ПРОФЕССИОНАЛИТЕТ, 2025, № 1 (005)

УДК *378.147.88:004.7*

И. М. Морозов[1]

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

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО МОНИТОРИНГУ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ОТЕЧЕСТВЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ И СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: МЕТОДИКА ПОСТРОЕНИЯ И АВТОМАТИЗИРОВАННАЯ ВЕРИФИКАЦИЯ РЕЗУЛЬТАТОВ

Аннотация. *Рассматривается проблема организации лабораторного практикума по дисциплинам, связанным с администрированием и мониторингом компьютерных сетей, в условиях перехода на отечественные операционные системы и импортонезависимые инструменты администрирования. Обосновывается необходимость двухэтапной проверки результатов выполнения лабораторных работ: автоматизированной верификации технического задания и экспертной оценки архитектурных решений. Описывается методика построения воспроизводимой учебной среды на основе стека GNS3 + VirtualBox + Vagrant + ALT Linux + Zabbix, позволяющей моделировать инфраструктуру малого предприятия. Представлены две лабораторные работы: по основам протокола SNMP и по настройке мониторинга сетевых устройств средствами Zabbix с построением карты сети. Показано, что применение механизма Vagrant box обеспечивает портируемость учебной среды, ускоряет подготовку аудитории к занятию и упрощает дистанционную работу студентов. Педагогическая эффективность предложенного подхода обосновывается через концепцию практико-ориентированного обучения, деятельностный подход и принцип профессиональной направленности содержания образования. Методика апробирована в рамках курса «Управление и мониторинг компьютерных сетей» магистерской программы «Компьютерные системы и сети» НИУ ВШЭ и адаптирована для уровня среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование». Результаты апробации подтверждают, что предложенная среда формирует у обучающихся устойчивые профессиональные умения и навыки работы с реальными инструментами мониторинга, применяемыми в ИТ-отрасли. Отдельное внимание уделяется связи лабораторных заданий с профессиональными компетенциями сетевого и системного администратора.*

Ключевые слова: *лабораторный практикум, мониторинг сетей, Zabbix, ALT Linux, SNMP, Vagrant, автоматизированная верификация.*

Введение

Современная система профессионального образования в области информационных технологий переживает период глубокой трансформации, обусловленной двумя взаимосвязанными процессами: стремительным развитием цифровой экономики и курсом на технологический суверенитет Российской Федерации. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование» (приказ Минпросвещения от 10.07.2023 № 519) прямо указывает на необходимость формирования у выпускников умений работать с отечественными программными продуктами и обеспечивать функционирование информационно-коммуникационных систем в условиях импортозамещения. Аналогичные требования предъявляет профессиональный стандарт 06.026 «Системный администратор информационно-коммуникационных систем» (приказ Минтруда от 29.09.2020 № 680н), закрепляющий в качестве трудовых функций администрирование операционных систем, настройку сетевого оборудования и организацию мониторинга инфраструктуры.

Вместе с тем практика показывает, что учебные лаборатории большинства образовательных организаций по-прежнему ориентированы на проприетарные зарубежные решения — симуляторы Cisco Packet Tracer, операционные системы семейства Windows Server, коммерческие системы мониторинга. Переход на импортонезависимый стек с отечественной операционной системой требует не только замены программного обеспечения, но и пересмотра методики организации лабораторного практикума: способов развёртывания учебной среды, методов проверки результатов, форм оценивания компетенций.

Как справедливо отмечает А. М. Новиков, «практическое обучение — это не просто выполнение практических заданий, это особая форма организации учебно-познавательной деятельности, в которой теоретические знания становятся инструментом решения

профессиональных задач» [1, с. 214]. Именно эта идея лежит в основе предлагаемой методики: лабораторный практикум строится не как иллюстрация теоретического материала, а как моделирование реальной профессиональной деятельности системного администратора в условиях, максимально приближенных к производственным.

Цель настоящей статьи — описать методику построения воспроизводимого лабораторного практикума по мониторингу компьютерных сетей на основе отечественной операционной системы и свободных инструментов администрирования, обосновать педагогическую эффективность предложенного подхода и представить конкретные примеры лабораторных работ, апробированных в учебном процессе.

1. Теоретико-методологические основания

1.1. Практико-ориентированный подход как методологическая база

Теоретическим фундаментом предлагаемой методики служит практико-ориентированный подход к профессиональному образованию, разработанный в трудах С. Я. Батышева, А. М. Новикова, Т. Ю. Ломакиной и других представителей отечественной профессиональной педагогики.

С. Я. Батышев, основоположник теории производственной педагогики, подчёркивал: «Подготовка квалифицированного рабочего и специалиста должна строиться на принципе единства теории и практики, причём практика должна не следовать за теорией, а предшествовать ей или сопровождать её, создавая мотивационную основу для усвоения теоретических знаний» [2, с. 187]. Применительно к подготовке системных администраторов это означает, что студент должен сначала столкнуться с реальной задачей — настроить мониторинг сети, диагностировать инцидент, восстановить работоспособность сервиса — и лишь затем получать теоретическое объяснение механизмов, лежащих в основе этих действий.

А. М. Новиков развивает эту идею в концепции учебно-профессиональной деятельности: «Учебная деятельность в профессиональном образовании должна быть организована таким образом, чтобы её предмет, средства, продукт и условия максимально совпадали с предметом, средствами, продуктом и условиями реальной профессиональной деятельности» [1, с. 231]. Именно этот принцип реализуется в предлагаемом практикуме: студент работает с теми же инструментами (Zabbix, GNS3, ALT Linux), теми же протоколами (SNMP, ICMP, SSH) и теми же задачами (настройка мониторинга, построение карты сети, диагностика инцидентов), с которыми он столкнётся на производстве.

Т. Ю. Ломакина, исследуя тенденции развития непрерывного профессионального образования, указывает на необходимость «опережающей подготовки специалистов, ориентированной не на вчерашние, а на завтрашние требования производства» [3, с. 94]. В контексте импортозамещения это требование приобретает особую остроту: специалист, подготовленный исключительно на западном программном обеспечении, оказывается профессионально беспомощным в условиях, когда отечественная ИТ-отрасль переходит на российские решения.

1.2. Деятельностный подход и формирование профессиональных компетенций

Деятельностный подход, восходящий к трудам А. Н. Леонтьева и получивший развитие в работах В. В. Давыдова, А. А. Вербицкого и других исследователей, рассматривает компетенцию не как совокупность знаний, а как способность к осуществлению деятельности в определённых условиях.

А. А. Вербицкий, разрабатывая концепцию контекстного обучения, утверждает: «Знания усваиваются не в логике учебного предмета, а в логике деятельности, имеющей для обучающегося личностный смысл. Это обеспечивает трансформацию учебной деятельности в профессиональную» [4, с. 56]. Лабораторный практикум, построенный на реальных профессиональных задачах, создаёт именно такой контекст: студент не «изучает Zabbix», а «настраивает мониторинг инфраструктуры предприятия» — и это принципиальное различие в мотивации и глубине усвоения.

Э. Ф. Зеер, исследуя профессиональное становление личности, выделяет ключевую роль «профессионально ориентированных технологий обучения, создающих условия для формирования профессиональной идентичности и субъектной позиции обучающегося» [5, с. 143].

Работа в среде, воспроизводящей реальную производственную инфраструктуру, формирует именно такую идентичность: студент начинает воспринимать себя не как учащегося, выполняющего задание, а как специалиста, решающего профессиональную задачу.

1.3. Проблема верификации результатов в практическом обучении

Одной из ключевых педагогических проблем лабораторного практикума по сетевым технологиям является объективная оценка результатов. В отличие от программирования, где существуют развитые системы автоматической проверки (ejudge, Codeforces, Яндекс.Контест), в области системного администрирования и сетевых технологий подобные инструменты практически отсутствуют.

Н. Г. Хмызова и Е. В. Кузнецова, исследуя практико-ориентированные модули формирования общепрофессиональных компетенций, подчёркивают: «Образовательная среда должна обеспечивать такой режим работы, при котором формируются, проверяются и оцениваются результаты выполнения конкретных практических заданий в условиях, максимально приближенных к реальным производственным» [6, с. 45]. Это требование предполагает не только наличие соответствующего программного обеспечения, но и разработку методики автоматизированной проверки, позволяющей объективно оценить как факт выполнения задания, так и качество архитектурного решения.

В. К. Разгоняев, анализируя опыт использования виртуальных компьютеров при преподавании дисциплин, связанных с информационными технологиями, указывает на то, что «виртуализация учебной среды позволяет не только снизить затраты на оборудование, но и обеспечить воспроизводимость условий выполнения заданий, что является необходимым условием объективного оценивания» [7, с. 38]. Именно воспроизводимость — ключевое свойство предлагаемой методики: каждый студент работает в идентичной среде, что исключает влияние случайных факторов на результат.

2. Архитектура учебной среды

2.1. Обоснование выбора программного стека

Выбор программного стека для лабораторного практикума определялся тремя критериями: соответствием требованиям импортозамещения, функциональной полнотой для решения учебных задач и возможностью автоматизации развёртывания и проверки.

Анализ доступных решений для импортонезависимого сетевого администрирования позволил выделить следующие ключевые компоненты:

- ALT Linux — отечественная операционная система на базе Linux, включённая в реестр российского программного обеспечения Минцифры России. Она может использоваться в качестве серверной и рабочей ОС в учебных и корпоративных инфраструктурах;
- Zabbix — система мониторинга с открытым исходным кодом, разработанная латвийской компанией Zabbix SIA, де-факто являющаяся стандартом мониторинга в российской ИТ-отрасли и широко применяемая в качестве замены проприетарным решениям (SolarWinds, PRTG, Nagios XI);
- GNS3 (Graphical Network Simulator-3) — эмулятор сетевой инфраструктуры с открытым исходным кодом, позволяющий запускать образы сетевых устройств в виртуальной среде;
- VirtualBox — гипервизор с открытым исходным кодом, обеспечивающий виртуализацию серверных компонентов учебной среды;
- Vagrant — инструмент автоматизации развёртывания виртуальных машин, позволяющий описать всю инфраструктуру в виде кода (Infrastructure as Code) и воспроизвести её на любом рабочем месте.

Принципиально важно, что выбранный стек не является «учебным упрощением»: он объединяет отечественную операционную систему и открытые инструменты, применимые в практико-ориентированной подготовке сетевых и системных администраторов. Это обеспечивает прямую связь формируемых компетенций с профессиональной деятельностью.

2.2. Концепция Vagrant box как основа воспроизводимой учебной среды

Центральным элементом предлагаемой методики является использование механизма Vagrant box для создания воспроизводимой учебной среды. Vagrant box представляет собой упакованный образ виртуальной машины (или набора машин), содержащий предустановленное и предварительно сконфигурированное программное обеспечение, готовое к немедленному развёртыванию.

В контексте лабораторного практикума по мониторингу сетей Vagrant box включает следующие компоненты:

- эмулятор сети GNS3 с предустановленными образами сетевых устройств (маршрутизаторы и коммутаторы);
- сервер ALT Linux с установленным и предварительно сконфигурированным Zabbix Server;
- набор скриптов автоматизированной проверки результатов выполнения лабораторных работ;
- документацию и методические указания в электронном виде.

Развёртывание всей учебной среды на рабочем месте студента или в учебной аудитории выполняется единственной командой:

vagrant up

После выполнения этой команды студент получает полностью готовую к работе инфраструктуру, идентичную той, что используется на всех остальных рабочих местах. Это решает сразу несколько педагогических проблем:

Во-первых, устраняется «проблема первого занятия» — значительная часть учебного времени традиционно тратится на установку и настройку программного обеспечения, что не является целью лабораторной работы. В предлагаемой методике студент с первых минут занятия работает непосредственно с учебным заданием.

Во-вторых, обеспечивается равенство стартовых условий для всех студентов группы, что является необходимым условием объективного оценивания.

В-третьих, решается проблема дистанционного обучения: студент может развернуть идентичную учебную среду на домашнем компьютере и выполнить лабораторную работу самостоятельно.

В-четвёртых, преподаватель получает возможность быстро «сбросить» среду в исходное состояние после занятия командой vagrant destroy && vagrant up, что исключает накопление ошибок конфигурации от группы к группе.

Готовые Vagrant box для различных учебных сценариев публикуются на платформе HashiCorp Vagrant Cloud (app.vagrantup.com), что обеспечивает их доступность для образовательных организаций по всей стране.

2.3. Топология учебной сети

Для наглядной связи теоретического описания с лабораторной методикой в статью включены пример учебной топологии и параметры стенда, используемые при выполнении практической работы по построению карты сети в Zabbix.

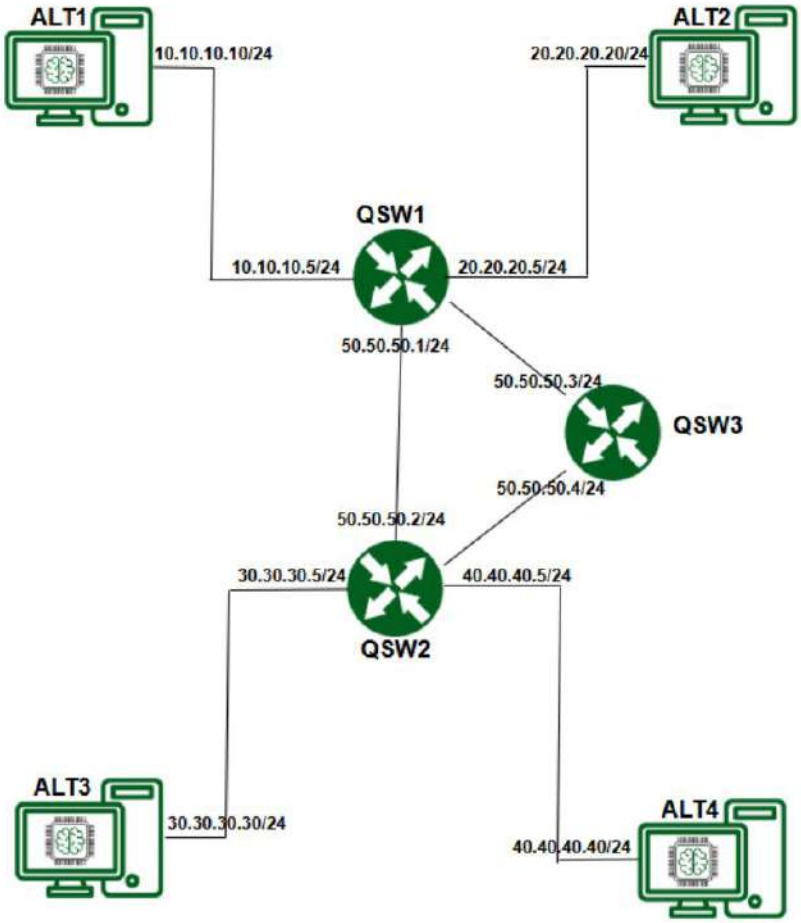

Рис. 1. Топология учебной сети для лабораторного практикума

Таблица 1 – Характеристики виртуальных машин учебного стенда

Устройство	HDD/SSD, ГБ	CPU	RAM, ГБ	ОС
ALT1	30	2	2	ОС Альт Сервер 11.0
ALT2	30	2	2	Альт Рабочая станция 11.1
ALT3	30	2	2	ОС Альт Сервер 11.0
ALT4	30	2	2	Альт Рабочая станция 11.1
vESR1	8	2	4	vesr-1.18.9-build3
vESR2	8	2	4	vesr-1.18.9-build3
QSW3	8	2	4	EcoRouterOS 3.2.1

Таблица 2 – Сетевые параметры узлов учебной топологии

Устройство	Интерфейс	IP-адрес / маска	Шлюз
ALT1	enp0s3	10.10.10.10/24	10.10.10.5
ALT2	enp0s3	20.20.20.20/24	20.20.20.5
ALT3	enp0s3	30.30.30.30/24	30.30.30.5
ALT4	enp0s3	40.40.40.40/24	40.40.40.5
vESR1	enp0s3	10.10.10.5/24	10.10.10.10
	enp0s8	20.20.20.5/24	20.20.20.20
	enp0s9	50.50.50.1/24	50.50.50.2
vESR2	enp0s3	50.50.50.2/24	50.50.50.1
	enp0s8	30.30.30.5/24	30.30.30.30
	enp0s9	40.40.40.5/24	40.40.40.40
QSW3	enp0s3	50.50.50.3/24	-
	enp0s8	50.50.50.4/24	-

В рассматриваемом варианте учебная топология моделирует сеть малого предприятия и включает следующие элементы:

– сервер ALT1 с Zabbix Server, выполняющий функции центрального узла мониторинга;
– рабочие станции и серверы ALT2–ALT4, выступающие в роли контролируемых узлов;

- маршрутизаторы vESR1 и vESR2, обеспечивающие маршрутизацию между сетевыми сегментами;
- маршрутизатор QSW3 на базе EcoRouterOS, используемый для расширения топологии и настройки дополнительного SNMP-мониторинга.

Данная топология намеренно упрощена по сравнению с производственными сетями, однако содержит ключевые элементы, необходимые для формирования базовых профессиональных компетенций: маршрутизируемую сеть, серверную инфраструктуру, рабочие станции, сетевые устройства и систему мониторинга.

3. Методика двухэтапной верификации результатов

3.1. Концептуальные основания двухэтапной проверки

Предлагаемая методика верификации результатов основана на разграничении двух принципиально различных аспектов профессиональной компетентности: операциональной (умение выполнить конкретное техническое действие) и архитектурной (умение принять обоснованное проектное решение).

Это разграничение соответствует классификации уровней профессиональной компетентности, предложенной в профессиональной педагогике. Как указывает В. А. Федоров, «профессиональная компетентность специалиста включает не только операциональный компонент — умение выполнять конкретные трудовые действия, — но и проектировочный компонент — умение планировать, обосновывать и оценивать профессиональную деятельность» [8, с. 67]. Именно эти два компонента проверяются на двух этапах верификации.

Первый этап — автоматизированная проверка технического задания — направлен на оценку операционального компонента: выполнил ли студент конкретные технические требования задания. Проверка осуществляется набором скриптов, которые анализируют конфигурационные файлы, состояние сервисов, параметры сетевых устройств и сравнивают их с эталонными значениями.

Второй этап — экспертная оценка архитектурного решения — направлен на оценку проектировочного компонента: насколько обоснованным, эффективным и масштабируемым является принятое студентом решение. Этот этап не поддаётся полной автоматизации и требует участия преподавателя-эксперта.

3.2. Автоматизированная верификация: принципы и реализация

Автоматизированная верификация строится на принципе сравнения фактического состояния системы с эталонным. Для каждой лабораторной работы разрабатывается набор проверочных скриптов, реализующих следующие типы проверок:

Структурные проверки — верификация наличия и содержимого конфигурационных файлов. Например, для лабораторной работы по настройке SNMP проверяется наличие файла /etc/snmp/snmpd.conf, корректность указанных в нём community-строк, разрешённых IP-адресов и версии протокола.

Функциональные проверки — верификация работоспособности настроенных сервисов. Скрипт выполняет реальный SNMP-запрос к настроенному устройству и проверяет корректность ответа:

```
snmpwalk -v2c -c public 192.168.1.1 1.3.6.1.2.1.1
```

Если устройство отвечает корректно — проверка пройдена; если нет — скрипт возвращает диагностическое сообщение с указанием возможных причин ошибки.

Интеграционные проверки — верификация взаимодействия компонентов системы. Для лабораторной работы по Zabbix проверяется, что сервер Zabbix успешно получает данные от настроенных хостов, триггеры срабатывают корректно, карта сети отображает актуальную топологию.

Проверки на наличие альтернативных решений — важный элемент, предотвращающий «формальное» выполнение задания. Скрипты проверяют не только наличие «правильного» решения, но и отсутствие некорректных альтернатив. Например, если студент настроил SNMP community-строку «public» вместо требуемого по заданию уникального значения — это фиксируется как нарушение требований безопасности.

Результаты автоматизированной проверки формируются в виде структурированного отчёта, который доступен как студенту (для самодиагностики), так и преподавателю (для итогового оценивания).

3.3. Экспертная оценка архитектурных решений

Второй этап верификации — экспертная оценка — проводится преподавателем на основе заранее разработанных критериев. Для каждой лабораторной работы формируется экспертный лист, включающий следующие критерии:

- обоснованность выбора параметров конфигурации (почему выбраны именно эти значения, а не другие);
- соответствие решения требованиям безопасности (использование безопасных версий протоколов, ограничение прав доступа, шифрование);
- масштабируемость решения (возможность расширения на большее количество устройств без переработки архитектуры);
- документированность решения (наличие комментариев в конфигурационных файлах, описание принятых решений).

Важно подчеркнуть, что для одного и того же технического задания может существовать несколько корректных архитектурных решений. Задача экспертной оценки — не проверить соответствие единственному «правильному» ответу, а оценить обоснованность и профессиональную зрелость принятого решения. Это соответствует принципу, сформулированному А. М. Новиковым: «В профессиональном образовании оценивается не только результат, но и процесс его достижения, не только правильность ответа, но и качество профессионального мышления» [1, с. 267].

4. Лабораторная работа № 1: Основы протокола SNMP

4.1. Место в учебном плане и формируемые компетенции

Лабораторная работа «Основы протокола SNMP» является первой в цикле работ по мониторингу сетей и предшествует работе по настройке Zabbix. Её цель — сформировать у студентов понимание механизмов, лежащих в основе систем мониторинга сетевого оборудования, прежде чем они начнут работать с высокоуровневыми инструментами.

В соответствии с ФГОС СПО 09.02.06 данная работа направлена на формирование следующих профессиональных компетенций:

- ПК 1.1 «Устанавливать и настраивать операционные системы»;
- ПК 1.3 «Настраивать сетевые протоколы и сервисы»;
- ПК 2.2 «Осуществлять мониторинг и анализ работы сети».

Профессиональный стандарт 06.026 связывает данные компетенции с трудовой функцией B/02.5 «Администрирование сетевых устройств», предполагающей умение «применять методы статической и динамической конфигурации параметров сетевых устройств» и «идентифицировать инциденты в работе сети».

4.2. Теоретические основы: протокол SNMP

Simple Network Management Protocol (SNMP) — протокол прикладного уровня модели OSI, предназначенный для управления и мониторинга сетевых устройств. Протокол определён в серии RFC: RFC 1157 (SNMPv1), RFC 1901–1908 (SNMPv2c), RFC 3411–3418 (SNMPv3).

Архитектура SNMP включает три ключевых компонента:

SNMP Manager (менеджер) — программный компонент, осуществляющий опрос управляемых устройств и обработку полученных данных. В учебной среде роль менеджера выполняет Zabbix Server.

SNMP Agent (агент) — программный компонент, запущенный на управляемом устройстве и отвечающий на запросы менеджера. На сетевых устройствах vESR и EcoRouter SNMP-агент настраивается средствами сетевой ОС; на серверах ALT Linux используется пакет net-snmp.

MIB (Management Information Base) — иерархическая база данных, описывающая структуру информации, доступной через SNMP. Каждый объект MIB идентифицируется

уникальным OID (Object Identifier) — последовательностью чисел, разделённых точками. Например, OID 1.3.6.1.2.1.1.1.0 соответствует системному описанию устройства (sysDescr).

В учебной среде студенты работают с тремя версиями протокола:

– SNMPv1 — базовая версия, использующая community-строку для аутентификации (не рекомендуется для производственного использования из-за отсутствия шифрования);
– SNMPv2c — расширенная версия с улучшенной обработкой ошибок и поддержкой 64-битных счётчиков;
– SNMPv3 — современная версия с поддержкой аутентификации и шифрования (рекомендуется для производственного использования).

4.3. Описание лабораторной работы

Цель работы: изучить принципы работы протокола SNMP, научиться настраивать SNMP-агент на сетевых устройствах и серверах под управлением ALT Linux, освоить инструменты командной строки для работы с SNMP.

Задание 1. Настройка SNMP-агента на маршрутизаторе vESR.

Студент подключается к маршрутизатору vESR через консольный интерфейс и выполняет базовую конфигурацию SNMP:

snmp-server
snmp-server community [community_string] ro
snmp-server host [zabbix_server_ip]
do commit

Параметры community-строки и адреса сервера мониторинга задаются индивидуально для каждого студента или учебной группы, что снижает вероятность механического копирования конфигурации и позволяет проверять корректность настройки по фактическому состоянию стенда.

Задание 2. Настройка SNMP-агента на сервере ALT Linux.

На сервере ALT Linux студент устанавливает и настраивает пакет net-snmp:
apt-get install net-snmp net-snmp-utils

Конфигурационный файл /etc/snmp/snmpd.conf редактируется в соответствии с требованиями задания: указывается community-строка, разрешённые IP-адреса для опроса, контактная информация и местоположение.

Задание 3. Работа с SNMP-утилитами командной строки.

Практическая фиксация работы SNMP выполняется через командный запрос к устройству. Такой скриншот используется в статье как подтверждение работоспособности базового канала мониторинга.

```
[root@ALT1 ~]# snmpwalk -v2c -c public 50.50.50.1 | grep "OID"
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: IP-MIB::ip
```

Рис. 2. Проверка доступности SNMP-агента средствами snmpwalk

Студент осваивает базовые утилиты пакета net-snmp:

– snmpget — получение значения одного OID:
snmpget -v2c -c [community] [ip_address] sysDescr.0
– snmpwalk — обход поддерева MIB:
snmpwalk -v2c -c [community] [ip_address] interfaces
– snmptrap — отправка SNMP-трапа:
snmptrap -v2c -c [community] [manager_ip] '' linkDown

Задание 4. Анализ трафика SNMP.

С помощью утилиты tcpdump студент захватывает SNMP-трафик и анализирует структуру PDU (Protocol Data Unit) в различных версиях протокола. Это задание формирует

понимание механизмов безопасности (точнее, их отсутствия в SNMPv1/v2c) и обосновывает необходимость использования SNMPv3 в производственных средах.

Задание 5. Настройка SNMPv3.

Студент настраивает SNMPv3 с аутентификацией (протокол SHA) и шифрованием (протокол AES):

```
snmpusm localhost create [username]
snmpusm localhost passwd "" [auth_password] [username]
snmpusm localhost passwd -x "" [priv_password] [username]
```

4.4. Автоматизированная проверка результатов

По завершении работы студент запускает скрипт проверки:

./check_lab1.sh

Скрипт выполняет следующие проверки:

1. Наличие и корректность конфигурационного файла /etc/snmp/snmpd.conf.
2. Работоспособность SNMP-агента на сервере ALT Linux (реальный SNMP-запрос).
3. Работоспособность SNMP-агента на маршрутизаторе vESR или EcoRouter.
4. Корректность параметров SNMPv3 (аутентификация и шифрование).
5. Отсутствие небезопасных конфигураций.

Результат проверки выводится в виде таблицы с указанием статуса каждой проверки (PASS/FAIL) и диагностических сообщений для неуспешных проверок.

5. Лабораторная работа № 2: Настройка мониторинга сетевых устройств средствами Zabbix с построением карты сети

5.1. Место в учебном плане и формируемые компетенции

Лабораторная работа «Настройка мониторинга сетевых устройств средствами Zabbix» является второй в цикле и строится на знаниях и навыках, полученных в первой работе. Её цель — сформировать у студентов практические умения работы с профессиональной системой мониторинга, применяемой в реальных производственных средах.

Данная работа направлена на формирование компетенций:

– ПК 2.2 «Осуществлять мониторинг и анализ работы сети»;
– ПК 2.3 «Обеспечивать защиту информации в сети»;
– ПК 3.1 «Устанавливать и настраивать серверное программное обеспечение».

5.2. Zabbix как инструмент профессионального мониторинга

– Zabbix — система мониторинга с открытым исходным кодом, разработанная в 2001 году Алексеем Владышевым и ставшая одним из распространённых решений для мониторинга ИТ-инфраструктуры. В учебном практикуме Zabbix используется как профессиональный инструмент для сбора метрик, настройки триггеров, визуализации состояния узлов и построения карты сети.

Архитектура Zabbix включает следующие компоненты:

– Zabbix Server — центральный компонент, осуществляющий сбор данных, обработку триггеров и хранение исторических данных. В учебной среде развёртывается на сервере ALT Linux.
– Zabbix Agent — лёгкий агент, устанавливаемый на контролируемые хосты для сбора локальных метрик (загрузка CPU, использование памяти, состояние дисков, сетевой трафик). В учебной среде агент устанавливается на серверы и рабочие станции ALT Linux.
– Zabbix Proxy — промежуточный компонент для мониторинга удалённых сегментов сети. В учебной среде не используется, однако его назначение объясняется в теоретической части.
– Zabbix Web Interface — веб-интерфейс для управления системой мониторинга, просмотра данных и настройки оповещений. Реализован на PHP и работает в связке с веб-сервером Apache или Nginx.

5.3. Описание лабораторной работы

Рубрика 3. Методология и технология профессионального образования

Цель работы: освоить процесс установки и настройки системы мониторинга Zabbix на сервере ALT Linux, научиться добавлять хосты для мониторинга, настраивать SNMP-мониторинг сетевых устройств, создавать триггеры и оповещения, строить карту сети.

Задание 1. Установка и первоначальная настройка Zabbix Server.

В учебной среде Zabbix Server предустановлен в Vagrant box, однако студент выполняет его первоначальную настройку: изменяет пароль администратора, настраивает параметры SMTP для отправки оповещений, проверяет работоспособность всех компонентов.

Для проверки работоспособности студент выполняет:

```
systemctl status zabbix-server
systemctl status zabbix-agent
systemctl status apache2
```

Задание 2. Добавление хостов для мониторинга.

В методических материалах добавление узлов в Zabbix раскрывается через последовательную настройку хоста и элемента данных. Эти материалы иллюстрируют переход от сетевой связности к регулярному сбору метрик.

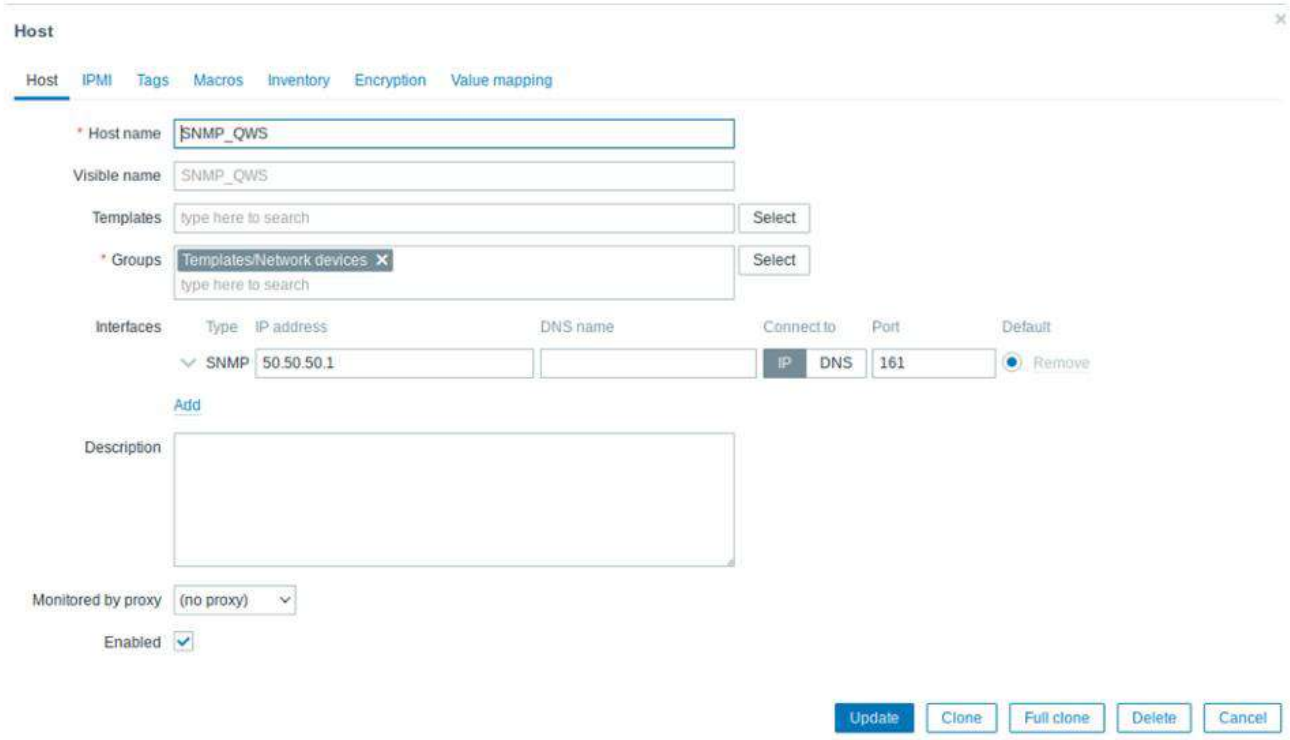

Рис. 3. Создание хоста в Zabbix для SNMP-мониторинга

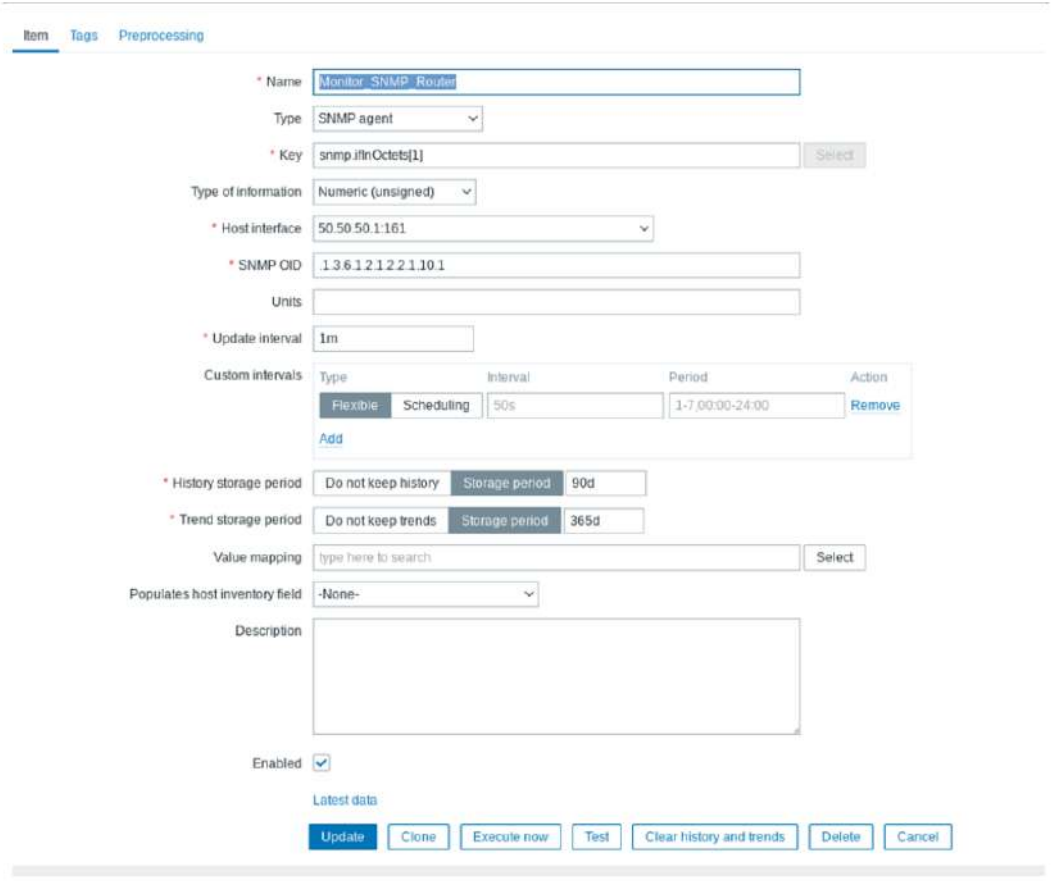

Рис. 4. Настройка элемента данных SNMP в Zabbix

Студент добавляет в Zabbix следующие хосты:

– сервер ALT Linux (мониторинг через Zabbix Agent);
– маршрутизатор vESR или EcoRouter (мониторинг через SNMP).

Для каждого хоста настраиваются:

– интерфейс подключения (IP-адрес, порт);
– метод мониторинга (Zabbix Agent или SNMP);
– шаблон мониторинга (например, Template OS Linux для сервера и типовой SNMP-шаблон сетевого устройства для маршрутизатора).

Задание 3. Настройка SNMP-мониторинга маршрутизатора.

Студент настраивает SNMP-мониторинг маршрутизатора, используя знания, полученные в первой лабораторной работе. Для устройства настраиваются следующие метрики:

– загрузка CPU (OID уточняется по MIB конкретной сетевой ОС);
– использование памяти (OID уточняется по MIB конкретной сетевой ОС);
– состояние интерфейсов (например, OID 1.3.6.1.2.1.2.2.1.8);
– входящий и исходящий трафик на интерфейсах (например, OID 1.3.6.1.2.1.2.2.1.10 и 1.3.6.1.2.1.2.2.1.16).

Задание 4. Создание триггеров и оповещений.

Студент создаёт триггеры для следующих событий:

– загрузка CPU маршрутизатора превышает 80% в течение 5 минут;
интерфейс маршрутизатора перешёл в состояние Down;
свободное место на диске сервера ALT Linux менее 10%.

Для каждого триггера настраивается действие: отправка оповещения на электронную почту администратора.

Задание 5. Построение карты сети.

Ключевым заданием лабораторной работы является построение карты сети в Zabbix. Карта сети выступает итоговым визуальным представлением лабораторного стенда: на ней объединяются хосты, маршрутизаторы, связи и индикаторы состояния.

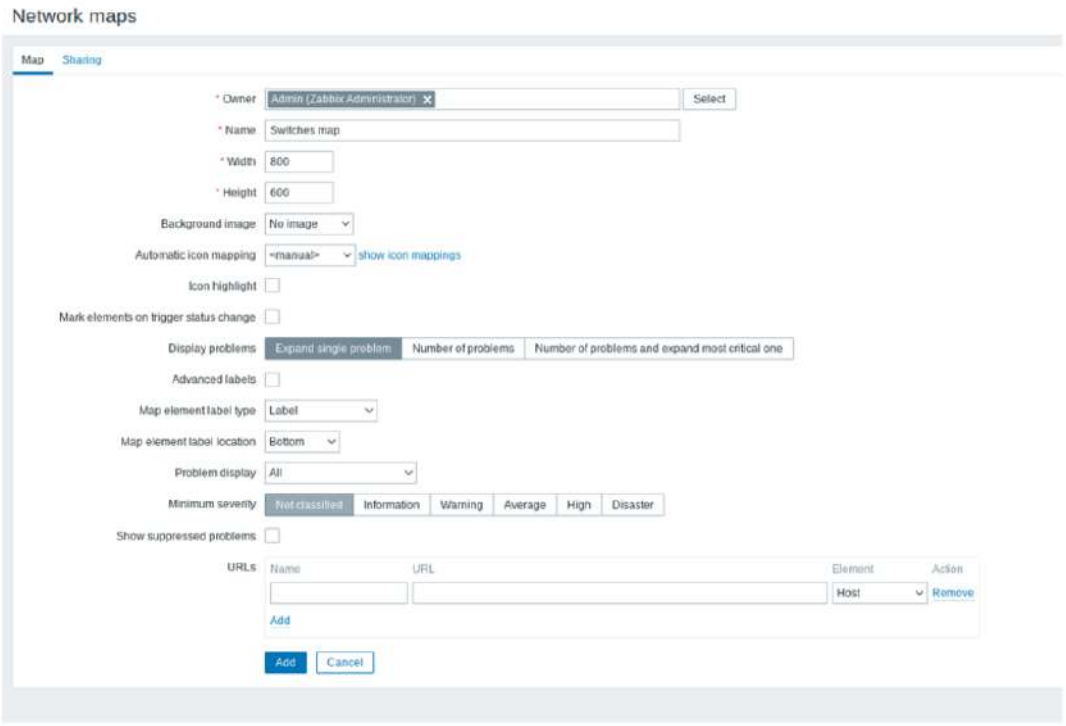

Рис. 5. Создание карты сети в веб-интерфейсе Zabbix

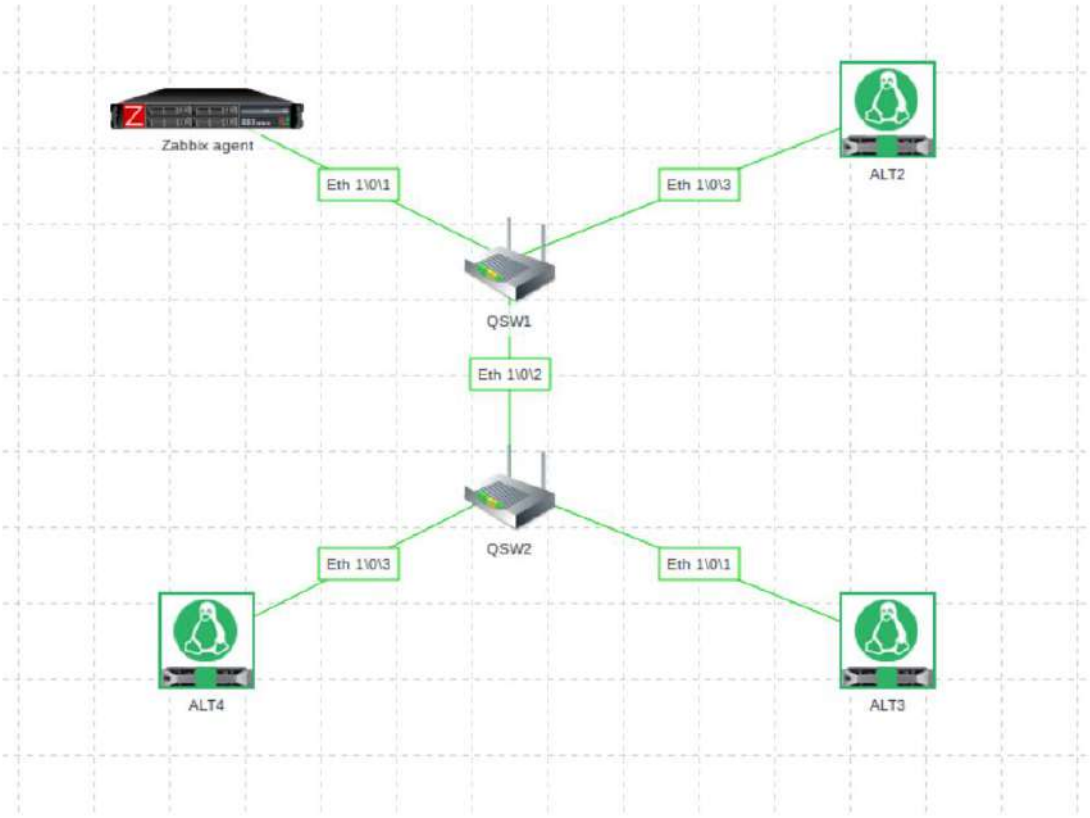

Рис. 6. Итоговая карта сети с настроенными связями между узлами

Дополнительно методика может включать пользовательские сценарии, позволяющие переходить от элемента карты к подключению по SSH или VNC. Это расширяет карту сети от статической схемы до интерактивного рабочего инструмента администратора.

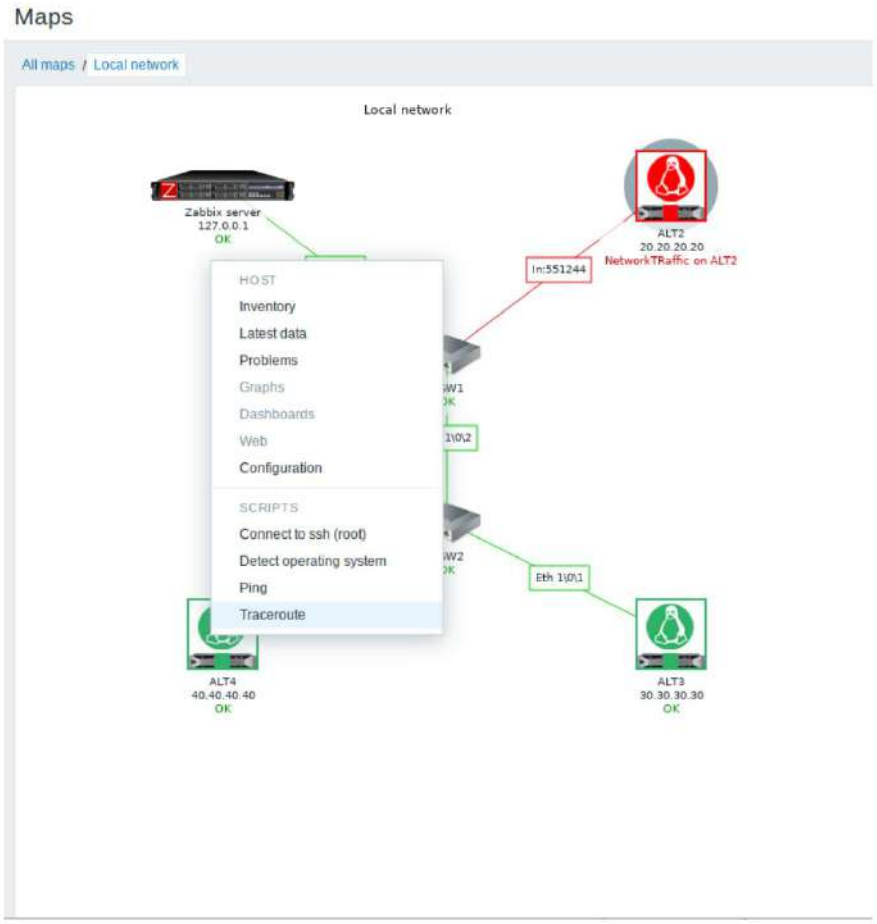

Рис. 7. Запуск пользовательского сценария подключения с карты сети

После создания карты студент размещает на ней элементы инфраструктуры, настраивает связи между ними и задаёт правила визуального отображения состояния устройств и каналов связи.

Студент создаёт карту сети, включающую:

– иконки всех контролируемых устройств (сервер ALT Linux, маршрутизаторы vESR/Eco-Router, рабочие станции);
– связи между устройствами с отображением состояния интерфейсов;
– цветовую индикацию состояния устройств (зелёный — норма, жёлтый — предупреждение, красный — критическая ошибка);
– подписи с ключевыми метриками (загрузка CPU, использование памяти).

Построение карты сети выполняется через веб-интерфейс Zabbix: Monitoring → Maps → Create map. Студент добавляет элементы карты (Map elements), настраивает их свойства и связи (Links), задаёт условия изменения цвета в зависимости от состояния триггеров.

Задание 6. Имитация инцидента и проверка системы мониторинга.

Для проверки корректности мониторинга целесообразно использовать не только факт добавления узлов, но и реакцию системы на изменение нагрузки или срабатывание триггеров.

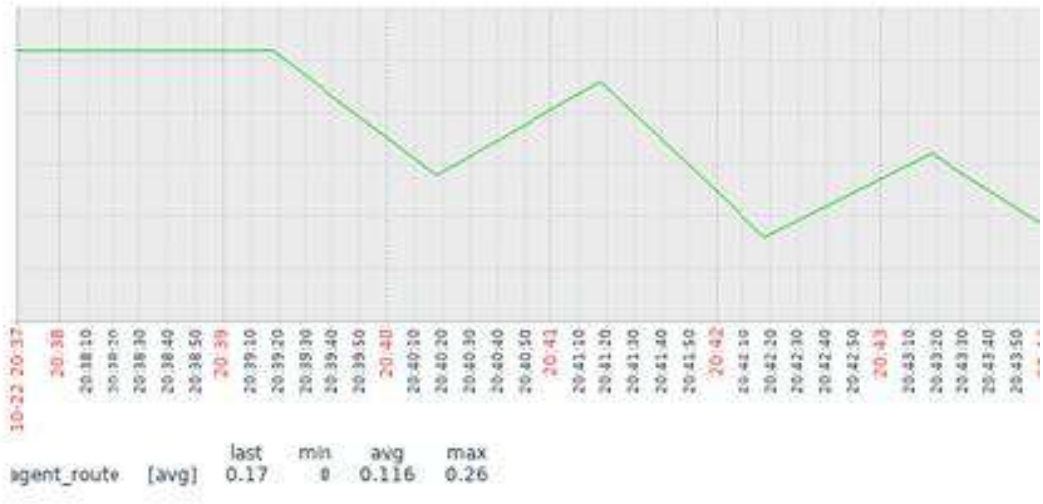

Рис. 8. Отображение изменения сетевого трафика на графике Zabbix

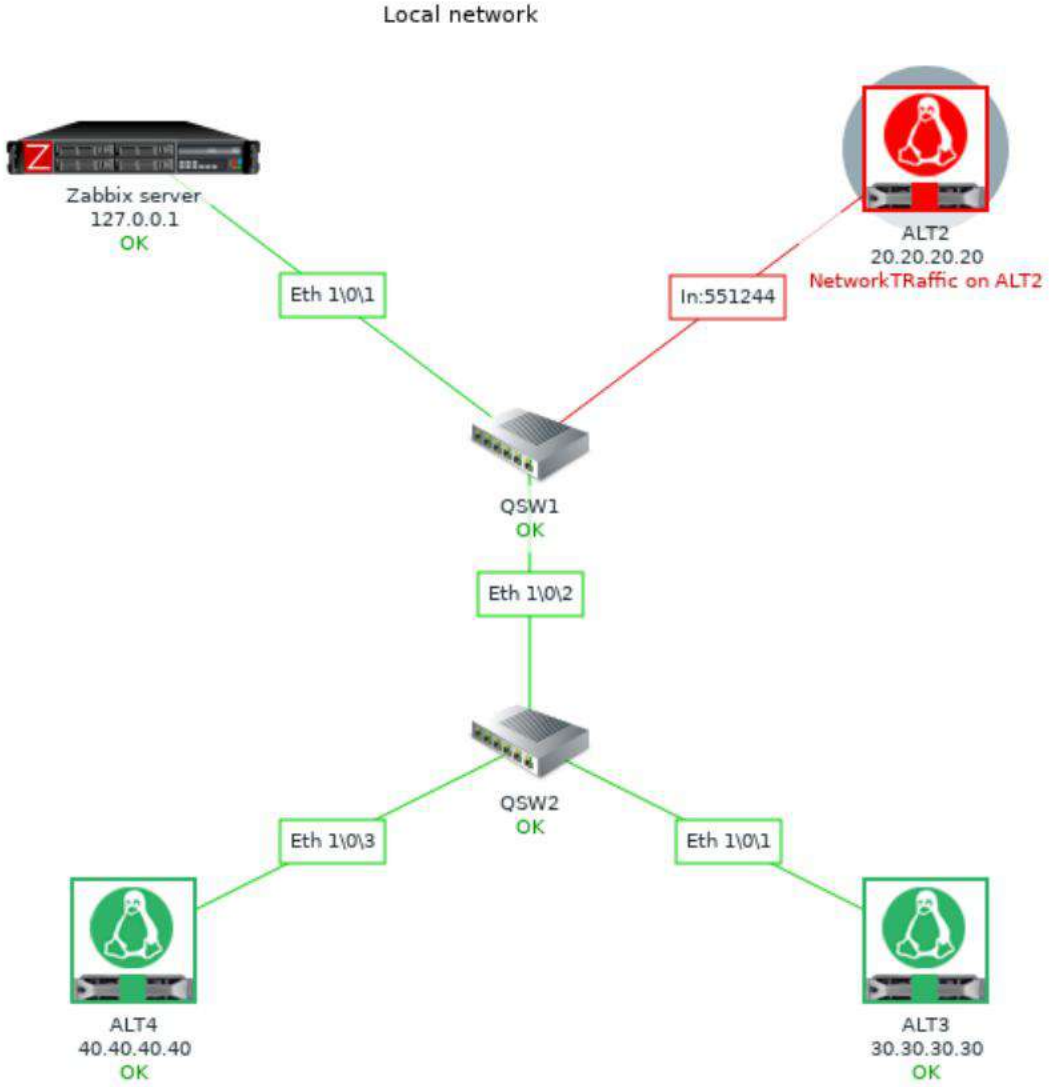

Рис. 9. Визуальное отображение срабатывания триггера на карте сети

Для проверки работоспособности настроенной системы мониторинга студент имитирует инцидент: переводит один из интерфейсов маршрутизатора в неактивное состояние, например командой shutdown в режиме настройки интерфейса:

shutdown

Студент наблюдает, как система мониторинга фиксирует изменение состояния интерфейса, срабатывает соответствующий триггер, на карте сети изменяется цвет связи, а ответственному специалисту отправляется оповещение. После восстановления интерфейса студент наблюдает автоматическое возвращение системы мониторинга в нормальное состояние.

Это задание формирует у студентов понимание полного цикла работы системы мониторинга: от возникновения инцидента до его обнаружения и оповещения ответственного специалиста.

5.4. Автоматизированная проверка результатов

По завершении работы студент запускает скрипт проверки:
./check_lab2.sh

Скрипт выполняет следующие проверки через Zabbix API:

1. Наличие всех требуемых хостов в системе мониторинга.
2. Корректность настройки SNMP-интерфейса для маршрутизатора.
3. Наличие и корректность настройки триггеров.
4. Наличие карты сети с требуемыми элементами.
5. Получение данных от всех хостов (проверка актуальности данных).
6. Корректность настройки оповещений.

Дополнительно скрипт проверяет историю событий Zabbix: был ли зафиксирован инцидент с отключением интерфейса и последующим его восстановлением (задание 6).

6. Педагогическая эффективность предложенного подхода

6.1. Формирование профессиональных компетенций

Предложенная методика обеспечивает формирование профессиональных компетенций в соответствии с пятикомпонентной моделью, принятой в профессиональной педагогике (знания, умения, навыки, практический опыт, профессионально значимые личностные качества).

Знания формируются через изучение теоретических основ протокола SNMP, архитектуры систем мониторинга, принципов работы Zabbix. Студент усваивает понятийный аппарат: OID, MIB, community-строка, триггер, шаблон мониторинга, карта сети.

Умения формируются через выполнение конкретных профессиональных задач: настройка SNMP-агента, добавление хостов в систему мониторинга, создание триггеров, построение карты сети. Каждое умение отрабатывается в условиях, максимально приближенных к производственным.

Навыки формируются через многократное повторение типовых операций: подключение к сетевому устройству через консоль, редактирование конфигурационных файлов, работа с командной строкой Linux, навигация в веб-интерфейсе Zabbix. К концу курса эти операции выполняются студентами автоматически, без обращения к инструкциям.

Практический опыт формируется через задание 6 (имитация инцидента): студент сталкивается с нестандартной ситуацией — отказом сетевого устройства — и должен не только зафиксировать факт инцидента, но и восстановить нормальное состояние системы. Это задание моделирует реальную профессиональную ситуацию, с которой системный администратор сталкивается в повседневной работе.

Профессионально значимые личностные качества — внимательность, аккуратность, способность работать в условиях неопределённости — формируются через требования к качеству выполнения заданий: некорректная конфигурация SNMP-агента, небезопасные параметры, отсутствие документирования фиксируются скриптом проверки и снижают оценку.

6.2. Роль импортозамещения в профессиональной подготовке

Использование отечественной операционной системы и импортонезависимых инструментов в лабораторном практикуме имеет не только организационное, но и педагогическое значение. Как отмечает Т. Ю. Ломакина, «содержание профессионального образования должно опережать текущее состояние производства и ориентироваться на перспективные требования рынка труда» [3, с. 112]. В условиях масштабного перехода российских предприятий на отечественные и открытые решения специалист, не имеющий опыта работы с ALT Linux,

Zabbix и аналогичными инструментами, оказывается менее конкурентоспособным на рынке труда.

Вместе с тем важно подчеркнуть, что предлагаемая методика не сводится к формальной замене одного программного продукта другим. Zabbix — функциональная и гибкая система мониторинга; ALT Linux — полноценная серверная операционная система, соответствующая требованиям учебного и производственного использования; GNS3 — профессиональный инструмент сетевого эмулирования. Использование такого стека не снижает качества подготовки, а переориентирует её на актуальные требования рынка труда.

6.3. Результаты апробации

Предложенная методика апробирована в рамках курса «Управление и мониторинг компьютерных сетей» магистерской программы «Компьютерные системы и сети» Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ). В апробации приняли участие студенты двух учебных групп (общее количество — 34 человека).

Апробация показала следующие результаты:

Сокращение времени на развёртывание учебной среды: в традиционном подходе (ручная установка и настройка программного обеспечения) подготовка рабочего места занимала 40–60 минут учебного времени. При использовании Vagrant box это время сократилось до 5–7 минут (время выполнения команды vagrant up).

Повышение однородности результатов: в традиционном подходе значительная часть ошибок студентов была обусловлена различиями в конфигурации рабочих мест (разные версии программного обеспечения, различные настройки операционной системы). При использовании Vagrant box все студенты работали в идентичной среде, что позволило сосредоточиться на содержательных аспектах задания.

Улучшение качества самодиагностики: наличие автоматизированного скрипта проверки позволило студентам самостоятельно выявлять и исправлять ошибки до сдачи работы преподавателю. По данным опроса, 78% студентов отметили, что скрипт проверки помог им обнаружить ошибки, которые они не заметили самостоятельно.

Повышение мотивации: работа в среде, воспроизводящей реальную производственную инфраструктуру, повысила мотивацию студентов. По данным опроса, 85% студентов отметили, что лабораторные работы «ощущались как реальная профессиональная задача», а не как учебное упражнение.

Авторы рассматривают опрос 34 участников как пилотное описательное исследование: поскольку анкета, абсолютные значения n/N по каждому вопросу и правила округления не приведены, указанные проценты не интерпретируются как статистически доказанный эффект.

Методика также адаптирована для уровня среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование». Адаптация включала упрощение теоретической части, добавление более подробных пошаговых инструкций и снижение требований к архитектурной части экспертной оценки. При этом технический стек и принципы автоматизированной проверки остались неизменными.

7. Обсуждение

7.1. Ограничения предложенного подхода

Предложенная методика имеет ряд ограничений, которые необходимо учитывать при её внедрении.

Аппаратные требования: развёртывание Vagrant box с GNS3 и несколькими виртуальными машинами требует значительных вычислительных ресурсов. Минимальные требования к рабочему месту студента: процессор с поддержкой аппаратной виртуализации (Intel VT-x или AMD-V), 8 ГБ оперативной памяти, 50 ГБ свободного места на диске. Это может быть ограничением для образовательных организаций с устаревшим парком компьютеров.

Кривая обучения для преподавателей: разработка и поддержка Vagrant box требует от преподавателя навыков работы с инструментами DevOps (Vagrant, VirtualBox, bash-скриптинг). Это может быть барьером для преподавателей, не имеющих соответствующего опыта.

Ограниченность эмуляции: несмотря на высокую степень реализма, эмулированная среда GNS3 не полностью воспроизводит поведение реального оборудования. Некоторые функции сетевых устройств (например, аппаратное ускорение, специфические ASIC-функции) недоступны в эмуляторе.

7.2. Перспективы развития

Перспективным направлением развития предложенной методики является интеграция с системами управления обучением (LMS). Автоматизированный скрипт проверки может быть адаптирован для передачи результатов непосредственно в LMS (Moodle, 1С:Образование), что позволит автоматизировать выставление оценок и формирование отчётности.

Другим перспективным направлением является расширение стека программного обеспечения, применимого в импортонезависимой инфраструктуре. В частности, представляет интерес включение в учебную среду систем автоматизации конфигураций, отечественных систем виртуализации (Р-Виртуализация, zVirt) и российских сетевых операционных систем (EcoRouter).

Наконец, перспективным является развитие методики в направлении геймификации: введение элементов соревновательности (рейтинг студентов по результатам автоматизированной проверки), сценарных заданий (студент выступает в роли системного администратора, получающего задачи от «руководства»), командных проектов (несколько студентов совместно администрируют общую инфраструктуру).

Заключение

В статье представлена методика организации лабораторного практикума по мониторингу компьютерных сетей на основе отечественной операционной системы и свободных инструментов администрирования. Ключевыми элементами методики являются:

- использование стека GNS3 + VirtualBox + Vagrant + ALT Linux + Zabbix, обеспечивающего моделирование учебной инфраструктуры, близкой к производственной;
- механизм Vagrant box, обеспечивающий воспроизводимость учебной среды и упрощающий её развёртывание;
- двухэтапная верификация результатов: автоматизированная проверка технического задания и экспертная оценка архитектурных решений;
- две лабораторные работы, последовательно формирующие компетенции в области SNMP-мониторинга и работы с системой Zabbix.

Педагогическая эффективность методики обоснована через концепцию практико-ориентированного обучения (С. Я. Батышев, А. М. Новиков), деятельностный подход (А. А. Вербицкий, Э. Ф. Зеер) и принцип опережающей профессиональной подготовки (Т. Ю. Ломакина). Результаты апробации в НИУ ВШЭ подтверждают, что предложенная методика сокращает непроизводительные затраты учебного времени, повышает однородность условий выполнения заданий, улучшает качество самодиагностики студентов и повышает их мотивацию.

Методика применима как на уровне высшего образования (магистерские программы по направлению «Информатика и вычислительная техника»), так и на уровне среднего профессионального образования (специальность 09.02.06 «Сетевое и системное администрирование»). Переход на такой программный стек не снижает качества подготовки, а переориентирует её на актуальные требования российского рынка труда в условиях цифрового суверенитета.

Библиографический список

1. Новиков, А. М. Методология учебной деятельности / А. М. Новиков. — Москва : Эгвес, 2005. — 176 с. — Текст : непосредственный.
2. Профессиональная педагогика : учебник / под ред. С. Я. Батышева, А. М. Новикова. — 3-е изд., перераб. — Москва : Эгвес, 2010. — 456 с. — Текст : непосредственный.
3. Ломакина, Т. Ю. Диверсификация профессионального образования / Т. Ю. Ломакина. — Москва : ЦПНО ИТОП РАО, 2000. — 145 с. — Текст : непосредственный.

Рубрика 3. Методология и технология профессионального образования

4. Вербицкий, А. А. Активное обучение в высшей школе: контекстный подход : методическое пособие / А. А. Вербицкий. — Москва : Высшая школа, 1991. — 207 с. — ISBN 5-06-002079-7. — Текст : непосредственный.
5. Зеер, Э. Ф. Психология профессионального образования : учебное пособие для студентов высших учебных заведений / Э. Ф. Зеер. — Москва : Издательский центр «Академия», 2009. — 378 с. — Текст : непосредственный.
6. Хмызова, Н. Г. Практико-ориентированные модули формирования общепрофессиональных компетенций у бакалавров профессионального обучения (по отраслям) / Н. Г. Хмызова, Е. В. Кузнецова. — Текст : электронный // Ученые записки Орловского государственного университета. Серия: Гуманитарные и социальные науки. — 2022. — № 1 (94). — С. 43–49. — URL: https://cyberleninka.ru/article/n/praktiko-orientirovannye-moduli-formirovaniya-obscheprofessionalnyh-kompetentsiy-u-bakalavrov-professionalnogo-obucheniya-po (дата обращения: 31.03.2025).
7. Разгоняев, В. К. Использование виртуальных компьютеров при преподавании дисциплин, связанных с информационными технологиями / В. К. Разгоняев. — Текст : электронный // Вестник СИБИТа. — 2020. — № 2 (34). — С. 35–42. — URL: https://sano.ru/magazine/N34/N34.pdf (дата обращения: 31.03.2025).
8. Федоров, В. А. Профессионально-педагогическое образование: теория, эмпирика, практика : монография / В. А. Федоров. — Екатеринбург : Изд-во Урал. гос. проф.-пед. ун-та, 2001. — 330 с. — ISBN 5-8050-0089-X. — Текст : непосредственный.
9. Уймин, А. Г. Инструментальные средства обучения компьютерным сетям. Развёртывание на базе российского программного обеспечения / А. Г. Уймин, Г. И. Токарев // Системы управления и информационные технологии. — 2022. — № 4 (90). — С. 88–92. — DOI 10.36622/VSTU.2022.90.4.019. — EDN KAMNET. — Текст : непосредственный.
10. Уймин, А. Г. Инструменты верификации обучаемого и оценки его эмоционально-психологического состояния при дистанционной работе / А. Г. Уймин // Педагогическое образование: история становления и векторы развития : материалы международной научно-практической конференции. — Москва : МПГУ, 2022. — С. 769–773. — Текст : непосредственный.
11. Гибадуллин, А. А. Методология использования интеллектуальных компьютерных игр в обучении информационным технологиям / А. А. Гибадуллин. — Текст : электронный // International Journal of Advanced Studies. — 2019. — Т. 9, № 4. — С. 11–14. — URL: https://cyberleninka.ru/article/n/metodologiya-ispolzovaniya-intellektualnyh-kompyuternyh-igr-v-obuchenii-informatsionnym-tehnologiyam (дата обращения: 31.03.2025).
12. Пирогов, В. Ю. О возможностях дистанционного преподавания программирования для студентов технических специальностей / В. Ю. Пирогов. — Текст : электронный // Мир науки. Педагогика и психология. — 2021. — Т. 9, № 6. — URL: https://mir-nauki.com/PDF/27PDMN621.pdf (дата обращения: 31.03.2025).
13. Matkurbanov, D. Analysis of network emulation and simulation software / D. Matkurbanov, K. Rakhimjanov // Sciences of Europe. — 2021. — No. 79-1. — P. 38–46. — DOI 10.24412/3162-2364-2021-79-1-38-46. — Текст : непосредственный.
14. Zenk, V. A comparative study of Docker and Vagrant regarding performance on machine level provisioning / V. Zenk, M. Malmström. — Malmö : Malmö University, 2020. — 58 p. — URL: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1444178 (дата обращения: 31.03.2025).
15. Арипова, Г. И. Использование категорий информационно-коммуникационных технологий при обучении студентов информатике / Г. И. Арипова. — Текст : электронный // Наука и образование сегодня. — 2022. — № 2 (71). — С. 28–34. — URL: https://cyberleninka.ru/article/n/ispolzovanie-kategoriy-informatsionno-kommunikatsionnyh-tehnologiy-pri-obuchenii-studentov-informatike (дата обращения: 31.03.2025).

References

1. Novikov, A. M. (2005). *Metodologiya uchebnoy deyatelnosti* [Methodology of educational activity]. Egves.
2. Batyshev, S. Ya., & Novikov, A. M. (Eds.). (2010). *Professionalnaya pedagogika* [Professional pedagogy] (3rd rev. ed.). Egves.
3. Lomakina, T. Yu. (2000). *Diversifikatsiya professionalnogo obrazovaniya* [Diversification of vocational education]. TsPNO ITOP RAO.
4. Verbitsky, A. A. (1991). *Aktivnoye obucheniye v vysshey shkole: kontekstnyy podkhod* [Active learning in higher education: A contextual approach]. Vysshaya shkola.
5. Zeer, E. F. (2009). *Psikhologiya professionalnogo obrazovaniya* [Psychology of vocational education]. Akademiya.
6. Khmyzova, N. G., & Kuznetsova, E. V. (2022). Praktiko-oriyentirovannyye moduli formirovaniya obshcheprofessionalnykh kompetentsiy u bakalavrov professionalnogo obucheniya (po otraslyam) [Practice-oriented modules for the formation of general professional competencies in bachelors of vocational training (by industry)]. *Uchenyye zapiski Orlovskogo gosudarstvennogo universiteta. Seriya: Gumanitarnyye i sotsialnyye nauki*, 1(94), 43–49. https://cyberleninka.ru/article/n/praktiko-orientirovannye-moduli-formirovaniya-obscheprofessionalnyh-kompetentsiy-u-bakalavrov-professionalnogo-obucheniya-po
7. Razgonyaev, V. K. (2020). Ispolzovaniye virtualnykh kompyuterov pri prepodavanii distsiplin, svyazannykh s informatsionnymi tekhnologiyami [Using virtual computers in teaching disciplines related to information technology]. *Vestnik SIBITa*, 2(34), 35–42. https://sano.ru/magazine/N34/N34.pdf
8. Fedorov, V. A. (2001). *Professionalno-pedagogicheskoye obrazovaniye: teoriya, empirika, praktika* [Vocational and pedagogical education: Theory, empirics, practice]. Ural State Vocational Pedagogical University Press.
9. Uymin, A. G., & Tokarev, G. I. (2022). Instrumentalnyye sredstva obucheniya kompyuternym setyam. Razvyortyvaniye na baze rossiyskogo programmnogo obespecheniya [Instrumental tools for teaching computer networks. Deployment based on Russian software]. *Sistemy upravleniya i informatsionnyye tekhnologii*, 4(90), 88–92. https://doi.org/10.36622/VSTU.2022.90.4.019
10. Uymin, A. G. (2022). Instrumenty verifikatsii obuchayemogo i otsenki yego emotsionalno-psikhologicheskogo sostoyaniya pri distantsionnoy rabote [Tools for learner verification and assessment of emotional-psychological state in remote work]. In *Pedagogicheskoye obrazovaniye: Istoriya stanovleniya i vektory razvitiya: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii* (pp. 769–773). MPGU.
11. Gibadullin, A. A. (2019). Metodologiya ispolzovaniya intellektualnykh kompyuternykh igr v obuchenii informatsionnym tekhnologiyam [Methodology of using intelligent computer games in teaching information technologies]. *International Journal of Advanced Studies*, 9(4), 11–14. https://cyberleninka.ru/article/n/metodologiya-ispolzovaniya-intellektualnyh-kompyuternyh-igr-v-obuchenii-informatsionnym-tehnologiyam
12. Pirogov, V. Yu. (2021). O vozmozhnostyakh distantsionnogo prepodavaniya programmirovaniya dlya studentov tekhnicheskikh spetsialnostey [On the possibilities of distance teaching of programming for students of technical specialties]. *Mir nauki. Pedagogika i psikhologiya*, 9(6), Article 27PDMN621. https://mir-nauki.com/PDF/27PDMN621.pdf
13. Matkurbanov, D., & Rakhimjanov, K. (2021). Analysis of network emulation and simulation software. *Sciences of Europe*, 79(1), 38–46. https://doi.org/10.24412/3162-2364-2021-79-1-38-46
14. Zenk, V., & Malmström, M. (2020). *A comparative study of Docker and Vagrant regarding performance on machine level provisioning*. Malmö University. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1444178
15. Aripova, G. I. (2022). Ispolzovaniye kategoriy informatsionno-kommunikatsionnykh tekhnologiy pri obuchenii studentov informatike [Using categories of information and communication technologies in teaching students informatics]. *Nauka i obrazovaniye segodnya*,

2(71), 28–34. https://cyberleninka.ru/article/n/ispolzovanie-kategoriy-informatsionno-kommunikatsionnyh-tehnologiy-pri-obuchenii-studentov-informatike

Информация об авторах

Морозов Илья Михайлович — ассистент, РГУ нефти и газа (НИУ) имени И. М. Губкина, г. Москва, Российская Федерация; e-mail: au-mail@ya.ru

LABORATORY WORKSHOP ON COMPUTER NETWORK MONITORING BASED ON A DOMESTIC OPERATING SYSTEM AND OPEN-SOURCE SOFTWARE: METHODOLOGY AND AUTOMATED VERIFICATION OF RESULTS

***Morozov I. M.*[1]**

[1] *National University of Oil and Gas "Gubkin University", Moscow, Russian Federation*

Abstract. *The article addresses the problem of organizing a laboratory workshop on computer network administration and monitoring disciplines in the context of transition to domestic operating systems and import-independent administration tools. The necessity of a two-stage verification of laboratory work results is substantiated: automated verification of technical specifications and expert evaluation of architectural solutions. A methodology for building a reproducible educational environment based on the GNS3 + VirtualBox + Vagrant + ALT Linux + Zabbix stack is described, enabling simulation of a small enterprise infrastructure. Two laboratory works are presented: on SNMP protocol fundamentals and on configuring network device monitoring using Zabbix with network map construction. It is shown that the use of the Vagrant box mechanism ensures portability of the educational environment, accelerates classroom preparation, and simplifies remote student work. The pedagogical effectiveness of the proposed approach is substantiated through the concept of practice-oriented learning, the activity-based approach, and the principle of professional orientation of educational content. The methodology was tested within the course "Computer Network Management and Monitoring" of the master's program "Computer Systems and Networks" at HSE University and adapted for the level of secondary vocational education in specialty 09.02.06 "Network and System Administration". The results confirm that the proposed environment develops students' stable professional skills in working with real monitoring tools used in the IT industry.*

Keywords: *laboratory workshop, network monitoring, Zabbix, ALT Linux, SNMP, Vagrant, automated verification.*

Information about the authors

Morozov Ilya Mikhailovich — Assistant, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation; e-mail: au-mail@ya.ru