УДК 004.42

А. В. Челнокова[1]✉

Система автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: chelalex1511@gmail.com

Аннотация. На обзор выносится проблема обеспечения подотчетности и неотказуемости объектов инфраструктуры предприятия, функционирующей на базе стека протоколов TCP/IP версии 4, посредством их автоматизированного развертывания и технологического сопровождения на каждом этапе жизненного цикла. С целью решения данной проблемы разработана система автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия. Утверждается, что представленная система позволяет предприятию реализовать автоматизацию настройки виртуальных машин, исключив при этом ошибки ручного конфигурирования. В качестве стека технологий выбрана система управления конфигурациями Ansible и инструмент управления внешними ресурсами Terraform. Тестовый стенд развертываемой инфраструктуры представлен на базе системы оркестрации Kubernetes. Областью применения представленной работы являются корпоративные вычислительные сети, функционирующие на основе стека протоколов TCP/IP.

Ключевые слова: инфраструктура как код, контейнеризация, оркестрация Kubernetes, мониторинг инфраструктуры, Ansible, Terraform

A. V. Chelnokova[1]✉

System of automated deployment and technological support of enterprise infrastructure

[1]National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: chelalex1511@gmail.com

Abstract. The problem of ensuring accountability and fault tolerance of enterprise infrastructure objects operating on the basis of TCP/IP version 4 protocol stack by means of their automated deployment and technological support at each stage of the life cycle is brought up for review. In order to solve this problem, a system of automated deployment and technological support of enterprise infrastructure is developed. It is argued that the presented system allows the enterprise to implement automation of virtual machine configuration, while eliminating manual configuration errors. Ansible configuration management system and Terraform external resource management tool are selected as the technology stack. A testbed of the deployed infrastructure is presented based on the Kubernetes orchestration system. The application area of the presented work is corporate computing networks operating on the basis of TCP/IP protocol stack.

Keywords: infrastructure as code, containerization, Kubernetes orchestration, infrastructure monitoring, Ansible, Terraform

Введение

Современные информационные технологии играют ключевую роль в функционировании предприятий, обеспечивая эффективность их работы и развитие. Однако

с ростом сложности и масштабов инфраструктуры увеличиваются и риски, связанные с безопасностью, производительностью и управлением. На фоне глобальных изменений, связанных с внедрением облачных технологий, контейнеризации и виртуализации, предприятия сталкиваются с необходимостью внедрения эффективных механизмов автоматизации развертывания и технологического сопровождения инфраструктуры. Эксперты организации Cloud Native Computing Foundation утверждают, что 41 % из всех организаций внедрили систему оркестрации Kubernetes, а в ближайшие 5 лет это число удвоится [1]. Проблематикой комплексной методологии интеллектуально-адаптивного управления информационной инфраструктурой предприятия занимается научная школа Басыни Е. А. [2, 3].

Эти механизмы должны обеспечивать стабильную работу всех компонентов инфраструктуры, соответствовать требованиям безопасности и быть устойчивыми к различным внешним и внутренним угрозам. Так в работах, представленных группой ученых Ammar Zeini, Ruth G. Lennon, Patrick Lennon, Abbas Medhi, Ranjan Walia, Syed Imran Abbas и Ankit Garg, исследуются проблемы безопасности подхода «Инфраструктура как код» (IaC) [4–6]. Несмотря на то, что данный подход предлагает значительные преимущества в развертывании и управлении инфраструктурой, он также создает серьезные проблемы безопасности, требующие тщательного анализа.

Развитие технологий контейнеризации и виртуализации оказало влияние на законодательный аспект данной области. Согласно требованиям ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», необходимо учитывать аспекты безопасности на всех этапах жизненного цикла программного обеспечения, включая проектирование, разработку, тестирование и эксплуатацию [7]. В связи с этим возникает необходимость не только в проектировании и разработке системы автоматизированного развертывания, но и в ее интеграции с существующими механизмами безопасности, что включает в себя обеспечение подотчетности всех действий, выполняемых в системе, а также неотказуемости, исключающей возможность отрицания выполненных операций. Эти аспекты играют ключевую роль в повышении надежности, отказоустойчивости и защищенности инфраструктуры.

В связи с существующей проблематикой становится актуальным решения класса задач по автоматизации развертывания и технологического сопровождения инфраструктуры предприятия.

Исследование предметной области

Несколько групп ученых занимаются исследованиями, посвященными вопросам обеспечения безопасности автоматизированных систем, включая подотчетность и неотказуемость операций. Так, в работе ученых Daniele Bringhenti, Guido Marchetto, Riccardo Sisto, Fulvio Valenza исследуется новый подход к конфигурированию и развертыванию графа функций безопасности, который позволил бы выбирать лучшие виртуальные функции безопасности среди большого пула, что делает принятие решений вручную невыполнимым [8]. Достоинства предложенного подхода заключаются в его способности оптимизировать процесс выбора и разверты-

вания виртуальных функций безопасности в условиях масштабных виртуальных сетей. Однако у предложенного решения имеются и недостатки. Во-первых, определение функциональной абстракции требует дальнейших исследований для выбора оптимального уровня детализации, что может усложнить процесс ее стандартизации и внедрения. Во-вторых, текущая реализация основывается на решении задач типа MaxSMT, что может оказаться недостаточно производительным для некоторых сценариев. Это указывает на необходимость разработки и внедрения альтернативных или дополнительных методов, таких как эвристики, для повышения общей производительности системы.

В исследовании, опубликованном учеными Ruiqi Zeng, Yiru Niu, Lanfei Qiao, предлагается новая технология построения автоматического развертывания и обновления многоэкземплярной системы микросервиса, позволяющая упростить развертывание и дальнейшее технологическое сопровождение инфраструктуры [9]. Достоинства предложенного подхода заключаются в его комплексности и автоматизации всех этапов работы с контейнеризованными микросервисными системами. Решение охватывает процесс разработки, сборки, развертывания и обновления, обеспечивая бесперебойную работу приложений даже в процессе их модернизации. Несмотря на вышеупомянутые достоинства, у работы имеются и недостатки. Во-первых, в исследовании уделено недостаточно внимания вопросам информационной безопасности, что особенно важно в условиях эксплуатации распределенных микросервисных систем. Во-вторых, тестирование предложенного решения проводится на ограниченном наборе сценариев, что может не полностью отражать все возможные сложности, возникающие при развертывании и обновлении в более масштабных и гетерогенных системах. Также работа недостаточно подробно рассматривает взаимодействие между компонентами платформы, что может вызывать вопросы относительно ее масштабируемости и интеграции с уже существующими инструментами разработки и управления.

В работе, опубликованной учеными Mohamed Oulaaffart, Remi Badonnel, Olivier Festor, исследуется подход автоматизации повышения безопасности облачных сервисов [10]. Достоинства работы заключаются в предложении системного подхода к автоматизации повышения безопасности облачных композитных сервисов в процессе миграции их ресурсов. Основное внимание уделено решению проблем, связанных с уязвимостями, возникающими при изменении конфигурации сервисов. Разработка алгоритмов для выбора адекватных механизмов безопасности на этапах до, во время и после миграции ресурсов подчеркивает глубокую проработку исследуемой темы. Недостатки работы связаны с отсутствием реализованного прототипа предложенного подхода, что ограничивает возможность оценки его производительности в реальных условиях. Использование иллюстративных примеров вместо тестирования на реальных сценариях снижает прикладную ценность результатов исследования.

Таким образом, в исследуемой области можно выделить несколько значимых проблем, а именно:

1) недостаточная подотчетность;

2) ошибки ручного конфигурирования;
3) отсутствие гарантий неотказуемости.

Постановка задачи

Целью настоящей работы является обеспечение подотчетности и неотказуемости объектов инфраструктуры предприятия, функционирующей на базе стека протоколов TCP/IP версии 4, посредством их автоматизированного развертывания и технологического сопровождения на каждом этапе жизненного цикла.

В ходе работы проведена ее декомпозиция на следующие задачи:

1) исследование предметной области;
2) проектирование системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия;
3) программная реализация спроектированной системы.

Предлагаемое решение

Системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия представляют собой комплексные информационно-технологические платформы, объединяющие инструменты автоматизации, методы оркестрации ресурсов, механизмы мониторинга и архитектурные решения для обеспечения эффективного управления жизненным циклом инфраструктуры. Эти системы играют ключевую роль в современных условиях, где требования к скорости развертывания, неотказуемости и подотчетности инфраструктуры становятся критически важными для успешного функционирования предприятий.

Метод автоматизированного развертывания инфраструктуры предприятия представляет собой последовательность взаимосвязанных этапов, направленных на обеспечение корректного создания и настройки инфраструктуры, а также последующего развертывания. На рис. 1 представлена блок-схема метода автоматизированного развертывания инфраструктуры предприятия.

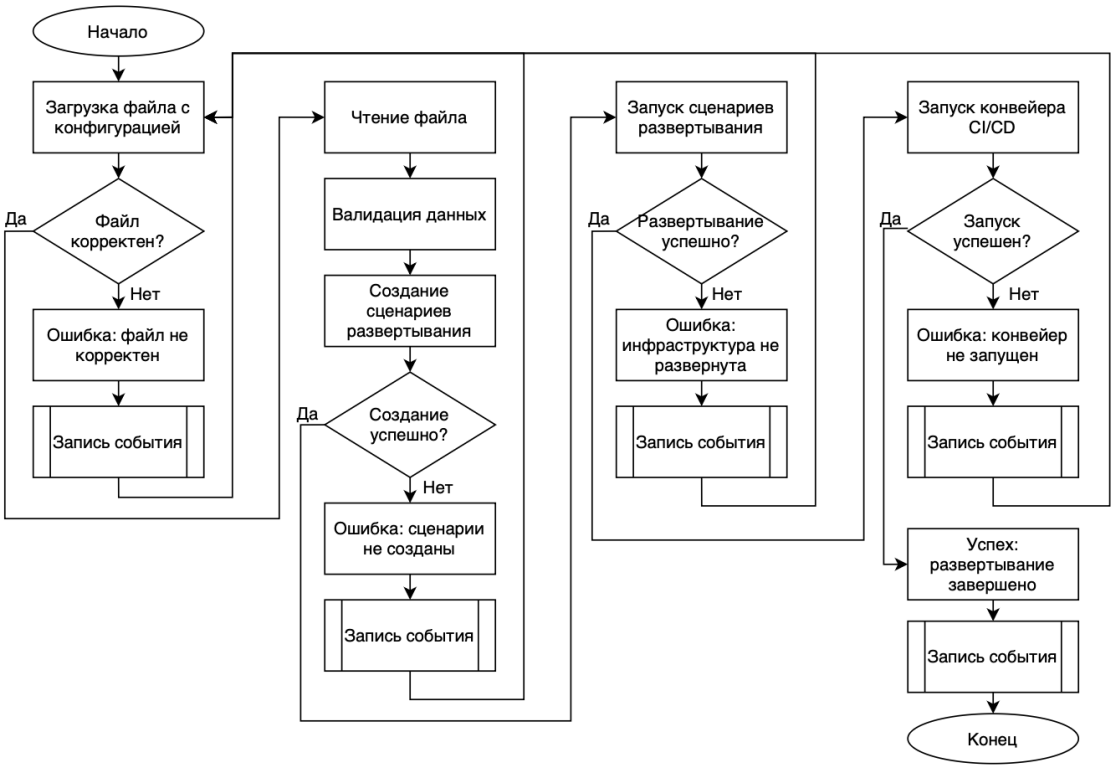

Рис. 1. Блок-схема метода автоматизированного развертывания инфраструктуры предприятия

На начальном этапе пользователь загружает файл конфигурации, содержащий описание инфраструктуры. Система проверяет корректность файла, включая его структуру и соответствие заданным требованиям. В случае обнаружения ошибок пользователь уведомляется и получает возможность загрузить исправленный файл.

После успешной проверки файла конфигурации система создает сценарии для развертывания. Если создание сценариев завершается неудачно, система предоставляет пользователю возможность исправить входные данные и повторить процесс.

Созданные сценарии последовательно выполняются для создания и настройки инфраструктуры. В случае возникновения ошибок на данном этапе система фиксирует их в событиях, уведомляет пользователя и предоставляет возможность повторного запуска сценариев после исправления параметров.

После успешного развертывания инфраструктуры система запускает конвейер CI/CD для развертывания сервисов. Если данный этап завершается с ошибкой, система регистрирует событие, уведомляет пользователя и предоставляет возможность повторного запуска после устранения неполадок.

В случае успешного завершения всех этапов система фиксирует результаты в событиях и уведомляет пользователя об успешном завершении процесса. Все

события регистрируются с помощью подпрограммы «Запись события». Ее блок-схема представлена на рис. 2.

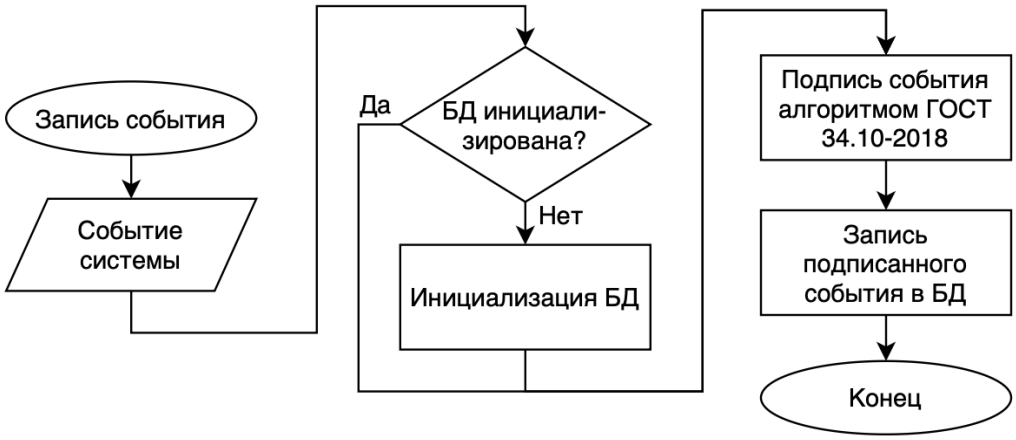

Рис. 2. Блок-схема подпрограммы «Запись события»

Формализованная подпрограмма представляет собой последовательность действий, направленных на обеспечение подотчетности и неотказуемости всех операций в системе. Подотчетность подразумевает возможность однозначно идентифицировать субъекта, ответственного за выполнение действия, а неотказуемость гарантирует, что субъект не сможет отрицать факт выполнения действия.

На начальном этапе система проверяет доступность и корректность базы данных. Если событие фиксируется впервые, то подпрограмма запускает процесс инициализации БД.

Подпрограмма принимает на вход событие системы, который содержит информацию о произошедшем действии, например, успешное развертывание инфраструктуры или ошибка в конвейере CI/CD. Запись включает в себя информацию о пользователе, время события и его описание.

Событие подписывается с использованием криптографического алгоритма ГОСТ 34.10-2018. Подпись связывает лог с конкретным пользователем, что обеспечивает неотказуемость: пользователь не сможет отрицать выполнение действия, так как подпись подтверждает его участие.

Подписанное событие сохраняется в базу данных. Это позволяет в дальнейшем использовать его для анализа, аудита и подтверждения факта выполнения действия. Проверка подписи событий осуществляется в соответствии с методом, представленным на рис. 3.

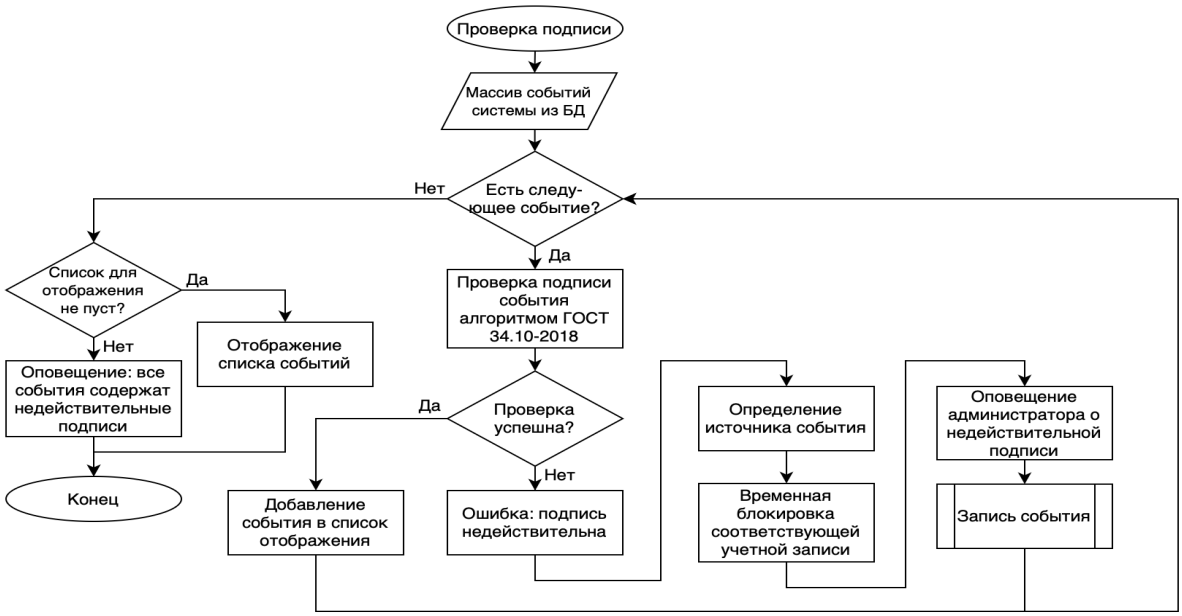

Рис. 3. Блок-схема метода проверки подписи события

На начальном этапе на вход подается массив событий из базы данных, которые содержат описание действия, метаданные (время, идентификатор пользователя и т. д.) и криптографическую подпись. Подпись была создана с использованием закрытого ключа пользователя, соответствующего открытому ключу, хранящемуся в системе (см. подпрограмму «Запись события»). В случае успешной проверки подпись признается валидной, что подтверждает неизменность данных с момента их подписания и участие пользователя в выполнении действия.

Если подпись успешно проверена, событие отображается в пользовательском интерфейсе, и процесс завершается успешно. Однако в случае обнаружения невалидной подписи подпрограмма переходит к обработке ошибки. На этом этапе система идентифицирует учетную запись пользователя, связанную с событием, и временно блокирует ее для предотвращения потенциально вредоносных действий. Одновременно с этим администраторы системы уведомляются о недействительной подписи, что позволяет оперативно реагировать на возможные угрозы. Само событие уведомления администраторов и блокировки пользователя фиксируется с помощью подпрограммы «Запись события» для последующего анализа и расследования.

В завершение метод отображает список действительных записей событий или в противном случае оповещает пользователя о том, что все события оказались с недействительными подписями.

На рис. 4 представлен снимок экрана, демонстрирующий работоспособность данной системы. На экране отображен результат анализа конфигурационного файла, а также выведено сообщение «Конфигурация успешно принята!»,

что свидетельствует о корректной работе системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия.

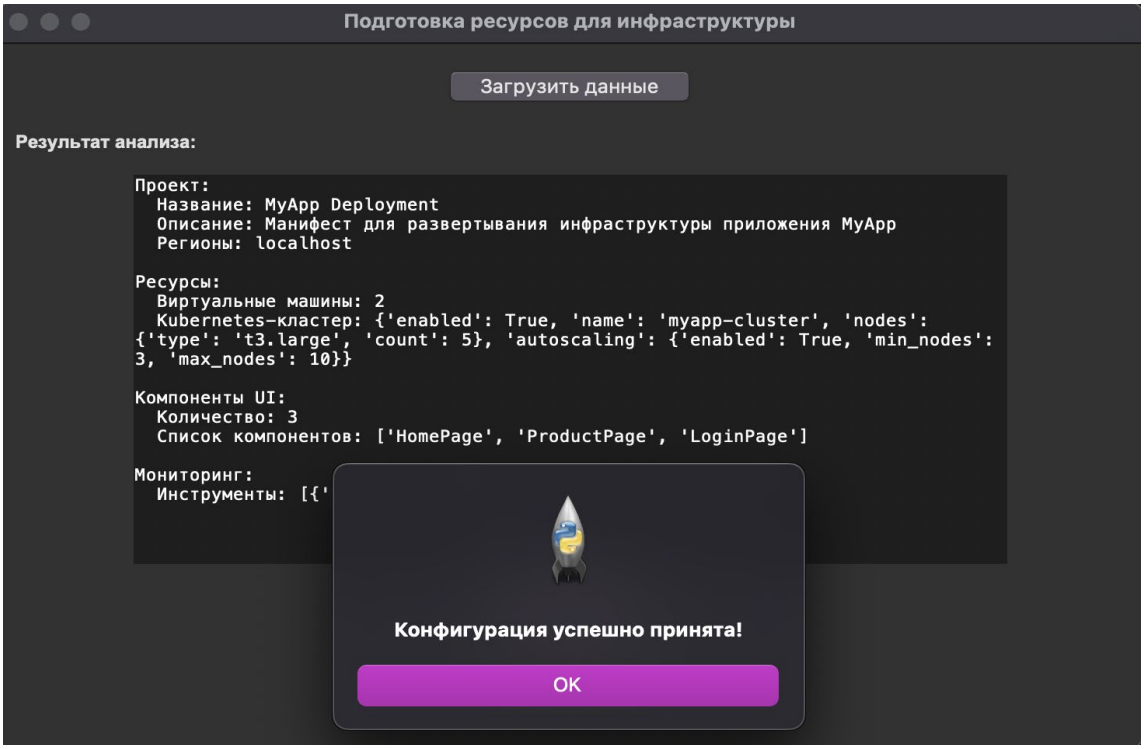

Рис. 4. Демонстрация работоспособности системы

Система демонстрирует модульность и гибкость, предоставляя возможность расширения функциональности, например, интеграции с инструментами Terraform и Ansible для автоматизации развертывания и настройки инфраструктуры. Таким образом, программная реализация сочетает в себе удобство взаимодействия с пользователем, эффективность обработки данных и потенциал для дальнейшего развития, что делает ее надежным решением для управления инфраструктурой предприятия.

Заключение

В рамках данной работы была предложена система, автоматизирующая развертывание инфраструктуры предприятия с дальнейшим технологическим сопровождением, которая была программно реализована и успешно продемонстрировала свою работоспособность.

Практическая значимость работы состоит в повышении безопасности инфраструктуры предприятия и в устранении ошибок ее ручного конфигурирования.

Новизна данной работы состоит в предложении новых методов автоматизированного развертывания инфраструктуры и ее дальнейшего сопровождения, повышающего подотчетности и неотказуемости объектов инфраструктуры предприятия на каждом этапе жизненного цикла.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. The voice of Kubernetes experts report 2024: the data trends driving the future of the enterprise // Cloud Native Computing Foundation URL: https://www.cncf.io/blog/2024/06/06/the-voice-of-kubernetes-experts-report-2024-the-data-trends-driving-the-future-of-the-enterprise/ (дата обращения: 28.03.2025).

2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия – Comprehensive Methodology of Intelligently Adaptive Management of an Enterprise Information Infrastructure / Е. А. Басыня. - Текст : непосредственный // Защита информации. Инсайд – Zasita informacii. Inside. - 2021. - № 5 (101). - С. 16-25.

3. Basinya E. A. Enterprise information infrastructure management [Electronic resource] / E. A. Basinya, D. S. Khudiakov // International multi-conference on industrial engineering and modern technologies (FarEastCon) : [proc.], Vladivostok, 6–9 Oct. 2020. – Vladivostok : IEEE, 2020. – 6 p. - Mode of access: https://ieeexplore.ieee.org/document/9271463/authors#authors. - Title from screen - DOI: 10.1109/FarEastCon50210.2020.9271463.

4. Zeini A., Lennon R. G., Lennon P. Securing Infrastructure as Code (IaC) through DevSecOps: A Comprehensive Risk Management Framework //2023 Cyber Research Conference-Ireland (Cyber-RCI). – IEEE, 2023. – С. 1-11.

5. Mehdi A., Walia R. Terraform: Streamlining Infrastructure Deployment and Management Through Infrastructure as Code // 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). – IEEE, 2023. – С. 851-856.

6. Abbas S. I., Garg A. Integrating Emerging Technologies with Infrastructure as Code in Distributed Environments // 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC). – IEEE, 2024. – С. 1138-1144.

7. ГОСТ Р 56939–2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования = Information protection. Secure software development. General requirements : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст : введен взамен ГОСТ Р 56939-2016 : дата введения 2024-12-20. – Москва : Стандартинформ, 2024. – 36 с. ; 29 см. – Текст : непосредственный.

8. Bringhenti D. et al. A novel approach for security function graph configuration and deployment // 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). – IEEE, 2021. – С. 457-463.

9. Zeng R., Niu Y., Qiao L. A Novel Construction Technology of Microservice Multi-Instance System Automatic Deployment and Upgrade // 2023 International Conference on Networking and Network Applications (NaNA). – IEEE, 2023. – С. 674-679.

10. Oulaaffart M., Badonnel R., Festor O. Towards Automating Security Enhancement for Cloud Services // 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). – IEEE, 2021. – С. 692-696.