УДК 004.056.5

Заева Маргарита Анатольевна, доцент кафедры компьютерных систем и технологий института интеллектуальных кибернетических систем, Национальный исследовательский университет “МИФИ”, г. Москва

Кургинян Элла Аршаковна, старший преподаватель кафедры компьютерных систем и технологий института интеллектуальных кибернетических систем, Национальный исследовательский университет “МИФИ”, г. Москва

Гулиев Тарлан Ариф оглы, магистрант кафедры компьютерных систем и технологий института интеллектуальных кибернетических систем, Национальный исследовательский университет “МИФИ”, г. Москва

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕХАНИЗМОВ БЕЗОПАСНОСТИ ВЕДУЩИХ РОССИЙСКИХ ОБЛАЧНЫХ ПЛАТФОРМ

Аннотация

В статье исследуется проблематика обеспечения информационной безопасности при миграции корпоративных инфраструктур на ведущие российские облачные платформы (Yandex Cloud, Cloud.ru, VK Cloud). Обоснована критическая необходимость оценки нативных механизмов защиты в условиях ускоренного импортозамещения и отказа от зарубежных сервисов. В качестве методологической основы предлагается глубокая интеграция концепции «разделяемой ответственности» (Shared Responsibility) при проектировании облачных архитектур. Главный акцент сделан на функциональном сравнении систем управления доступом (IAM), сетевой микросегментации, криптографической защиты данных и безопасности сред контейнеризации (DevSecOps). Исследована специфика каждой платформы с учетом требований национальных регуляторов (ФСТЭК России, 152-ФЗ). В аналитической части детально сопоставлены встроенные инструменты провайдеров, включая работу

сервисов централизованного сбора логов (Audit Trails), защиту кластеров Kubernetes и реализацию SECaaS-модели с поддержкой ГОСТ-алгоритмов. Доказано, что отечественные решения достигли высокого уровня зрелости для обеспечения технологического суверенитета, однако для минимизации рисков теневого ИТ и мисконфигурации требуется внедрение систем автоматического контроля (CSPM) и переход к архитектуре «Нулевого доверия» (Zero Trust).

Annotation

The article investigates the challenges of ensuring information security during the migration of corporate infrastructures to leading Russian cloud platforms (Yandex Cloud, Cloud.ru, VK Cloud). The critical need to evaluate native defense mechanisms in the context of accelerated import substitution and the abandonment of foreign services is substantiated. A deep integration of the Shared Responsibility model in the design of cloud architectures is proposed as a methodological foundation. The main emphasis is placed on the functional comparison of Identity and Access Management (IAM) systems, network microsegmentation, cryptographic data protection, and container environment security (DevSecOps). The specifics of each platform are examined, taking into account the requirements of national regulators (FSTEC of Russia, Federal Law No. 152-FZ). The analytical section provides a detailed comparison of the providers' built-in tools, including the operation of centralized log collection services (Audit Trails), Kubernetes cluster protection, and the implementation of the SECaaS model supporting GOST algorithms. It is proven that domestic solutions have reached a high level of maturity to ensure technological sovereignty; however, minimizing the risks of shadow IT and misconfiguration requires the implementation of Cloud Security Posture Management (CSPM) systems and a transition to a Zero Trust architecture.

Ключевые слова: облачные вычисления, информационная безопасность, облачная безопасность, импортозамещение, модель разделяемой

ответственности, защита персональных данных, DevSecOps, IaaS, Yandex Cloud, Cloud.ru, VK Cloud.

Key words: cloud computing, information security, cloud security, import substitution, shared responsibility model, personal data protection, DevSecOps, IaaS, Yandex Cloud, Cloud.ru, VK Cloud.

Глобальная трансформация российского ИТ-рынка, обусловленная уходом транснациональных вендоров и облачных провайдеров, форсировала переход корпоративного и государственного секторов на отечественные облачные решения. По данным аналитических агентств, рынок российских облачных сервисов IaaS/PaaS показывает ежегодный рост более чем на 30%. Однако стремительная миграция обостряет проблемы информационной безопасности. Векторы атак непрерывно усложняются: злоумышленники активно используют уязвимости в API облачных сервисов, атакуют цепочки поставок (Supply Chain) и эксплуатируют ошибки конфигурации развернутых сред.

Целью данного исследования является систематизация и сравнительный анализ нативных инструментов защиты, которые российские провайдеры предоставляют клиентам для обеспечения безопасности их инфраструктур, а также выявление сильных и слабых сторон отечественного сегмента Cloud Security.

Основополагающим принципом безопасности в облачной парадигме [8] является модель разделяемой ответственности (Shared Responsibility Model). Суть данной концепции заключается в четком разграничении зон контроля между поставщиком услуг и арендатором вычислительных мощностей. Провайдер несет ответственность за безопасность самой инфраструктуры, что включает в себя физическую защиту центров обработки данных, надежность аппаратного обеспечения, изоляцию гипервизоров и базовую сегментацию сетей.

В свою очередь, клиент берет на себя ответственность за безопасность внутри развернутого облака. В эту зону входит настройка гостевых операционных систем, управление правами доступа пользователей к конкретным ресурсам, шифрование конфиденциальных данных и корректная настройка межсетевых экранов. Практика проведения независимых аудитов информационной безопасности [3] показывает, что большинство инцидентов происходит не вследствие компрометации ядра провайдера, а из-за ошибок на стороне клиента, таких как открытие публичного доступа к базам данных или утечка API-ключей. В связи с этим критически важно оценивать инструментарий, который платформа предоставляет пользователю для минимизации «человеческого фактора».

В качестве объектов исследования были выбраны платформы, занимающие лидирующие позиции на рынке IaaS-решений Российской Федерации: Yandex Cloud, Cloud.ru (ранее SberCloud) и VK Cloud.

Для обеспечения объективности сравнения была сформирована комплексная система критериев. В первую очередь анализировались подсистемы управления идентификацией и доступом (IAM), включая возможности гранулярного распределения ролей по модели Zero Trust и интеграцию с внешними корпоративными каталогами. Следующим аспектом стала сетевая безопасность, где оценивалось наличие межсетевых экранов уровня приложения (WAF), инструментов микросегментации сетей и защиты от DDoS-атак. Также в фокус исследования попали сервисы криптографической защиты данных и управления ключами (KMS), средства безопасности контейнерных сред в рамках методологии DevSecOps, а также возможности централизованного аудита действий в облаке. Дополнительным, но не менее важным критерием стала оценка соответствия инфраструктуры требованиям регуляторов, в частности приказам ФСТЭК России [2] и базовым положениям Федерального закона № 152-ФЗ [1].

Yandex Cloud

Платформа Yandex Cloud выделяется развитой экосистемой сервисов, изначально спроектированной с прицелом на Cloud-Native разработку [5]. Подсистема управления доступом Yandex IAM обеспечивает строгую ролевую модель и бесшовную интеграцию с корпоративными каталогами по протоколу SAML 2.0. Особого внимания заслуживает сервис Yandex Audit Trails, который агрегирует события безопасности со всех ресурсов облака и позволяет легко выгружать телеметрию в корпоративные SIEM-системы. В контексте методологии DevSecOps [4] провайдер предлагает сервис Container Registry со встроенным функционалом автоматического сканирования Docker-образов на наличие известных уязвимостей (CVE). В области криптографии Key Management Service поддерживает интеграцию с аппаратными модулями безопасности (HSM), что является критичным для финансового сектора. Сама инфраструктура полностью аттестована по наивысшему уровню защищенности персональных данных (УЗ-1) [1] и международному стандарту PCI DSS [5].

Cloud.ru

Инфраструктура платформы Cloud.ru (редакция Advanced/Enterprise) исторически сфокусирована на крупном корпоративном бизнесе и государственном секторе, где предъявляются наиболее жесткие требования к информационной безопасности. Защита сетей здесь во многом предоставляется по модели SECaaS [6] с глубокой интеграцией решений отечественных ИБ-вендоров, таких как UserGate, что позволяет разворачивать полноценные NGFW непосредственно в облачной среде. Мощная подсистема Cloud Trace Service обеспечивает непрерывный мониторинг изменений API. Ключевым конкурентным преимуществом платформы выступает развитая поддержка алгоритмов ГОСТ-шифрования, что делает ее оптимальным выбором для размещения государственных информационных систем [2] и критической информационной инфраструктуры (КИИ) [6].

VK Cloud

Архитектура VK Cloud, построенная на базе открытых стандартов OpenStack [7], делает серьезный упор на защиту микросервисов и оркестраторов.

Сетевая изоляция реализуется через продвинутые механизмы Security Groups, позволяющие гибко сегментировать трафик между виртуальными машинами. Защита от веб-атак и DDoS-угроз интегрирована непосредственно в панель управления в партнерстве с профильными компаниями, такими как Kaspersky. В рамках поддержки DevSecOps-практик [4] сервис Managed Kubernetes обладает глубокой интеграцией с сетевыми политиками Calico, что дает возможность изолировать контейнеры друг от друга и минимизировать радиус потенциального поражения при компрометации отдельного узла. Управление секретами реализовано с использованием нативного сервиса Barbican, а сама инфраструктура аттестована для работы с ИСПДн [1] и ГИС [7].

Основные функциональные характеристики рассмотренных платформ систематизированы и представлены в таблице 1 для наглядного сопоставления.

Таблица 1. Детализированное сравнение механизмов безопасности российских облачных платформ

Критерий ИБ	**Yandex Cloud**	**Cloud.ru**	**VK Cloud**
Интеграция IAM	SAML 2.0, Active Directory	Active Directory, SAML	OpenID Connect, SAML
Защита сети и WAF	Встроенные Smart Web Security и Anti-DDoS	SECaaS сервисы и партнерские решения	Нативные опции и интеграция с Kaspersky
Криптография (KMS)	Поддержка аппаратных модулей (HSM)	Поддержка ГОСТ-шифрования	Служба управления секретами (Barbican)
DevSecOps	Встроенный сканнер Container Registry	Реализуется через инструменты партнеров	Тесная интеграция с CI/CD инструментами
Аудит API	Сервис Yandex Audit Trails	Сервис Cloud Trace Service	Сервис CloudTrail (OpenStack)
Аттестация ФСТЭК	УЗ-1, 1Г, 1К	УЗ-1, К1, 1Г	УЗ-1, К1

Несмотря на объективно высокий уровень защищенности самих платформ, эксплуатационная практика выявляет ряд системных проблем. Наиболее критичной из них остаются риски мисконфигурации [3]. Инженеры на стороне

клиента регулярно допускают ошибки при настройке прав доступа к объектным хранилищам или сетевым интерфейсам. Ситуация осложняется тем, что на российском рынке пока недостаточно широко представлены нативные инструменты класса CSPM (Cloud Security Posture Management) — системы, способные в автоматическом режиме проверять конфигурацию облака на соответствие эталонным практикам безопасности.

Другой важной особенностью отечественного рынка является высокая зависимость провайдеров от партнерских ИБ-решений. В отличие от глобальных лидеров рынка, разрабатывающих большинство инструментов защиты in-house, российские компании часто прибегают к интеграции продуктов сторонних вендоров. Это обеспечивает высокое качество узкоспециализированной защиты, но может создавать сложности при построении бесшовной архитектуры безопасности и управлении инцидентами из единого окна консоли. Кроме того, серьезным барьером для безопасного использования облаков остается острый дефицит специалистов, обладающих квалификацией на стыке системного администрирования, разработки и информационной безопасности (DevSecOps-инженеров) [4].

Проведенное исследование подтверждает, что ведущие российские провайдеры успешно преодолели этап базового инфраструктурного становления. На сегодняшний день Yandex Cloud, Cloud.ru и VK Cloud представляют собой зрелые платформы, обладающие достаточным техническим арсеналом для обеспечения информационной безопасности корпоративного уровня и поддержания технологического суверенитета страны.

Анализ показал, что каждая платформа имеет выраженную специализацию. Yandex Cloud предоставляет наиболее цельную экосистему для современной микросервисной разработки, Cloud.ru является предпочтительным выбором для сложных государственных проектов благодаря поддержке стандартов ГОСТ, а VK Cloud отличается глубокой проработкой защиты контейнерных оркестраторов. Ожидается, что следующим эволюционным шагом для всего отечественного рынка IaaS станет массовый переход к

архитектуре «Нулевого доверия» на уровне гипервизора, а также внедрение технологий искусственного интеллекта для автоматического выявления аномалий в поведении облачных ресурсов.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.
2. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
3. Марков А.С., Цирлов В.Л. Опыт аудита информационной безопасности облачных инфраструктур // Вопросы кибербезопасности. – 2022. – № 1(47). – С. 15-22.
4. Барабанов А.В., Дорофеев А.В. Методология DevSecOps в облачных средах: проблемы и пути решения // Информационная безопасность компьютерных систем и сетей. – 2023. – № 4. – С. 112-118.
5. Официальная документация по безопасности Yandex Cloud. [Электронный ресурс]. URL: https://yandex.cloud/ru/docs/security/ (дата обращения: 09.06.2026).
6. Архитектура безопасности облачной платформы Cloud.ru (Advanced). [Электронный ресурс]. URL: [https://cloud.ru/ru/docs/](https://www.google.com/search?q=https://cloud.ru/ru/docs/) (дата обращения: 09.06.2026).
7. Практики обеспечения ИБ в оркестраторах Kubernetes // Документация VK Cloud. [Электронный ресурс]. URL: [https://cloud.vk.com/docs/base/security](https://www.google.com/search?q=https://cloud.vk.com/docs/base/security) (дата обращения: 09.06.2026).

8. Mell, P., Grance, T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Special Publication 800-145, 2011.

References

1. Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" // Sobranie zakonodatelstva RF [Collection of Legislation of the Russian Federation]. 2006. No. 31 (Part 1). Art. 3451. (In Russ.)
2. Order of the FSTEC of Russia No. 21 dated February 18, 2013 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during their Processing in Personal Data Information Systems". (In Russ.)
3. Markov A.S., Tsirlov V.L. Experience of Information Security Audit in Cloud Infrastructures // Voprosy kiberbezopasnosti [Cybersecurity Issues]. – 2022. – No. 1(47). – P. 15-22. (In Russ.)
4. Barabanov A.V., Dorofeev A.V. DevSecOps Methodology in Cloud Environments: Problems and Solutions // Informatsionnaya bezopasnost kompyuternykh sistem i setey [Information Security of Computer Systems and Networks]. – 2023. – No. 4. – P. 112-118. (In Russ.)
5. Official Security Documentation for Yandex Cloud. [Electronic resource]. URL: https://yandex.cloud/ru/docs/security/ (accessed: 09.06.2026). (In Russ.)
6. Security Architecture of the Cloud.ru (Advanced) Platform. [Electronic resource]. URL: https://cloud.ru/ru/docs/ (accessed: 09.06.2026). (In Russ.)
7. Information Security Practices in Kubernetes Orchestrators // VK Cloud Documentation. [Electronic resource]. URL: https://cloud.vk.com/docs/base/security (accessed: 09.06.2026). (In Russ.)
8. Mell, P., Grance, T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Special Publication 800-145, 2011.