12. *Saihua Cai, Yingwei Zhao, Jiaao Lyu, Shengran Wang, Yikai Hu, Mengya Cheng, Guofeng Zhang.* DDP-DAR: Network intrusion detection based on denoising diffusion probabilistic model and dual-attention residual network, *Neural Networks*, 2025, Vol. 184, 107064. ISSN 0893-6080. Available at: https://doi.org/10.1016/j.neunet.2024.107064.
13. *Wang Z., Guan Z., Liu X., Qiao M., Sun X., Li J*. Diffusion–Attention Traffic Generation: Traffic Generation Based on the Fusion of a Diffusion Model and a Self-Attention Mechanism, *Electronics*, 2025, 14, 1977. Available at: https://doi.org/10.3390/electronics14101977.
14. *Kotenko I., Saenko I., Lauta O., Kribel' A.* Metod rannego obnaruzheniya kiberatak na osnove integratsii fraktal'nogo analiza i statisticheskikh metodov [Method of early detection of cyberattacks based on the integration of fractal analysis and statistical methods], *Pervaya milya* [First Mile], 2021, No. 6 (98), pp. 64-71. DOI 10.22184/2070-8963.2021.98.6.64.70. EDN KRIUAD.
15. *Jonathan Ho, Ajay Jain, and Pieter Abbeel.* Denoising diffusion probabilistic models, *In Proceedings of the 34th International Conference on Neural Information Processing Systems (NIPS '20). Curran Associates Inc., Red Hook, NY, USA, 2020*, Article 574, pp. 6840-6851.
16. *Yang Song and Stefano Ermon.* Generative modeling by estimating gradients of the data distribution, *Proceedings of the 33rd International Conference on Neural Information Processing Systems. Curran Associates Inc., Red Hook, NY, USA, 2019*, Article 1067, pp. 11918-11930.
17. *Leevy J.L., Khoshgoftaar T.M.* A survey and analysis of intrusion detection models based on CSE-CSE-CIC-IDS2018 Big Data, *J Big Data*, 2020, 7, 104. Available at: https://doi.org/10.1186/s40537-020-00382-x.
18. *Moustafa N., Slay J.* The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, *Inf. Secur. J. A Glob. Perspect*, 2016, 25, pp. 18-31.
19. *Kadam V., & Verma R.* A Critical Review of Performance Metrics in Intrusion Detection Systems, *Journal of Engineering Science and Technology Review*, 2025, 18 (1), pp. 199-209.
20. *Morehead A., Cheng J.* Geometry-complete diffusion for 3D molecule generation and optimization, *Commun Chem*, 2024, 7, 150. Available at: https://doi.org/10.1038/s42004-024-01233-z.

**Балыбердин Алексей Викторович** – Финансовый университет при Правительстве РФ; e-mail: balyberdinav@gmail.com; г. Москва, Россия; аспирант; https://orcid.org/0009-0005-1264-9290.

**Balyberdin Alexey Viktorovich** – Financial University under the Government of the Russian Federation; e-mail: balyberdinav@gmail.com; Moscow, Russia; graduate student; https://orcid.org/0009-0005-1264-9290.

УДК 004.056.5 DOI 10.18522/2311-3103-2026-3-18-31

**К.С. Дунюшкина, И.В. Машкина**

## РАЗРАБОТКА МОДЕЛИ УГРОЗ В ИНФОРМАЦИОННОЙ СРЕДЕ ГИПЕРКОНВЕРГЕНТНОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ПОСТРОЕНИЯ СЦЕНАРИЕВ МНОГОКОМПОНЕНТНЫХ АТАК

*Целью данного исследования является разработка формализованной модели угроз безопасности информации гиперконвергентной инфраструктуры (Hyper-Converged Infrastructure – HCI) на основе построения сценариев многокомпонентных атак с использованием EPC-моделирования (Event-driven Process Chain (EPC), с учетом архитектурных особенностей гетерогенной HCI, каскадного характера распространения угроз, специфических объектов воздействия угроз и мультитенантной модели доступа. В работе применены метод системного анализа, принцип методологии ARIS (Architecture of Integrated Information Systems), а также метод формализации сценариев многокомпонентных атак. Технической базой послужили: методика ФСТЭК России по оценке угроз безопасности информации, реестр угроз безопасности информации и сведения об уязвимостях из банка данных угроз ФСТЭК и международной базы (NVD). В результате исследования выявлены ключевые архитектурные особенности гиперконвергентной инфраструктуры как объекта защиты: тесная интеграция компонентов (вычислений, хранения, сети), программная определяемость компонентов, мультитенантность, каскадный характер распространения угроз. Предложена классификация нарушителей по уровню привилегий. Разработаны два формализованных сценария многокомпонентных атак на специфические объекты воздействия угроз в HCI. Сценарии представлены в виде EPC-диаграмм, что позволяет не только визуализировать действия нарушителя, наглядно представить используемые им тактики и техники, но и численно оценить вероятности реализации сценариев. На основе исследования структурно-функциональных характеристик HCI и с учетом модели оценки угроз ФСТЭК разработана обобщенная модель угроз гиперконвергентной инфраструктуры с примерами заполнения для некоторых объектов воздействия. Научная новизна исследования*

*заключается в адаптации метода EPC-моделирования угроз для гиперконвергентной инфраструктуры с учетом ее архитектурных особенностей и мультитенантности, а также в разработке формализованных сценариев атак, отражающих реальные цепочки эксплуатации уязвимостей, опубликованных в 2025-2026 годах.*

*Гипреконвергентная инфраструктура (HCI); модель угроз; EPC-диаграмма; сценарий атаки; нарушитель; виртуальная машина; контейнер; Kubernetes.*

**K.S. Dunyushkina, I.V. Mashkina**

## DEVELOPING A THREAT MODEL FOR THE INFORMATION ENVIRONMENT OF HYPERCONVERGED INFRASTRUCTURE BASED ON CONSTRUCTING MULTI-COMPONENT ATTACK SCENARIOS

*This study aims to develop a formalized information security threat model for hyperconverged infrastructure by constructing multi-component attack scenarios using the EPC (Event-driven Process Chain) methodology, taking into account the architectural features of HCI, the cascading nature of threat propagation, specific security objects, and the multitenant access model. The method of system analysis, the principle of the ARIS (Architecture of Integrated Information Systems) methodology, as well as the method of formalization of multicomponent attack scenarios are applied in the work. The technical basis was the FSTEC of Russia's methodology for assessing information security threats, the register of information security threats, and vulnerability information from the FSTEC Threat databank and the International Database (NVD). The study revealed the key architectural features of hyperconverged infrastructure as an object of protection close integration of components (computing, storage, and network), software definability of components, multitenancy, cascading nature of threat propagation. A classification of violators by privilege level is proposed. Two formalized scenarios of multicomponent attacks on specific threat targets in HCI have been developed. The scenarios are presented in the form of EPC diagrams, which allows not only to visualize the actions of the violator, visually present the tactics and techniques used by him, but also to numerically assess the probabilities of the scenarios. Based on the study of the structural and functional characteristics of HCI and taking into account the FSTEC threat assessment model, a generalized threat model of hyperconverged infrastructure with examples of filling for some affected objects has been developed. The scientific novelty of the study lies in the adaptation of the EPC threat modeling method for hyperconverged infrastructure, taking into account its architectural features and multitenancy, as well as in the development of formalized attack scenarios reflecting real vulnerability exploitation chains published in 2025-2026.*

*Hyperconverged infrastructure (HCI); threat model; EPC diagram; attack scenario; intruder; VM; container; Kubernetes.*

**Введение.** В условиях цифровой трансформации требования к отказоустойчивости и масштабируемости ИТ-инфраструктуры вступают в противоречие с классическими архитектурами и даже конвергентными [1]. Гетерогенная гиперконвергентная инфраструктура объединяет: программно-определяемые вычислительные мощности (Software-Defined Compute – SDC), программно-определяемое хранилище данных (Software-Defined Storage – SDS) и программно-определяемые сетевые ресурсы (Software-Defined Network – SDN), а также технологии гипервизорной виртуализации и контейнеризации с оркестратором, – в едином физическом кластере, управляемом из центральной консоли. HCI позволяют решить проблемы отказоустойчивости и масштабируемости. Термин гиперконвергенция отражает принципиальное отличие HCI от традиционной трехзвенной архитектуры, где системы хранения и сетевое оборудование существуют как отдельные компоненты, что усложняет масштабирование и требует узкоспециализированных специалистов для обслуживания каждого из них. Такая конвергентная инфраструктура (CI) объединяет эти компоненты в предварительно интегрированные комплексы, но сохраняет их логическую обособленность и зависимость от выделенных систем хранения данных. В гиперконвергентной инфраструктуре все необходимые виртуализированные ресурсы работают автономно внутри унифицированных модулей – узлов, каждый из которых сочетает в себе вычислительные мощности, хранилище и сетевые функции. Однако интеграция компонентов HCI в единую программно-определяемую платформу, обеспечивая преимущества в эксплуатации, приводит к появлению специфических угроз безопасности информации, поскольку границы ответственности между всеми компонентами становятся программно-определяемыми, а традиционный периметр защиты – размытым.

Можно выделить следующие особенности гиперконвергентной инфраструктуры как объекта защиты: все компоненты, входящие в состав архитектуры, управляются программно, что расширяет поверхность атаки за счет интерфейсов управления (API). Поскольку компоненты функционируют как единое целое, реализация угроз приводит к каскадному распространению их воздействия на все составляющие инфраструктуры. HCI является мультитенантной, то есть имеет возможность одновременно обслуживать множество пользователей (тенантов) с изоляцией их ресурсов. Еще одна немаловажная особенность – это сложность верификации состояний: динамическая природа гиперконвергентной инфраструктуры затрудняет контроль целостности и неизменности конфигураций [2].

Исследования последних лет показали, что до 73% инцидентов в сложных инфраструктурных системах затрагивают более одного уровня декомпозиции, именно поэтому требуется разработка специализированных моделей угроз [3], которые будут учитывать перекрестные зависимости между компонентами архитектуры HCI.

**Обоснование необходимости разработки специализированной модели угроз для HCI.** Ключевым методическим документом в Российской Федерации, определяющим порядок и содержание работ по определению угроз безопасности информации, является «Методика оценки угроз безопасности информации», утвержденная ФСТЭК России от 05.02.2021 года [4]. Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация которых возможна в информационно-телекоммуникационных инфраструктурах, центрах обработки данных и облачных инфраструктурах. Гиперконвергентная инфраструктура, которая сочетает в себе признаки как центров обработки данных, так и облачных сред, полностью попадает под область применения данной Методики.

Необходимость разработки модели угроз для HCI может быть обусловлена следующими факторами. Один из факторов – отсутствие сведений об отраслевых документах. Методика ФСТЭК предусматривает возможность разработки отраслевых, ведомственных методик оценки угроз, которые учитывают особенности функционирования систем и сетей в соответствующих областях деятельности, но при условии, что они не будут противоречить положениям настоящей Методики. Гиперконвергентные инфраструктуры являются относительно новым классом систем и требуют адаптации общих подходов к своей специфике. Следующий фактор – это каскадный характер угроз: интеграция множества компонентов гиперконвергеной инфраструктуры чаще всего приводит к тому, что реализация угрозы в одном компоненте неизбежно влияет на доступность другого, что требует дополнительного анализа межкомпонентных взаимодействий. Еще одним важным фактором является то, что HCI содержит программно-определяемые интерфейсы управления: API – интерфейсы гиперконвергентной инфраструктуры создают дополнительные векторы атак, которые, в свою очередь, требуют учета при моделировании угроз. Кроме того, в HCI традиционное деление на внешнего и внутреннего нарушителя является неприменимым, так как тенанты обладают легитимным доступом к некоторой части ресурсов и могут действовать как изнутри, так и снаружи инфраструктуры. Еще одним фактором, обуславливающим разработку специализированной модели угроз, является то, что HCI очень часто используются для периферийных вычислений, то есть узлы кластера могут размещаться вне защищенных дата центров, что создает дополнительные риски физического доступа к оборудованию. Такие развертывания требуют особого внимания к физической безопасности в модели угроз, учитывающей возможность компрометации оборудования через прямой физический доступ.

Методика ФСТЭК представляет собой наиболее полный и систематизированный подход к оценке угроз безопасности информации. Этот подход является обязательным для применения в государственных информационных системах (ГИС), информационных системах персональных данных (ИСПДн), значимых объектах критической информационной инфраструктуры (ЗО КИИ), а также рекомендованным для иных систем.

Данная Методика предписывает следующий порядок оценки угроз безопасности информации: инвентаризация систем и сетей, определение негативных последствий от реализации угроз, определение возможных объектов воздействия, определение источников угроз, оценка способов реализации угрозы, оценка возможности реализации угрозы и определение актуальности, оценка сценариев реализации угроз безопасности информации в

системах и сетях. Методика позволяет использовать общий перечень угроз из банка данных угроз ФСТЭК, применять описания векторов компьютерных атак из международных баз, таких как CAPEC, ATT&CK, OWASP.

Таким образом, Методика создает основу для разработки специализированных моделей многокомпонентных угроз, применяемых к гиперконвергентной инфраструктуре, при этом позволяя адаптировать общие положения к специфике HCI при сохранении преемственности и непротиворечивости.

**Модель нарушителя в гиперконвергентной инфраструктуре.** Модель угроз информационной безопасности по Методике ФСТЭК [4] включает в себя модель нарушителя, которая позволяет оценить его возможный потенциал. В настоящей модели предлагается классифицировать нарушителей не по признаку физического нахождения относительно периметра, а по уровню привилегий, поскольку в условиях мультитенантной HCI-среды граница между «внутри» и «снаружи» становится условной.

К первой категории нарушителя при классификации по уровню привилегий относится субъект – киберпреступник, не имеющий легитимного доступа к гиперконвергентной инфраструктуре, но получивший возможность действовать от имени легитимного тенанта в результате компрометации учетных данных пользователя (тенанта), используя, например, фишинг, перехват или подбор данных, эксплуатируя уязвимости клиентского программного обеспечения (ПО), которое тенант использует для доступа к инфраструктуре, а также при возможности использования украденных сертификатов или сессионных токенов. Данный нарушитель обладает следующими возможностями: имеет доступ к имеющимся у тенанта виртуальным ресурсам (вычислительным мощностям, хранилищам данных или сетевым сервисам) в пределах выделенных этому тенату квот, имеет возможность развертывания собственного ПО и использования легитимных каналов связи с гиперконвергентной инфраструктурой для дальнейшего развития атаки, но при этом у нарушителя будут некоторые ограничения, которые накладываются политиками изоляции тенантов – отсутствие доступа к ресурсам других тенантов и к плоскости управления HCI.

Ко второй категории относится легитимный тенант HCI, действующий исключительно в рамках предоставленных ему прав, но при этом потенциально способный использовать их в ущерб инфраструктуре или другим тенантам. Данная категория включает в себя как добросовестных пользователей, которые могут стать жертвой атаки, в этом случае их учетная запись может быть использована нарушителем, отнесенным к первой категории, так и недобросовестных тенантов, намерено нарушающих условия использования ресурсов HCI.

Тенант второй категории характеризуется следующими признаками: наличием легитимной учетной записи, доступом к строго определенному набору ресурсов, в соответствии с его правами, отсутствием доступа к инфраструктуре за пределами выделенного ему сегмента. Потенциальные деструктивные действия такого нарушителя могут включать в себя использование имеющихся у тенанта ресурсов для атак на информационные системы, попытки преодолеть изоляцию для получения доступа к ресурсам других тенантов, а также возможность проведения атак на интерфейсы управления с целью получения повышенных привилегий или несанкционированного доступа (НСД) к ресурсам.

Третья категория – суперпользователь – лица, обладающие высокими привилегиями в инфраструктуре HCI. К данной категории относятся администраторы гипервизорной виртуализации и оркестратора, администраторы SDS, SDN и SDC, администраторы безопасности HCI, а также DevOps – инженеры, которые имеют доступ к управляющим консолям и плоскостям управления.

Пользователи, относящиеся к данной категории, обладают следующими возможностями: имеют полный доступ ко всем виртуальным ресурсам всех тенантов (в соответствии с RBAC), имеют возможность управления конфигурацией инфраструктуры, т.е. могут создавать, удалять и проводить модификацию ВМ, сетей и хранилищ, имеют доступ к журналам аудита и мониторинга, имеют возможность изменения политик безопасности и параметров средств защиты информации; часть суперпользователей имеет физический доступ к серверному оборудованию в соответствии со своими правами. Угрозы со стороны суперпользователей могут быть как преднамеренными, – инсайдеры, действующие в корыстных целях, так и непреднамеренными, например, ошибки в конфигурации или нарушения технологических процессов.

Предлагаемая классификация позволяет более точно описывать модель нарушителя информационной безопасности для гиперконвергентной инфраструктуры, учитывая при этом распределённый характер доступа (удаленная работа тенантов), наличие программно-определяемых интерфейсов управления как потенциальных векторов атак и специфику компрометации учетных записей, как начального этапа сложных атак.

**Объекты воздействия в гиперконвергентной инфраструктуре.** В соответствии с Методикой ФСТЭК [4], одним из этапов оценки угроз безопасности информации (УБИ) является определение возможных объектов воздействия угроз. В этом случае, под объектом воздействия понимается компонент системы или сети, на который направлено деструктивное воздействие при реализации многокомпонентной атаки. Для HCI характерны специфические объекты воздействия, которые обусловлены ее архитектурой и программно-определяемыми компонентами [5].

Одним из ключевых компонентов HCI является гипервизор, который, в свою очередь, обеспечивает изоляцию ВМ и распределение вычислительных ресурсов, объектами воздействия на данном уровне будут являться ядро, модули, драйверы, конфигурационные файлы и параметры настройки гипервизора, локальные или удаленные интерфейсы управления гипервизором, а также область резервирования и восстановления. Реализация угроз на этом уровне может привести к нарушению изоляции ВМ, а также к получению НСД к данным всех тенантов или полной компрометации узла HCI.

Следующим рассматриваемым компонентом HCI является программно-определяемое хранилище. В гиперконвергентной инфраструктуре функция хранения данных реализуется программно, поверх локальных дисков узлов кластера. Объектами воздействия здесь являются: распределенная файловая система, метаданные, описывающие размещение данных на узлах, механизмы репликации и отказоустойчивости, образы ВМ, интерфейсы доступа к самому хранилищу, а также механизмы шифрования данных на уровне хранилища и клиента. Угрозы, такие как DoS-атаки, повреждение или шифрование файлов киберпреступником, а также НСД, для SDS могу приводить к нарушению доступности, целостности и конфиденциальности данных.

Следующий компонент – программно-определяемая сеть. Сетевой уровень HCI обеспечивает связанность компонентов и изоляцию тенантов. В этом случае так же есть свои специфические объекты воздействия, а именно: контроллер программно-определяемой сети (SDN-контроллер), виртуальные коммутаторы и маршрутизаторы, политики сетевой безопасности, встроенные или внешние балансировщики нагрузки, а также шлюзы для подключения к внешним сетям. Атаки на компоненты SDN приводят к нарушению доступности сетевых сервисов, перехвату трафика, а также к преодолению изоляции между тенантами.

Особенностью HCI является то, что управление инфраструктурой может быть федеративным, то есть распространяться на всю инфраструктуру, поэтому компрометация плоскости управления дает киберпреступнику полный контроль над всей HCI. Компрометация etcd – модуля Kubernetes, приводит к утрате данных о состоянии кластера, нарушению целостности конфигураций, а также к раскрытию всех секретов кластера.

Следующий компонент – это узлы кластера (физические серверы), они являются строительными блоками всей инфраструктуры, объединяющими в себе SDS, SDN и SDC. Каждый узел состоит из множества отдельных специфических компонентов, на каждом из узлов работает Kubelet – агент Kubernetes, который управляет подами.

Следующие важные компоненты – это поды и контейнеры, которые в Kubernetes представляют собой наименьшие развертываемые единицы, они содержат в себе один или несколько контейнеров с общими томами и сетевым пространством имен. В этом случае ключевым специфическим компонентом являются сервисные аккаунты, они используются для аутентификации подов при обращении к API-серверу, каждый под монтирует токен своего сервис-аккаунта.

Угрозами для подов являются: внедрение вредоносного кода в под, (может осуществляться через уязвимости приложений или образов), кража данных, компрометация сервис-аккаунта, выход из пода на узел кластера (через эксплуатацию уязвимостей контейнеризации) или создание привилегированного пода. В контексте безопасности важно отметить, что узлы могут быть размещены вне защищенных дата-центров, а именно на периферии сети. Такая особенность создает дополнительные риски физического доступа [6].

В HCI существуют различные типы учетных записей, которые также являются специфическими объектами воздействия, эти учетные записи пронизывают все уровни инфраструктуры и включают в себя: учетные записи тенантов, администраторов HCI, доменные учетные записи, учетные записи приложений, а также сервисные аккаунты Kubernetes. Управление этими компонентами должно включать многофакторную аутентификацию и строгие политики паролей, ведь компрометация или получение повышенных привилегий может привести к необратимым последствиям.

Управление гиперконвергентной инфраструктурой осуществляется через централизованную консоль оркестратора, координирующую работу всех его компонентов. К ним относятся: API-сервер (kube-apiserver), распределенное хранилище etcd, kube-scheduler – компонент, отвечающий за размещение новых виртуальных машин и контейнеров на физических узлах с учетом доступных ресурсов и политик, kube-controller-manager – набор контроллеров (Node Controller, Deployment Controller, ReplicaSet Controller и др.), которые обеспечивают автоматическое поддержание желаемого состояния всех информационных сервисов. К ним относится: база данных конфигураций, веб-интерфейс администратора, службы аутентификации, службы (сервисы) kubernetes, а также политики безопасности. Компрометация плоскости управления предоставляет нарушителю полный контроль над всей инфраструктурой HCI [7].

Каждый тенант обладает определенным, выделенным ему набором виртуальных ресурсов, которые также могут выступать объектами воздействия, к ним можно отнести: ВМ и их образы, виртуальные диски и данные на них, виртуальные сети тенанта, его учетные данные для доступа к HCI, приложения и сервисы, развёрнутые самим тенантом. Особенностью таких объектов является двойственная ответственность за их безопасность, так как часть рисков лежит на разработчике HCI, например, риски, связанные с изоляцией и доступностью, а часть на самом тенанте – это конфигурация приложений.

Гиперконвергентная инфраструктура представляет собой сложную многоуровневую систему, где все компоненты тесно интегрированы и функционируют как единое целое на каждом узле кластера, именно поэтому при реализации угроз на одном уровне, например, при компрометации гипервизора, поверхность угрозы распространяется на другие уровни, вызывая при этом каскадные последствия [8].

**Применение графического стандарта моделирования процессов для разработки сценариев многокомпонентных атак.** Поскольку в соответствии с Методикой ФСТЭК в модель угроз могут быть включены только те угрозы, для которых построены сценарии реализации, возникает необходимость их разработки. Известны работы [9, 10], в которых для моделирования угроз в промышленной сети предложено использовать принципы методологии ARIS [11]. Разработка EPC-диаграмм сценариев угроз позволяет отразить на одной схеме все значимые этапы многокомпонентной атаки. Данный подход позволяет просмотреть четко обозначенные события как результаты развития атаки. EPC-диаграмма сценария угрозы представляет собой отображение (сверху вниз) последовательности выполнения техник, начиная от исходного действия киберпреступника до достижения им цели – нарушение одного из свойств безопасности информации объекта воздействия [12].

Рассмотрим построение сценария атаки в HCI с использованием уязвимости CVE-2026-23990, обнаруженной 21 января 2026 года, со значением CVSS равным 5,3 балла, BDU:2024-00973 (CVE-2024-21626), со значением CVSS равным 8,6 балла, CVE-2024-41110 со значением CVSS равным 9,9 балла (представлен на Рисунке 1). В результате успешной реализации уязвимости CVE-2026-23990 атакующий получает возможности обойти имитацию RBAC Kubernetes и выполнить запросы API с привилегиями учётной записи оператора. Уязвимость CVE-2026-23990 возникает при настройке Flux Operator с поставщиком OIDC, который выдаёт токены без ожидаемых утверждений (например, email и groups) или при настройке пользовательских выражений CEL, кроме того, библиотека Kubernetes client-go не добавляет заголовки имитации к запросам API. Для устранения данной уязвимости рекомендуется выполнить обновление Flux Operator до более поздней версии [17].

В результате реализации уязвимости BDU:2024-21626 Нарушитель может встроить специально сформированный образ контейнера, скрипт которого устанавливает process.cwd на путь в хостовой файловой системе, доступный через утечку файлового дескриптора. Это позволяет нарушителю выполнять произвольные команды с правами root, получить доступ

ко всем данным на хосте и в других контейнерах, использовать хост как плацдарм для дальнейших атак. Для устранения данной уязвимости рекомендуется устанавливать обновления программного обеспечения из доверенных источников [18].

Реализация уязвимости CVE-2024-41110 в Docker Engine позволяет обойти плагины авторизации. Нарушитель может получить доступ к чувствительным ресурсам, таким как облачные токены, учётные записи сервисов Kubernetes и другие привилегированные идентификаторы, а также незаконный контроль над критической инфраструктурой [19].

Проведем численную оценку вероятности реализации атаки, описанной выше.

Исходные данные и допущения. В соответствии с Методикой оценки угроз и статьёй [12]:

Для операторов XOR вероятность исхода «Уязвимость найдена» принимается равной 0,5 (при отсутствии данных о существовании уязвимости).

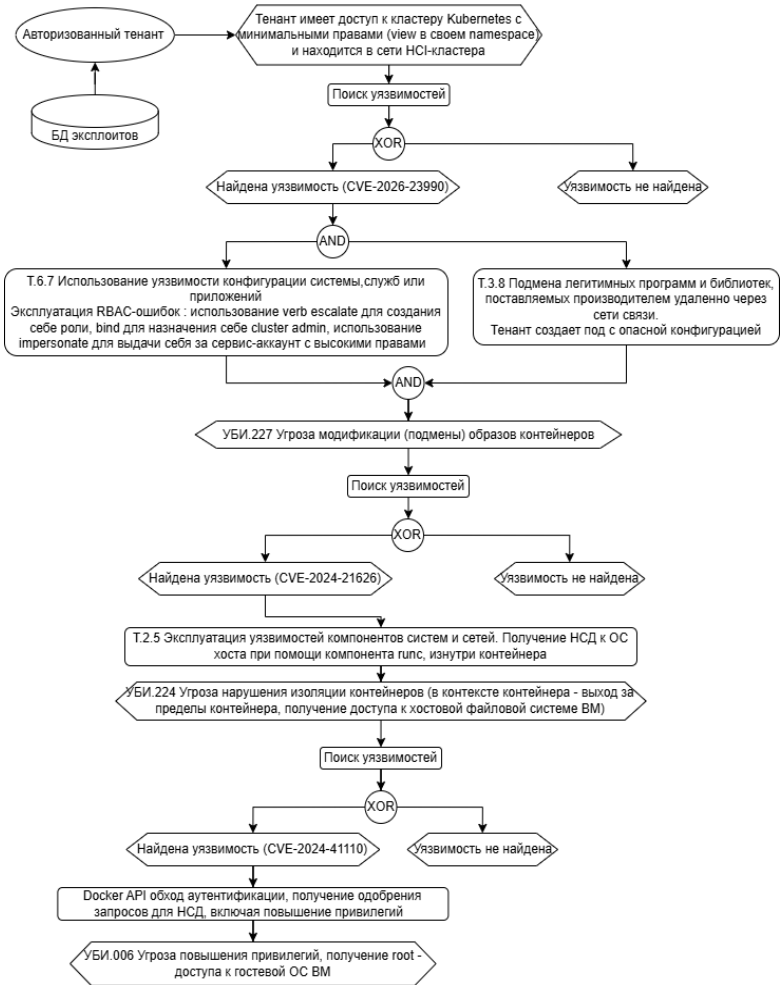


*Рис. 1. EPC-модель сценария атаки в HCI с использованием уязвимостей CVE 2026-23990 и BDU: 2024-21626*

Для техник, не имеющих ассоциированных CVE (T.3.8, T.6.7, T.2.5), вероятность успеха принимается равной 0,5.

Для техник с известными CVE вероятность успеха равна нормированному значению CVSS Base Score (Base Score / 10).

Для оператора OR вероятность успеха вычисляется по формуле (1):

$$P_{OR} = 1 - \prod_{i=1}^{n}(1 - p_i), \quad (1)$$

В случае «Уязвимость не найдена» сценарий прекращается (вероятность 0).

В табл. 1 представлены значения уязвимостей и техник (на основе CVSS 3.x).

Таблица 1

**Значения уязвимостей и техник**

| № | Элемент | CVE / Тип | Base Score | Нормированная вероятность |
|---|---|---|---|---|
| 1 | XOR1 (уязвимость найдена) | Условие | — | 0,5 |
| 2 | CVE-2026-23990 | Уязвимость | 5.3 (HIGH) | **0,53** |
| 3 | T.3.8, T.6.7 | Техника (нет CVE) | — | **0,5** |
| 4 | **Итого этап 1** | | | 0,5×0,53×0,5=0,1325 |
| 5 | XOR2 (уязвимость найдена) | Условие | — | 0,5 |
| 6 | CVE-2024-21626 | Уязвимость | 8.6 (HIGH) | **0,86** |
| 7 | **Итого этап 2** | | | 0,5×0,86=0,43 |
| 8 | XOR3 (уязвимость найдена) | Условие | — | 0,5 |
| 9 | CVE-2024-41110 | Уязвимость | 9.9 (CRITICAL) | **0,99** |
| 10 | **Итого этап 3** | | | 0,5×0,99=0,495 |

Произведем расчет вероятности по этапам:

*Этап 1* (УБИ.227):

$$P_1 = 0{,}5 \times 0{,}53 \times 0{,}5 = 0{,}1325$$

*Этап 2* (УБИ.224):

$$P_2 = 0{,}5 \times 0{,}86 = 0{,}43$$

Последовательное выполнение этапов 1 и 2:

$$P_{12} = P_1 \times P_2 = 0{,}1325 \times 0{,}43 = 0{,}056975$$

*Этап 3* (XOR3):

$$P_3 = 0{,}5 \times 0{,}99 = 0{,}495$$

Итоговая вероятность сценария:

$$P_{сц} = P_{12} \times P_3$$

$$P_{сц} = 0{,}056975 \times 0{,}495 = 0{,}028202625$$

$$P_{сц} \approx 0{,}0282$$

На рис. 2 представлен вариант построения сценария атаки в HCI с использованием уязвимости BDU: 2025-02354 (CVE 2025-22224) со значением CVSSv3 равным 9,3 балла, который является логическим продолжением сценария, представленного выше. В результате проведения успешной атаки нарушитель с локальными привилегиями на ВМ может выполнить код от имени процесса VMX на хосте, то есть в самом гипервизоре. В марте 2025 года компания Broadcom зафиксировала случаи использования уязвимости в реальных атаках, однако не раскрыла деталей о методах эксплуатации или группах нарушителей, использующих эту уязвимость.

Уязвимость возникает из-за состояния гонки, то есть система проверяет состояние ресурса и использует его без обеспечения согласованности между двумя действиями. Процесс VMX имеет повышенные привилегии, что позволяет атакующему потенциально скомпрометировать всю хост-систему. Данная уязвимость особенно опасна в многопользовательских средах, где на одном хосте работает несколько ВМ. Важно, что для данных уязвимостей не существует обходных решений, поэтому для их предупреждения необходимо своевременно устанавливать обновления [13].

Для предотвращения подобных атак рекомендуется изолировать ESXi-хосты, ограничить права администраторов, предоставлять им минимально необходимые привилегии, а также использовать двухфакторную аутентификацию для повышения защиты учетных записей [14–16].

В табл. 2 представлены значения уязвимостей и техник (на основе CVSS 3.x) для сценария, описанного выше.

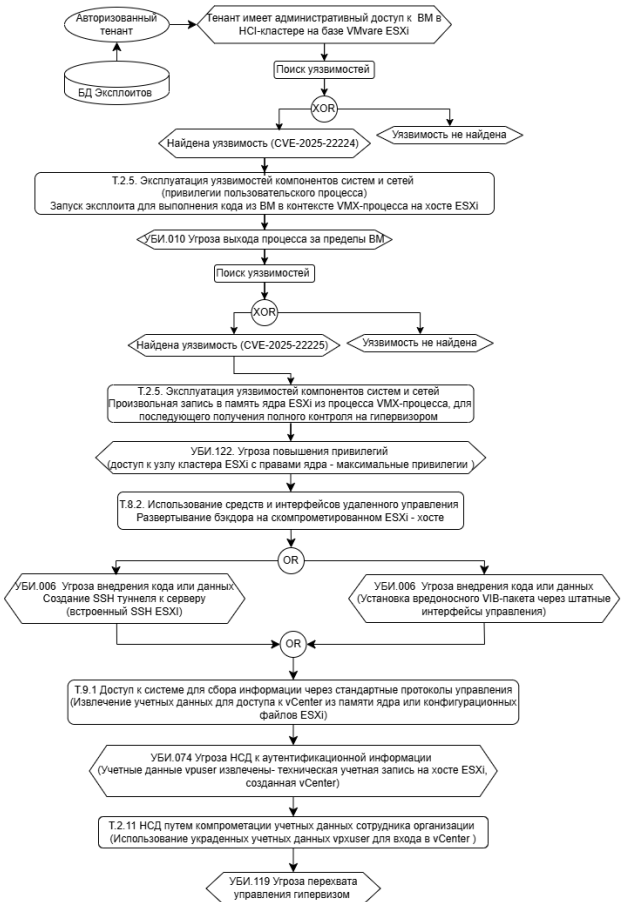


*Рис. 2. EPC-модель сценария атаки в HCI с использованием уязвимости BDU: 2025-02354 (CVE 2025-22224)*

Таблица 2

**Значения уязвимостей и техник**

| № | Элемент | CVE / Тип | Base Score | Нормированная вероятность |
|---|---|---|---|---|
| 1 | XOR1 (уязвимость найдена) | Условие | — | 0,5 |
| 2 | CVE-2025-22224 | Уязвимость | 8.2 (HIGH) | **0,82** |
| 3 | **Итого этап 1** | | | 0,5×0,82=0,41 |
| 4 | XOR2 (уязвимость найдена) | Условие | — | 0,5 |
| 5 | CVE-2025-22225 | Уязвимость | 8.1 (HIGH) | 0,81 |
| 6 | **Итого этап 2** | | | 0,5×0,81=0,405 |
| 7 | T.8.2 | Техника (нет CVE) | — | **0,5** |
| 8 | SSH-туннель (OR) | Техника (нет CVE) | — | 0,5 |
| 9 | VIB-пакет (OR) | Техника (нет CVE) | — | 0,5 |
| 10 | **OR1** | Оператор | — | $1-(1-0{,}5)^2=0{,}75$ |
| 11 | T.9.1 | Техника (нет CVE) | — | **0,5** |
| 12 | T.2.11 | Техника (нет CVE) | — | **0,5** |

Произведем расчет вероятности по этапам:
*Этап 1* (УБИ.010):

$$P_1 = 0{,}5\times0{,}82 = 0{,}41$$

*Этап 2* (УБИ.122):

$$P_2 = 0{,}5\times0{,}81 = 0{,}405$$

Последовательное выполнение этапов 1 и 2:

$$P_{12} = P_1 \times P_2 = 0{,}41 \times 0{,}405 = 0{,}16605$$

*Этап 3* (T.8.2 и OR1):

$$P_3 = 0{,}5 \times 0{,}75 = 0{,}375$$

*Этап 4* (T.9.1 и T.2.11):

$$P_4 = 0{,}5 \times 0{,}5 = 0{,}25$$

Итоговая вероятность сценария:

$$P_{сц} = P_{12} \times P_3 \times P_4$$

$$P_{сц} = 0{,}16605 \times 0{,}375 \times 0{,}25 = 0{,}0155671875$$

$$P_{сц} \approx 0{,}0156$$

Поскольку каждая платформа HCI российского производителя, (например, гиперконвергентные решения: ОТВ эв3 от ООО «Открытые технологии виртуализации», «Алькор» от компании Звезда, vStack и другие), имеет свои особенности разработки, свои специфические уязвимости, для каждого решения должны разрабатываться свои сценарии и конкретная модель угроз.

В общей теории моделирования обобщенная модель отражает свойства, характеристики и связи, существенные для решаемой задачи. Термин может использоваться для описания *универсальных* подходов к анализу объекта или системы как *основа* для построения моделей в информационном поле.

Ниже представлена табличная форма обобщенной модели угроз гиперконвергентной инфраструктуры *с примерами заполнения* для некоторых объектов воздействия платформы VMware, поскольку необходимые данные об особенностях оркестраторов и уязвимостях продуктов российского производителя отсутствуют. В модели заполнены строки в соответствии с EPC-моделями сценариев, разработанных в рамках настоящего исследования, а также для ранее разработанного сценария атаки в HCI с использованием уязвимости BDU:2025-0322031 (CVE-2025-24514), представленного в [20].

Таблица 3

**Обобщённая модель угроз HCI с примерами заполнения**

| **Объект воздействия угрозы** | **Источник угрозы** | **Способ реализации** | **Возможности реализации (CVE / уязвимости)** | **Негативные последствия (CIA)** |
|---|---|---|---|---|
| **Гипервизор и плоскость управления** (Компонент - Гипервизор VMware ESXi) | Авторизованный тенант (тенант-нарушитель) | T2.5, T3.5, T4.2, T8.2, T9.1, T2.11/ УБИ.010, УБИ.122, УБИ.006, УБИ.074, УБИ.119 | CVE-2025-22224 (привилегии пользовательского процесса – выход за пределы ВМ), CVE-2025-22225 (произвольная запись в память ядра ESXi из VMX-процесса) | К: компрометация аутентификационной информации (vruser), доступ к данным всех ВМ<br>Ц: внедрение вредоносного VIB-пакета, модификация ядра ESXi<br>Д: полный контроль над гипервизором, отказ в обслуживании |
| **Программно-определяемая сеть (SDN)** (Компонент - Ingress-контроллер) | Киберпреступник (хакер) | T3.15, T4.1/ УБИ.006, УБИ.074, УБИ.128 | CVE-2025-24514 (недостаточная проверка входных данных в обработке аннотации в контроллере ingress-nginx.) | К: полное раскрытие конфиденциальной информации, в том числе паролей и ключей API<br>Ц: полная компрометация целостности данных<br>Д: полная блокировка доступности ресурса, что может привести к сбоям в работе критически важных приложений |

| | | | | |
|---|---|---|---|---|
| **ВМ** | Авторизованный тенант (тенант-нарушитель) | Т.6.7, Т3.8, Т.2.5 /УБИ.227, УБИ.224, УБИ 006 | CVE 2026-23990 (обход аутентификацию RBAC Kubernetes и выполнять запросы API с привилегиями учётной записи оператора) CVE-2024-41110 (обходид плагины авторизации (AuthZ) при определённых условиях, повышение привилегий) | К: раскрытие данных, доступ к секретам Kubernetes через повышение привилегий. Ц: возможность изменять конфигурации, внедрять вредоносный код, управлять виртуальными машинами Д: блокировка или шифрование виртуальных машин, отказ в обслуживании, потеря контроля над инфраструктурой |
| **Плоскость упаврления (Control Plane) Модули оркестратора** | … | … | … | … |
| **Программно-определяемое хранилище (SDS)** | … | … | … | … |
| **Узлы кластера (физические серверы)** | … | … | … | … |
| **Поды и контейнеры** | … | … | … | … |
| **Учетные записи и доступ Pod definition file, Service definition file** | … | … | … | … |

Обобщенная модель угроз безопасности информации HCI разработана на основе исследования объекта защиты и его стуктурно-функциональных характеристик. Модель применима для разработки модели угроз любому конкретному кластеру HCI потому, что содержит перечень всех возможных объектов воздействия угроз в гетерогенной HCI, обоснован перечень потенциально возможных источников угроз, предложена методика построения возможных сценариев (применимая к любому кластеру). Сценарии угроз некоторым объектам воздействия приведены *для примера*, поскольку в модель угроз по Методике ФСТЭК могут быть занесены только *актуальные* угрозы, то есть те, для которых разработаны сценарии. А сценарии могут быть разработаны только с учетом характеристик конкретной HCI: какое решение гиперконвергентной виртуализации используется в кластере, какое решение Kubernetes, при использовании технологии VDI, продукт какого производителя. От этого будет зависеть перечень уязвимостей, эксплуатируемых нарушителем, сами возможные векторы атак.

Разработанные авторами сценарии угроз показывают уязвимости, характерные для платформы зарубежного производителя; сведения об уязвимостях решений российских разработчиков пока не появились.

Представлены примеры сценариев атак на гиперконвергентную инфраструктуру на базе VMware ESXi. Модель демонстрирует характерный для современных технических атак каскадный принцип, в котором отражается последовательное повышение привилегий, горизонтальное и вертикальное перемещение внутри инфраструктуры с использованием цепочек уязвимостей и штатных инструментов администрирования.

**Заключение.** Гиперконвергентная инфраструктура, объединяющая в себе программно-определяемые вычисления, хранение и сети в единой платформе, обладает специфическими особенностями, влияющими на безопасность. Такие особенности требуют отказа от традиционного деления нарушителей на «внешних» и «внутренних» в пользу представленной в исследовании классификации по уровню привилегий.

В результате проведенного исследования решена актуальная научно-практическая задача – разработка формализировнной модели угроз безопасности информации для гиперконвергентной инфраструктуры, на основе построения сценариев многокомпонентных атак с использованием EPC-моделирования, определен перечень специфических объектов HCI, проведен анализ возможных нарушителей, в качестве примера представлены три возможных сценария реализации многокомпонентных атак.

Преимущество EPC-моделирования сценариев угроз потенциально возможным объектам воздействия HCI заключается не только в возможности визуализировать действия нарушителя, наглядно представить используемые им тактики и техники, но и в возможности численно оценить вероятности реализации сценариев, что делает возможным получить значение риска в количественном выражении в дальнейших исследованиях.

Дальнейшее исследование предполагает так же разработку полной модели угроз гиперконвергентной инфраструктуры для какой-либо конкретной платформы виртуализации российского производителя с оркестратором Kubernetes (гетерогенная HCI) на основе сведений о возможных специфических уязвимостях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. *Azeem S.A., Sharma S.K.* Study of Converged Infrastructure & Hyper Converge Infrastructre As Future of Data Centre // International Journal of Advanced Research in Computer Science. Computer Science, Engineering. – May-June 2017. – Vol. 8, No. 5.
2. *Егоров В.Б.* Программное определение сети в конвергентной и гиперконвергентной инфраструктурах // Системы и средства информатики. – 2023. – Т. 33, № 1. – С. 105-113.
3. Объем, прогноз и основные тенденции мирового рынка гиперконвергентной инфраструктуры на 2025-2037 гг. – researchnester.com. – URL: https://www.researchnester.com/ru/reports/hyper-converged-infrastructure-market/4792 (дата обращения: 09.02.2026).
4. Методический документ от 05.02.2021г.: федеральная служба по техническому и экспортному контролю методический документ методика оценки угроз безопасности информации. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 09.03.2025).
5. *Сагалаев Ю.Р., Ромашкова О.Н.* Анализ гиперконвергентной вычислительной инфраструктуры для хранения о обработки данных высоконагруженных информационных систем // Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2021. – № 6. – С. 118-124.
6. *Шуватова, Е.А., Мартыненко Т.В.* Анализ методов определения эффективной архитектуры программных систем // Информатика, управляющие системы, математическое и компьютерное моделирование (ИУСМКМ-2024): XV Международная научно-техническая конференция в рамках X Международного Научного форума Донецкой Народной Республики, Донецк, 29-30 мая 2024 года. – Донецк: Донецкий национальный технический университет, 2024. – С. 125-130.
7. *Нестеренко А.А., Влацкая И.В.* Безопасность контейнеризации: уязвимости Docker и Kubernetes. разбор CVE, Escape-атак и неправильных конфигураций // Актуальные вопросы обеспечения комплексной безопасности: Матер. национальной научно-практической конференции с международным участием, посвященной 35-летию МЧС России и 95-летию Оренбургского ГАУ. – Оренбург, 2025. – С. 360-363.
8. *Горелов П.Д., Лысов Д.А., Морозова К.В., Денисеня Д.И*. Разработка эффективных методов защиты контейнеров программного обеспечения kubernetes // Безопасность информационного пространства – 2024: Сб. материалов XXIII всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – Курган, 2025. – С. 190-195.
9. *Машкина И.В., Гарипов И.Р.* Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Безопасность информационных технологий, [S.I.]. – 2019. – Т. 26, № 4. – С. 6-20. – ISSN 2074-7136. – DOI: http://dx.doi.org/10.26583/bit.2019.4.01.
10. *Заид Алкилани М.О., Машкина И.В.* Разработка сценариев атак для оценки угроз нарушения информационной безопасности в промышленной сети // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 1 (58). – С. 96-109. – DOI 10.48612/jisp/xvkx-k619-3f2z 25.04.2024. – EDN: PDNEWN.
11. *Шеер А.В.* ARIS-моделирование бизнес-процессов. – М.: Вильямс, 2000. – 175 с.
12. *Машкина И.В., Уразаев А.М.* Метод разработки базы знаний сценариев угроз для системы реагирования на инциденты (IRP) // Известия ЮФУ. Технические науки. – 2024. – № 5 (241). – С. 79-88. – DOI 10.18522/2311-3103-2024-5-79-88.

13. NIST - National vulnerability database NVD CVE-2025-22224. – URL: https://nvd.nist.gov/vuln/ detail/CVE-2025-22224 (дата обращения: 09.03.2026).
14. *Попов А.Д.* Контейнерная виртуализация как основа облачных автоматизированных систем // Промышленные АСУ и контроллеры. – 2024. – № 9. – С. 23-33.
15. *Зима В.М., Крюков Р.О.* Подход к безопасному использованию контейнерной виртуализации в критически важных автоматизированных системах // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2022. – № 11–12 (173–174). – С. 89-99.
16. *Королев А.С., Быркov В.А., Рачишкин А.А*. Технология docker: контейнеризация и развертывание проекта // Образование в XXI веке: проблемы и перспективы: Сб. статей XV Международной научно-практической конференции. – Пенза, 2023. – С. 69-73.
17. NIST - National vulnerability database NVD CVE-2025-23990. – URL: https://nvd.nist.gov/vuln/ detail/CVE-2026-23990 (дата обращения: 09.03.2026).
18. NIST - National vulnerability database NVD CVE-2024-05045. – URL: https://nvd.nist.gov/vuln/ detail/CVE-2024-21626 (дата обращения: 09.03.2026).
19. NIST - National vulnerability database NVD CVE-2024-41110. – URL: https://nvd.nist.gov/ vuln/detail/CVE-2024-41110 (дата обращения: 09.03.2026).
20. *Машкина И.В., Дунюшкина К.С.* Анализ гиперконвергентной инфраструктуры как объекта защиты // Вопросы кибербезопасности. – 2026. – № 1 (71). – С. 42-50. – DOI: 10.21681/2311-3456-2026-1-42-50.

REFERENCES

1. *Azeem S.A., Sharma S.K.* Study of Converged Infrastructure & Hyper Converge Infrastructre As Future of Data Centre, *International Journal of Advanced Research in Computer Science. Computer Science, Engineering,* May-June 2017, Vol. 8, No. 5.
2. *Egorov V.B.* Programmnoe opredelenie seti v konvergentnoy i giperkonvergentnoy infrastrukturakh [Software definition of a network in converged and hyperconverged infrastructures], *Sistemy i sredstva informatiki* [Systems and Computer Science Tools], 2023, Vol. 33, No. 1, pp. 105-113.
3. Ob"em, prognoz i osnovnye tendentsii mirovogo rynka giperkonvergentnoy infrastruktury na 2025-2037 gg. [Volume, forecast and main trends of the global hyperconverged infrastructure market for 2025-2037]. researchnester.com. Available at: https://www.researchnester.com/ru/reports/hyper-converged-infrastructure-market/4792 (accessed 09 February 2026).
4. Metodicheskiy dokument ot 05.02.2021g.: federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu metodicheskiy dokument metodika otsenki ugroz bezopasnosti informatsii [Methodological document dated 02/05/2021: Federal Service for Technical and Export Control methodological document methodology for assessing information security threats]. Available at: https://fstec.ru/dokumenty/ vse-dokumenty/spetsialnye-normativnyedokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed 09 March 2025).
5. *Sagalaev Yu.R., Romashkova O.N*. Analiz giperkonvergentnoy vychislitel'noy infrastruktury dlya khraneniya o obrabotki dannykh vysokonagruzhennykh informatsionnykh sistem [Analysis of hyperconverged computing infrastructure for data storage and processing of highly loaded information systems], *Sovremennaya nauka: Aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki* [Modern science: Actual problems of theory and practice. Series: Natural and Technical Sciences], 2021, No. 6, pp. 118-124.
6. *Shuvatova, E.A., Martynenko T.V.* Analiz metodov opredeleniya effektivnoy arkhitektury programmnykh sistem [Analysis of methods for determining the effective architecture of software systems], *Informatika, upravlyayushchie sistemy, matematicheskoe i komp'yuternoe modelirovanie (IUSMKM-2024): XV Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya v ramkakh X Mezhdunarodnogo Nauchnogo foruma Donetskoy Narodnoy Respubliki, Donetsk, 29-30 maya 2024 goda* [Informatics, control systems, mathematical and Computer modeling (IUSMKM-2024): XV International Scientific and Technical Conference within the framework of the X International Scientific Forum of the Donetsk People's Republic, Donetsk, May 29-30, 2024]. Donetsk: Donetskiy natsional'nyy tekhnicheskiy universitet, 2024, pp. 125-130.
7. *Nesterenko A.A., Vlatskaya I.V.* Bezopasnost' konteynerizatsii: uyazvimosti Docker i Kubernetes. razbor CVE, Escape-atak i nepravil'nykh konfiguratsiy [Containerization security: vulnerabilities of Docker and Kubernetes. analysis of CVE, Escape attacks and incorrect configurations], *Aktual'nye voprosy obespecheniya kompleksnoy bezopasnosti: Mater. natsional'noy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem, posvyashchennoy 35-letiyu MCHS Rossii i 95-letiyu Orenburgskogo GAU* [Topical issues of ensuring integrated security: Materials of the national scientific and practical conference with international participation dedicated to the 35th anniversary of the Russian Ministry of Emergency Situations and the 95th anniversary of the Orenburg State Agrarian University]. Orenburg, 2025, pp. 360-363.

8. *Gorelov P.D., Lysov D.A., Morozova K.V., Denisenya D.I.* Razrabotka effektivnykh metodov zashchity konteynerov programmnogo obespecheniya kubernetes [Development of effective methods for protecting kubernetes software containers], *Bezopasnost' informatsionnogo prostranstva – 2024: Sb. materialov XXIII vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh* [Information space security – 2024: Proceedings of the XXIII All-Russian scientific and practical conference of students, postgraduates and young scientists]. Kurgan, 2025, pp. 190-195.
9. *Mashkina I.V., Garipov I.R.* Razrabotka ERS-modeley ugroz narusheniya informatsionnoy bezopasnosti avtomatizirovannoy sistemy upravleniya tekhnologicheskimi protsessami [Development of EPC models of threats to information security violations of an automated process control system], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], [S.I.], 2019, Vol. 26, No. 4, pp. 6-20. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.01.
10. *Zaid Alkilani M.O., Mashkina I.V.* Razrabotka stsenariev atak dlya otsenki ugroz narusheniya informatsionnoy bezopasnosti v promyshlennoy seti [Development of attack scenarios for assessing threats to information security in an industrial network], *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Problems of information security. Computer systems], 2024, No. 1 (58), pp. 96-109. DOI 10.48612/jisp/xvkx-k619-3f2z 25.04.2024. EDN: PDNEWN.
11. *Sheer A.V.* ARIS-modelirovanie biznes-protsessov [ARIS-modeling of business processes]. Moscow: Vil'yams, 2000, 175 p.
12. *Mashkina I.V., Urazaev A.M.* Metod razrabotki bazy znaniy stsenariev ugroz dlya sistemy reagirovaniya na intsidenty (IRP) [A method for developing a knowledge base of threat scenarios for an incident response system (IRP)], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 5 (241), pp. 79-88. DOI 10.18522/2311-3103-2024-5-79-88.
13. NIST - National vulnerability database NVD CVE-2025-22224. Available at: https://nvd.nist.gov/ vuln/ detail/CVE-2025-22224 (accessed 09 March 2026).
14. *Popov A.D.* Konteynernaya virtualizatsiya kak osnova oblachnykh avtomatizirovannykh sistem [Container virtualization as the basis of cloud automated systems], *Promyshlennye ASU i kontrollery* [Industrial Automated Control Systems and Controllers], 2024, No. 9, pp. 23-33.
15. *Zima V.M., Kryukov R.O.* Podkhod k bezopasnomu ispol'zovaniyu konteynernoy virtualizatsii v kriticheski vazhnykh avtomatizirovannykh sistemakh [An approach to the safe use of container virtualization in critically important automated systems], *Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskie sredstva protivodeystviya terrorizmu* [Issues of defense technology. Series 16: Technical means of countering terrorism], 2022, No. 11–12 (173–174), pp. 89-99.
16. *Korolev A.S., Byrkov V.A., Rachishkin A.A.* Tekhnologiya docker: konteynerizatsiya i razvertyvanie proekta [Docker technology: containerization and project deployment], *Obrazovanie v XXI veke: problemy i perspektivy: Sb. statey XV Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Education in the XXI century: problems and prospects. Collection of articles of the XV International Scientific and Practical Conference]. Penza, 2023, pp. 69-73.
17. NIST - National vulnerability database NVD CVE-2025-23990. Available at: https://nvd.nist.gov/ vuln/detail/CVE-2026-23990 (accessed 09 March 2025).
18. NIST - National vulnerability database NVD CVE-2024-05045. Available at: https://nvd.nist.gov/ vuln/detail/CVE-2024-21626 (accessed 09 March 2025).
19. NIST - National vulnerability database NVD CVE-2024-41110. Available at: https://nvd.nist.gov/ vuln/detail/CVE-2024-41110 (accessed 09 March 2025).
20. *Mashkina I.V., Dunyushkina K.S.* Analiz giperkonvergentnoy infrastruktury kak ob"ekta za-shchity [Analysis of hyperconverged infrastructure as an object of protection], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2026, No. 1 (71), pp. 42-50. DOI: 10.21681/2311-3456-2026-1-42-50.

**Дунюшкина Ксения Сергеевна** – Уфимский университет науки и технологий; e-mail: dynushkinaks@yandex.ru; г. Уфа, Россия; тел.: 89177837868; кафедра вычислительной техники и защиты информации; аспирант.

**Машкина Ирина Владимировна** – Уфимский университет науки и технологий; e-mail: profmashkina@mail.ru; г. Уфа, Россия; тел.: +79279277089; кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

**Dunyushkina Kseniya Sergeevna** – Ufa University of Science and Technology; e-mail: dynushkinaks@yandex.ru; Ufa, Russia; phone: +79177837868; the Department of Computer Engineering and Information Security; postgraduate student.

**Mashkina Irina Vladimirovna** – Ufa University of Science and Technology; e-mail: profmashkina@mail.ru; Ufa, Russia; phone: +79279277089; the Department of Computer Science and Information Security; dr. of eng. sc.; professor.