

- assessing the information security of telecommunication systems. *Elektrosvyaz*, 2022, no. 2, pp. 61–66. (In Russ.)
10. Kotenko I., Parashchuk I. Analysis of threats to information security of industrial automation systems using euclidean and hamming distances between fuzzy sets. *Conference Proceedings: International Russian Automation Conference (RusAutoCon)*, 2023, pp. 13–18. (In Russ.)

Received 18.01.2024

УДК 004.7; 372.862

СПЕЦИАЛИСТ ПО ЭКСПЛУАТАЦИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ: ЗНАНИЯ, УМЕНИЯ, НАВЫКИ

Галич С.В., Сафонова О.Е.

Волгоградский государственный университет, Волгоград, РФ

E-mail: galich.sv@volsu.ru

В статье проведен анализ российских разработок в сфере программно-конфигурируемых сетей, профессионального стандарта и вакансий с целью определения требуемых от специалистов знаний, умений, навыков. Показано, что рынок труда испытывает явную потребность в кадрах, способных эксплуатировать и разрабатывать решения, функционирующие на основе принципов программно-конфигурируемых сетей. Сделаны выводы о том, что наблюдается недостаток пособий практической направленности для подготовки специалистов в данной сфере, а также предложены возможные темы лабораторных работ для учебных пособий. Данная статья может быть полезна преподавателям образовательных учреждений средне-специального и высшего образования, а также дополнительного профессионального образования при разработке рабочих программ дисциплин, лекций и лабораторных практикумов, посвященных программно-конфигурируемым сетям, а также обучающимся вышеупомянутых образовательных учреждений при планировании индивидуального плана обучения, выпускникам и молодым специалистам при планировании своего профессионального и карьерного развития.

Ключевые слова: программно-конфигурируемые сети, виртуализация сетевых функций, знания, умения, навыки, образование

Введение

В 2022 году уход с российского рынка крупнейших мировых производителей сетевого оборудования, аннулирование ими в одностороннем порядке действующих лицензий и прекращение технической поддержки закупленного оборудования продемонстрировали уязвимость набравшей популярность сервисной модели предоставления услуг и оборудования.

Сетевые устройства со встроенными интеллектуальными функциями, такие как межсетевые экраны нового поколения (NGFW), по воле производителя лишались большей части своего функционала быстрее, чем администраторы успевали предпринять какие-либо действия. Особо уязвимы оказались устройства, функционирующие в соответствии с принципами технологии программно-конфигурируемых сетей (ПКС, англ. SDN), подразумевающей отделение плоскости управления (англ. control plane) от плоскости передачи (англ. data plane), при этом плоскость управления в лице SDN-контроллера совершенно не обязательно территориально располагать в центре обработки данных (ЦОД) или серверной эксплуатирующей организации. SDN-контроллер

вполне может функционировать в облаке производителя устройства, более того, подобный подход в ряде случаев может быть выгодным для потребителя с точки зрения затрат и лицензирования, а именно позволяет реализовать одно из достоинств SDN как концепции и переводить капитальные затраты на оборудование в операционные [1].

В крайне деструктивных действиях была замечена компания Cisco: например, компания не ограничилась отключением устройств Cisco Meraki от облачных сервисов, но и захватила контроль над устройствами на территории Российской Федерации и создала открытый SSID (Service Set Identifier) вида «12345-Sanctions». Продукты серии Cisco vEdge SD-WAN (Software-Defined Networking in a Wide Area Network, программно-определяемая глобальная сеть) имеют целый набор различных проблем: от невозможности добавить новое устройство до истекших 9 мая 2023 года сертификатов безопасности, приводящих к неработоспособности устройств после перезагрузки и обновление которых невозможно без обращения в поддержку производителя (который, опять же, ушел с российского рынка).

В подобных действиях, возможно, не столь разрушительных, замечена большая часть ушедших с рынка производителей оборудования, ранее занимавших лидирующие позиции в России.

SD-WAN-решения являются реализацией концепции SDN для корпоративных сетей передачи данных и наибольшую выгоду могут принести компаниям с распределенной филиальной сетью, для которых крайне важно снизить время подключения новых офисов, таких как ретейлеры и банки [2].

Глобальными лидерами среди производителей сетевого оборудования в сегменте SD-WAN принято считать компании Cisco, Fortinet, VMWare, HPE (Aruba), Palo Alto Networks, Versa Networks. Именно такую оценку давали аналитические компании IDC [3] и Gartner [4] в 2021 и 2022 годах. Аналитики из TeleGeography [5] в качестве однозначных лидеров выделяют Cisco и VMWare; также помимо вышеперечисленных в топ-10 производителей SD-WAN включают Nuage Networks, Juniper Networks, Palo Alto Networks, Riverbed. Тем не менее российские производители воспользовались уникальным шансом заполнить освободившиеся после ухода лидеров индустрии ниши и предложили в том числе решения класса SD-WAN.

Российские разработки SDN и SD-WAN

В России исследования в сфере программно-конфигурируемых сетей получили свое развитие во многом благодаря Московскому государственному университету им. М.В. Ломоносова и НП «Центр прикладных исследований компьютерных сетей» (НП «ЦПИКС»), создавших Консорциум «ПКС – технологии в научно-образовательной среде», в состав которого вошли ведущие вузы страны. На базе разработок НП «ЦПИКС» запущены стартапы NFWare и WiMark Systems, разработан контроллер RunOS (две версии: коммерческая и open-source) и платформа виртуализации сетевых функций (ВСФ, англ. NFV) C2 Cloud Conductor. НП «ЦПИКС» имеет опыт реализации пилотных проектов на основе своих решений в сетях операторов связи [6], в частности совместно с операторами связи «Вымпелком», «Воентелеком» и «Ростелеком». Судя по имеющимся публикациям сотрудников [7], ведутся и разработки в направлении SD-WAN, однако свежих новостей в открытых источниках от НП «ЦПИКС» не обнаружено.

В Российской Федерации именно ПАО «Ростелеком» является крупнейшим испытателем программно-конфигурируемых сетей (ПКС). Необходимость развития решений ПКС и ВСФ как неотъемлемой части сетей 5G указана в «Ком-

плексной программе содействия развитию 5G в России» [8]. Помимо тестирования решений НП «ЦПИКС», оператором связи был реализован пилотный проект с Brain4Net Controller (разработка ООО «Программируемые сети», резидент «Сколково») [9] и осуществлялось тестирование транспортной ПКС (Transport SDN) совместно с западными производителями Huawei, NEC и Nokia [9].

В 2021 году совместными усилиями Tele2 и «Ростелеком» был реализован пилотный проект по внедрению технологии SD-WAN в сети торговых точек. Тестирование проводилось на базе Brain4Net Service Platform с использованием оборудования компании «Булат» (совместное предприятие «Ростелеком» и «Ростех») и сим-карт Tele2. Благодаря техническим преимуществам от внедрения SD-WAN, среди которых повышение отказоустойчивости и снижение риска недоступности канала связи в точке продаж, бизнес может предоставлять посетителям точек продаж более качественный сервис в силу снижения вероятности возникновения очереди из-за сбоев кассового оборудования и цифровых информационных панелей [10; 11].

В октябре 2021 года «Лаборатория Касперского» приобрела ООО «Программируемые сети», расширив свое портфолио продуктов сетевым решением класса SD-WAN. Таким образом «Лаборатория Касперского» пошла по пути компаний Cisco, VMWare, Nokia, в портфолио решений которых SD-WAN также появлялся путем приобретения стартапов Viptela, VeloCloud, Nuage. Стоит отметить, что «Лаборатория Касперского» остается компанией, разрабатывающей программное обеспечение, а не аппаратное. Поэтому Kaspersky Edge Service Router (KESR) является наименованием линейки маршрутизаторов, разработанных партнерами «Лаборатории Касперского». Линейка включает в себя пять моделей: от младшей KESR Model 1 с пропускной способностью 30 Мбит/с до старшей KESR Model 5, обеспечивающей 10 Гбит/с [12]. Выяснить наименование конкретных моделей не удалось, однако можно сделать предположение, что в линейку KESR входят устройства «Булат» BS5120, поскольку имеется упоминание применения оборудования «Булат» в рамках пилотного проекта [10; 11].

Среди других российских вендоров сетевого оборудования протокол OpenFlow 1.0/1.3.4 поддерживают также устройства Eltex MES5448 и MES7048 [13]. В модельном ряду Qtech обнаружилась линейка QSW-6510, однако согласно информации на сайте производителя [14] она более не производится.

На российском рынке пионером внедрения SD-WAN стала компания МТС (облачный провайдер CloudMTS), начавшая в 2020 году использовать решения Fortinet.

Свой вклад в популяризацию технологии внесла компания BI.ZONE, выпустившая в 2021 году первое отечественное решение SD-WAN. Именно о переходе на решения BI.ZONE объявила компания МТС в январе 2023 года. Крайне интересным решением является применение в составе BI.ZONE Secure SD-WAN протокола Wireguard с поддержкой шифрования по алгоритму «Кузнечик» (ГОСТ Р 34.12–2015). Реализация размещена на Github, планируется ее сертификация по требованиям ФСБ России. Модельный ряд маршрутизаторов включает в себя семь моделей: младшая CyberEdge 10 обеспечивает пропускную способность 20 Мбит/с, старшая BI.ZONE CyberEdge 3000 – 3 Гбит/с [15].

Еще одной компанией, имеющей в портфолио SD-WAN-решение, является Network Systems Group (NSG), предлагающая продукт «Богатка SD-WAN». Разработка отмечена дипломом технологического конкурса 5G SmartTech 2022, проводившегося фондом «Московский инновационный кластер». По мнению авторов статьи, продукт очень интересный и самобытный, но, к сожалению, в открытом доступе представлено крайне мало информации, за исключением руководства администратора системы [16].

В таблице 1 приведен обзор стека технологий и протоколов, применяемого в российских разработках SD-WAN. В ходе проводимого сравнения не ставилась задача определения лучшей разработки или лидера рынка. По мнению авторов, такие выводы можно сделать только на основе пилотных проектов и опыта эксплуатации. В данной работе сравнение проводится с целью выяс-

Таблица 1. Обзор технологий и протоколов, задействованных в составе решений SD-WAN от российских компаний

Параметр сравнения	Kaspersky SD-WAN	BI.ZONE Secure SD-WAN	NSG Богатка SD-WAN	RunOS SDN (open-source)
Протокол Control Plane	OpenFlow 1.3.4	BCMP (BI.ZONE CPE Management Protocol)	SSH, bash-скрипты	OpenFlow 1.3
Операционная система	Astra Linux 1.7	Astra Linux 1.7, Альт Линукс СП 8, Ubuntu	Linux (Ubuntu)	Linux (Ubuntu)
Протокол Overlay-туннелирования	GENEVE с TLS 1.3 и шифрованием ChaCha20	Wireguard с поддержкой шифрования ГОСТ	Собственная разработка «Клещ» VPN совместно с TLS 1.3; «Клещ» VPN совместно с IPsec, OpenVPN	VxLAN
Совместимое оборудование CPE	Kaspersky Edge Service Router; uCPE на базе стандартных серверов x86 архитектуры	BI-ZONE CyberEdge и CyberEdge VM на базе стандартных серверов x86 архитектуры	NSG-17xx, NSG-1810/1820/1830, NSG-20xx, NSG-30xx	Программный коммутатор RunAR на базе стандартных серверов x86 архитектуры; Программно-аппаратный коммутатор RunDR на базе сетевого процессора
Менеджер Виртуализации сетевых функций	OpenStack	Собственная разработка «Оркестратор функций безопасности», управляющий виртуальными сетевыми функциями на CPE	н/д	C2 (Cloud Conductor)
Мониторинг	Zabbix	Имеется	Zabbix	Имеется

нить, какие технологии и протоколы задействованы в составе решений, а также владение какими навыками и знаниями инструментов требуется от специалиста по эксплуатации SD-WAN.

Из представленных на российском рынке решений бесплатной для образовательных учреждений является только open-source версии RunOS. Это решение однозначно следует рассматривать в рамках лабораторных занятий наряду с другими известными в исследовательском сообществе open-source-проектами, такими как ONOS и OpenDaylight [17; 18]. В качестве сетевых узлов можно использовать персональный компьютер с развернутыми на них Open vSwitch. Касательно же решений Kaspersky, BI.ZONE, NSG – возможно, производители предложат некоторые демонстрационные версии для загрузки (по примеру компании «Код Безопасности» [19]) или развернут демо-стенды на своих мощностях. По крайней мере, со стороны «Лаборатории Касперского» подобные действия уже предпринимались: в рамках технического онлайн-марафона «Kaspersky SD-WAN 2.0: функциональные возможности и практический опыт», проводившегося с 29.05.23 по 02.06.23 гг., участникам предлагалось записаться на открытую лабораторную работу. Образовательным учреждениям для оснащения учебных лабораторий необходимо налаживать партнерство с российскими же производителями SDN и SD-WAN решений. В этом случае учебный процесс будет построен с использованием решений, внедряемых в эксплуатацию, что повысит востребованность выпускников таких образовательных учреждений.

В таблице 2 приведены сведения о наличии сертификатов соответствия регуляторов сфер информационных технологий и информационной безопасности. Отметим, что все рассматриваемые решения зарегистрированы в реестре российского программного обеспечения. На момент подготовки статьи рассматриваемые решения не

имели сертификатов соответствия от Федеральной службы технического и экспортного контроля (ФСТЭК) как средства защиты информации (СЗИ) и от Федеральной службы безопасности (ФСБ) как средства криптографической защиты информации (СКЗИ). Сама по себе сертификация рассматриваемых решений в силу специфики проведения данной процедуры оценки соответствия и эксплуатации сертифицированных изделий в строгом соответствии с требованиями формуляра может привести к потере некоторых преимуществ SDN, в частности гибкости, масштабируемости и скорости внедрения новых разработок. Тем не менее компаниями Kaspersky и BI.ZONE планируется сертификация своих решений SD-WAN в качестве межсетевых экранов (МЭ). Касательно сертификации в качестве средств криптографической защиты информации эти две компании выбрали различный подход: BI.ZONE планирует сертифицировать решение, а Kaspersky предлагает вариант развертывания своего решения поверх существующих VPN-туннелей с ГОСТ-шифрованием на базе сертифицированных СКЗИ. Само же наличие сертификата от регуляторов отрасли расширяет сферы применения российских решений с точки зрения соответствия требованиям законодательства, а значит, с позиции конечного потребителя SDN, свидетельствует о зрелости решения и его готовности к внедрению в эксплуатацию.

Анализ опубликованных вакансий и требований, предъявляемых работодателями

Как видно, на российском рынке уже имеются отечественные решения SD-WAN, которые применяются для модернизации существующих и построения новых сетей связи. Для того чтобы определить ожидания работодателей от квалификации и технических навыков специалистов

Таблица 2. Сертификация решений SD-WAN от российских компаний

Параметр сравнения	Kaspersky SD-WAN	BI.ZONE Secure SD-WAN	NSG Богатка SD-WAN	RunOS SDN (open-source)
Запись в реестре отечественного ПО	№ 5840 от 20.09.2019 г. (как B4N Orchestrator)	№ 9005 от 28.01.2021 г.	№ 12257 от 09.12.2021 г.	№ 14817 от 12.09.2022 г.
Сертификация ФСТЭК	Планируется сертификация СРЕ как МЭ	Планируется как МЭ	Отсутствует	Отсутствует
Сертификация ФСБ	Отсутствует; SD-WAN способна работать поверх ГОСТ-туннелей	Планируется как СКЗИ по классу КС 1-3	Отсутствует	Отсутствует

по эксплуатации программно-конфигурируемых сетей в современных условиях, был проведен анализ размещенных в открытом доступе вакансий на сайтах по трудоустройству *hh.ru* и *career.habr.com*, а также разделах «Вакансии» на сайтах крупнейших телеком-операторов МТС, «Мегафон», «Билайн», «Ростелеком». Мониторинг вакансий осуществлялся в мае и октябре 2023 года. Поиск осуществлялся по ключевым словам: SDN, SD-WAN, NFV, VNF, OpenFlow. Если на разных источниках была размещена одна и та же вакансия, она считалась как один обнаруженный объект анализа. Если вакансия размещена дочерней организацией материнской компании, вакансия учитывалась в статистике материнской компании.

В мае всего было обнаружено 26 вакансий, в описании к которым так или иначе упоминались искомые ключевые слова. Из них вакансий, описывающих специалистов эксплуатационного направления – 17 шт., оставшиеся 9 вакансий содержат требования к специалистам по разработке и тестированию. В октябре всего обнаружено 33 вакансии, из которых к специалистам по эксплуатации относятся 24 шт., и 9 вакансий описывают требования к навыкам специалистов по разработке и тестированию. Для абсолютного большинства специалистов требуется минимальный стаж работы от 3 лет, только в описании пяти вакансий в требованиях к стажу указан 1 год, и всего одна вакансия явно содержит указание на то, что работодатель готов взять выпускника ВУЗа без опыта работы. Распределение вакансий по отраслям показано на рисунке 1. Примечательно, что среди работодателей наибольшую долю вакансий обе-

спечивают российские разработчики SDN-решений (Kaspersky (B4N), BI.ZONE, NFWare), ведущие телеком-операторы («Билайн», «Мегафон», МТС, «Ростелеком») и производители оборудования (Zelax).

Исходя из сведений, представленных на рисунке 1, соискатель (выпускник образовательного учреждения) сможет получить представление о том, в каких отраслях наиболее востребованы специалисты по эксплуатации программно-конфигурируемых сетей.

Анализ показал, что компании-работодатели хотят видеть у специалистов по эксплуатации программно-конфигурируемых сетей следующие знания и технические навыки:

- понимание принципов концепций программно-конфигурируемых сетей SDN и виртуализации сетевых функций NFV, работы протокола OpenFlow, технологии SD-WAN;
- понимание архитектуры сетей масштаба оператора связи, в том числе мобильных сетей 5G/LTE/3G, понимание принципов работы биллинговых систем;
- владение инструментами автоматизации конфигурирования: скриптовыми языками *bash*, *python*, системой управления конфигурациями *Ansible*;
- навыки администрирования систем мониторинга, знание протоколов мониторинга сетевых устройств: *Zabbix*, *ELK*, *Prometheus*, *Netflow*, *SNMP*;
- уверенное пользование системами управления версиями *Git*;
- опыт администрирования, знание архитектуры и сетевого стека операционных систем: *Linux*, *Windows*;

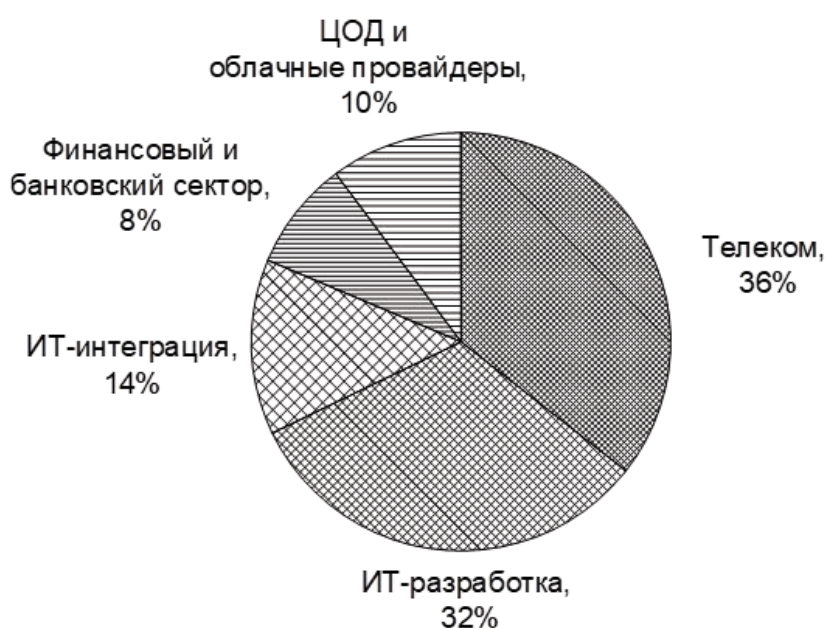


Рисунок 1. Структура предложения вакансий на рынке труда по отраслям (май, октябрь 2023 г.)

- уверенные навыки (на уровне сертификации CCNA/CCNP или аналогов) в работе с сетевыми протоколами, протоколами туннелирования и протоколами аутентификации, авторизации, учета: NAT, DHCP, ARP, DNS, IGMP, VLAN, STP, LACP, HSRP, OSPF, EIGRP, BGP, VRF, PBR, bird/ftt/exabgp, EVPN, VXLAN, MPLS, VPN, DMVPN, IPSEC, Wireguard, TACACS, RADIUS;

- навыки работы с базами данных, понимание языка запросов SQL;

- понимание и владение технологиями виртуализации и контейнеризации: KVM, QEMU, OpenStack, VMware NSX-V/T, Docker;

- навыки администрирования межсетевых экранов и сетевого оборудования, в том числе отечественных производителей: Cisco (ASA, NGFW, Fire-power), Checkpoint, Fortinet, Континент, Usergate, Sterra, Vipnet, Eltex, Qtech и др.;

- владение утилитами диагностики сетей: Wireshark, tcpdump, iperf.

Для анализа частоты упоминания терминов в описании вакансий в сфере эксплуатации авторами с использованием Python-скрипта было сгенерировано облако слов (word cloud), показанное на рисунке 2.



Рисунок 2. Облако слов для вакансий в сфере эксплуатации программно-конфигурируемых сетей

Требуемые работодателями знания и навыки в большинстве своем совпадают с технологиями и протоколами, задействованными в составе решений SD-WAN от российских компаний.

В таблицу 3 сведено то программное и аппаратное обеспечение, практический опыт настройки и эксплуатации которых, по мнению работодателей, необходим соискателям на должность специалиста по эксплуатации программно-конфигурируемых сетей.

Отдельно отметим, что приведенные в таблице 3 модели устройств и программного обеспечения являются компонентами для построения SDN-инфраструктур из портфолио ушедших из России

производителей, упоминаемых в начале статьи. Большая же часть из указанного оборудования упоминается также и в работе [20].

Таблица 3. Упоминаемое в вакансиях в сфере эксплуатации ПКС программное и аппаратное обеспечение

Производитель	Сетевые устройства, программное обеспечение
Cisco	Nexus 5000/9000, ASR 1000/9000, ISR4000
VMWare	NSX-V/T
Juniper	Juniper (QX, MX, EX, SRX), TungstenFabric (OpenContrail)
Citrix	NetScaler
Huawei	CloudEngine (CE)
Cumulus	OS Cumulus Linux

К специалистам в области разработки и тестирования предъявляются несколько менее жесткие требования в области знания сетевых технологий, но набор навыков должен быть значительно расширен в следующих областях:

- языки программирования C/C++, Go, JavaScript, Java, P4, PHP, Tcl;

- навыки работы с RESTful API, понимание форматов данных JSON и XML;

- знание протоколов SSL/TLS, библиотеки OpenSSL;

- владение eBPF, DPDK для оптимизации производительности обработки сетевых пакетов;

- понимание принципов, методов управления жизненным циклом программного обеспечения (SDLC) и безопасной разработки (SSDL), опыт применения инструментов статического (SAST) и динамического анализа кода (DAST), инструментов поиска и анализа уязвимостей (IDA, windbg/gdb, fuzzing tools);

- знание Free5GC и Open5GS (для разработок в сфере телеком-индустрии).

Также облако слов было сгенерировано и для анализа частоты упоминания терминов в описании вакансий в сфере разработки и тестирования (рисунок 3). Как видно, существенно большее внимание уделяется знанию инструментов автоматизации и разработки.

В целом можно сделать вывод, что рассмотренные вакансии являются скорее экспертными и работодатели на позициях специалистов по эксплуатации программно-конфигурируемых сетей хотели бы видеть сетевых инженеров с опытом эксплуатации, обнаружения и решения проблем в традиционных коммутируемых и маршрутизируемых IP-сетях достаточно большого масштаба, т.е. либо распределенных корпоративных сетях,

либо сетях операторов связи. Вчерашний выпускник ВУЗа без опыта работы по специальности такими навыками, конечно же, обладать не может.

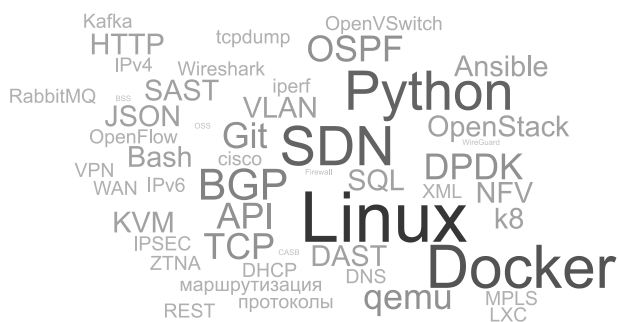


Рисунок 3. Облако слов для вакансий в сфере разработки и тестирования программно-конфигурируемых сетей

Требования, предъявляемые профессиональным стандартом

В настоящее время в России действует профессиональный стандарт (ПС) «Специалист по поддержке программно-конфигурируемых информационно-коммуникационных сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 16.11.2020 года № 768н. Примечательно, что это уже вторая версия стандарта: первая была введена в 2017 году (приказ Министерства труда и социальной защиты Российской Федерации от 26.06.2017 года № 514н). Разработчиками ПС являются НП «ЦПИКС», ФГБОУ ВО МТУСИ, ПАО «Ростелеком», ФГБУ «ВНИИТ» Министерства труда и социальной защиты Российской Федерации.

Согласно ПС выделяют пять обобщенных трудовых функций (ОТФ), каждая из которых включает в себя несколько трудовых функций (ТФ). Для осуществления каждой ОТФ требуется определенный уровень квалификации. Рассмотрим кратко каждую ОТФ:

– ОТФ 1. Поддержка сетевых устройств ПКС. Включает в себя следующие ТФ: установка сетевых устройств, настройка программного обеспечения сетевых устройств, установка специальных средств управления сетевыми устройствами. Требуемый уровень квалификации – среднее профессиональное образование (СПО);

– ОТФ 2. Проведение регламентных и восстановительных работ на сетевых устройствах и операционных системах ПКС. Включает в себя следующие ТФ: осуществление регламентных работ по поддержке сетевых устройств (СУ) и операционных систем (ОС), восстановление параметров СУ и ОС. Требуемый уровень квалификации – СПО;

– ОТФ 3. Планирование модернизации и восстановления ПКС. Включает в себя следующие ТФ: планирование модернизации СУ и ОС, планирование и подготовка восстановления работы ПКС. Требуемый уровень квалификации – СПО;

– ОТФ 4. Эксплуатация ресурсов, виртуализация сетевых функций и тарификация ПКС. Включает в себя следующие ТФ: настройка компонента администрирования и оркестрации, поддержка инфраструктуры виртуализации сетевых функций, управление средствами тарификации сетевых ресурсов и ОС. Требуемый уровень квалификации – высшее образование (бакалавриат) (ВО) или СПО;

– ОТФ 5. Выявление, локализация и устранение несоответствий сетевых устройств и операционных систем. Включает в себя следующие ТФ: диагностика и выявление ошибок СУ и ОС, устранение отказов и сбоев СУ и ОС. Требуемый уровень квалификации – ВО (специалитет, магистратура).

Таким образом, ПС содержит высокоуровневое описание выполняемых специалистом трудовых функций и требуемых ему для этого знаний и навыков. А значит, разработчиками рабочих программ дисциплин и учебно-методических комплексов должна быть выполнена конкретизация навыков и знаний с учетом лабораторной базы конкретного учебного заведения.

Ориентируясь на данный ПС, можно разрабатывать образовательные стандарты, учебные планы и рабочие программы дисциплин, в которых уже необходимо четко сформулировать компетенции, знания, навыки и умения (в том числе включая технические средства и инструменты), которыми должен овладеть обучающийся за минимально допустимое количество учебных часов.

Знания должны включать в себя принципы функционирования, стандарты, протоколы ПКС [21–22], оформленные в виде набора разделов и теоретических тем соответствующей дисциплины, а навыки и умения по работе с техникой и инструментами должны быть получены и закреплены в ходе практических и лабораторных работ.

Российскими учеными и преподавателями высшей школы уже разработаны и выпущены в свет учебники и учебные пособия, детально описывающие архитектурные особенности и принципы функционирования ПКС и ВСФ [23–26]. Но, по мнению авторов, наблюдается недостаток настолько же качественных пособий для практических занятий – лабораторных практикумов и учебных пособий с расчетными задачами, освещающих вопросы проектирования ПКС и планирования ресурсов.

На основании проведенного обзора вакансий можно сделать вывод, что для освоения технологий SDN и SD-WAN требуется достаточно большой объем знаний и навыков работы с сетевыми протоколами и языками программирования. Учитывая этот факт, образовательная дисциплина по программно-конфигурируемым сетям должна читаться для студентов старших курсов, обучающихся по программам высшего образования (4 курс бакалавриата, 4–5 курс специалитета).

Таким образом, ориентируясь на рассмотренные источники, необходимо разрабатывать рабочие программы и учебно-методические комплексы дисциплин с четко сформулированными компетенциями, знаниями и навыками с учетом требований работодателей и предлагаемых на рынке технологических решений.

Для наиболее эффективного освоения рассматриваемых технологий и приобретения навыков необходим полноценный курс, раскрывающий не только теоретические аспекты, но и содержащий большой лабораторный практикум, позволяющий эти навыки отработать.

В качестве примера можно рассмотреть рабочую программу дисциплины «Проектирование и поддержка программно-конфигурируемых сетей», изучаемой на 4 курсе направления подготовки 09.03.01 «Информатика и вычислительная техника» (бакалавриат) в Рязанском государственном радиотехническом университете имени В.Ф. Уткина [27]. Общая трудоемкость дисциплины включает в себя 180 часов. Разработчиками рабочей программы являются В.П. Корячко и Д.А. Перепелкин, также являющиеся авторами учебника [23]. Достаточно подробно рассматриваются теоретические аспекты функционирования ПКС. Практическая часть курса (включающая лабораторные работы и семинарские занятия) сфокусирована на детальном рассмотрении алгоритмов маршрутизации и сегментации в ПКС, что необходимо и для специалистов по эксплуатации, и для специалистов по разработке ПКС.

Учитывая требования работодателей и быстрое развитие технологий, авторы хотели бы предложить свое видение теоретических разделов дисциплины и практической ее части. В качестве основных разделов курса предлагаются следующие:

1. История появления и развития программно-конфигурируемых сетей.
2. Общие принципы построения сетей.
3. Протокол OpenFlow и язык программирования правил маршрутизации пакетов P4.
4. Архитектура и экосистема ПКС.

5. Проекты с открытым исходным кодом.

Примерные темы лабораторных работ, входящих в состав практикума, могут быть следующими:

1. Установка и первоначальная настройка SDN-контроллера.
2. Настройка базовых приложений SDN-контроллера.
3. Инструменты и методы тестирования производительности SDN-контроллера.
4. Методы обеспечения отказоустойчивости SDN-контроллера.
5. Интеграция SDN-контроллера с NFV-платформой.
6. Создание и исследование модели SDN-сети.
7. Принципы работы с интерфейсами прикладного программирования SDN-контроллера.
8. Основные уязвимости и принципы обеспечения безопасности SDN.

Дополнительное профессиональное образование в области программно-конфигурируемых сетей

Следует отметить, что в условиях же быстрого развития и обновления модельного ряда оборудования, появления новых языков программирования, фреймворков, средств автоматизации в развитии специалиста существенно увеличивается роль ДПО.

В соответствии с Федеральным законом «Об образовании в Российской Федерации» (№ 273-ФЗ от 29.12.2012 года) целью ДПО является обеспечение соответствия квалификации человека меняющимся условиям профессиональной деятельности и социальной среды. Программы ДПО в сфере ПКС могут быть посвящены как продуктам и решениям конкретных производителей, так и отдельным компонентам технологического стека ПКС, например операционным системам, языкам программирования, интерфейсам прикладного программирования, средствам виртуализации серверной и сетевой инфраструктуры.

Помимо этого, на базе учреждений ДПО в России была организована и система подготовки и сдачи международных сертификационных экзаменов в области сетевых технологий. Учитывая тот факт, что с 2022 года все международные сертификации для граждан России более недоступны, возможно, было бы полезно и своевременно предложить собственный сертификационный экзамен в области ПКС.

Наиболее известным международным сертификационным экзаменом в области ПКС является ONF-Certified SDN Associate Exam (OCSA-2.0)

Таблица 4. Разделы и темы сертификационного экзамена ONF-Certified SDN Associate Exam

Раздел	Темы
История появления и развития программно-конфигурируемых сетей	История программно-конфигурируемых сетей
	Отличительные особенности концепции программно-конфигурируемых сетей
	Наложенные Overlay-сети
	Устройства программно-конфигурируемых сетей
	Применение принципов ПКС в мобильных сетях
	Применение принципов ПКС в центрах обработки данных
	Применение принципов ПКС в кампусных и корпоративных сетях
Общие принципы построения сетей	Функции коммутаторов и маршрутизаторов
	Протоколы маршрутизации
	Оптические сети
	Протоколы IPv4 и IPv6
	Функционал уровней L2/L3 OSI
	Сетевой стек ОС Linux
	Основы виртуализации сетей
Протокол OpenFlow и язык программирования правил маршрутизации пакетов P4	Типы сообщений OpenFlow
	Различия между версиями OpenFlow
	Протоколы OF-Config, Netflow
	Установление сессий между контроллером и коммутатором
	Принципы обработки пакетов в pipeline
	Синтаксис, структура, абстракции языка P4
	Запуск и тестирование программ P4
Архитектура и экосистема ПКС	Стратегии миграции и гибридные коммутаторы
	Сравнение архитектуры ПКС и традиционных сетей
	Назначение и функционал контроллера программно-конфигурируемых сетей
	Приложения для программно-конфигурируемых сетей, виртуальные сетевые функции
	Northbound API
	Объединения и консорциумы
	Безопасность и доступность
	Стандартизирующие организации
	Центры научных разработок
Проекты с открытым исходным кодом	Контроллеры программно-конфигурируемых сетей (ONOS, ODL, RYU)
	OpenVSwitch
	Оркестраторы
	Утилиты и инструменты (Wireshark, Mininet, OpenFlow Manager))

[28], разработанный Open Network Foundation (ONF). В 2011 году Deutsche Telekom, Facebook, Google, Microsoft, Verizon, Yahoo основали консорциум ONF, целью которого является популяризация и стандартизация программно-конфигурируемых сетей. В настоящее время в состав консорциума входит более 100 компаний.

Экзамен позиционируется как сертификация начального уровня и направлен на проверку концептуальных знаний в области программно-конфигурируемых сетей без привязки к продуктам конкретного производителя. Экзаменуемому предлагается за 60 минут дать ответ на 40 вопросов. Экзамен считается успешно сданным

при доле верных ответов выше 70%. Пул вопросов включает в себя следующие разделы: общие принципы построения сетей (15%), история появления и развития ПКС (25%), протокол OpenFlow и язык программирования правил маршрутизации пакетов P4 (25%), архитектура и экосистема ПКС (25%), проекты с открытым исходным кодом (10%). В таблице 4 приведены разделы и темы рассматриваемого экзамена.

К достоинствам данного экзамена можно отнести отсутствие привязки к решениям конкретного производителя. Явным же недостатком является тот факт, что экзамен подразумевает проверку исключительно теоретических знаний. Темы, включенные в экзамен, весьма подробно рассмотрены в учебниках и учебных пособиях российских авторов [23–27], за исключением языка программирования P4.

В случае разработки российского экзамена необходимо предусмотреть и проверку практических навыков, требуемых для реализации обобщенных трудовых функций из рассмотренного выше профессионального стандарта. Разрабатываться такой экзамен должен непременно в тесном взаимодействии образовательного сообщества, работодателей и реальных российских производителей ПКС-решений.

Выводы

Разработки российских производителей, реализующие концепции SDN и SD-WAN, в частности, достигли определенного уровня зрелости: проведены пилотные проекты, имеются готовые решения на рынке и примеры внедрения. Конечно, у каждого из решений имеются свои недоработки в плане функционала, но есть и конкурентные преимущества перед зарубежными разработками.

Компаниям, ранее купившим и внедрившим продукты зарубежных производителей, несмотря на всю болезненность сложившейся ситуации с прекращением поддержки, есть из чего выбирать. Вероятно, у отечественных компаний будет возможность занять большую часть российского и, вероятно, некоторую часть мирового рынка решений программно-конфигурируемых сетей [29].

В то же время рынок труда испытывает явную потребность в кадрах, способных эксплуатировать и разрабатывать SDN- и SD-WAN-решения. Для отрасли эксплуатации требуется сетевой инженер, обладающий опытом администрирования сетевых устройств и навыками автоматизации, отладки проблем в функционировании сетевых протоколов, имеющий представление о концеп-

циях ПКС и ВСФ. Для отрасли разработки требуются специалисты, владеющие несколькими языками программирования, имеющими опыт работы с API, DPDK, понимающими принципы безопасной разработки и функционирования сетевых протоколов.

Для подготовки кадров уже имеются учебники и учебные пособия, однако, по мнению авторов, наблюдается недостаток пособий по практическим и лабораторным работам, а также возможны сложности с оснащением учебных лабораторий. Тем не менее эти проблемы не кажутся неразрешимыми.

Необходима разработка полноценных практических курсов и теоретических пособий, способных подготовить обучающегося к сдаче сертификационного экзамена в области ПКС, разработка которого тоже является немаловажной задачей.

Для реализации поставленных задач полезно учесть требования, предъявляемые профессиональным стандартом, работодателями и международным экзаменом ONF-Certified SDN Associate Exam.

Литература

1. Леонов В. Развитие SD-WAN как инструмента оптимизации сетевой составляющей распределенной ИТ-инфраструктуры // Connect. Мир информационных технологий. 2021. № 9–10. С. 87–89.
2. Плешаков Д. Особенности построения корпоративных сетей на базе SD-WAN-решений // Connect. Мир информационных технологий. 2022. № 9–10. С. 88–90.
3. Cisco Named a Leader in the IDC MarketScape for SD-WAN Infrastructure 2021. URL: <https://blogs.cisco.com/networking/cisco-named-a-leader-in-the-idc-marketscape-for-sd-wan-infrastructure-2021> (дата обращения: 20.05.2023).
4. Palo Alto Networks Hat Trick: 2022 Gartner Magic Quadrant for SD-WAN. URL: <https://www.paloaltonetworks.com/blog/2022/09/hat-trick-2022-gartner-mq-for-sd-wan/> (дата обращения: 20.05.2023).
5. 2022 SD-WAN Guide. URL: <https://drive.google.com/viewerng/viewer?url=https://www.communicationstoday.co.in/wp-content/uploads/2022/04/2022-SD-WAN-Guide.pdf&hl=en&pid=explorer&efh=false&a=v&chrome=false&embedded=true> (дата обращения: 20.05.2023).
6. Роль технологий SDN/NFV в инфраструктуре цифровой экономики. Опыт тестирования и внедрения / В.А. Ефимушкин [и др.] // Электросвязь. 2018. № 3. С. 27–36.

7. Пантюхин Л.К., Антоненко В.А. Разработка алгоритма распределения трафика для SD-WAN-решения // Программные системы и инструменты: тематический сборник. М.: МАКС Пресс, 2019. Т. 19. С. 66–79.
8. Комплексная программа развития 5G в России. URL: https://www.company.rt.ru/upload/iblock/b79/Комплексная_программа_5G.pdf (дата обращения: 23.05.2023).
9. Голышко А. SDN как окончательная цифровая трансформация телекома // Connect. Мир информационных технологий. 2019. № 4. С. 74–77.
10. Посетители салонов Tele2 получают более качественный сервис благодаря технологии SD-WAN. URL: <https://www.company.rt.ru/press/news/d460395> (дата обращения: 23.05.2023).
11. Росляков А.В., Марыков М.В. Сеть связи как облачная услуга NAAS // Инфокоммуникационные технологии. 2022. Т. 20, № 1. С. 70–82. DOI: 10.18469/ikt.2022.20.1.09
12. Kaspersky SD-WAN. URL: <https://www.kaspersky.ru/enterprise-security/sd-wan> (дата обращения: 23.05.2023).
13. Официальный сайт Eltex. URL: <https://eltex-co.ru> (дата обращения: 05.05.2023).
14. Официальный сайт Qtech. URL: <https://www.qtech.ru> (дата обращения: 05.05.2023).
15. Официальный сайт BI.ZONE. URL: <https://bi.zone/catalog/products/secure-sd-wan/?tb=tab3> (дата обращения: 23.05.2023).
16. Официальный сайт NSG. URL: <https://nsg.ru/products/bogatka.php> (дата обращения: 23.05.2023).
17. Семеновых А.А., Лапонина О.Р. Сравнительный анализ SDN-контроллеров // International Journal of Open Information Technologies. 2018. Vol. 6, no. 7. P. 50–56.
18. Исследование производительности ПКС-контроллера OpenDaylight на сетях разных масштабов / С.В. Галич [и др.] // Известия ЮФУ. Технические науки. 2016. № 9(182). С. 121–133.
19. Официальный сайт «Код Безопасности». URL: https://www.securitycode.ru/download_center/?section=stands (дата обращения: 23.05.2023).
20. Калмыков Н.С. Анализ рынка оборудования и решений ПКС // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 116–124.
21. Сравнительный анализ архитектур и протоколов программно-конфигурируемых сетей / В.А. Ефимушкин [и др.] // Электросвязь. 2014. № 8. С. 9–14.
22. Международная стандартизация программно-конфигурируемых сетей / В.А. Ефимушкин [и др.] // Электросвязь. 2014. № 8. С. 3–9.
23. Корячко В.П., Перепелкин Д.А. Программно-конфигурируемые сети: учебник для вузов. М.: Горячая линия – Телеком, 2021. 288 с.
24. Смелянский Р.Л., Антоненко В.А. Концепции программного управления и виртуализации сетевых сервисов в современных сетях передачи данных: учеб. пособие. М.: КУРС, 2020. 152 с.
25. Программно-конфигурируемые сети SDN. Протокол OpenFlow: учеб. пособие / Б.С. Гольдштейн [и др.]. СПб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. 48 с.
26. Основы программно-конфигурируемых сетей: учеб. пособие / Н.Ф. Бахарева [и др.]. Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. 111 с.
27. Корячко В.П., Перепелкин Д.А. Рабочая программа дисциплины «Проектирование и поддержка программно-конфигурируемых сетей». URL: https://edu.rsreu.ru/res/specialities/disc_edu_programs/69157-edu_program-file-%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B3%D1%83%D1%80%D0%B8%D1%80%D1%83%D0%B5%D0%BC%D1%8B%D1%85_%D1%81%D0%B5%D1%82%D0%B5%D0%B9.pdf (дата обращения: 23.11.2023).
28. ONF-Certified SDN Associate Exam (OCSA-2.0). URL: <https://opennetworking.org/wp-content/uploads/2020/09/ONF-Certified-SDN-Associate-2.0-Examination-Blueprint-2020-general-v2.pdf> (дата обращения: 23.05.2023).
29. Феофанов М.А., Евдакова Л.Н. Анализ развития рынка программно-конфигурируемых сетей // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики: материалы I Международной научно-практической конференции. Екатеринбург: Сибирский государственный университет телекоммуникаций и информатики, 2021. С. 281–284.

Получено 23.10.2023

Галич Сергей Владимирович, к.т.н., доцент кафедры телекоммуникационных систем (ТКС) Волгоградского государственного университета (ВолГУ). 400062, Российская Федерация, г. Волгоград, Университетский проспект, 100. Тел. +7 442 46-03-69. E-mail: galich.sv@volsu.ru

Сафонова Ольга Евгеньевна, к.э.н., доцент кафедры ТКС ВолГУ. 400062, Российская Федерация, г. Волгоград, Университетский проспект, 100. Тел. +7 442 46-03-69. E-mail: olgasafonova2504@mail.ru

KNOWLEDGE AND SKILLS FOR SOFTWARE-DEFINED NETWORKS MAINTENANCE ENGINEER

Galich S.V., Savonova O.E.

Volgograd State University, Volgograd, Russian Federation

E-mail: galich.sv@volsu.ru

In this article we analyze the Russian developments in the field of software-defined networks and software-defined wide area networks, professional standards and job vacancies in order to determine knowledge and skills required of specialists. We conclude that there is a lack of practical manuals for training network engineers, and suggest possible topics for laboratory exercises for educational textbooks. This article can be useful for teachers of educational institutions of vocational secondary education, higher education, supplementary education in the development of work programs of disciplines, lecture material and laboratory workshops in the field of software-defined networks, as well as for students of the educational institutions and for junior network engineers.

Keywords: SDN, SD-WAN, NFV, VNF, knowledge, skills, education

DOI: 10.18469/ikt.2023.21.3.06

Galich Sergei Vladimirovich, Volgograd State University, 100, Universitetsky Avenue, Volgograd, 400062, Russian Federation; Associated Professor of Telecommunication Systems Department, PhD in Technical Science. Tel. +7 842 46-03-69. E-mail: galich.sv@volsu.ru

Safonova Olga Evgenyevna, Volgograd State University, 100, Universitetsky Avenue, Volgograd, 400062, Russian Federation; Associated Professor of Telecommunication Systems Department, PhD in Economics. Tel. +7 442 46-03-69. E-mail: olgasafonova2504@mail.ru

References

1. Leonov V. Development of SD-WAN as an instrument for optimizing the network component of a distributed IT infrastructure. *Connect. Mir informacionnykh tekhnologij*, 2021, no. 9–10, pp. 87–89. (In Russ.)
2. Pleshakov D. Features of building corporate networks based on SD-WAN solutions. *Connect. Mir informacionnykh tekhnologij*, 2022, no. 9–10, pp. 88–90. (In Russ.)
3. Cisco Named a Leader in the IDC MarketScape for SD-WAN Infrastructure 2021. URL: <https://blogs.cisco.com/networking/cisco-named-a-leader-in-the-idc-marketscape-for-sd-wan-infrastructure-2021> (accessed: 20.05.2023).
4. Palo Alto Networks Hat Trick: 2022 Gartner Magic Quadrant for SD-WAN. URL: <https://www.paloaltonetworks.com/blog/2022/09/hat-trick-2022-gartner-mq-for-sd-wan/> (accessed: 20.05.2023).
5. 2022 SD-WAN Guide. URL: <https://drive.google.com/viewerng/viewer?url=https://www.communicationstoday.co.in/wp-content/uploads/2022/04/2022-SD-WAN-Guide.pdf&hl=en&pid=explorer&efh=false&a=v&chrome=false&embedded=true> (accessed: 20.05.2023).
6. Efimushkin V.A. et al. Role of SDN/NFV technologies in the digital economy infrastructure. Experience of testing and implementation. *Elektrosvyaz'*, 2018, no. 3, pp. 27–36. (In Russ.)
7. Pantyuhin L.K., Antonenko V.A. Development of a traffic distribution algorithm for SD-WAN solutions. *Programmnye sistemy i instrumenty: tematicheskij sbornik*. Moscow: MAKSPress, 2019, pp. 66–79. (In Russ.)

8. Comprehensive 5G development program in Russia. URL: https://www.company.rt.ru/upload/iblock/b79/Комплексная_программа_5G.pdf (accessed: 23.05.2023). (In Russ.)
9. Golyshko A. SDN as the final digital transformation of telecom. *Connect. Mir informacionnykh tekhnologij*, 2019, no. 4, pp. 74–77. (In Russ.)
10. Visitors of Tele2 stores receive better service thanks to SD-WAN technology. URL: <https://www.company.rt.ru/press/news/d460395> (accessed: 23.05.2023). (In Russ.)
11. Roslyakov A.V., Marykov M.V. Communication network as a NAAS cloud service. *Infokommunikacionnye tekhnologii*, 2022, vol. 20, no. 1, pp. 70–82. (In Russ.)
12. Kaspersky official site. URL: <https://www.kaspersky.ru/enterprise-security/sd-wan> (accessed: 23.05.2023). (In Russ.)
13. Eltex official site. URL: <https://eltex-co.ru> (accessed: 05.05.2023). (In Russ.)
14. Qtech official site. URL: <https://www.qtech.ru> (accessed: 05.05.2023). (In Russ.)
15. BI.ZONE official site. URL: <https://bi.zone/catalog/products/secure-sd-wan/?tb=tab3> (accessed: 23.05.2023). (In Russ.)
16. NSG official site. URL: <https://nsg.ru/products/bogatka.php> (accessed: 23.05.2023). (In Russ.)
17. Semenovych A.A., Laponina O.R. Comparative analysis of SDN controllers. *International Journal of Open Information Technologies*, 2018, no. 7, pp. 50–56. (In Russ.)
18. Galich S.V. et al. OpenDaylight SDN controller: a study of performance scaling on networks of different sizes. *Izvestiya YUFU. Tekhnicheskie nauki*, 2016, no. 9 (182), pp. 121–134. (In Russ.)
19. Security Code official site. URL: https://www.securitycode.ru/download_center/?section=stands (accessed: 23.05.2023). (In Russ.)
20. Kalmykov N.S. SDN Equipment and solutions market analysis. *Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki*, 2020, no. 1, pp. 116–124. (In Russ.)
21. Efimushkin V.A. et al. Comparative analysis of software-defined networks architectures and protocols. *Elektrosvyaz'*, 2014, no. 8, pp. 9–14. (In Russ.)
22. Efimushkin V.A. et al. Software-defined networks international standardization. *Elektrosvyaz'*, 2014, no. 8, pp. 3–9. (In Russ.)
23. Koryachko V.P., Perepelkin D.A. *Software-defined networks: Textbook*. Moscow: Goryachaya liniya-Telecom, 2021, 288 p. (In Russ.)
24. Smelyanskij R.L., Antonenko V.A. *Concepts of Software Management and Virtualization of Network Services in Modern Data Communication Networks: Textbook*. Moscow: KURS, 2020, 152 p. (In Russ.)
25. Goldshtejn B.S. et al. *Software-Defined Networks: OpenFlow protocol*. Saint-Petersburg: Prof. M.A. Bonch-Bruевич St. Petersburg State University of Telecommunications, 2018, 48 p. (In Russ.)
26. Bahareva N.F. et al. *Fundamentals of Software-Configurable Networks: Textbook*. Samara: PSUTI, 2015, 111 p. (In Russ.)
27. Koryachko V.P., Perepelkin D.A. Design and Support of Software-Defined Networks. URL: https://edu.rsreu.ru/res/specialities/disc_edu_programs/69157-edu_program-file-%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B3%D1%83%D1%80%D0%B8%D1%80%D1%83%D0%B5%D0%BC%D1%8B%D1%85_%D1%81%D0%B5%D1%82%D0%B5%D0%B9.pdf (accessed: 23.11.2023).
28. ONF-Certified SDNA Associate Exam (OCSA-2.0). URL: <https://opennetworking.org/wp-content/uploads/2020/09/ONF-Certified-SDN-Associate-2.0-Examination-Blueprint-2020-general-v2.pdf> (accessed: 23.05.2023).

29. Feofanov M.A., Evdakova L.N. Analysis of the market development of software-defined networks. *Infokommunikacionnye tekhnologii: aktualnye voprosy cifrovoj ehkonomiki: materialy i mezhdunarodnoj nauchno-prakticheskoy konferencii*. Ekaterinburg: Sibirskij gosudarstvennyj universitet telekommunikacij i informatiki, 2021, pp. 281–284. (In Russ.)

Received 23.10.2023

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 621.7

ТЕХНОЛОГИИ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ДЕФЕКТОВ ЦИЛИНДРИЧЕСКИХ ОБЪЕКТОВ

Захарова О.И.

Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ

E-mail: o.zaharova@psuti.ru

В настоящее время развитие компьютерного зрения позволяет решать множество задач обнаружения дефектов на различных промышленных объектах. Одним из перспективных направлений применения данных технологий является выявление несоответствий геометрических параметров на цилиндрических изделиях. Цель данной работы заключается в обзоре и систематизации современных методов компьютерного зрения, применяемых для решения задачи детектирования дефектов на вертикальных цилиндрических поверхностях. В рамках исследования был проведен анализ существующих подходов к извлечению пространственных характеристик объектов, включая методы стереовидения, пространственной фильтрации и 3D-реконструкции. Были рассмотрены алгоритмы выделения основных ориентиров на цилиндрической поверхности, что позволяет осуществлять привязку координатной системы и локализацию областей возможных дефектов. Также изучены методы оценки геометрических отклонений на поверхности, которые могут выступать в качестве критериев обнаружения дефектов. В результате проведенного анализа была предложена классификация методов компьютерного зрения, применимых для задачи выявления дефектов на цилиндрических объектах. Были определены перспективные направления дальнейших исследований в области повышения точности обнаружения дефектов за счет комбинации различных алгоритмов обработки изображений.

Ключевые слова: компьютерное зрение, обнаружение дефектов, цилиндрические объекты, стереовидение, 3D-реконструкция, геометрические отклонения

Введение

В настоящее время в промышленном производстве наблюдается стремительное развитие методов автоматизированного контроля качества с использованием передовых алгоритмов компьютерного зрения и глубокого машинного обучения. Особую актуальность приобретают задачи выявления различных дефектов на цилиндрических поверхностях, поскольку такие объекты, как трубы, баллоны, стержни, валы и другие детали подобной формы, широко используются в современной промышленности.

Эффективная идентификация несоответствий геометрических параметров цилиндрических изделий требует применения специализированных методов компьютерного зрения, позволяющих учитывать особенности изображений объектов данного типа. В частности, необходим учет искажений, вносимых кривизной поверхности, а также разработка алгоритмов, инвариантных к ракурсу наблюдения.

В данной статье предпринимается попытка систематизации существующих подходов к решению

задачи обнаружения дефектов на цилиндрических поверхностях с использованием методов компьютерного зрения и анализа цифровых изображений.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести обзор и сравнительный анализ методов восстановления трехмерной структуры цилиндрических объектов, включая стереоскопическое зрение, пассивную и активную 3D-реконструкцию, оптическое сканирование.

2. Рассмотреть подходы к выделению характерных особенностей и локальных дескрипторов на поверхности цилиндрических объектов в целях последующей локализации потенциальных дефектов.

3. Проанализировать алгоритмы оценки отклонений геометрических параметров локальных участков цилиндрической поверхности от эталонных значений для идентификации областей дефектов.

4. Предложить классификацию методов компьютерного зрения для решения задачи обнару-