использование порта UDP 443 действительно позволяет успешно обходить стандартные ограничения межсетевых экранов на порт 445, создавая эффект защищенного туннеля. Однако утверждение о том, что SMB over QUIC является универсальной заменой классическим VPN-решениям, требует существенного уточнения. Данный протокол защищает исключительно трафик файлового доступа (SMB), но не обеспечивает маршрутизацию всего сетевого трафика, как это делает полноценный VPN. Кроме того, его безопасное применение в производственной среде невозможно без развернутой инфраструктуры открытых ключей с доверенным центром сертификации, строгой настройки политик аутентификации и аудита.

Перспективные направления дальнейших исследований включают: проведение сравнительного нагрузочного тестирования SMB over QUIC и классического SMB over TCP с принудительно включенным SMB Encryption в условиях высокой интенсивности трафика, исследование механизмов интеграции SMB over QUIC с полноценными корпоративными инфраструктурами открытых ключей (в частности, Active Directory Certificate Services) и сценариев автоматического обновления сертификатов, а также анализ устойчивости соединения QUIC при миграции клиента между разнородными сетями (например, при переходе с Wi-Fi на мобильный интернет) с количественной оценкой времени восстановления сессии. Особый интерес представляет изучение влияния обязательного шифрования TLS 1.3 на производительность файловых операций в высоконагруженных средах, что позволит определить оптимальные сценарии применения протокола. Результаты данной работы могут быть использованы системными администраторами и специалистами по информационной безопасности при проектировании защищенных сценариев удаленного доступа к файловым ресурсам в современных гибридных ИТ-инфраструктурах.

Библиографический список

1. Адживапаев, М. М. Современные транспортные протоколы: TCP, UDP и QUIC Текст научной статьи по специальности «Компьютерные и информационные науки» / М. М. Адживапаев // Информационные технологии и вычислительные системы. – 2025. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/sovremennyye-transportnye-protokoly-tcp-udp-i-quic> (дата обращения: 18.08.2026).
2. Безопасность SMB. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security> (дата обращения: 22.08.2026).
3. Андреев, Н. С. Исследование клиент-серверных протоколов для повышения отказоустойчивости и безопасности соединения / Н. С. Андреев // Вестник науки и образования. – 2024. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/issledovanie-klient-servernyh-protokolov-dlya-povysheniya-otkazoustoychivosti-i-bezopasnosti-soedineniya> (дата обращения: 21.08.2026).
4. SMB over QUIC. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-over-quic> (дата обращения: 21.08.2026).

Рубрика 2. Методы и системы защиты информации, информационная безопасность

5. TLS 1.3 в Windows Server. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/security/tls/tls-1.3> (дата обращения: 18.08.2026).
6. IETF RFC 9000. QUIC: A UDP-Based Multiplexed and Secure Transport. – [Электронный ресурс] // IETF: [сайт]. – URL: <https://www.rfc-editor.org/rfc/rfc9000.html> (дата обращения: 19.08.2026).
7. IETF RFC 9001. Using TLS to Secure QUIC. – [Электронный ресурс] // IETF: [сайт]. – URL: <https://www.rfc-editor.org/rfc/rfc9001.html> (дата обращения: 21.08.2026).
8. QUIC Working Group Documentation. – [Электронный ресурс] // IETF GitHub: [сайт]. – URL: <https://quicwg.github.io/> (дата обращения: 20.08.2026).
9. Симачев, А. Ю. Оценка скрытых каналов по памяти в протоколе QUIC и методы их обнаружения / А. Ю. Симачев // Информационная безопасность регионов России. – 2022. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/otsenka-skrytykh-kanalov-po-pamyati-v-protokole-quic-i-metody-ih-obnaruzheniya> (дата обращения: 20.08.2026).
10. Смирнов, И. А. HTTP/3 и протокол QUIC: будущее высокопроизводительных веб-сервисов / И. А. Смирнов // Молодой ученый. – 2025. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/http-3-i-protokol-quic-budushchee-vysokoproizvoditelnyh-veb-servisov> (дата обращения: 19.08.2026).
11. Галимуллина, А. В. Получение событий с клиента и статусе состояния клиентов средствами Samba AD / А. В. Галимуллина // Информационные технологии. – 2024. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/poluchenie-sobytiy-s-klienta-i-statuse-sostoyaniya-klientov-sredstvami-samba-ad> (дата обращения: 21.08.2026).

References

1. Adzhivapaev, M. M. (2025). Sovremennye transportnye protokoly: TCP, UDP i QUIC [Modern transport protocols: TCP, UDP and QUIC]. *Informatsionnye tekhnologii i vychislitel'nye sistemy*. <https://cyberleninka.ru/article/n/sovremennye-transportnye-protokoly-tcp-udp-i-quic>
2. Microsoft Learn. (n.d.). *SMB security*. <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security>
3. Andreyanov, N. S. (2024). Issledovanie klient-servernykh protokolov dlya povysheniya otkazoustoychivosti i bezopasnosti soedineniya [Study of client-server protocols to improve fault tolerance and connection security]. *Vestnik nauki i obrazovaniya*. <https://cyberleninka.ru/article/n/issledovanie-klient-servernykh-protokolov-dlya-povysheniya-otkazoustoychivosti-i-bezopasnosti-soedineniya>
4. Microsoft Learn. (n.d.). *SMB over QUIC*. <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-over-quic>
5. Microsoft Learn. (n.d.). *TLS 1.3 in Windows Server*. <https://learn.microsoft.com/ru-ru/windows-server/security/tls/tls-1.3>
6. IETF. (2021). *RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport*. <https://www.rfc-editor.org/rfc/rfc9000.html>
7. IETF. (2021). *RFC 9001: Using TLS to Secure QUIC*. <https://www.rfc-editor.org/rfc/rfc9001.html>
8. IETF GitHub. (n.d.). *QUIC Working Group Documentation*. <https://quicwg.github.io/>
9. Simachev, A. Y. (2022). Otsenka skrytykh kanalov po pamyati v protokole QUIC i metody ikh obnaruzheniya [Assessment of memory covert channels in the QUIC protocol and methods for their detection]. *Informatsionnaya bezopasnost' regionov Rossii*. <https://cyberleninka.ru/article/n/otsenka-skrytykh-kanalov-po-pamyati-v-protokole-quic-i-metody-ih-obnaruzheniya>
10. Smirnov, I. A. (2025). HTTP/3 i protokol QUIC: budushchee vysokoproizvoditel'nykh veb-servisov [HTTP/3 and QUIC protocol: the future of high-performance web services]. *Molodoy*

uchenyy. <https://cyberleninka.ru/article/n/http-3-i-protokol-quic-buduschee-vysokoproizvoditelnyh-veb-servisov>

11. Galimullina, A. V. (2024). Poluchenie sobytiy s klienta i statuse sostoyaniya klientov sredstvami Samba AD [Obtaining events from the client and the status of clients using Samba AD]. *Informatsionnye tekhnologii*. <https://cyberleninka.ru/article/n/poluchenie-sobytiy-s-klienta-i-statuse-sostoyaniya-klientov-sredstvami-samba-ad>

Информация об авторе

Васильев Никита Сергеевич - студент кафедры “Безопасность информационных технологий”, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация, e-mail: nikita.vasilev.1901@list.ru

SECURITY RESEARCH AND NETWORK TRAFFIC ANALYSIS OF THE SMB OVER QUIC PROTOCOL IN WINDOWS SERVER 2025 INFRASTRUCTURE

Vasilev N. S.¹

¹ National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. With growing data volumes and remote work, file resource security has become critical. Traditional SMB over TCP (port 445) is vulnerable to passive traffic interception and is often blocked by firewalls. This article examines SMB over QUIC, which encapsulates SMB traffic into a secure QUIC tunnel over UDP (port 443) with mandatory TLS 1.3 encryption. The study aims to practically verify the deployment methodology of this protocol and to comparatively analyze its network traffic with classic SMB. During the experiment, an isolated laboratory environment based on Windows Server 2025 (version 24H2, build 26100.32230) and Windows 11 Pro (version 25H2, build 26200.7840) was deployed. Using Wireshark 4.6.8 analyzer, traffic of both protocols was intercepted and investigated. The results showed that in an SMB over QUIC session, the analyzer displays the payload exclusively as Protected Payload, without decoding protocol commands or file names. In a control session of classic SMB over TCP (with default settings without forcibly enabled SMB Encryption), the same operations (Create Request, Read, Close) and the file name test.txt (size 1 KB) appear in plain text. It is concluded that SMB over QUIC is a potential alternative to classic VPN solutions exclusively for secure file access, provided that the Public Key Infrastructure (PKI), strict authentication, and auditing are correctly configured, but it does not replace a full-fledged VPN for routing all network traffic. The limitations of the study include the use of a self-signed certificate and a laboratory network without modeling real operating conditions.

Keywords: SMB over QUIC, Windows Server 2025, network security, Wireshark, TLS 1.3, QUIC protocol, file share.

Information about the author

Vasilev Nikita Sergeevich - Student, Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation, e-mail: nikita.vasilev.1901@list.ru

Т. И. Ефименко¹

¹ Санкт-Петербургское государственное автономное профессиональное образовательное учреждение «Колледж туризма и прикладных технологий», Санкт-Петербург, Россия

ОТЕЧЕСТВЕННЫЙ СТЕК ТЕХНОЛОГИЙ: ОТ ЗАДАНИЯ ДО УЧЕБНОГО ПРОЦЕССА

Аннотация. Статья описывает организационно-педагогическую модель переноса отечественного стека технологий в подготовку специалистов среднего звена по компетенции «Сетевое и системное администрирование». Проблема исследования состоит в том, что требования отдельного работодателя не всегда отражают разнообразие инфраструктуры, с которой выпускники столкнутся в профессиональной деятельности. В качестве альтернативы рассматривается работа команды управления компетенцией, объединяющей экспертов, преподавателей, практиков и производителей технологий. Материалом для анализа служит конкурсное задание регионального этапа чемпионата «Профессионалы» цикла 2026–2027 годов; экспериментальная оценка эффективности модели не проводилась. Состав задания систематизирован по пяти функциональным уровням: передача данных, операционные системы и базовые службы, защита периметра, данные и наблюдаемость, контур разработки и эксплуатации. Для каждого уровня рассмотрены применяемые продукты, их назначение и происхождение. Показан порядок преобразования задания в карту соответствия дисциплинам учебного плана, учебный стенд и фонд задач нарастающей сложности. Рассмотрены три формы взаимодействия с производителями: профессиональные мероприятия, межорганизационные соглашения и региональные образовательные площадки, включая примеры Армавира и Мурманска. Установлены границы описания: представленный материал является анализом одного случая; количественные рыночные данные опираются на отраслевые публикации, а количественные оценки образовательного охвата требуют самостоятельного подтверждения. Предположение о влиянии автоматизации на массовость подготовки специалистов сформулировано как гипотеза, нуждающаяся в эмпирической проверке.

Ключевые слова: среднее профессиональное образование, профессиональные компетенции, отечественное программное обеспечение, конкурсное задание, профессиональное сообщество, содержание образования, сетевое и системное администрирование.

Введение

Российский рынок инфраструктурного программного обеспечения по итогам 2025 года достиг 158 млрд рублей и вырос на 16 % при росте рынка информационных технологий в целом на 13 %; доля российских производителей, по оценке аналитиков Strategy Partners, поднялась с 8 % до 68 % [1, 2]. Оценка выполнена по выручке. Объём сегмента операционных систем составил 31 млрд рублей, систем управления базами данных – 44 млрд рублей [2]; рынок резервного копирования достиг 10,6 млрд рублей при росте 18,5 % за год [3]. Для средств контейнеризации обзор прогнозирует рост около 22 % в год до 2030 года [2]. Определения сегментов и расчётная методика приведены в полной версии обзора [1]; в публикациях прессы они не раскрыты, поэтому приведённые цифры служат отраслевым ориентиром и не характеризуют отдельный продукт.

Скорость обновления технологического контура опережает цикл пересмотра образовательных программ. Возникает педагогическая проблема: содержание профессиональной подготовки расходится с составом продуктов, применяемых в производственной практике. Готовность системы среднего профессионального образования к технологическому суверенитету рассмотрена в работе В. И. Блинова, Е. Ю. Есениной и И. С. Сергеева [4]. Закреплённый в системе механизм согласования, то есть взаимодействие образовательной организации с работодателем, для информационно-технологического профиля работает ограниченно.

Цель статьи – описать организационно-педагогическую модель, сложившуюся в компетенции «Сетевое и системное администрирование», и показать на материале конкурсного задания регионального этапа цикла 2026–2027 годов порядок переноса отечественного стека технологий в учебный процесс. Под отечественным стеком технологий понимается согласованный набор программных продуктов разных классов, совместная работа

которых образует действующую информационно-коммуникационную систему; платформенную основу набора составляют продукты российских разработчиков, дополненные открытыми проектами международных сообществ (таблица 1).

Материал и границы описания

Статья описывает один случай и не содержит экспериментальной проверки. Материалом служат конкурсное задание регионального этапа цикла 2026–2027 годов по компетенции «Сетевое и системное администрирование» [5] (организатор – Всероссийское чемпионатное движение по профессиональному мастерству «Профессионалы» [6]), отраслевые обзоры [1–3] и публичные сообщения об отраслевых событиях (раздел 6). Утверждения о результатах модели сформулированы как наблюдения автора и сопровождаются источником. Утверждения о причинном влиянии модели на качество подготовки не выдвигаются: для них нужны сравнительные данные, которых в статье нет.

Ограничение парной модели «образовательная организация – работодатель»

Классическая модель социального партнёрства сложилась вокруг массовых рабочих профессий. Машиностроительное предприятие ежегодно принимает десятки сварщиков, автотранспортное – десятки автомехаников; парк оборудования однотипен, перечень трудовых операций устойчив. Образовательная организация выстраивает отношения с одним предприятием и получает ориентир, охватывающий значительную часть выпуска.

Информационно-технологические специальности устроены иначе. Гостиничный комплекс, транспортная компания, районная больница, торговая сеть среднего размера содержат одного–двух системных администраторов; штат из десяти работников этого профиля встречается в организациях, для которых информационные технологии составляют основной вид деятельности. Договор с единственным работодателем даёт запрос в одну–две вакансии за несколько лет и требования, отражающие инфраструктуру конкретной организации. Этот тезис является наблюдением автора и опирается на типовую структуру штатов; количественная проверка на выборке организаций остаётся задачей отдельного исследования.

Литература фиксирует смежные явления. Ю. О. Климова на материале вузов Вологодской области описала проблемы формирования компетенций ИТ-специалистов [7]. А. В. Карпов, А. А. Карпов и С. О. Присяжнюк рассмотрели специфику формирования профессиональных компетенций специалистов ИТ-сферы [8]. О. Н. Ромашкова и Д. И. Мухаммад предложили модели управления развитием профессиональных компетенций в организационных системах ИТ-компаний [9]. Три работы относятся к вузовскому образованию и корпоративной среде, поэтому прямого описания механизма согласования содержания среднего профессионального образования с ИТ-отраслью они не дают. Этот пробел и определяет предмет статьи.

Второе ограничение относится к оцениванию. Региональные особенности внешней оценки качества подготовки в системе СПО проанализированы С. Ю. Алашеевым, Н. Ю. Посталюк и В. А. Прудниковой [10]; сопряжение государственной итоговой аттестации с независимой оценкой квалификаций рассмотрено В. А. Фёдоровым, Н. В. Третьяковой и Г. А. Туриной [11]. Обе работы исходят из единых процедур и согласованных измерительных материалов. Требования единственного работодателя такой основы не образуют.

Команда управления компетенцией как единое окно

С 2023 года в компетенции «Сетевое и системное администрирование» посредником между отраслью и системой образования выступает профессиональное сообщество. Развёртывание модели включало три шага. На базе действующего сообщества экспертов, преподавателей и практикующих системных администраторов сформирована команда управления компетенцией. К работе команды привлечены российские производители технологий: разработчики операционных систем, маршрутизаторов, межсетевых экранов, средств резервного копирования, платформ разработки. Принятые решения оформлены документами, пригодными для прямого использования образовательной организацией.

Организационно команда работает по принципу многофункционального центра предоставления государственных услуг: заявитель обращается в одну точку и получает результат, для которого требуется взаимодействие нескольких ведомств. Образовательная

Рубрика 3. Методология и технология профессионального образования

организация получает от команды согласованный комплект: перечень продуктов стека, условия их учебного использования, описание стенда с расчётом ресурсов, конкурсное задание с критериями оценки, программы повышения квалификации преподавателей. Без единого окна колледжу пришлось бы вести не менее шести самостоятельных переговоров по числу российских производителей, перечисленных в таблице 1, причём каждый предлагает собственный формат материалов и собственные требования к площадке.

По документам чемпионата, задания прежних лет допускали зарубежное и отечественное программное обеспечение, а с 2024 года в обязательный технологический контур заданий введены российские платформенные продукты [5]; ключевые документы чемпионата размещены на сайте Всероссийского чемпионатного движения. Отечественная платформенная основа здесь означает использование российских маршрутизаторов, операционных систем, межсетевого экрана, средства резервного копирования и платформы управления исходным кодом; другие компоненты, включая проекты международных сообществ, сохраняют собственное происхождение (таблица 1). Сведений о затратах образовательных организаций на согласование в статье нет, поэтому вывод о сокращении издержек не формулируется.

Отраслевой ориентир содержания

Состав стека определяется сегментами рынка с подтверждённой динамикой внедрения. Обзор Strategy Partners называет операционные системы (31 млрд рублей) и системы управления базами данных (44 млрд рублей) крупнейшими сегментами и прогнозирует для них рост до 52 и 79 млрд рублей к 2030 году [2]. Резервное копирование растёт быстрее рынка инфраструктурного программного обеспечения второй год подряд [3]. Контейнеризация входит в число самых быстрорастущих сегментов [2].

Выбор уровней задания согласуется с этой картиной: в таблице 1 представлены все названные сегменты. Автор выдвигает интерпретацию: после первой волны замещения организация, развернувшая российскую операционную систему, российскую платформу виртуализации и систему управления базами данных, сталкивается с задачей согласованного управления набором, поэтому в задании выделен модуль эксплуатации и наблюдаемости. Обзор [2] этого вывода не содержит, интерпретация требует проверки на данных о вакансиях.

Стек технологий в конкурсном задании

Конкурсное задание регионального этапа цикла 2026–2027 годов рассчитано на 15 часов и три конкурсных дня, оценивается по 100-балльной шкале и состоит из трёх модулей: «Аудит» (вариативный, 4 часа, 20 баллов), «Настройка технических и программных средств информационно-коммуникационных систем» (инвариантный, 6 часов, 40 баллов), «DevOps» (инвариантный, 5 часов, 40 баллов) [5]. Конкурсант получает виртуальный стенд из четырнадцати машин, объединённых в сеть учебного предприятия с центром обработки данных, каналом провайдера и защищённым сегментом.

Содержание задания удобно представить пятью уровнями; каждый опирается на нижележащий, как инженерные сети здания опираются на несущие конструкции. Таблица 1 фиксирует продукты, роли и происхождение компонентов. Версии указаны по инфраструктурному листу задания [5]. Происхождение определено по правообладателю продукта.

Таблица 1 – Состав стека технологий по уровням конкурсного задания

Уровень	Продукт (версия по заданию [5])	Роль в задании	Происхождение
1. Передача данных	EcoRouter OS (РДП.РУ); Eltex vESR (Элтекс); Open vSwitch	Маршрутизация IS-IS, OSPF, BGP; агрегирование каналов LACP; коммутация защищённого сегмента	Российские продукты (EcoRouter OS, Eltex vESR); открытый проект международного сообщества (Open vSwitch)

Уровень	Продукт (версия по заданию [5])	Роль в задании	Происхождение
2. Операционные системы и базовые службы	«Альт Сервер 11», «Альт Рабочая станция 11» (Базальт СПО); Kea-DHCPv4; chrony; OpenSSL; служба DNS	Служба имён, выдача адресов с обновлением записей, синхронизация времени, удостоверяющий центр, хранилище по протоколу iSCSI	Российские операционные системы; открытые проекты международных сообществ
3. Защита периметра	Ideco NGFW NOVUM 22 (Ideco)	Межсетевое экранирование, политика доступа	Российский продукт
4. Данные и наблюдаемость	PostgreSQL 18, pgAdmin4; Zabbix 7.0 с NGINX; «Кибер Бэкап» (Киберпротект)	Хранение данных, мониторинг узлов, резервное копирование СУБД и операционной системы	Открытые проекты (PostgreSQL, pgAdmin4, Zabbix, NGINX); российский продукт («Кибер Бэкап»)
5. Контур разработки и эксплуатации	Docker; Nexus; GitFlic (установка на собственные серверы); Grafana, Prometheus, Loki, Tempo, Grafana Alloy	Сборка и публикация образа, репозиторий артефактов, хранение исходного кода, метрики, журналы и трассировки	Российский продукт (GitFlic); зарубежные продукты с открытым исходным кодом или открытой редакцией (остальные)

Из таблицы следует, что слово «отечественный» в названии стека относится к платформенной основе: маршрутизаторам, операционным системам, межсетевому экрану, резервному копированию и платформе управления исходным кодом. Происхождение остальных компонентов международное, их разрабатывают открытые сообщества и зарубежные компании.

Уровень первый – передача данных. Маршрутизатор выбирает путь для порции данных между сетями, протоколы маршрутизации задают правила, по которым устройства сообщают друг другу о доступных путях. В задании применены IS-IS и OSPF внутри автономных систем, BGP между ними. Отдельная задача – распределение адресного диапазона между тремя площадками с потребностью 6, 30 и 62 узловых адреса. Адресное пространство ограничено, и конкурсант распределяет его так, чтобы остаток сохранил пригодность для расширения. В оригинале задания использован публичный диапазон 78.23.0.0/24; блок 78.0.0.0/8 выделен организации RIPE NCC [12]. Для публикации и учебного использования пример заменён диапазоном 198.51.100.0/24 (TEST-NET-2), зарезервированным для документации [13]. Требуемые размеры подсетей сохранены (таблица 2); метод распределения блоков разного размера основан на бесклассовой адресации [14]. Для учебного стенда рекомендуется изолированная сеть и документационный диапазон: использование чужого публичного адресного пространства закрепляет ошибочную практику.

Таблица 2 – Распределение диапазона 198.51.100.0/24 по требованиям задания

Площадка	Требуется узловых адресов	Префикс	Блок	Диапазон узловых адресов
А	62	/26	198.51.100.0/26	.1–.62
Б	30	/27	198.51.100.64/27	.65–.94
В	6	/29	198.51.100.96/29	.97–.102
Резерв	–	/29, /28, /25	198.51.100.104/29, .112/28, .128/25	152 адреса для расширения

Блоки распределены по убыванию размера, каждый выровнен по границе своего размера. Остаток 198.51.100.104–255 разбивается на три выровненных блока и сохраняет пригодность для расширения.

Уровень второй – операционные системы и базовые службы. Серверы и рабочая станция работают под управлением «Альт Сервер 11» и «Альт Рабочая станция 11». На этом уровне

Рубрика 3. Методология и технология профессионального образования

разворачиваются службы, без которых сеть остаётся набором адресов: служба доменных имён переводит имена в числовые адреса; Kea-DHCPv4 выдаёт адреса и обновляет записи имён; chrony синхронизирует время с эталонным сервером ФГУП «ВНИИФТРИ»; удостоверяющий центр на OpenSSL выпускает сертификаты внутренних веб-сервисов. Диск удалённого массива доступен серверу по протоколу iSCSI как локальный.

Уровень третий – защита периметра. Граница между внутренней сетью и внешним миром закрыта межсетевым экраном Ideco NGFW NOVUM 22, который разграничивает потоки данных и служит точкой применения политики доступа.

Уровень четвёртый – данные и наблюдаемость. Сервер баз данных работает под управлением PostgreSQL 18, администрирование выполняется через pgAdmin4. Состояние узлов контролирует Zabbix 7.0: узлы распределены по группам, к ним применены шаблоны наблюдения, отказ узла фиксируется автоматически. Сохранность данных обеспечивает «Кибер Бэкап» с агентами для PostgreSQL и операционной системы.

Уровень пятый – контур разработки и эксплуатации. Модуль DevOps выполняется на инфраструктуре предыдущего модуля. Конкурсант разворачивает Docker, репозиторий артефактов Nexus и российскую платформу управления исходным кодом GitFlic на собственных серверах, регистрирует исполнителей сборки, готовит описание сборки, собирает образ и публикует его версию. Подсистема наблюдаемости на связке Grafana, Prometheus, Loki, Tempo и Grafana Alloy собирает показатели, журналы и трассировки; связь между трассировкой и журналом позволяет пройти от замедлившегося запроса к записи о причине замедления.

Вариативный модуль «Аудит» меняет позицию конкурсанта. Он получает результат работы другого исполнителя и оценочную ведомость, оформляет заключение в формате ODT и подтверждает каждое решение снимком экрана. Умение читать чужую конфигурацию оценивается наравне с умением создавать собственную.

Совместимость продуктов описывается для проверенной комбинации версий из таблицы 1. Критерий успеха – выполнение пунктов оценочной ведомости модулей на всех четырнадцати машинах стенда при подготовке задания¹. Выводы о совместимости других версий, платформ виртуализации и условий лицензирования из описания не следуют.

Связность уровней придаёт заданию диагностическую ценность. Ошибка в распределении адресов первого уровня проявится недоступностью веб-интерфейса пятого; неверно выпущенный сертификат второго уровня остановит публикацию образа. Конкурсант удерживает картину системы целиком, что отвечает принципу подтверждения компетенции действием.

Преобразование задания в содержание учебного процесса

Конкурсное задание представляет собой сжатое описание отраслевого технологического контура. Образовательная организация выводит из него три производных продукта.

Первый – карта соответствия уровней стека дисциплинам и профессиональным модулям учебного плана. Уровень передачи данных распределяется между дисциплинами сетевого цикла, уровень операционных систем – между модулями администрирования, уровень данных и наблюдаемости – между дисциплинами баз данных и эксплуатации, контур разработки – между модулями сопровождения программного обеспечения. Раздел стека, не закреплённый ни за одной дисциплиной, обозначает дефицит содержания.

Второй – учебный стенд. Четырнадцать машин конкурсного стенда развёртываются на учебном оборудовании средствами вложенной виртуализации, при которой среда виртуализации запускается внутри другой среды виртуализации. Стенд служит полигоном: обучающийся работает с полной инфраструктурой и вносит изменения, не затрагивая действующих систем. Близкая архитектура применяется в киберполигонах подготовки специалистов по защите информации [15]. Расчёт ресурсов и порядок настройки зависят от платформы виртуализации образовательной организации и выходят за рамки статьи.

¹ <https://pro.firpo.ru/meropriyatiya/itogi/itogi2325/>

Параметры сетевых протоколов на отечественных маршрутизаторах изучены в лабораторных условиях: время переключения VRRP в EcoRouterOS зависит от интервала анонсов и режима вытеснения [16]; авторы указанной работы квалифицируют результаты как предварительные единичные наблюдения, поэтому для учебных задач значения параметров проверяются на стенде образовательной организации.

Третий – фонд учебных задач нарастающей сложности. Конкурсное задание целиком непосильно для второго курса, поэтому оно разбирается на последовательность задач: настройка одного узла, связка двух узлов, слой целиком, стек целиком. Последовательность соответствует переходу от изолированных операций к целостной задаче, обоснованному в четырёхкомпонентной модели педагогического дизайна и применённому Е. Г. Литвак к проектированию баз данных [17]. Итоговая задача воспроизводит конкурсное задание в полном объёме.

Условие, относящееся к преподавателю: уровни стека осваиваются преподавателем до того, как выносятся на занятие. Единое окно обеспечивает подготовку программами повышения квалификации, согласованными с производителями технологий.

Компетенция как опорная точка партнёрства производителей технологий

Стек собран из продуктов разных производителей, часть которых конкурирует в смежных сегментах рынка. Операционная система одного производителя работает с маршрутизатором второго, межсетевым экраном третьего и системой резервного копирования четвёртого. Компетенция выступает опорной точкой, вокруг которой производители выстраивают отношения между собой и с системой образования. Описание ниже построено по публичным сообщениям организаторов; независимой оценки эффективности этих событий в статье нет.

Первый уровень партнёрства – совместные мероприятия. 20 марта 2026 года на площадке Колледжа автоматизации и информационных технологий № 20 прошёл отраслевой форум «Сетевое и системное администрирование – основа подготовки ИТ-специалистов»; по сведениям организаторов, в нём участвовали более 150 человек из более чем пятнадцати субъектов Российской Федерации, среди которых преподаватели и мастера производственного обучения СПО составили 57 %, представители высшего образования – 13 %, представители реального сектора экономики – 20 %². Вебинар «Подготовка ИТ-кадров в СПО: от новых ФГОС к практическим решениям» вёлся непосредственно с занятия в учебном центре производителя операционных систем «Альт». Ежегодным событием остаётся Международная олимпиада «Основы сетевых технологий» памяти В. Г. Аверина.

Второй уровень – соглашения производителей между собой. По сообщению прессы от 5 июня 2026 года, компании «Базальт СПО», «АДЕМ-инжиниринг» и «Новотех» заключили на площадке РГУ нефти и газа (НИУ) имени И. М. Губкина трёхстороннее соглашение о развитии отечественных цифровых решений и подготовке кадров [18]. Соглашение соединяет системное и инфраструктурное программное обеспечение, промышленное программное обеспечение с системами автоматизированного проектирования и разработку образовательных программ с обучением преподавателей.

Третий уровень – региональные площадки подготовки. 13 февраля 2026 года в Армавирском юридическом техникуме открылась учебно-исследовательская лаборатория отечественных ИТ-решений, созданная компаниями «Базальт СПО» и Ideco совместно с интегратором ARinteg; обучение ведётся на «Альт» и Ideco NGFW NOVUM [19]. 18 июня 2026 года в Мурманском колледже экономики и информационных технологий прошёл круглый стол о сотрудничестве с производителями отечественного оборудования и программного обеспечения; по сведениям организаторов, колледж заключил соглашения с компаниями «РДП Инновации» (EcoRouter) и «Базальт СПО» об использовании российского программного обеспечения и сетевого оборудования в подготовке ИТ-кадров Мурманской области³.

² <https://esim.firpo.ru>

³ <https://t.me/+1IMVKRSm2YwxZDky>

Рубрика 3. Методология и технология профессионального образования

Эти события показывают, как стек конкурсного задания может переходить в региональные образовательные организации. Данных о том, что условия подготовки в регионах стали ближе к условиям федерального уровня, в статье нет: для такого вывода нужно сравнение результатов демонстрационных экзаменов по регионам до и после открытия лабораторий. Численность выпускников и образовательных организаций, охваченных моделью, не приводится: сопоставимые данные и правило подсчёта в использованных материалах отсутствуют. Демонстрационный экзамен как форма государственной итоговой аттестации регламентирован Порядком проведения ГИА по программам СПО [20].

Обратный контур и гипотеза о массовости подготовки

Модель единого окна работает в двух направлениях. Прямое направление – передача стека в образовательные организации. Обратное – передача производителю сведений о том, где и как готовят выпускников, владеющих его продуктами. Производитель видит площадки, задания и результаты чемпионата и получает основание рекомендовать партнёрской сети выпускников конкретных образовательных организаций: вместе с продуктом заказчик получает указание на источник подготовленных работников. Эффективность обратного контура в статье не измерялась.

Далее изложена гипотеза автора; установленным результатом она не является. Операции первого квалификационного уровня (устранение типичных инцидентов по документированным процедурам, инвентаризация, подготовка отчётов) могут переходить к средствам автоматизации. Основания для гипотезы косвенные. Работа Eloundou и соавторов оценивает потенциальное влияние больших языковых моделей на профессиональные задачи по занятиям и не содержит прогноза для конкретной профессии системного администратора [21]. Обзор Notaro, Cardoso и Gerndt описывает методы AIOps для обнаружения, диагностики и прогнозирования отказов в вычислительных системах [22]. Прямых исследований автоматизации трудовых функций системного администратора в статье нет, поэтому вывод о сокращении массовой подготовки не формулируется. Проверка гипотезы требует анализа вакансий и трудовых функций профессионального стандарта.

Установленный в статье педагогический факт ограничен следующим: пятнадцать часов работы с четырнадцатью машинами и пятью уровнями стека задают меру сложности итоговой задачи, к которой образовательная организация может выстраивать фонд учебных задач.

Заключение

Описанная модель заменяет парное партнёрство с работодателем взаимодействием с профессиональным сообществом и производителями технологий. Причина замены – малая численность информационно-технологических подразделений в организациях, которая делает запрос единственного работодателя нерепрезентативным. Команда управления компетенцией выполняет функцию единого окна между производителями и образовательными организациями. По документам чемпионата, в заданиях с 2024 года приоритет отдан российским платформенным продуктам, используемым совместно с открытыми решениями [5].

Конкурсное задание служит формой передачи отраслевого технологического контура в систему образования. Разбор по пяти уровням, сведённый в таблицу «уровень – продукт и версия – роль – происхождение», даёт образовательной организации карту содержания, основу спецификации учебного стенда и фонд учебных задач. Происхождение компонентов показывает, что отечественным в стеке является платформенная основа, а открытые проекты международных сообществ дополняют её.

События 2026 года (форум, трёхстороннее соглашение производителей, лаборатории в Армавире и Мурманске) образуют последовательность партнёрских шагов вокруг конкурсной площадки. Для оценки результативности модели необходимы документированные данные: реестр площадок с правилами подсчёта, сравнение результатов демонстрационных экзаменов по регионам, сведения о затратах на согласование. Сбор этих данных определяет направление дальнейшей работы.

Библиографический список

1. Обзор российского рынка инфраструктурного ПО и перспективы его развития / Strategy Partners. – Москва, 2026. – URL: <https://strategy.ru/research/research/47> (дата обращения: 06.10.2026).
2. Strategy Partners: рынок инфраструктурного ПО в России вырос до 158 млрд рублей // Телеспутник. – 2026. – 21 июля. – URL: <https://telesputnik.ru/materials/trends/news/strategy-partners-rynok-infrastrukturnogo-po-v-rossii-vyros-do-158-mlrd-rublei> (дата обращения: 06.10.2026).
3. Рынок резервного копирования в России разогнался до 10,6 млрд рублей // Anti-Malware.ru. – 2026. – 21 авг. – URL: <https://www.anti-malware.ru/news/2026-08-21-111332/51145> (дата обращения: 06.10.2026).
4. Блинов, В. И. Готовность отечественной системы среднего профессионального образования к достижению технологического суверенитета: результаты исследования / В. И. Блинов, Е. Ю. Есенина, И. С. Сергеев // Профессиональное образование и рынок труда. – 2023. – Т. 11, № 2. – С. 6–31. – DOI 10.52944/PORT.2023.53.2.001.
5. Конкурсное задание регионального этапа чемпионата «Профессионалы» по компетенции «Сетевое и системное администрирование», цикл 2026–2027 гг. – 2026.
6. Всероссийское чемпионатное движение по профессиональному мастерству «Профессионалы» : официальный сайт. – URL: <https://pro.firpo.ru/> (дата обращения: 13.06.2026).
7. Климова, Ю. О. Проблемы формирования компетенций ИТ-специалистов в вузах Вологодской области / Ю. О. Климова // Вопросы территориального развития. – 2021. – Т. 9, № 1 (56). – С. 5–18. – DOI 10.15838/tdi.2021.1.56.5. – EDN VZKEYP.
8. Карпов, А. В. Специфика формирования профессиональных компетенций специалистов ИТ-сферы / А. В. Карпов, А. А. Карпов, С. О. Присяжнюк // Национальный психологический журнал. – 2024. – Т. 19, № 4. – С. 201–214. – DOI 10.11621/npj.2024.0414.
9. Ромашкова, О. Н. Модели управления развитием профессиональных компетенций специалистов в организационных системах ИТ-компаний / О. Н. Ромашкова, Д. И. Мухаммад // Современные наукоёмкие технологии. – 2025. – № 9. – С. 123–131. – DOI 10.17513/snt.40496.
10. Алашеев, С. Ю. Внешняя оценка качества подготовки в системе СПО: региональные особенности / С. Ю. Алашеев, Н. Ю. Посталюк, В. А. Прудникова // Профессиональное образование и рынок труда. – 2025. – Т. 13, № 3 (62). – С. 6–27. – DOI 10.52944/PORT.2025.62.3.001.
11. Фёдоров, В. А. Сопряжение процедур государственной итоговой аттестации и независимой оценки квалификаций в СПО / В. А. Фёдоров, Н. В. Третьякова, Г. А. Турина // Профессиональное образование и рынок труда. – 2022. – Т. 10, № 3 (50). – С. 35–54. – DOI 10.52944/PORT.2022.50.3.007.
12. IANA IPv4 Address Space Registry. – URL: <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml> (дата обращения: 06.10.2026).
13. RFC 5737. IPv4 Address Blocks Reserved for Documentation / J. Arkko, M. Cotton, L. Vegoda. – Internet Engineering Task Force, 2010. – DOI 10.17487/RFC5737.
14. RFC 4632. Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan / V. Fuller, T. Li. – Internet Engineering Task Force, 2006. – DOI 10.17487/RFC4632.
15. Прохоров, А. И. Киберполигон как современный инструмент обеспечения информационной безопасности / А. И. Прохоров // Информатизация в цифровой экономике. – 2023. – Т. 4, № 4. – С. 363–378. – DOI 10.18334/ide.4.4.119301.
16. Чаков, И. А. Исследование функционала и времени восстановления VRRP на базе решений EcoRouter / И. А. Чаков, М. С. Евтюхов, В. В. Павловский // Профессионалитет. – 2025. – № 4 (008). – С. 33–43.

Рубрика 3. Методология и технология профессионального образования

17. Литвак, Е. Г. Методика преподавания проектирования баз данных на основе четырёхкомпонентной модели педагогического дизайна / Е. Г. Литвак // Информатика и образование. – 2022. – Т. 37, № 4. – С. 46–53. – DOI 10.32517/0234-0453-2022-37-4-46-53. – EDN QHQUNG.
18. «Базальт СПО», «АДЕМ-инжиниринг» и «Новотех» объединяют усилия для подготовки ИТ-кадров // CNews. – 2026. – 5 июня. – URL: https://www.cnews.ru/news/line/2026-06-05_bazalt_spodem-inzhiniring (дата обращения: 06.10.2026).
19. В Армавирском юридическом техникуме открыли лабораторию отечественного ПО // CNews. – 2026. – 13 февр. – URL: https://www.cnews.ru/news/line/2026-02-13_administrirovanie_i_informatsionnaya (дата обращения: 06.10.2026).
20. Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования : приказ Министерства просвещения Российской Федерации от 8 нояб. 2021 г. № 800 (с изменениями и дополнениями).
21. Eloundou, T. GPTs are GPTs: Labor market impact potential of LLMs / T. Eloundou, S. Manning, P. Mishkin, D. Rock // Science. – 2024. – Vol. 384, № 6702. – P. 1306–1308. – DOI 10.1126/science.adj0998.
22. Notaro, P. A survey of AIOps methods for failure management / P. Notaro, J. Cardoso, M. Gerndt // ACM Transactions on Intelligent Systems and Technology. – 2021. – Vol. 12, № 6. – Art. 81. – DOI 10.1145/3483424.

References

1. Strategy Partners. (2026). Obzor rossiyskogo rynka infrastruktornogo PO i perspektivy ego razvitiya [Review of the Russian infrastructure software market and its development prospects]. <https://strategy.ru/research/research/47>
2. Telesputnik. (2026, July 21). Strategy Partners: Rynok infrastruktornogo PO v Rossii vyros do 158 mlrd rubley [The Russian infrastructure software market reached RUB 158 billion]. <https://telesputnik.ru/materials/trends/news/strategy-partners-rynok-infrastruktornogo-po-v-rossii-vyros-do-158-mlrd-rublei>
3. Anti-Malware.ru. (2026, August 21). Rynok rezervnogo kopirovaniya v Rossii razognalsya do 10,6 mlrd rubley [The Russian backup market reached RUB 10.6 billion]. <https://www.anti-malware.ru/news/2026-08-21-111332/51145>
4. Blinov, V. I., Esenina, E. Yu., & Sergeev, I. S. (2023). Gotovnost otechestvennoy sistemy srednego professionalnogo obrazovaniya k dostizheniyu tekhnologicheskogo suvereniteta: Rezultaty issledovaniya [Readiness of the Russian secondary vocational education system to achieve technological sovereignty: Research results]. *Professionalnoe obrazovanie i ryok truda*, 11(2), 6–31. <https://doi.org/10.52944/PORT.2023.53.2.001>
5. Konkursnoe zadanie regionalnogo etapa chempionata “Professionaly” po kompetentsii “Setevoe i sistemnoe administrirovanie,” tsikl 2026–2027 [Competition task for the regional stage of the Professionals Championship in Network and System Administration]. (2026).
6. Vserossiyskoe chempionatnoe dvizhenie po professionalnomu masterstvu “Professionaly” [All-Russian Professionals skills championship movement]. (n.d.). <https://pro.firpo.ru/>
7. Klimova, Yu. O. (2021). Problemy formirovaniya kompetentsiy IT-spetsialistov v vuzakh Vologodskoy oblasti [Problems of developing IT specialists’ competencies at universities in the Vologda region]. *Voprosy territorialnogo razvitiya*, 9(1), 5–18. <https://doi.org/10.15838/tdi.2021.1.56.5>
8. Karpov, A. V., Karpov, A. A., & Prisyazhnyuk, S. O. (2024). Spetsifika formirovaniya professionalnykh kompetentsiy spetsialistov IT-sfery [Specific features of developing professional competencies of IT specialists]. *Natsionalnyy psikhologicheskiy zhurnal*, 19(4), 201–214. <https://doi.org/10.11621/npj.2024.0414>
9. Romashkova, O. N., & Mukhammad, D. I. (2025). Modeli upravleniya razvitiem professionalnykh kompetentsiy spetsialistov v organizatsionnykh sistemakh IT-kompaniy [Models for managing

- professional competency development in IT companies]. *Sovremennye naukoemkie tekhnologii*, (9), 123–131. <https://doi.org/10.17513/snt.40496>
10. Alasheev, S. Yu., Postalyuk, N. Yu., & Prudnikova, V. A. (2025). Vneshnyaya otsenka kachestva podgotovki v sisteme SPO: Regionalnye osobennosti [External assessment of training quality in secondary vocational education: Regional specifics]. *Professionalnoe obrazovanie i rynek truda*, 13(3), 6–27. <https://doi.org/10.52944/PORT.2025.62.3.001>
 11. Fedorov, V. A., Tretyakova, N. V., & Turina, G. A. (2022). Sopryazhenie protsedur gosudarstvennoy itogovoy attestatsii i nezavisimoy otsenki kvalifikatsiy v SPO [Alignment of state final certification and independent qualification assessment in secondary vocational education]. *Professionalnoe obrazovanie i rynek truda*, 10(3), 35–54. <https://doi.org/10.52944/PORT.2022.50.3.007>
 12. Internet Assigned Numbers Authority. (n.d.). *IANA IPv4 address space registry*. <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>
 13. Arkko, J., Cotton, M., & Vegoda, L. (2010). *IPv4 address blocks reserved for documentation* (RFC 5737). Internet Engineering Task Force. <https://doi.org/10.17487/RFC5737>
 14. Fuller, V., & Li, T. (2006). *Classless inter-domain routing (CIDR): The Internet address assignment and aggregation plan* (RFC 4632). Internet Engineering Task Force. <https://doi.org/10.17487/RFC4632>
 15. Prokhorov, A. I. (2023). Kiberpoligon kak sovremennyy instrument obespecheniya informatsionnoy bezopasnosti [Cyber range as a modern tool for information security]. *Informatizatsiya v tsifrovoy ekonomike*, 4(4), 363–378. <https://doi.org/10.18334/ide.4.4.119301>
 16. Chakov, I. A., Evtyukhov, M. S., & Pavlovsky, V. V. (2025). Issledovanie funktsionala i vremeni vosstanovleniya VRRP na baze resheniy EcoRouter [Study of VRRP functionality and recovery time based on EcoRouter solutions]. *Professionalitet*, (4), 33–43.
 17. Litvak, E. G. (2022). Metodika prepodavaniya proektirovaniya baz dannykh na osnove chetyrekhkomponentnoy modeli pedagogicheskogo dizayna [Methodology for teaching database design based on the four-component instructional design model]. *Informatika i obrazovanie*, 37(4), 46–53. <https://doi.org/10.32517/0234-0453-2022-37-4-46-53>
 18. CNews. (2026, June 5). “Bazalt SPO,” “ADEM-inzhiniring” i “Novotekh” obedinyayut usiliya dlya podgotovki IT-kadrov [Basalt SPO, ADEM Engineering and Novotekh join forces to train IT specialists]. https://www.cnews.ru/news/line/2026-06-05_bazalt_spoadem-inzhiniring
 19. CNews. (2026, February 13). V Armavirskom yuridicheskom tekhnike otkryli laboratoriyu otechestvennogo PO [A domestic software laboratory opened at Armavir Law College]. https://www.cnews.ru/news/line/2026-02-13_administrirovanie_i_informatsionnaya
 20. Ministerstvo prosveshcheniya Rossiyskoy Federatsii. (2021, November 8). Ob utverzhdenii Poryadka provedeniya gosudarstvennoy itogovoy attestatsii po obrazovatelnyim programmam srednego professionalnogo obrazovaniya [On approval of the state final certification procedure for secondary vocational education] (Order No. 800).
 21. Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2024). GPTs are GPTs: Labor market impact potential of LLMs. *Science*, 384(6702), 1306–1308. <https://doi.org/10.1126/science.adj0998>
 22. Notaro, P., Cardoso, J., & Gerndt, M. (2021). A survey of AIOps methods for failure management. *ACM Transactions on Intelligent Systems and Technology*, 12(6), Article 81. <https://doi.org/10.1145/3483424>

Информация об авторах

Ефименко Татьяна Ивановна — преподаватель, Санкт-Петербургское государственное автономное профессиональное образовательное учреждение «Колледж туризма и прикладных технологий», Санкт-Петербург, Россия, e-mail: tatef1@mail.ru

DOMESTIC TECHNOLOGY STACK: FROM COMPETITION TASK TO THE EDUCATIONAL PROCESS

T. I. Efimenko¹

¹ Saint Petersburg State Autonomous Vocational Educational Institution “College of Tourism and Applied Technologies”, Saint Petersburg, Russia

Abstract. The article presents a case study describing an organizational and pedagogical model for incorporating a domestic technology stack into secondary vocational training in Network and System Administration. The central problem is that the requirements of a single employer do not necessarily reflect the diversity of infrastructure that graduates may encounter in professional practice. As an alternative, the article examines a skill management team bringing together experts, teachers, practicing administrators, and technology vendors. The material analyzed is a competition task for the regional stage of the Professionals Championship in the 2026–2027 cycle. The effectiveness of the model has not been tested experimentally. The task is organized into five functional layers: data transmission, operating systems and basic services, perimeter protection, data and observability, and development and operations. The products, functions, and origins of the components are summarized for each layer. The article explains how the task can be converted into curriculum alignment, a training environment, and progressively more complex practical assignments. Three forms of vendor cooperation are described: professional events, inter-organizational agreements, and regional educational sites, including examples from Armavir and Murmansk. The study concerns a single case; market figures derive from industry publications, while quantitative statements about educational coverage require independently verified records and counting rules. The expected influence of automation on the scale of specialist training is presented as a hypothesis requiring empirical testing.

Keywords: secondary vocational education, professional competencies, domestic software, competition task, professional community, educational content, network and system administration.

Information about the authors

Efimenko Tatyana Ivanovna — lecturer, Saint Petersburg State Autonomous Vocational Educational Institution “College of Tourism and Applied Technologies”, Saint Petersburg, Russia, e-mail: tatef1@mail.ru

Е. Ю. Комов ¹

¹Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики», г. Ростов-на-Дону, Российская Федерация

МОДЕЛЬ ПОДГОТОВКИ УЧАСТНИКОВ ЧЕМПИОНАТА ПРОФЕССИОНАЛЬНОГО МАСТЕРСТВА ПО КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Аннотация. Введение. Чемпионат профессионального мастерства служит внешней оценкой профессиональных компетенций студентов колледжей. Модели подготовки участников с обоснованными связями между решениями и измеримыми показателями в рассмотренной выборке из 16 работ не найдены. Обзор литературы не является систематическим; вывод о новизне ограничен 16 рассмотренными работами. Цель – построить и обосновать модель подготовки участников чемпионата по компетенции «Сетевое и системное администрирование».

Материалы и методы. Ретроспективное обобщение педагогического опыта колледжа за 2023–2026 гг.; анализ итоговых протоколов региональных чемпионатов, на каждом этапе выступали не менее 10 участников; описание положения колледжа внутри каждого этапа отношением балла колледжа к баллу лучшего соперника (результаты разных лет не сопоставляются); систематизация решений наставника. Результаты. Предложена модель из восьми методических решений в трёх контурах: контуре резерва, кадровом контуре и контуре соревновательной готовности. Определено институциональное условие её работы: учебный процесс признаёт компетенции, подтверждённые на чемпионате. Для каждого решения определены величина, расчёт и предварительный экспертный ориентир показателя. На региональных этапах 2023–2026 гг. колледж занял 2, 3, 1 и 1 места.

Обсуждение и выводы. Модель согласуется с исследованиями целенаправленной практики и экспертного наставничества. Причинная связь между моделью и результатами не установлена: опыт получен в одной организации, контрольной группы нет.

Ключевые слова: чемпионат профессионального мастерства, подготовка участников, наставничество, администрирование сетевых систем, среднее профессиональное образование, целенаправленная практика, пробный чемпионат.

Конфликт интересов. Автор является экспертом «Новотех» и сертифицированным преподавателем программ «Базальт СПО», EcoRouter, «Элтекс», «Киберпротект». Перечисленные организации не финансировали исследование и не влияли на его результаты.

Введение

Чемпионат «Профессионалы» оценивает профессиональные компетенции студентов среднего профессионального образования (СПО) и задаёт ориентир для содержания подготовки. Задания по компетенции «Сетевое и системное администрирование» воспроизводят производственные ситуации повышенной сложности. Оценка опирается на итоговое состояние сетевой инфраструктуры. Такая оценка реализует принцип «валидации действием», который сформулировали А. Г. Уймин и И. М. Морозов: «“арбитром” правильности действия выступает [...] реакция моделируемой системы на управляющие воздействия обучающегося» [1, с. 196]. Задания меняются от сезона к сезону. Наставник формирует у участника способность решать задачу в инфраструктуре, которую участник видит впервые.

Подготовка одного участника занимает более года. В ней работают наставник, педагоги колледжа, психологи, представители работодателей и участники прошлых лет. Наставнику

Рубрика 3. Методология и технология профессионального образования

нужна модель, которая связывает эти ресурсы и позволяет проверять каждое решение по показателю.

Обзор литературы

Участников чемпионатов WorldSkills наиболее последовательно изучали в Финляндии. Л. Пюльвяс и П. Нокелайнен опросили 18 призёров, их коллег и работодателей. Они заключили, что «формальное профессиональное образование в сочетании с целенаправленной практикой и подготовкой на основе экспертного наставничества улучшало долговременное профессиональное продвижение и профессиональное мастерство призёров» [2, с. 95] (здесь и далее перевод цитат с английского языка наш). По их данным, половина призёров отметила: «найти работу после выпуска было легче благодаря контактам, полученным на соревнованиях» [2, с. 106]. Предмет этой работы – характеристики призёра. Устройство подготовки со стороны наставника и колледжа в ней не раскрыто.

Отечественные работы рассматривают чемпионатное движение со стороны оценивания и ресурсов. А. Г. Мокроносов с соавторами установили, что «в среднем только 30,86 % студентов подтвердили соответствие полученных знаний стандартам WorldSkills». Среди причин авторы назвали «нехватку оборудования, расходных материалов, методических разработок, рассогласованность критериев оценки с содержанием образовательных программ» [3, с. 70]. О. А. Романова и К. В. Анисимова изучили подготовку к демонстрационному экзамену по предпринимательским компетенциям и отметили, что в лучших практиках «ключевым методом обучения являются долгосрочные междисциплинарные проекты студентов» [4, с. 55].

Исследования наставничества образуют вторую линию. П. Н. Осипов и И. И. Ирисметова определяют наставника как человека, «обладающего определенным опытом и знаниями, высоким уровнем коммуникации, стремящегося помочь своему подопечному приобрести опыт, необходимый для овладения профессией» [5, с. 110]. Ю. А. Плужникова и М. А. Ерофеева выделили конкурсное наставничество: оно ориентировано «на конкретный, измеримый результат (победа в конкурсе, получение гранта и др.) в условиях ограниченного времени», и роль наставника в нём «смыкается с ролью тренера» [6, с. 62]. Авторы изучали наставничество в вузах. Устройство конкурсного наставничества в СПО остаётся неописанным.

Третья линия – психологические основания мастерства. К. А. Эрикссон, Р. Т. Крампе и К. Теш-Рёмер связали высокий уровень исполнения с целенаправленной практикой. Они сформулировали условия: «обучающиеся должны получать немедленную информативную обратную связь и сведения о результатах выполнения» и «многократно выполнять одинаковые или сходные задания» [7, с. 367]. Б. Макнамара, Д. Хэмбрик и Ф. Освальд в метаанализе пришли к выводу: «целенаправленная практика важна, но не настолько, как утверждалось» [8, с. 1608]. По исправленным авторами данным, практика объясняет около 4–5 % дисперсии результата в образовании и около 1 % в профессиональной деятельности. Р. Субботник, П. Ольшевски-Кубилиус и Ф. Воррелл показали, что «психосоциальные переменные поддаются изменению и должны целенаправленно развиваться» [9, с. 3].

Характеристики призёров и процедуры оценивания изучены. Модели подготовки, где решения связаны прямыми и обратными связями, снабжены показателями и соотнесены с условиями колледжа, в рассмотренной выборке не найдены. Выборка не исчерпывает литературу, поэтому вывод о новизне ограничен ею. Сопоставление модели с наиболее близкими работами приведено в таблице 1.

Таблица 1 – Сопоставление модели с ближайшими работами

Работа	Объект и результат	Состав решений и показателей	Отличие модели
Пюльвяс, Нокелайнен [2]	Интервью с 18 призёрами WorldSkills Финляндии, их коллегами и работодателями	Условия развития мастерства: профессиональное образование, целенаправленная практика, экспертное наставничество; показатели подготовки не заданы	Условия развёрнуты в восемь решений со связями и показателями
Мокроносов и др. [3]	Соответствие выпускников СПО стандартам WorldSkills	Доля подтвердивших соответствие (30,86 %); причины: оборудование, методические разработки, критерии оценки	Решения 3, 7, 8 отвечают на названные причины; показатели привязаны к решениям
Романова, Анисимова [4]	Демонстрационный экзамен в предпринимательском образовании СПО и вузов	Ведущий метод – долгосрочные междисциплинарные проекты	Техническая компетенция, жёсткие сроки, тренировка на полигоне
Осипов, Ирисметова [5]	Обзор исследований наставничества	Определение наставника; формы наставничества	Форма «студент – студент» для подготовки к чемпионату
Плужникова, Ерофеева [6]	Наставнические практики в вузах	Конкурсное наставничество как вид; роль наставника близка к роли тренера	Распределение функций между наставником, студентом-наставником и психологом; показатели; институциональное условие

Источник: составлено автором по работам [2–6].

Цель статьи – построить и обосновать модель подготовки участников чемпионата по компетенции «Сетевое и системное администрирование».

Задачи: 1) описать результаты подготовки 2023–2026 гг. по этапам; 2) выделить решения модели и связи между ними; 3) обосновать решения данными исследований; 4) определить показатели контроля; 5) установить ограничения модели и условия её работы.

Материалы и методы

Исследование выполнено как ретроспективное обобщение педагогического опыта в одной образовательной организации – государственном бюджетном профессиональном образовательном учреждении Ростовской области «Ростовский-на-Дону колледж связи и информатики». Подготовка по компетенции «Сетевое и системное администрирование» шла в 2023–2026 гг. На каждом региональном этапе выступали не менее 10 участников. Резерв составляли не менее трёх кандидатов на каждый чемпионат.

Здесь и далее участник – студент, выступающий на чемпионате, кандидат – студент резерва, наставник – педагог, готовящий участника, студент-наставник – участник прошлых лет, консультирующий кандидатов. Полигон – лабораторная среда, которая воспроизводит инфраструктуру задания чемпионата и проверяет итоговое состояние автоматически.

Эмпирическим материалом служили итоговые протоколы региональных этапов чемпионата «Профессионалы» 2023–2026 гг. Ростовской области и результаты финала. Для каждого этапа указаны число участников и место колледжа. Состав заданий, максимум баллов и уровень соперников менялись по годам, поэтому результаты разных лет между собой не сопоставляются. Для описания положения колледжа внутри одного этапа введён коэффициент К, равный отношению балла участника колледжа к баллу лучшего из остальных участников

Рубрика 3. Методология и технология профессионального образования

того же этапа. Значение $K > 1$ означает первое место, $K < 1$ – отставание от победителя. Коэффициент не служит шкалой динамики подготовки.

Методические решения выделены рефлексивным анализом практики наставника и материалов подготовки. Связи между решениями определены по потокам: результат одного решения служит входом другого.

Литература отобрана в РИНЦ, DOAJ и на сайтах журналов по запросам «чемпионат профессионального мастерства», «WorldSkills», «наставничество», «skills competitions», «deliberate practice». Включены эмпирические исследования, обзоры и метаанализы с DOI или EDN. Работы 1990–2000-х гг. привлечены при наличии современной критики или метаанализа. Критерии включения: работа описывает подготовку участников соревнований, наставничество или условия развития мастерства и доступна в полном тексте. Исключены работы без полного текста и без эмпирических или обзорных данных. Из найденных 42 записей в статью вошли 16. Точные запросы и число записей по базам не фиксировались, поэтому обзор не систематический, а вывод о новизне ограничен выборкой. Работы сопоставлены с моделью по составу решений, обратным связям, показателям и условиям применения (табл. 1).

Этические аспекты. Среди участников подготовки есть несовершеннолетние. Персональные данные и журналы действий на полигоне в статье не публикуются. Использованы агрегированные итоговые результаты из открытых протоколов. Фотография размещена с согласия изображённого лица.

Результаты

Результаты подготовки 2023–2026 гг.

В финале чемпионата «Профессионалы» 2025 участники колледжа получили четыре медали: первое место в основном, индустриальном и международном зачётах и второе место в командном зачёте⁴. Международный зачёт проводился среди участников из иностранных государств. Результаты региональных этапов приведены в таблице 2 и на рисунке 1.

Таблица 2 – Результаты колледжа на региональных чемпионатах (внутри этапов)

Год	Участников на этапе	Место	Балл колледжа	Балл лучшего соперника	К
2023	≥ 10	2	38,1	52,9	0,72
2024	≥ 10	3	27,7	38,05	0,73
2025	≥ 10	1	95,5	69,0	1,38
2026	≥ 10	1	92,2	29,9	3,08

Источник: итоговые протоколы региональных чемпионатов 2023–2026; расчёт автора. К сравнивается только внутри строки таблицы.

⁴ <https://pro.firpo.ru/meropriyatiya/itogi/itogi2325/>

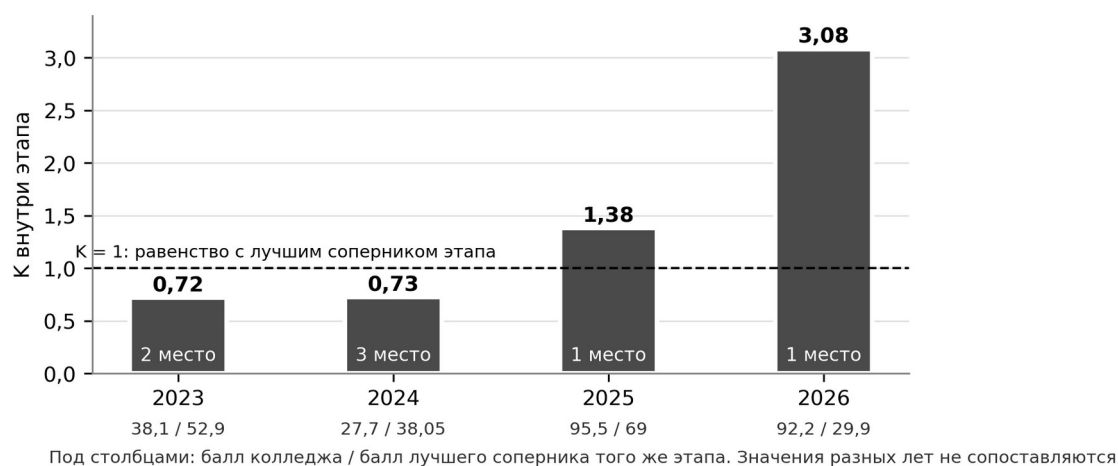
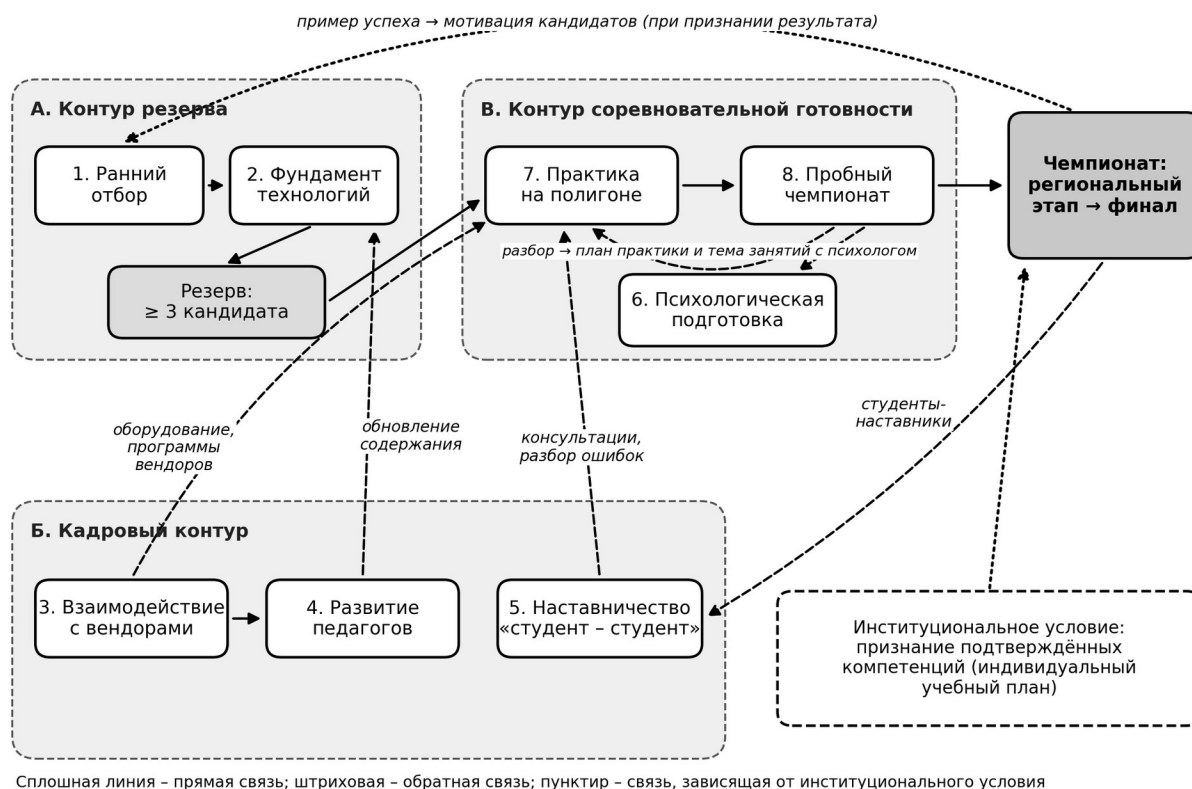


Рис. 1. Коэффициент К на региональных этапах (значения разных лет не сопоставляются). Источник: расчёт автора по итоговым протоколам региональных чемпионатов

На каждом этапе К описывает положение колледжа относительно лучшего соперника этого же этапа. В 2023 и 2024 гг. К составил 0,72 и 0,73, колледж занял второе и третье места. В 2025 и 2026 гг. колледж занял первое место (К = 1,38 и 3,08). Значение 3,08 определяется низким баллом лучшего соперника (29,9) при баллах колледжа 92,2 в 2026 г. и 95,5 в 2025 г. Поскольку условия этапов различались, К разных лет не сравниваются, а вывод об эффективности подготовки по ним не делается. Сравнение лет возможно при одинаковых максимуме и структуре баллов. По наблюдению наставника, мотивация следующего поколения кандидатов упала. Чемпион 2025 г. получил престижную работу, а колледж требовал от него посещать занятия по компетенциям, уже подтверждённым на чемпионате.

Модель подготовки

Модель объединяет восемь решений в три контура. Контур – группа решений с общей функцией (рис. 2).



Рубрика 3. Методология и технология профессионального образования

Рис. 2. Модель подготовки участников чемпионата: решения, контуры и обратные связи. Источник: разработано автором

Контур резерва (А) включает ранний отбор (решение 1) и фундамент технологий (решение 2). Результат контура – кандидаты на два следующих чемпионата. *Кадровый контур (Б)* включает взаимодействие с вендорами, то есть производителями оборудования и программ (3), развитие педагогов (4) и наставничество «студент – студент» (5). Результат контура – оборудование, квалификация педагогов и опыт участников прошлых лет. *Контур соревновательной готовности (В)* включает психологическую подготовку (6), практику на полигоне (7) и пробный чемпионат (8). Результат контура – готовность кандидата к региональному этапу.

Решения связаны обратными связями в трёх местах. Разбор пробного чемпионата (8) определяет план практики (7) и тему занятий с психологом (6). Обучение педагогов у вендоров (3 → 4) обновляет содержание фундамента (2). Участники прошлых лет становятся студентами-наставниками резерва (результат чемпионата → 5). Последняя связь возвращает результат чемпионата в следующий цикл подготовки.

Связь «результат чемпионата → мотивация кандидатов» зависит от институционального условия. Если колледж признаёт подтверждённые компетенции через индивидуальный учебный план, успех участника становится примером для кандидатов. Без признания та же связь снижает мотивацию, как в сезоне 2026 г.

Решения модели и их основания

Решение 1. Ранний отбор. Наставник отбирает кандидатов на занятиях дополнительного образования во втором семестре первого курса и в первом семестре второго курса. Он наблюдает семь признаков: интерес к технологиям, самостоятельное обращение к документации, внимательность к деталям, анализ причин ошибок, усидчивость, инициативность, стрессоустойчивость. В опыте наставника интерес и мотивация прогнозировали результат лучше, чем стартовый уровень знаний. Это наблюдение требует проверки. А. Дакуорт с соавторами показали, что «достижение трудных целей требует не только таланта, но и устойчивого и сосредоточенного применения таланта на протяжении времени» [10, с. 1087]. М. Креде с соавторами в метаанализе 88 выборок установили, что компонент «упорство в усилиях» «имеет значительно более высокую критериальную валидность, чем постоянство интересов» [11, с. 492]. Наставник учитывает признак «усидчивость» как поведение в конкретной задаче и не применяет опросники настойчивости для отбора.

Решение 2. Фундамент технологий. Подготовка начинается с шести блоков: архитектура вычислительных систем и сетевой инфраструктуры, модели OSI и TCP/IP, администрирование операционных систем, организация компьютерных сетей, сетевые сервисы, устранение неисправностей. Д. Йонассен и У. Хунг предлагают строить обучение поиску неисправностей так, чтобы обучающиеся «соотносили каждое действие с концептуальной моделью системы и спрашивали опытных специалистов по поиску неисправностей, как поступили бы они» [12, с. 77]. Перенос знания между платформами показывает Л. Г. Хорошилов и Н. А. Костин: «использование native VLAN по умолчанию на транковых портах делает сетевую инфраструктуру уязвимой к атаке Double Tagging независимо от производителя оборудования» [13, с. 60]. Поэтому студент осваивает механизм атаки и защиты, а настройку конкретного производителя изучает как реализацию механизма. Новичок получает образцы решений и подсказки. П. Кишнер, Дж. Свеллер и Р. Кларк

обосновали это: «преимущество руководства начинает снижаться лишь тогда, когда у обучающихся достаточно высокий уровень предшествующих знаний» [14, с. 75]. Наставник снимает подсказки по мере роста самостоятельности кандидата.

Решение 3. Взаимодействие с вендорами. Сотрудничество даёт колледжу программы вендоров, лабораторный практикум, сертификацию наставника и сильнейших кандидатов, разбор заданий экспертами отрасли. Решение отвечает на причины низкой подготовленности, названные А. Г. Мокроносовым с соавторами: нехватку оборудования, расходных материалов и методических разработок [3, с. 70].

Решение 4. Развитие педагогов. Обучение у вендоров даёт педагогам современное содержание. Колледж проводит семинары с практикой на полигоне не реже раза в семестр и ведёт техническое сообщество педагогов. Э. Ф. Зеер и А. А. Коновалов обследовали 213 педагогов профессионального образования и назвали «две негативные тенденции в личностном портрете педагога профессионального образования (тревожность и ригидность) и одну положительную (лабильность)» [15, с. 149]. Мы допускаем, что регулярный разбор новых технологий на оборудовании снижает ригидность педагога. Допущение требует проверки.

Решение 5. Наставничество «студент – студент». Участники прошлых чемпионатов консультируют кандидатов, помогают на тренировках и разбирают типовые ошибки. Для этой формы выбран термин «наставничество». Термин «тьюторство» в отечественной педагогике закреплён за сопровождением индивидуальной образовательной траектории, а студент-наставник траекторию кандидата не сопровождает. Определение наставника у П. Н. Осипова и И. И. Ирисметовой [5, с. 110] подходит студенту-наставнику, если «опыт, необходимый для овладения профессией» понимать как опыт чемпионата. Ю. А. Плужникова и М. А. Ерофеева отнесли к компетенциям конкурсного наставника «способность и готовность мотивировать наставляемых, особенно в условиях стресса» [6, с. 62]. Наставник закрепляет студента-наставника за кандидатом, утверждает график консультаций и правило: студент-наставник указывает направление поиска и не выдаёт готовое решение.

Решение 6. Психологическая подготовка. Психологи колледжа диагностируют стрессоустойчивость, развивают саморегуляцию и обучают приёмам работы со стрессом. Основанием служит вывод Л. Пюльвеса и П. Нокелайнена: среди наиболее значимых элементов профессионального мастерства бывшие призёры назвали «навыки решения проблем, креативность, социальные навыки и навыки саморегуляции» [2, с. 95]. Р. Субботник с соавторами обосновывают развитие таких качеств целенаправленной работой [9, с. 3]. Задания с лимитом времени в решениях 7 и 8 приближают тренировку к условиям чемпионата.

Решение 7. Практика на полигоне. Кандидаты получают доступ к полигону вне расписания, в том числе удалённо из дома. Занятие строится по условиям целенаправленной практики [7, с. 367]: цель, выполнение, проверка по критериям, разбор, повтор сложного фрагмента. Рабочее место участника показано на рисунке 3. Проверка по критериям использует итоговое состояние инфраструктуры. Разбор опирается на журнал команд. А. Г. Уймин и И. М. Морозов предложили оценивать по журналам, «использует ли обучающийся диагностические команды (show, debug, status) перед изменениями или действует методом неструктурированного перебора» [1, с. 198]. Наставник разбирает с кандидатом порядок команд и итог. Ограничение, найденное Б. Макнамарой с соавторами [8, с. 1608], задаёт границу решения: время практики объясняет малую долю различий в результате, поэтому наставник контролирует качество разбора, а часы практики берёт как вспомогательный показатель.



Рис. 3. Участник колледжа за рабочим местом на площадке чемпионата «Профессионалы» 2025. Фото из архива автора

Решение 8. Пробный чемпионат. Пробный чемпионат включает комплексное задание, строгий лимит времени и оценку по критериям чемпионата. Регламент состоит из четырёх шагов: до начала объявляются правила и критерии; первые минуты участник читает всё задание и строит план; наставник фиксирует время и события и не вмешивается; после завершения проводится разбор по журналу действий и критериям. Регламент реализует условия Эрикссона с соавторами: «немедленную информативную обратную связь» и повторное выполнение сходных заданий [7, с. 367]. Влияние пробных чемпионатов на итоговый результат в литературе не измерено, и мы считаем его гипотезой.

Показатели контроля подготовки

Показатели решений приведены в таблице 3. Для каждого показателя определены величина, расчёт, период и регистрация. Ориентиры предварительные и экспертные, ориентир пробного чемпионата взят из шкалы [1]. Ориентир пробного чемпионата привязан к трёхуровневой шкале сформированности компетенции: базовый уровень – 0–40 баллов, продуктивный – 41–70, профессиональный – 71–100.

Таблица 3 – Показатели контроля подготовки

№	Показатель и расчёт	Ориентир	Основание ориентира	Регистрация
1	Число кандидатов в резерв: студенты, прошедшие отбор и занимающиеся на полигоне не менее месяца, на каждый ближайший чемпионат; замер раз в семестр	≥ 3	Экспертный: резерв позволяет заменить выбывшего кандидата	Журнал наставника

№	Показатель и расчёт	Ориентир	Основание ориентира	Регистрация
2	Доля заданий без подсказки на оборудовании другого производителя: задания контрольной серии, выполненные без подсказки, делённые на число заданий серии; серия в конце семестра. Подсказка – готовая конфигурация или указание наставника	$\geq 80 \%$	Экспертный	Протокол полигона
3	Сертификация: число пройденных курсов вендоров у наставника и число сертифицированных кандидатов за учебный год	наставник – 1 курс; кандидаты – ≥ 1	Экспертный: ежегодное обновление квалификации	Реестр сертификатов
4	Семинары: число семинаров с практикой на полигоне за семестр; доля педагогов профильной цикловой комиссии, выполнивших задание на полигоне	≥ 1 ; $\geq 50 \%$	Экспертный	Протоколы семинаров
5	Число консультаций студента-наставника с одним кандидатом за календарный месяц	≥ 4	Экспертный: консультация раз в неделю	Журнал разобранных ошибок
6	Снижение балла при лимите времени: разность баллов (в процентах от максимума) за задание без лимита и за задание той же структуры с лимитом чемпионата у одного кандидата	≤ 10 процентных пунктов	Экспертный	Протоколы тренировок
7	Доля заданий без подсказки при практике вне расписания за месяц (расчёт как в строке 2); часы практики фиксируются без целевого значения	$\geq 70 \%$	Экспертный	Журнал полигона
8	Балл пробного чемпионата по критериям чемпионата (шкала 0–100); число пробных чемпионатов за сезон	≥ 71 за месяц до этапа; ≥ 3	71 – нижняя граница профессионального уровня шкалы [1]; число пробных – экспертное	Протоколы пробных чемпионатов

Примечание. Ориентиры установлены по опыту наставника и не прошли статистической проверки.

Наставник сверяет показатели с ориентирами перед каждым пробным чемпионатом и в конце семестра. Если показатель ниже ориентира в двух замерах подряд, пересматривается связанное решение: показатель 1 – отбор (решение 1); 2 – задания фундамента на другом оборудовании (решения 2, 3); 3 и 4 – план обучения педагогов (решения 3, 4); 5 – закрепление студентов-наставников (решение 5); 6 – доля тренировок с лимитом времени и занятия с психологом (решения 6, 7); 7 – содержание практики (решение 7); 8 – план практики и психологической подготовки (решения 7, 6). Ориентиры пересматриваются по данным следующих циклов.

Обсуждение

Модель согласуется с финскими данными о целенаправленной практике и экспертном наставничестве [2, с. 95]. Эти условия реализуют решения 7 и 8 и кадровый контур. Трудоустройство чемпиона 2025 г. совпадает с наблюдением финских призёров о роли соревнований в поиске работы [2, с. 106]. Е. В. Ломтева с соавторами пишут, что «около 50 % студентов [профессиональных образовательных организаций] не работали во время обучения» [16, с. 78]. Чемпионат даёт такому студенту результат, подтверждённый внешней оценкой.

Модель отличается от известных работ двумя положениями. Первое: подготовка описана как совокупность решений с обратными связями. Результат чемпионата возвращается в

Рубрика 3. Методология и технология профессионального образования

следующий цикл через наставничество «студент – студент» и мотивацию резерва. Второе: работа модели зависит от институционального условия. Федеральная норма признаёт результаты финала на выходе: приказом Минпросвещения России от 22.11.2024 № 812 в пункт 63 Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования внесено изменение, по которому победителям и призёрам финала чемпионата «Профессионалы» засчитывается оценка «отлично» за демонстрационный экзамен; изменение действует с 1 марта 2025 г. до 1 сентября 2028 г. Норма относится к выпускникам и к государственной итоговой аттестации. Зачёт подтверждённых компетенций в текущем учебном процессе федеральной нормой не установлен и остаётся решением колледжа. Опыт 2026 г. показывает, что отказ от такого учёта ослабляет резерв. Конкурсное наставничество [6, с. 62] получает в модели устройство с распределением функций между наставником, студентом-наставником и психологом.

Смена мест с 2–3 в 2023–2024 гг. на первое в 2025–2026 гг. допускает альтернативные объяснения: ошибку отбора (решение 1 отбирает мотивированных студентов), различия когорт и состава соперников, изменение заданий и структуры баллов между сезонами. Коэффициент К описывает положение внутри этапа и эти различия не устраняет. Имеющиеся данные такие объяснения не исключают.

Ограничения исследования: одна организация, нет контрольной группы, четыре сезона, данные полигона не публикуются. Вклад отдельных решений не оценивался. Перенос модели на другие ИТ-компетенции требует полигона с автоматической проверкой итогового состояния и отдельной проверки.

Дальнейшие исследования: сравнение колледжей с разной полнотой модели; обезличенный анализ динамики показателей таблицы 3 при согласии законных представителей.

Выводы

- На региональных этапах 2023–2026 гг. колледж занял 2, 3, 1 и 1 места. Коэффициент К (0,72; 0,73; 1,38; 3,08) описывает положение внутри этапа, годы не сопоставляет и эффективность подготовки не измеряет.
- Предложена модель из восьми решений в трёх контурах: резерва, кадровом и соревновательной готовности. Обратные связи соединяют разбор пробного чемпионата с практикой и психологической подготовкой, обучение педагогов с содержанием фундамента, участников прошлых лет с наставничеством резерва.
- Решения обоснованы исследованиями целенаправленной практики, психосоциальных условий развития таланта, поиска неисправностей, наставничества и руководства обучением.
- Для каждого решения определены величина, расчёт, предварительный экспертный ориентир и процедура регистрации; результаты мониторинга задают условия пересмотра решений. Ориентиры требуют проверки на данных наблюдений.
- Модель работает при институциональном условии: учебный процесс колледжа признаёт компетенции, подтверждённые на чемпионате (федеральная норма охватывает только государственную итоговую аттестацию). Причинная связь между моделью и результатами не установлена из-за ограничений дизайна исследования.

Библиографический список

1. Уймин, А. Г. Критериально-диагностический инструментарий оценки уровня сформированности компетенций в среде цифрового двойника / А. Г. Уймин, И. М. Морозов

- // Современные информационные технологии и ИТ-образование. – 2026. – Т. 22, № 1. – С. 194–202. – DOI 10.25559/SITITO.022.202601.194-202. – EDN BODBMU.
2. Pylväs, L. Finnish WorldSkills achievers' vocational talent development and school-to-work pathways / L. Pylväs, P. Nokelainen // International Journal for Research in Vocational Education and Training. – 2017. – Vol. 4, No. 2. – P. 95–116. – DOI 10.13152/IJRVET.4.2.1.
 3. Оценка компетенций выпускника среднего профессионального образования по стандартам WorldSkills / А. Г. Мокроносов, А. Е. Плахин, Е. С. Огородникова [и др.] // Образование и наука. – 2022. – Т. 24, № 9. – С. 69–91. – DOI 10.17853/1994-5639-2022-9-69-91.
 4. Романова, О. А. Демонстрационный экзамен в непрерывном предпринимательском образовании в системах СПО и ВО / О. А. Романова, К. В. Анисимова // Высшее образование в России. – 2023. – Т. 32, № 6. – С. 54–75. – DOI 10.31992/0869-3617-2023-32-6-54-75.
 5. Осипов, П. Н. Наставничество как объект научных исследований / П. Н. Осипов, И. И. Ирисметова // Профессиональное образование и рынок труда. – 2020. – № 2. – С. 109–115. – DOI 10.24411/2307-4264-2020-10234.
 6. Плужникова, Ю. А. Видовое многообразие наставнических практик в подготовке высококвалифицированных специалистов / Ю. А. Плужникова, М. А. Ерофеева // Интеграция образования. – 2026. – Т. 30, № 1. – С. 49–76. – DOI 10.15507/1991-9468.030.202601.049-076.
 7. Ericsson, K. A. The role of deliberate practice in the acquisition of expert performance / K. A. Ericsson, R. T. Krampe, C. Tesch-Römer // Psychological Review. – 1993. – Vol. 100, No. 3. – P. 363–406. – DOI 10.1037/0033-295X.100.3.363.
 8. Macnamara, B. N. Deliberate practice and performance in music, games, sports, education, and professions: a meta-analysis / B. N. Macnamara, D. Z. Hambrick, F. L. Oswald // Psychological Science. – 2014. – Vol. 25, No. 8. – P. 1608–1618. – DOI 10.1177/0956797614535810.
 9. Subotnik, R. F. Rethinking giftedness and gifted education: a proposed direction forward based on psychological science / R. F. Subotnik, P. Olszewski-Kubilius, F. C. Worrell // Psychological Science in the Public Interest. – 2011. – Vol. 12, No. 1. – P. 3–54. – DOI 10.1177/1529100611418056.
 10. Grit: perseverance and passion for long-term goals / A. L. Duckworth, C. Peterson, M. D. Matthews, D. R. Kelly // Journal of Personality and Social Psychology. – 2007. – Vol. 92, No. 6. – P. 1087–1101. – DOI 10.1037/0022-3514.92.6.1087.
 11. Credé, M. Much ado about grit: a meta-analytic synthesis of the grit literature / M. Credé, M. C. Tynan, P. D. Harms // Journal of Personality and Social Psychology. – 2017. – Vol. 113, No. 3. – P. 492–511. – DOI 10.1037/pspp0000102.
 12. Jonassen, D. H. Learning to troubleshoot: a new theory-based design architecture / D. H. Jonassen, W. Hung // Educational Psychology Review. – 2006. – Vol. 18, No. 1. – P. 77–114. – DOI 10.1007/s10648-006-9001-8.
 13. Хорошилов, Л. Г. Анализ эффективности защиты от атаки Double Tagging в гетерогенных сетях (Cisco, MikroTik, Eltex) / Л. Г. Хорошилов, Н. А. Костин // Профессионалитет. – 2025. – № 1 (005). – С. 60–70.
 14. Kirschner, P. A. Why minimal guidance during instruction does not work: an analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching / P.

Рубрика 3. Методология и технология профессионального образования

- A. Kirschner, J. Sweller, R. E. Clark // *Educational Psychologist*. – 2006. – Vol. 41, No. 2. – P. 75–86. – DOI 10.1207/s15326985ep4102_1.
15. Зеер, Э. Ф. Профессиональное развитие педагогов: психологический портрет / Э. Ф. Зеер, А. А. Коновалов // *Образование и наука*. – 2025. – Т. 27, № 4. – С. 149–174. – DOI 10.17853/1994-5639-2025-4-149-174.
16. Ломтева, Е. В. Стратегии выхода выпускников СПО на рынок труда: социологический анализ / Е. В. Ломтева, Д. М. Логинов, М. А. Янковская // *Профессиональное образование и рынок труда*. – 2024. – Т. 12, № 3. – С. 71–82. – DOI 10.52944/PORT.2024.58.3.005.

Нормативные правовые акты

НПА 1. О внесении изменения в пункт 63 Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования, утверждённого приказом Министерства просвещения Российской Федерации от 8 ноября 2021 г. № 800 : приказ Министерства просвещения Российской Федерации от 22.11.2024 № 812 : зарегистрирован в Минюсте России 28.11.2024, № 80354. – URL: <http://publication.pravo.gov.ru/document/0001202411280013> (дата обращения: 06.10.2026).

References

1. Uymin, A. G., & Morozov, I. M. (2026). Criteria and diagnostic tools for assessing the level of competence formation in a digital twin environment. *Modern Information Technologies and IT-Education*, 22(1), 194–202. (In Russ.). <https://doi.org/10.25559/SITITO.022.202601.194-202>
2. Pylväs, L., & Nokelainen, P. (2017). Finnish WorldSkills achievers' vocational talent development and school-to-work pathways. *International Journal for Research in Vocational Education and Training*, 4(2), 95–116. <https://doi.org/10.13152/IJRVET.4.2.1>
3. Mokronosov, A. G., Plakhin, A. E., Ogorodnikova, E. S., Mavrina, I. N., & Selezneva, M. V. (2022). Competency assessment of a secondary vocational education graduate according to WorldSkills standards. *The Education and Science Journal*, 24(9), 69–91. (In Russ.). <https://doi.org/10.17853/1994-5639-2022-9-69-91>
4. Romanova, O. A., & Anisimova, K. V. (2023). Demonstration exam in continuing entrepreneurial education within the VET and HE systems. *Higher Education in Russia*, 32(6), 54–75. (In Russ.). <https://doi.org/10.31992/0869-3617-2023-32-6-54-75>
5. Osipov, P. N., & Irismetova, I. I. (2020). Mentorship as an object of scientific research. *Vocational Education and Labour Market*, (2), 109–115. (In Russ.). <https://doi.org/10.24411/2307-4264-2020-10234>
6. Pluzhnikova, Yu. A., & Erofeeva, M. A. (2026). Diversity of mentoring practices in the training of highly qualified specialists. *Integration of Education*, 30(1), 49–76. (In Russ.). <https://doi.org/10.15507/1991-9468.030.202601.049-076>
7. Ericsson, K. A., Krampe, R. T., & Tesch-Römer, C. (1993). The role of deliberate practice in the acquisition of expert performance. *Psychological Review*, 100(3), 363–406. <https://doi.org/10.1037/0033-295X.100.3.363>
8. Macnamara, B. N., Hambrick, D. Z., & Oswald, F. L. (2014). Deliberate practice and performance in music, games, sports, education, and professions: A meta-analysis. *Psychological Science*, 25(8), 1608–1618. <https://doi.org/10.1177/0956797614535810>
9. Subotnik, R. F., Olszewski-Kubilius, P., & Worrell, F. C. (2011). Rethinking giftedness and gifted education: A proposed direction forward based on psychological science. *Psychological Science in the Public Interest*, 12(1), 3–54. <https://doi.org/10.1177/1529100611418056>

10. Duckworth, A. L., Peterson, C., Matthews, M. D., & Kelly, D. R. (2007). Grit: Perseverance and passion for long-term goals. *Journal of Personality and Social Psychology*, 92(6), 1087–1101. <https://doi.org/10.1037/0022-3514.92.6.1087>
11. Credé, M., Tynan, M. C., & Harms, P. D. (2017). Much ado about grit: A meta-analytic synthesis of the grit literature. *Journal of Personality and Social Psychology*, 113(3), 492–511. <https://doi.org/10.1037/pspp0000102>
12. Jonassen, D. H., & Hung, W. (2006). Learning to troubleshoot: A new theory-based design architecture. *Educational Psychology Review*, 18(1), 77–114. <https://doi.org/10.1007/s10648-006-9001-8>
13. Khoroshilov, L. G., & Kostin, N. A. (2025). Analysis of protection effectiveness against Double Tagging attacks in heterogeneous network environments (Cisco, MikroTik, Eltex). *Professionalitet*, (1), 60–70. (In Russ.).
14. Kirschner, P. A., Sweller, J., & Clark, R. E. (2006). Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching. *Educational Psychologist*, 41(2), 75–86. https://doi.org/10.1207/s15326985ep4102_1
15. Zeer, E. F., & Konovalov, A. A. (2025). Professional development of teachers: A psychological profile. *The Education and Science Journal*, 27(4), 149–174. (In Russ.). <https://doi.org/10.17853/1994-5639-2025-4-149-174>
16. Lomteva, E. V., Loginov, D. M., & Yankovskaya, M. A. (2024). Strategies of entering the labour market by secondary vocational education graduates: Sociological analysis. *Vocational Education and Labour Market*, 12(3), 71–82. (In Russ.). <https://doi.org/10.52944/PORT.2024.58.3.005>

Regulatory acts

Order of the Ministry of Education of the Russian Federation of 22 November 2024 No. 812 “On amending paragraph 63 of the Procedure for State Final Assessment under Secondary Vocational Education Programmes”, registered by the Ministry of Justice on 28 November 2024, No. 80354. Available at: <http://publication.pravo.gov.ru/document/0001202411280013> (accessed 06.10.2026).

Информация об авторах

Комов Евгений Юрьевич – преподаватель, государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики», г. Ростов-на-Дону, Российская Федерация, e-mail: e@komow.ru

A MODEL FOR PREPARING PARTICIPANTS OF A VOCATIONAL SKILLS CHAMPIONSHIP IN THE “NETWORK AND SYSTEM ADMINISTRATION” SKILL

Komov E. Yu.¹

¹*State Budgetary Professional Educational Institution of the Rostov Region “Rostov-on-Don College of Communications and Informatics”, Rostov-on-Don, Russian Federation*

Abstract. *Introduction. Vocational skills championships serve as an external assessment of professional competencies in secondary vocational education. In the reviewed sample, models of competitor preparation with justified links between decisions and measurable indicators were not found. The literature review is not systematic, and the novelty claim is limited to 16 works. Aim. To build and justify a model for preparing championship participants in the “Network and System Administration” skill.*

Materials and Methods. A retrospective generalisation of teaching practice at one college in 2023–2026; analysis of regional championship protocols, with at least 10 participants at each stage; description of the college’s position within

Рубрика 3. Методология и технология профессионального образования

each stage by the ratio of the college score to the best competitor score, without comparing results across years; and systematisation of the mentor's decisions. Results. The model combines eight methodological decisions into three contours: reserve, staff and competitive readiness. An institutional condition is identified: competencies confirmed at the championship are recognised in the educational process. Each decision has a defined indicator, calculation and preliminary expert benchmark. The college took 2nd, 3rd, 1st and 1st places at the regional stages of 2023–2026.

Discussion and Conclusions. The model is consistent with evidence on deliberate practice and expert mentoring in the development of vocational excellence. A causal link between the model and the results has not been established because the data come from one college without a control group.

Keywords: vocational skills championship, competitor preparation, mentoring, network systems administration, secondary vocational education, deliberate practice, mock championship.

Conflict of interest. The author is a “Novotech” expert and a certified instructor of Basalt SPO, EcoRouter, Eltex and Cyberprotect programmes. These organisations did not fund the study or influence its results.

Information about the authors

Komov Evgeniy Yuryevich – Lecturer, State Budgetary Professional Educational Institution of the Rostov Region “Rostov-on-Don College of Communications and Informatics”, Rostov-on-Don, Russian Federation, e-mail: e@komow.ru

Аристархова А. А., Чеков М. В.

Российский государственный университет нефти и газа (национальный исследовательский университет)
имени И. М. Губкина, Москва, Россия

ЛАБОРАТОРНЫЙ РАЗБОР SWITCH SPOOFING И DOUBLE TAGGING В КОНФИГУРАЦИИ ROUTER-ON-A-STICK НА CISCO

Аннотация. В статье описана настройка Router-on-a-Stick с маршрутизатором Cisco 1941 и коммутатором Cisco Catalyst 2960, а также два лабораторных эпизода с Yersinia: Switch Spoofing и Double Tagging. Текст фиксирует конфигурацию VLAN и транкового соединения, подключение атакующего узла и показанные в рукописи кадры и состояния портов. Эксперименты относятся к указанному стенду Cisco; таблица с конфигурациями Eltex и MikroTik содержит справочные настройки, но не результаты атак на этих устройствах. Работа не представляет контролируемого сравнения производителей, не сообщает повторность опытов и не измеряет общий уровень защищенности архитектуры Router-on-a-Stick. Практические рекомендации по Cisco ограничены ручной настройкой trunk/access-портов, отключением DTP там, где оно не требуется, контролем разрешенных VLAN и выбором выделенной native VLAN с учетом совместимости устройств. Double Tagging связан с условиями обработки тегов и native VLAN, поэтому его нельзя считать неизбежным следствием самого Router-on-a-Stick. Результаты иллюстрируют конкретный случай и не подтверждают поведение иных моделей или прошивок. В работе не сравниваются разные версии ПО, не приводятся повторные контрольные серии и не оцениваются эксплуатационные риски для иной топологии. Снимки фиксируют отдельные моменты настройки и передачи пакетов; их недостаточно для оценки вероятности успешного повторения атаки, влияния нагрузки или устойчивости конфигурации после перезапуска оборудования. Настройки сопоставлялись с IEEE 802.1Q и документацией производителей коммутаторов и маршрутизатора.

Ключевые слова: Router-on-a-Stick, Cisco Catalyst, VLAN, DTP, Switch Spoofing, Double Tagging.

Введение

Крупные организации используют VLAN для логической сегментации сети. Межвлановая маршрутизация позволяет организовать обмен между сегментами согласно заданной политике; один из вариантов — Router-on-a-Stick с субинтерфейсами маршрутизатора на trunk-соединении.

В работе описывается конфигурация Router-on-a-Stick на оборудовании Cisco и два сценария, показанных авторами на этом стенде. Возможность атак зависит от настроек конкретного порта, протоколов согласования и обработки тегов; она не является неизбежным свойством архитектуры.

Ошибочная настройка VLAN и trunk-портов может создавать условия для атак канального уровня. Такая возможность зависит от конкретной конфигурации, используемых протоколов и топологии; архитектура Router-on-a-Stick сама по себе не означает автоматической уязвимости.

Актуальность работы — в описании конкретного Cisco-стенда и двух показанных сценариев. Полученные наблюдения не переносятся на все реализации межвлановой маршрутизации.

Объект исследования: конфигурация Router-on-a-Stick на указанном лабораторном стенде Cisco.

Предмет исследования: условия выполнения Switch Spoofing и Double Tagging в данной конфигурации и настройки trunk/VLAN, показанные в материалах опыта.

Цель работы: описать конфигурацию Router-on-a-Stick на Cisco и зафиксировать результаты двух лабораторных проверок, ограничив выводы наблюдениями конкретного стенда.

Материалы и методы

Router-on-a-Stick использует один физический интерфейс маршрутизатора и логические субинтерфейсы, сопоставленные с VLAN. Безопасность зависит от настроек маршрутизатора и коммутатора. В исходных материалах приводилось процентное утверждение о влиянии

Рубрика 2. Методы и системы защиты информации, информационная безопасность

коммутатора, однако экспериментальных данных для его проверки нет; здесь оно не используется.

Работа рассматривает два отдельных Cisco-сценария без универсальных выводов о защищённости архитектуры.

Исследовательские методы включали анализ конфигурации лабораторного стенда Cisco, выполнение двух учебных сценариев и изучение представленных захватов Wireshark. Единого сравнительного протокола для разных производителей, повторных измерений и оценки статистической значимости в исходных данных нет.

Эмпирическая часть охватывала маршрутизатор Cisco 1941, коммутатор Cisco Catalyst 2960 и рабочие станции Linux. Таблица 1 дополнительно содержит конфигурационные фрагменты Eltex и MikroTik, но атаки и защитные меры на этих платформах не представлены как результаты. Настройки сопоставлялись с IEEE 802.1Q и документацией производителей коммутаторов и маршрутизатора [1–7].

Испытания охватывали два сценария на Cisco: Switch Spoofing и Double Tagging. Изменение подключений и отсутствие общего контрольного протокола не позволяют трактовать их как сравнение производителей.

Практическая часть

Практическая часть описывает маршрутизатор Cisco 1941 и коммутатор Cisco Catalyst 2960. Испытания двух сценариев проводились на оборудовании Cisco. Примеры конфигураций других производителей приведены справочно и не считаются результатами тестирования.

Схема лабораторной сети Router-on-a-Stick представлена на рис. 1.

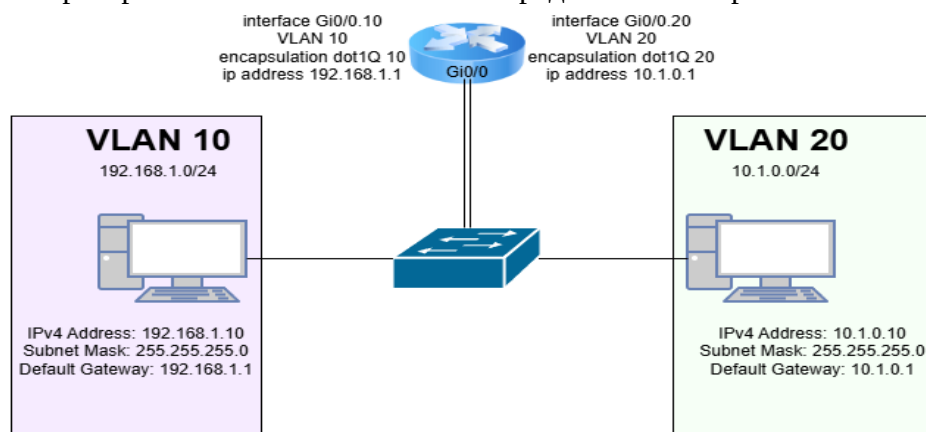


Рис. 1. Схема маршрутизации между VLAN 10 и VLAN 20 по технологии Router-on-a-Stick

Оборудование лабораторного стенда:

- коммутаторы Cisco Catalyst 2960, Eltex MES1428 и MikroTik;
- Маршрутизатор Cisco 1941;
- Рабочие станции под управлением операционной системы Linux;
- Ethernet-кабели.

Последовательность настройки:

В эксперименте использовали маршрутизатор Cisco 1941 и коммутатор Cisco Catalyst 2960. Примеры для других производителей в таблице 1 носят справочный характер. Для анализа архитектуры использованы материалы IEEE 802.1Q и документация производителей [1–7].

Конфигурация маршрутизатора Cisco 1941 приведена в листинге 1.

Листинг 1 – Пример конфигурации субинтерфейсов маршрутизатора Cisco 1941

```
Router> enable
Router# config t
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/0.10
Router(config-if)# encapsulation dot1Q 10
```

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/0.20
Router(config-if)# encapsulation dot1Q 20
Router(config-if)# ip address 10.1.0.1 255.255.255.0
Router(config-if)# exit
```

Таблица 1 содержит конфигурационные фрагменты для Cisco Catalyst 2960, Eltex MES1428 и MikroTik. Эти примеры иллюстрируют настройки VLAN и не означают, что описанные далее атаки были испытаны на Eltex или MikroTik.

Таблица 1 – Примеры настройки VLAN на Cisco, Eltex и MikroTik

Cisco 2960	Eltex mes1428	Mikrotik
enable config t vlan 10 name A vlan 20 name M exit interface range Fa0/1-4 description CLI switchport mode access switchport access vlan 10 exit interface range Fa0/15-18 description SERV switchport mode access switchport access vlan 20 exit interface Fa0/9 description LINK switchport mode trunk exit	enable configure terminal vlan 10 name A exit vlan 20 name M exit interface range fastEthernet 1/0/1-4 description CLI switchport mode access switchport access vlan 10 exit interface range fastEthernet 1/0/15-18 description SERV switchport mode access switchport access vlan 20 exit interface fastEthernet 1/0/9 description LINK switchport mode trunk exit	/interface bridge add name=bridge1 vlan-filtering=yes /interface bridge port add bridge=bridge1 interface=ether1 add bridge=bridge1 interface=ether2 add bridge=bridge1 interface=ether3 add bridge=bridge1 interface=ether4 add bridge=bridge1 interface=ether15 add bridge=bridge1 interface=ether16 add bridge=bridge1 interface=ether17 add bridge=bridge1 interface=ether18 add bridge=bridge1 interface=ether9 /interface bridge vlan add bridge=bridge1 tagged=ether9 untagged=ether1,ether2,ether3,ether4 vlan-ids=10 add bridge=bridge1 tagged=ether9 untagged=ether15,ether16,ether17,ether18 vlan-ids=20

Далее рассматриваются только два сценария, выполненные на Cisco: Switch Spoofing и Double Tagging. Анализ ограничен представленными результатами работы Yersinia и Wireshark.

В первом сценарии тестовый узел Kali Linux был подключён к Cisco, после чего с помощью Yersinia передавались DTP-кадры. На рис. 2 представлена изменённая топология, на рис. 3 — выполнение сценария, а в листинге 2 — состояние портов. Автоматическое согласование trunk зависит от режима DTP конкретного интерфейса.

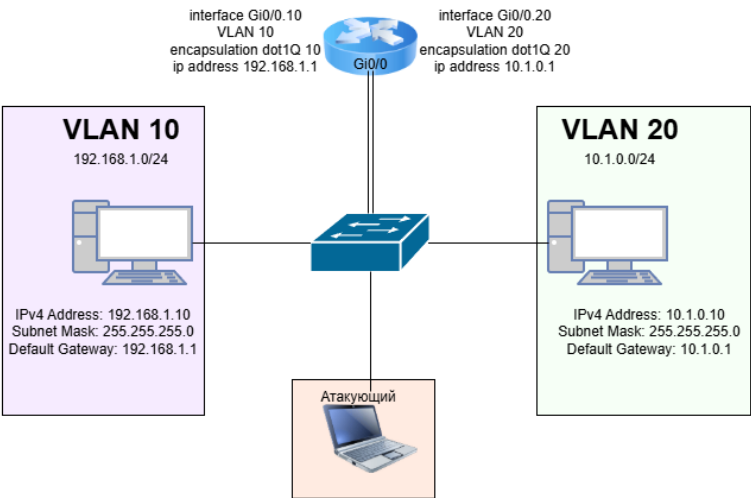


Рис. 2. Подключение тестового узла к коммутатору Cisco в лабораторной топологии

Рубрика 2. Методы и системы защиты информации, информационная безопасность

В листинге 2 интерфейс Fa0/11 отображается в режиме trunk. Возможность Switch Spoofing зависит от динамической настройки соединения. На пользовательских портах Cisco её следует отключать, если она не требуется; в работе этот сценарий на Eltex и MikroTik не испытывался.

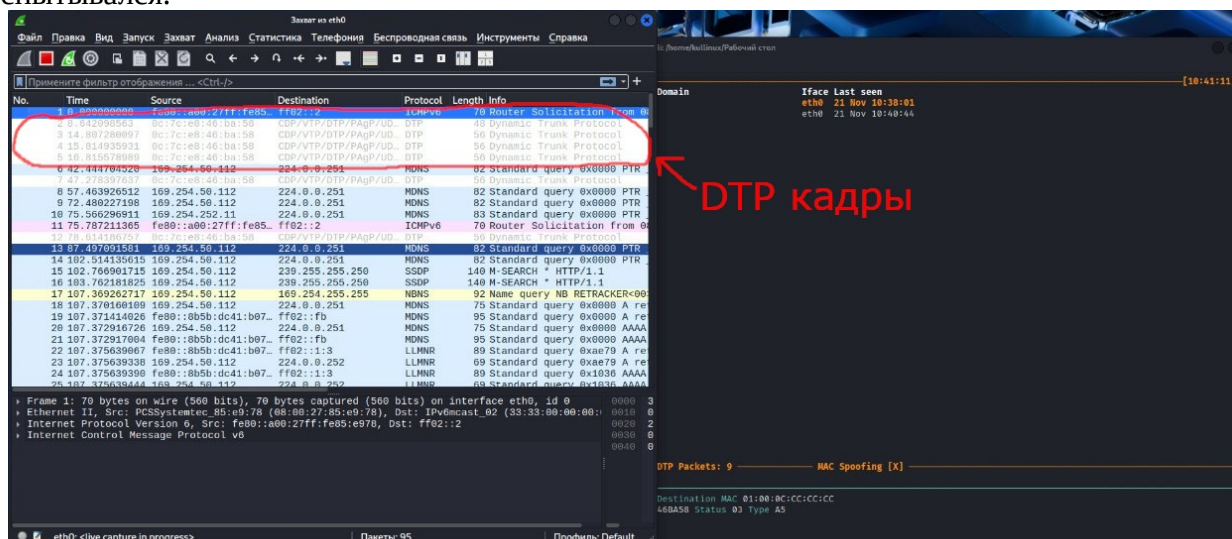


Рис. 3. Выполнение сценария Switch Spoofing и наблюдение DTP-кадров

DTP относится к представленному сценарию Cisco. Это наблюдение не устанавливает отсутствие других вариантов VLAN hopping на иных платформах и не является сравнительным испытанием производителей.

Листинг 2 – Вывод show interfaces status на Cisco Catalyst 2960

Switch>show int status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	ANNA	connected	10	auto	auto	10/100BaseTX
Fa0/2	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/3	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/4	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9	LINK	connected	trunk	a-full	a-100	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/12		notconnect	1	auto	auto	10/100BaseTX
Fa0/13		notconnect	1	auto	auto	10/100BaseTX
Fa0/14		notconnect	1	auto	auto	10/100BaseTX
Fa0/15	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/16	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/17	MAX	connected	20	a-full	a-100	10/100BaseTX
Fa0/18	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/19		notconnect	1	auto	auto	10/100BaseTX
Fa0/20		notconnect	1	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	10/100BaseTX
Fa0/22		notconnect	1	auto	auto	10/100BaseTX
Fa0/23		notconnect	1	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		notconnect	1	auto	auto	10/100/1000BaseTX
Gi0/2		notconnect	1	auto	auto	10/100/1000BaseTX

Во втором сценарии на Cisco проверяли Double Tagging с использованием двух тегов VLAN. Условия прохождения кадров зависят от VLAN атакующего, native VLAN, параметров trunk и обработки тегов; сама архитектура Router-on-a-Stick недостаточна для вывода об успешности атаки.

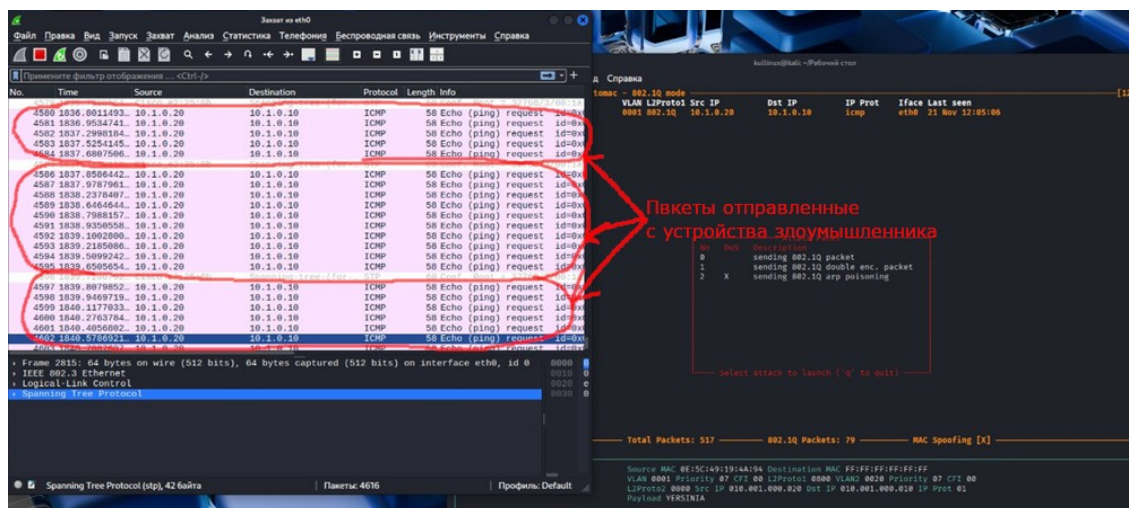


Рис. 4. Выполнение сценария Double Tagging

В описанном эпизоде кадр передавался через trunk-соединение. Дальнейшая обработка зависит от параметров native VLAN и конфигурации маршрутизатора и коммутатора. Представленные данные относятся к указанному стенду.

На рис. 5 представлен захват Wireshark, который авторы интерпретируют как доставку тестового пакета в VLAN 20. Повторные измерения и полный сетевой путь пакета в материалах не представлены.

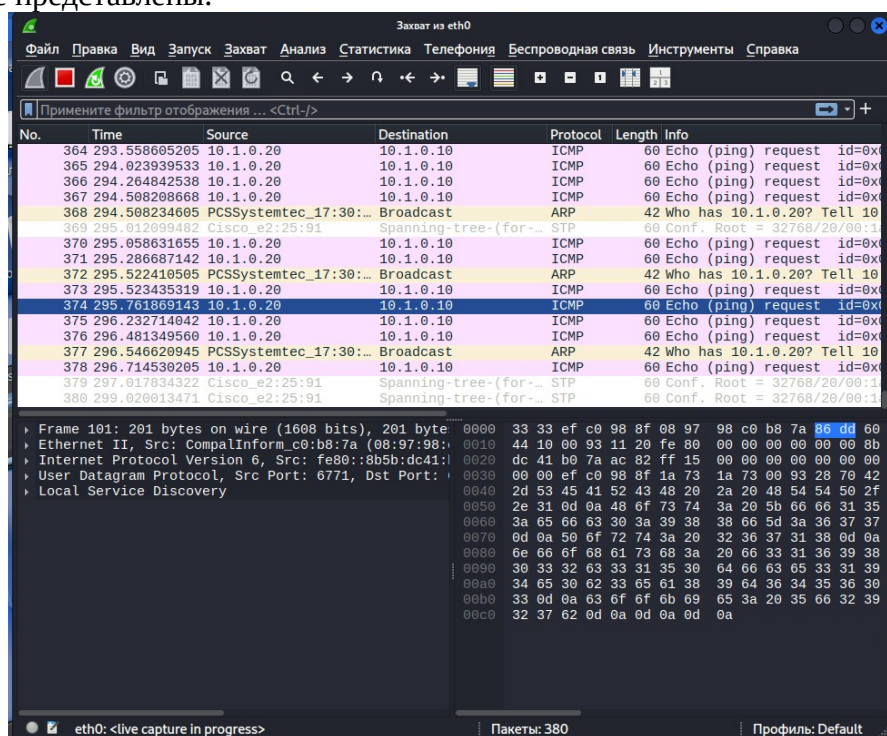


Рис. 5. Захват тестовых сетевых пакетов в Wireshark

Представленный захват авторы интерпретируют как успешную передачу в целевой сегмент в одном запуске. Он не позволяет оценить частоту успеха или перенести результат на другие модели и конфигурации.

В таблице 2 собраны рекомендации по настройке с указанием границ применимости. В работе непосредственно проверялись только конфигурация и сценарии Cisco; сведения по другим платформам не являются экспериментально подтверждёнными результатами.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Таблица 2 – Меры снижения рисков Switch Spoofing и Double Tagging

	Cisco Catalyst 2960	Eltex MES1428	MikroTik
Switch Spoofing	На пользовательских портах явно задать access. Для статического trunk применять switchport mode trunk и при отсутствии необходимости в DTP — switchport nonegotiate; соседний порт настроить вручную [2, 3].	В работе не проверены поведение DTP и эффективность противодействия на Eltex. Требуется руководство для конкретной модели и версии ПО [6].	Сценарий Switch Spoofing на MikroTik не испытывался; отсутствие Cisco DTP не подтверждает отсутствие иных атак VLAN hopping [5].
Double Tagging	Явно настроить native VLAN, исключить пользовательские access-порты из неё и ограничить разрешённые VLAN. Возможность тегирования native VLAN зависит от платформы [2, 4].	Double Tagging на Eltex не проверялся. Меры следует выбирать по документации модели и подтверждать испытанием trunk-конфигурации [6].	Double Tagging на MikroTik не проверялся. Вывод об отсутствии уязвимостей по этим материалам не делается [5].

Для MikroTik приведены справочные параметры bridge/VLAN. Отсутствие DTP Cisco не доказывает отсутствия иных атак VLAN hopping или полной защищённости платформы. В данной работе атаки на MikroTik не проводились.

Заключение

На лабораторном стенде Cisco представлены конфигурация Router-on-a-Stick и два сценария исследования VLAN hopping. Работа не является сравнительной оценкой производителей или исчерпывающим исследованием архитектуры.

Доступные наблюдения показывают переход указанного интерфейса Cisco в trunk и захват тестового трафика, интерпретированный авторами как Double Tagging. Эти фрагменты не подтверждают универсальную уязвимость технологии или свойства других платформ.

Рекомендации ниже относятся к конфигурации Cisco и требуют проверки на конкретной модели, версии ПО и топологии.

Основные рекомендации:

- На пользовательских портах следует явно задавать режим access и отключать динамическое согласование trunk там, где оно не требуется [3];
- Для статически настроенного Cisco trunk документация указывает возможность отключить DTP командой switchport nonegotiate; соседний интерфейс также настраивают вручную [2];
- Native VLAN и список разрешённых VLAN следует задавать явно; не следует без необходимости размещать пользовательские устройства в native VLAN. Меры против Double Tagging зависят от платформы и топологии; Cisco описывает отдельные варианты снижения риска [4, 5].

Возможные направления дальнейших исследований:

- Исследование устойчивости архитектуры Router-on-a-stick к комбинированным атакам;
- Анализ безопасности альтернативных методов межвлановой маршрутизации;
- Разработка автоматизированных сценариев защиты и обнаружения атак на уровне управления сетью.

Библиографический список

1. IEEE. IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks (IEEE 802.1Q-2022) [Электронный ресурс]. URL: <https://standards.ieee.org/ieee/802.1Q/10323/> (дата обращения: 12.10.2026).
2. Cisco. Configure VLAN Trunking, Cisco IOS XE 17 [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/lyr2-fwd/vlan/vlan-configuration-guide/configure-vlan-trunks.html> (дата обращения: 12.10.2026).

3. Cisco. Catalyst 2960 configuration guide: Configuring VLAN Trunks [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_3_e/consolidated_guide/b_1523e_2960p_2960c_cg/b_1522e_2960_2960c_2960s_2960sf_2960p_cg_chapter_01101.html (дата обращения: 12.10.2026).
4. Cisco. Campus Network for High Availability Design Guide: Preventing Double 802.1Q Encapsulated VLAN Hopping [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html (дата обращения: 12.10.2026).
5. MikroTik. Bridge VLAN Table: RouterOS Documentation [Электронный ресурс]. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/28606465/Bridge%20VLAN%20Table> (дата обращения: 12.10.2026).
6. Eltex. MES: настройка порта коммутатора в режиме Trunk [Электронный ресурс]. URL: <https://docs.eltex-co.ru/pages/viewpage.action?pageId=619644036> (дата обращения: 12.10.2026).
7. Cisco. Configure Inter-VLAN Routing with the Use of an External Router [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html> (дата обращения: 12.10.2026).

References

1. IEEE. (2022). *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks* (IEEE 802.1Q-2022). Retrieved October 12, 2026, from <https://standards.ieee.org/ieee/802.1Q/10323/>.
2. Cisco. (n.d.). *Configure VLAN Trunking, Cisco IOS XE 17*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/lyr2-fwd/vlan/vlan-configuration-guide/configure-vlan-trunks.html>.
3. Cisco. (n.d.). *Catalyst 2960 configuration guide: Configuring VLAN Trunks*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_3_e/consolidated_guide/b_1523e_2960p_2960c_cg/b_1522e_2960_2960c_2960s_2960sf_2960p_cg_chapter_01101.html.
4. Cisco. (n.d.). *Campus Network for High Availability Design Guide: Preventing Double 802.1Q Encapsulated VLAN Hopping*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html.
5. MikroTik. (n.d.). *Bridge VLAN Table: RouterOS Documentation*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/28606465/Bridge%20VLAN%20Table>.
6. Eltex. (n.d.). *MES: Configuring a switch port in Trunk mode*. Retrieved October 12, 2026, from <https://docs.eltex-co.ru/pages/viewpage.action?pageId=619644036>.
7. Cisco. (n.d.). *Configure Inter-VLAN Routing with the Use of an External Router*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html>.

Информация об авторах

Аристархова А. А. — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: anya_aristarkhova906@mail.ru.

Чеков М. В. — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; для корреспонденции через соавтора А. А. Аристархову: anya_aristarkhova906@mail.ru.

SWITCH SPOOFING AND DOUBLE TAGGING IN A CISCO ROUTER-ON-A-STICK LABORATORY CASE

Aristarkhova A. A., Chekov M. V.

Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. *This article describes a Router-on-a-Stick configuration using a Cisco 1941 router and Cisco Catalyst 2960 switch, together with two laboratory episodes using Yersinia: Switch Spoofing and Double Tagging. It records the*

Рубрика 2. Методы и системы защиты информации, информационная безопасность

VLAN and trunk configuration, connection of the attacker host, and packet and port states shown in the manuscript. The experiments concern the stated Cisco setup; a table containing Eltex and MikroTik configurations provides setup examples, not attack results for those devices. The work is not a controlled vendor comparison, reports no repeated trials, and does not measure the overall security of the Router-on-a-Stick architecture. Cisco-focused recommendations are limited to explicit trunk and access port configuration, disabling DTP where it is unnecessary, controlling allowed VLANs, and choosing a dedicated native VLAN subject to device compatibility. Double Tagging depends on tag processing and native-VLAN conditions and should not be treated as an inevitable consequence of Router-on-a-Stick itself. The results illustrate one case and do not establish behavior on other models or software versions. The study does not compare software releases, provide repeated control trials, or assess operational risk in other topologies. Configuration examples were checked against IEEE 802.1Q and the switch and router vendors' documentation [1–7].

Keywords: Router-on-a-Stick, Cisco Catalyst, VLAN, DTP, Switch Spoofing, Double Tagging.

Information about the authors

Aristarkhova A. A. — third-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: anya_aristarkhova906@mail.ru.

Chekov M. V. — third-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence via co-author A. A. Aristarkhova: anya_aristarkhova906@mail.ru.

Э. Б. Бекнеев¹, М. В. Марченко¹

¹ 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
T6. Журналы и время	show logging; разбор syslog; сверка NTP	deny и входы связаны по времени	Примеры deny/login; полный журнал и сверка NTP не приложены
T7. 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. Bekneev¹, M. V. Marchenko¹

¹ 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

УСЛОВИЯ И ПОРЯДОК НАПРАВЛЕНИЯ МАТЕРИАЛОВ

Редакция научного журнала «ПРОФЕССИОНАЛИТЕТ» принимает к рассмотрению статьи, исправленные версии рукописей, ответы на замечания редакции и рецензентов, а также сопроводительную переписку по конкретной статье. Направление материалов осуществляется в электронной форме в соответствии с внутренним регламентом редакции.

Каждое письмо должно содержать информативную тему и заполненный сопроводительный текст. Переписка ведется в официально-деловом стиле. В теме письма указываются тип обращения, фамилия автора, краткое название статьи и, при необходимости, номер итерации исправления.

В тексте письма обязательно приводятся полное название статьи, сведения обо всех авторах, дисциплина (если применимо), номер итерации исправления и контактные данные ответственного автора. Для исправленных версий дополнительно рекомендуется указывать, на какое письмо редакции или рецензии дается ответ, и кратко обозначать внесенные исправления.

Файл рукописи направляется в формате .docx, на кириллице, по установленной форме наименования. Исправленные версии направляются исключительно ответом на письмо редакции с обязательным указанием номера итерации в теме письма, тексте письма и имени файла.

Материалы, оформленные с нарушением установленных требований, могут быть возвращены без рассмотрения до устранения технических замечаний.

Контактные данные редакционной коллегии

Почта России · Москва, Ленинский пр-кт, 65/1 Отделение почтовой связи № 119296

ДО ВОСТРЕБОВАНИЯ

Получатель Павловский Владимир Владимирович

Тел. +7(950) 632-04-38

e-mail: organizers@au-team.ru

главный редактор – Уймин Антон Григорьевич;

ответственный секретарь - Уймина Ольга Ивановна;

технический редактор - Козлов Глеб Васильевич.

ПРОФЕССИОНАЛИТЕТ, 2026, № 2 (010)

Научное электронное издание.

Сведения о программном обеспечении, использованном для создания электронного издания:

LibreOffice — набор, вёрстка текста, генерация PDF

<https://ru.libreoffice.org>

Техническая обработка и подготовка материалов выполнены авторами.

Подписано к использованию: 10.01.2024.

Объём издания: 76,6 Мб.

Комплектация издания: pdf.

Запись на физический носитель: Уймин А. Г., тел. +7 (950) 632-04-38.

Издатель — редакция научного журнала «ПРОФЕССИОНАЛИТЕТ».

Место издания: Москва.

Электронная версия подготовлена редакцией журнала для распространения в локальной и сетевой форме.

Носитель электронного издания: URALOLIMP.WEBSITE

