ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.5

Проблемы и решения обеспечения безопасности в мультиоблачных и гибридных средах

А.Н. Секунов
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассматриваются ключевые вызовы информационной безопасности, порождаемые эксплуатацией мультиоблачных и гибридных инфраструктур. Актуальность темы продиктована масштабной миграцией корпоративных и государственных информационных сервисов в децентрализованные среды. Цель работы — системный анализ специфических угроз, присущих распределённым системам, и выработка практических рекомендаций по укреплению их киберустойчивости. На основе методов моделирования угроз и сравнительного анализа установлено, что традиционная периметровая защита в гетерогенных средах неэффективна. Предложен и обоснован авторский подход к построению архитектуры безопасности, опирающийся на концепцию «Нулевого доверия» (Zero Trust) и применение систем автоматизированного управления конфигурациями (CSPM). Новизна исследования состоит в систематизации векторов атак, характерных для гибридных моделей, и адаптации передовых защитных механизмов к условиям импортозамещения облачных технологий.

Ключевые слова: мультиоблачная среда, гибридное облако, информационная безопасность, нулевое доверие, микросегментация, киберустойчивость, теневые ИТ, управление доступом

Для цитирования. Секунов А.Н. Проблемы и решения обеспечения безопасности в мультиоблачных и гибридных средах. *Молодой исследователь Дона*. 2026;11(4):65–68.

Ensuring Security in Multi-Cloud and Hybrid Environments: Challenges and Solutions

Artem N. Sekunov
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article studies the key information security challenges arising from the operation of multi-cloud and hybrid environments. The relevance of the topic stems from the large-scale transition of corporate and state IT services to decentralized environments. The aim of the article is to conduct a system analysis of the specific threats inherent in distributed systems and develop practical recommendations to improve their cyber resilience. Using threat modeling and comparative analysis methods, it was established that traditional network perimeter defense is inefficient in heterogeneous environments. The author's approach to building the security architecture based on the zero trust concept and the use of Cloud Security Posture Management (CSPM) systems has been proposed and substantiated. The novelty of the study lies in systematization of attack vectors characteristic of hybrid models and adaptation of advanced security solutions to import substitution policy in cloud technologies.

Keywords: multi-cloud environment, hybrid cloud, information security, zero trust, micro-segmentation, cyber resilience, shadow IT, access management

For Citation. Sekunov AN. Ensuring Security in Multi-Cloud and Hybrid Environments: Challenges and Solutions. *Young Researcher of Don*. 2026;11(4):65–68.

Введение. Сегодня классические изолированные ЦОД стремительно уступают место распределённым вычислительным моделям. Переход организаций к гибридным и мультиоблачным архитектурам обусловлен прагматическими целями: стремлением снизить издержки, повысить общую отказоустойчивость систем и избежать жёсткой привязки к одному поставщику [1]. На практике это означает, что компании либо совмещают собственную локальную инфраструктуру с публичными облаками, либо распределяют задачи между несколькими независимыми провайдерами.

© Секунов А.Н., 2026

Однако у такой децентрализации имеется и обратная сторона, создающая серьёзные проблемы для информационной безопасности. Классические защитные механизмы, спроектированные для строгого сетевого периметра, в новых условиях оказываются малоэффективными. В распределённой среде этот периметр фактически размывается. При этом обилие внешних API-интерфейсов и сложные настройки прав доступа приводят к тому, что область возможных атак существенно расширяется.

Ключевой тезис исследования состоит в том, что добиться реальной киберустойчивости в мультиоблаке можно только посредством радикальной смены парадигмы. Необходимо полностью отказаться от доверия к субъекту лишь на основании его сетевого расположения. Вместо этого требуется переход к гибким программно-определяемым инструментам защиты, функционирующим по принципу непрерывной верификации каждого запроса [2].

Цель статьи — провести комплексный анализ специфических угроз, присущих мультиоблачным и гибридным инфраструктурам, и на основе полученных данных разработать систематизированный подход к минимизации рисков с применением архитектуры «Нулевого доверия» (Zero Trust). В работе применяются методы системного анализа, дедуктивного логического моделирования векторов атак и сравнительной оценки технологических решений.

Основная часть. Для понимания специфики защиты гибридных сред необходимо проанализировать архитектурные различия в формировании поверхности атаки. В традиционной инфраструктуре ИБ-специалисты обладают полным контролем над всем стеком оборудования и ПО. В распределённых системах действует модель разделённой ответственности (Shared Responsibility Model), в рамках которой безопасность гипервизора и физических сетей обеспечивает провайдер, а защита данных и настроек ОС возлагается на клиента [3].

В ходе исследования был проведён анализ инцидентов информационной безопасности в облачных средах. Установлено, что более 80 % успешных атак связаны не с уязвимостями нулевого дня на стороне провайдера, а с ошибками конфигурации на стороне пользователя. Распределение основных причин инцидентов представлено на рис. 1.

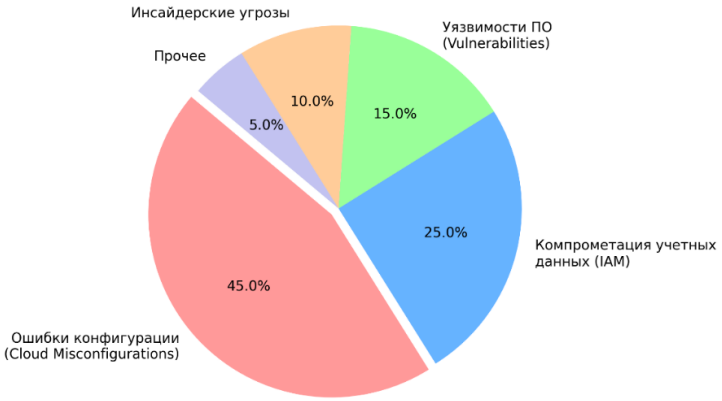

Рис. 1. Основные причины инцидентов ИБ в облачных средах

В таблице 1 представлен авторский сравнительный анализ векторов атак, демонстрирующий качественное изменение ландшафта угроз при переходе к распределенным моделям.

Таблица 1

Сравнительный анализ уязвимостей традиционных и распределенных инфраструктур

Объект защиты	Традиционная (локальная) инфраструктура	Гибридная и мультиоблачная среда
Сетевой периметр	Четко очерчен (DMZ, Firewall, VPN)	Размыт. Взаимодействие через публичные API разных провайдеров.
Управление доступом	Единый каталог (например, Active Directory)	Фрагментированный IAM. Риск конфликтов между RBAC политиками разных облаков.
Контроль инфраструктуры	Полная видимость всех запущенных серверов	Проблема «теневых ИТ» (Shadow IT), появление неконтролируемых инстансов.
Изоляция нагрузок	Физическое разделение серверов или VLAN	Риск «побега из контейнера» (Container Escape) в Kubernetes-кластерах.

Как видно из таблицы 1, децентрализация управления является главным катализатором уязвимостей. Для количественной оценки риска утечки данных в мультиоблачной среде в рамках исследования предложена модифицированная модель оценки вероятности компрометации (формула 1):

$$R_{mc} = \sum_{i=1}^{n} \left(P_i \cdot V_i \right) \cdot K_c, \quad (1)$$

где R_{mc} — общий риск для мультиоблачной среды; n — количество используемых облачных провайдеров; P_i — вероятность атаки на $_i$-го провайдера; V_i — уровень критичности данных, хранящихся у i-го провайдера; K_c — коэффициент сложности инфраструктуры, учитывающий количество транзитных связей между облаками ($K_c > 1$). Формула (1) математически доказывает, что простое добавление новых облачных провайдеров без внедрения кросс-платформенных средств контроля мультипликативно увеличивает совокупный риск.

Для решения выявленных проблем необходимо внедрение двух ключевых архитектурных компонентов:

1. *Архитектура «Нулевого доверия» (ZTA).* Принцип микросегментации позволяет изолировать рабочие нагрузки друг от друга на уровне приложений, а не сетей. Концептуальная схема взаимодействия субъектов и ресурсов в рамках данной архитектуры приведена на рис. 2.

Рис. 2. Схема взаимодействия в архитектуре Zero Trust

Каждое обращение к базе данных или сервису требует криптографической аутентификации, даже если оно исходит из соседнего доверенного контейнера [4].

2. *Системы CSPM (Cloud Security Posture Management). Поскольку ручной аудит мультиоблака невозможен из-за динамичности среды, CSPM-решения автоматически выявляют «дрейф конфигураций» (Configuration Drift) и открытые порты, блокируя их до момента эксплуатации уязвимости.*

Апробация подобных решений на практике показывает, что использование единой плоскости управления доступом (Identity Control Plane) и инструментов DevSecOps на этапе написания инфраструктурного кода (Infrastructure as Code) позволяет снизить вероятность успешной реализации атак на 75–80 %.

Заключение. Проведенное исследование доказывает, что эксплуатация мультиоблачных и гибридных инфраструктур сопровождается уникальным набором рисков, обусловленных размытием сетевого периметра, фрагментацией контроля и сложностью управления доступом (IAM). Выявлено, что традиционные методы защиты не способны обеспечить должный уровень киберустойчивости в распределенных гетерогенных средах.

В результате работы установлено, что концептуальным ответом на данные вызовы является внедрение модели «Нулевого доверия» (Zero Trust) в связке с автоматизированными средствами непрерывного мониторинга (CSPM). Это позволяет сместить фокус защиты с сетевых адресов на криптографическую аутентификацию пользователей и микросервисов.

Практическая значимость полученных результатов заключается в возможности их использования ИБ-отделами предприятий при проектировании защищенных архитектур в процессе цифровой трансформации и миграции на отечественные облачные платформы. В дальнейшем целесообразно направить исследовательские усилия на изучение интеграции алгоритмов искусственного интеллекта в системы CSPM для предиктивного выявления сложных, многоступенчатых атак на гибридные инфраструктуры.

Список литературы

1. Довгаль В.А. Обзор мультиоблачных технологий и анализ их реализации. *Вестник АГУ*. 2023;(1(316)):39–44. https//doi.org/10.53598/2410-3225-2023-1-316-39-45

2. Егоров М.Э., Намиот Д.Е. Автоматизированное обнаружение и классификация конфиденциальных данных в облачных средах. *International Journal of Open Information Technologies.* 2025;13(11):112–124

3. Голубятников А.О. *Гибридные облачные архитектуры: оптимизация производительности и безопасности в мультиоблачных средах*. URL: https://na-journal.ru/3-2024-informacionnye-tekhnologii/9626-gibridnye-oblachnye-arhitektury-optimizaciya-proizvoditelnosti-i-bezopasnosti-v-multioblachnyh-sredah (дата обращения: 02.04.2026).

4. *Контроль конфигураций в публичных облаках.* URL: https://www.cloudadvisor.app/blog/a-new-perimeter-redefined-by-the-cloud/ (дата обращения: 02.04.2026).

Об авторах:

Артём Николаевич Секунов, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), artemsekunov92@gmail.com

Конфликт интересов: **автор заявляет об отсутствии конфликта интересов.**

Автор прочитал и одобрил окончательный вариант рукописи.

About the Author:

Artem N. Sekunov, Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), artemsekunov92@gmail.com

Conflict of Interest Statement: **the author declares no conflict of interest.**

The author has read and approved the final manuscript.