

Научно-исследовательский центр «Иннова»

НАУЧНЫЕ ИССЛЕДОВАНИЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ В УСЛОВИЯХ ФОРМИРОВАНИЯ МНОГОПОЛЯРНОГО МИРА

Сборник научных трудов по материалам
XXII Международной научно-практической конференции,
22 сентября 2026 года, г.-к. Анапа



Анапа
2026

УДК 00(082) + 001.18 + 001.89

ББК 94.3 + 72.4: 72.5

НЗ4

Научный редактор:
Скорикова Екатерина Николаевна

Редакционная коллегия:

Бондаренко С. В., к.э.н., профессор (Россия, г. Краснодар), **Дегтярев Г. В.**, д.т.н., профессор (Россия, г. Краснодар), **Хилько Н. А.**, д.э.н., доцент (Россия, г. Анапа), **Ожерельева Н. Р.**, к.э.н., доцент (Россия, г. Анапа), **Жиянова Н. Э.**, к.э.н., профессор (Узбекистан, г. Ташкент), **Климов С. В.** к.п.н., доцент (Россия, г. Пермь), **Михайлов В. И.** к.ю.н., доцент (Россия, г. Москва).

НЗ4 Научные исследования: проблемы и перспективы в условиях формирования многополярного мира. Сборник научных трудов по материалам XXII Международной научно-практической конференции (г.-к. Анапа, 22 сентября 2026 г.). – Анапа: НИЦ ЭСП в ЮФО, 2026. – 40 с.

В настоящем издании представлены материалы XXII Международной научно-практической конференции «Научные исследования: проблемы и перспективы в условиях формирования многополярного мира», состоявшейся 22 сентября 2026 года в г.-к. Анапа. Материалы конференции посвящены актуальным проблемам науки, общества и образования. Рассматриваются теоретические и методологические вопросы в социальных, гуманитарных и естественных науках.

Издание предназначено для научных работников, преподавателей, аспирантов, всех, кто интересуется достижениями современной науки.

За содержание и достоверность статей, а также за соблюдение законов об интеллектуальной собственности ответственность несут авторы. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

Информация об опубликованных статьях размещена на платформе научной электронной библиотеки (eLIBRARY.ru). Договор № 2341-12/2017К от 27.12.2017 г.

Электронная версия сборника находится в свободном доступе на сайте:
www.innova-science.ru.

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5

ISBN 978-5-97873-111-8

© Коллектив авторов, 2026.
© ООО «НИЦ ЭСП» в ЮФО
(подразделение НИЦ «Иннова»), 2026.

СОДЕРЖАНИЕ

ТЕХНИЧЕСКИЕ НАУКИ

БЕЗОПАСНОСТЬ КОНТЕЙНЕРИЗИРОВАННЫХ ПРИЛОЖЕНИЙ (DOCKER/KUBERNETES): УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Арванова Саният Мухамедовна, Колякова Амина Владимировна

Курданов Халид Солтанович, Залиханов Къурман Русланович 4

ОЦЕНКА ЗАЩИЩЁННОСТИ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ МЕТОДОЛОГИИ OWASP: ПРАКТИЧЕСКИЙ ПОДХОД

Арванова Саният Мухамедовна, Колякова Амина Владимировна

Курданов Халид Солтанович, Залиханов Къурман Русланович 12

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ API В АРХИТЕКТУРЕ МИКРОСЕРВИСОВ И МЕТОДЫ ИХ МИТИГАЦИИ

Арванова Саният Мухамедовна, Колякова Амина Владимировна

Хежев Дамир Муратович, Карданова Фатимат Мухамедовна 19

ЭКОНОМИЧЕСКИЕ НАУКИ

СТРАТЕГИИ МИНИМИЗАЦИИ БЮДЖЕТНЫХ РИСКОВ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

Косых Елизавета Александровна..... 26

ПОЛИТОЛОГИЧЕСКИЕ НАУКИ

МНОГОВЕКТОРНАЯ ДИПЛОМАТИЯ ГВИНЕИ КАК СТРАТЕГИЯ АДАПТАЦИИ МАЛОГО ГОСУДАРСТВА К ФОРМИРУЮЩЕМУСЯ МНОГОПОЛЯРНОМУ МИРУ

Курума Юнуса..... 33

ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.75:004.056

БЕЗОПАСНОСТЬ КОНТЕЙНЕРИЗИРОВАННЫХ ПРИЛОЖЕНИЙ (DOCKER/KUBERNETES): УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Арванова Саният Мухамедовна

старший преподаватель

Колякова Амина Владимировна

Курданов Халид Солтанович

Залиханов Къурман Русланович

студенты бакалавриата

Научный руководитель: Нагоев Саламин Нургалиевич,

старший преподаватель

ФГБОУ ВО «Кабардино-Балкарский государственный университет

имени Х. М. Бербекова»,

город Нальчик

***Аннотация.** Статья посвящена анализу угроз информационной безопасности, характерных для контейнеризированных приложений, разворачиваемых с использованием технологий Docker и Kubernetes. Рассмотрены основные категории угроз: уязвимости образов контейнеров, недостатки конфигурации оркестратора, атаки на сетевой уровень и на среду выполнения (runtime). Предложена многоуровневая архитектура защиты, охватывающая этапы сборки образа, хранения в реестре, контроля допуска, оркестрации, сетевого взаимодействия и мониторинга во время выполнения. Проведён сравнительный анализ классов инструментов обеспечения безопасности контейнерных сред. По данным отраслевого исследования Red Hat (2024), около 90% организаций*

столкнулись хотя бы с одним инцидентом безопасности, связанным с контейнерами или Kubernetes, за последние 12 месяцев. Сформулированы практические рекомендации по построению защищённого конвейера DevSecOps для контейнеризированных приложений.

The article analyzes information security threats specific to containerized applications deployed using Docker and Kubernetes technologies. The main threat categories are considered: container image vulnerabilities, orchestrator misconfigurations, network-layer attacks and runtime attacks. A multilayer protection architecture is proposed, covering image build, registry storage, admission control, orchestration, network interaction and runtime monitoring stages. A comparative analysis of container security tool classes is carried out. According to a Red Hat industry survey (2024), about 90% of organizations experienced at least one container- or Kubernetes-related security incident within the past 12 months. Practical recommendations for building a secure DevSecOps pipeline for containerized applications are formulated.

Ключевые слова: *информационная безопасность; контейнеризация; Docker; Kubernetes; DevSecOps; оркестрация; защита контейнеров; кибербезопасность*

Keywords: *information security; containerization; Docker; Kubernetes; DevSecOps; orchestration; container security; cybersecurity*

Контейнеризация с использованием платформы Docker и оркестратора Kubernetes стала фактическим стандартом развёртывания программного обеспечения: контейнеры обеспечивают унификацию окружения, ускоряют цикл разработки и позволяют эффективно масштабировать распределённые системы. Вместе с тем стремительное распространение контейнерных технологий сопровождается появлением новых классов угроз, нехарактерных для традиционных серверных инфраструктур.

В отличие от виртуальных машин контейнеры совместно используют ядро операционной системы хоста, что расширяет поверхность атаки и повышает риски эскалации привилегий при компрометации одного из контейнеров. Дополнительную сложность создаёт динамический характер контейнерных сред:

жизненный цикл отдельного контейнера может измеряться минутами, а количество экземпляров в кластере Kubernetes нередко исчисляется сотнями и тысячами.

Целью настоящей работы является анализ угроз безопасности контейнеризированных приложений на всех этапах их жизненного цикла и разработка многоуровневой архитектуры защиты, объединяющей организационные и технические меры.

Для достижения поставленной цели решались следующие задачи:

- рассмотреть основные категории угроз безопасности контейнеров и оркестратора Kubernetes;
- разработать многоуровневую архитектуру защиты контейнеризированных приложений;
- провести сравнительный анализ классов инструментов защиты контейнерных сред;
- сформулировать практические рекомендации по построению защищённого конвейера DevSecOps.

1. Классификация угроз безопасности контейнеризированных сред

Анализ научных публикаций и отраслевых отчётов [1, 2] позволяет выделить несколько групп угроз безопасности, свойственных контейнеризированным приложениям. Первая группа связана с образами контейнеров: использование базовых образов с известными уязвимостями, встраивание секретов (паролей, ключей доступа) непосредственно в слои образа, отсутствие проверки целостности и происхождения образа.

Вторая группа угроз охватывает уровень оркестрации: избыточные права доступа в модели RBAC, отсутствие ограничений Pod Security Standards, небезопасные настройки API-сервера Kubernetes. Третья группа относится к сетевому взаимодействию между микросервисами, четвёртая — к среде выполнения (runtime), включая попытки выхода из контейнера (container escape) и повышения привилегий [3, 4].

Обобщённая классификация угроз с указанием типичных проявлений и

последствий представлена в таблице 1.

Таблица 1 – Классификация угроз безопасности контейнеризированных сред

Группа угроз	Типичные проявления	Возможные последствия
Образ контейнера	уязвимые базовые образы, секреты в слоях, отсутствие подписи	компрометация приложения ещё до запуска
Реестр образов	несанкционированный доступ, подмена образа	распространение вредоносного кода по инфраструктуре
Оркестрация (Kubernetes)	избыточные права RBAC, открытый API-сервер	компрометация всего кластера
Сеть	отсутствие сегментации, открытый межсервисный трафик	латеральное перемещение злоумышленника
Runtime	container escape, повышение привилегий	доступ к хост-системе и соседним контейнерам

2. Многоуровневая архитектура защиты контейнеризированных приложений

Для противодействия перечисленным угрозам предлагается архитектура защиты, реализующая принцип эшелонированной обороны (defense in depth) на каждом этапе жизненного цикла контейнера — от сборки образа до эксплуатации в производственной среде. Обобщённая схема архитектуры представлена на рисунке 1.

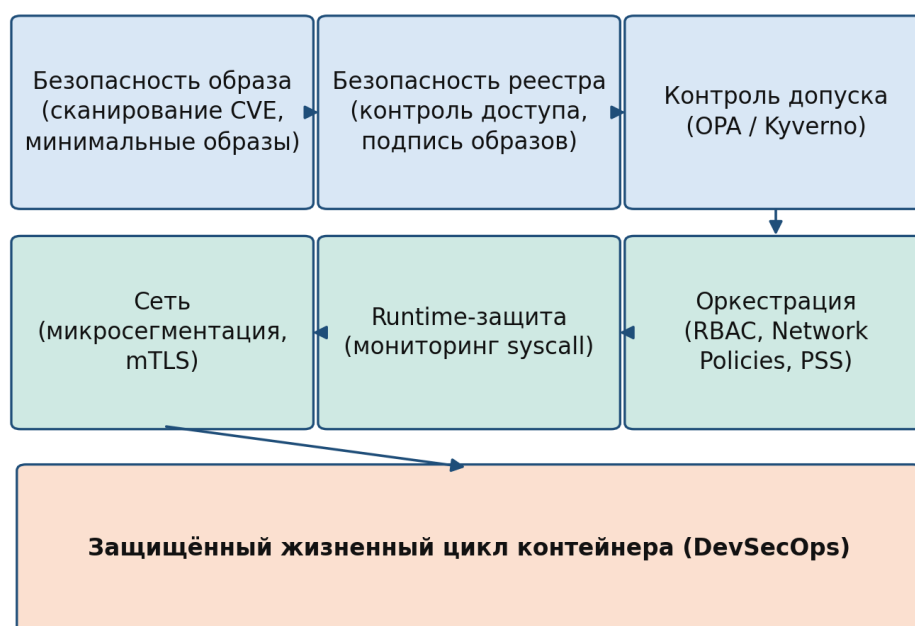


Рисунок 1 – Многоуровневая архитектура защиты контейнеризированных приложений

На этапе сборки образа применяется статическое сканирование на наличие известных уязвимостей (CVE) и используются минимальные базовые образы (distroless, scratch), что уменьшает поверхность атаки [5]. Реестр образов защищается посредством контроля доступа и цифровой подписи образов.

На уровне оркестрации задач контроллеров допуска (Open Policy Agent, Kyverno) является предотвращение развёртывания подов, нарушающих политики безопасности, — например, запуска контейнеров от имени пользователя root или без ограничений по ресурсам. Средства runtime-защиты обеспечивают мониторинг системных вызовов и поведенческий анализ для обнаружения аномальной активности внутри работающих контейнеров, а сетевая микросегментация и взаимная TLS-аутентификация (mTLS) ограничивают распространение атаки в случае компрометации отдельного сервиса [6].

3. Методика сравнительного анализа средств защиты

Для оценки применимости различных классов средств защиты выполнен сравнительный анализ по критериям: этап жизненного цикла, на котором применяется инструмент, и основная решаемая им задача. Результаты анализа представлены в таблице 2.

Таблица 2 – Сравнение классов инструментов защиты контейнерных сред

Класс инструмента	Этап применения	Основная функция
Сканер образов (Trivy, Gype)	сборка / CI-конвейер	поиск известных уязвимостей и небезопасных зависимостей
Контроллер допуска (OPA, Kyverno)	развёртывание в Kubernetes	применение политик безопасности перед запуском пода
Runtime-защита (Falco)	эксплуатация	обнаружение аномального поведения по системным вызовам
Средства сетевой политики (Cilium, Calico)	эксплуатация	микросегментация и контроль сетевого трафика

4. Результаты и обсуждение

Практическую значимость рассматриваемой проблемы подтверждают данные отраслевого исследования Red Hat State of Kubernetes Security (2024): около 90% опрошенных организаций столкнулись хотя бы с одним инцидентом безопасности, связанным с контейнерами или Kubernetes, за последние 12 месяцев,

а 67% респондентов сообщили о задержке развёртывания приложений из-за проблем информационной безопасности [7]. Диаграмма основных показателей приведена на рисунке 2.

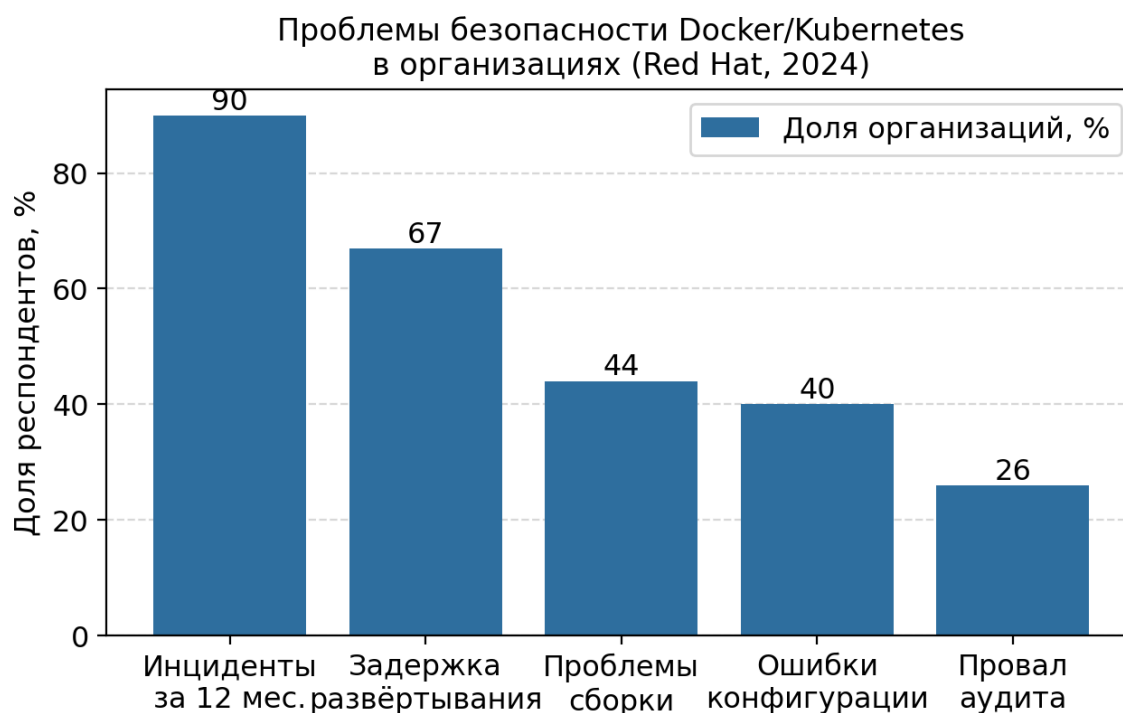


Рисунок 2 – Влияние проблем безопасности Docker/Kubernetes на организации, по данным Red Hat (2024)

Приведённые данные показывают, что проблемы безопасности контейнерных сред затрагивают не только технический, но и организационный уровень: значительная доля инцидентов связана с ошибками конфигурации (40%) и выявляется уже на этапе аудита (26%), что свидетельствует о недостаточной интеграции средств защиты в процессы разработки. Это подтверждает целесообразность применения многоуровневой архитектуры защиты, предложенной в разделе 2, а также необходимость встраивания инструментов сканирования и контроля политик непосредственно в конвейер CI/CD в рамках подхода DevSecOps [8].

Заключение

В результате проведённого исследования систематизированы основные группы угроз безопасности контейнеризированных приложений, охватывающие уровни образа, реестра, оркестрации, сети и среды выполнения. Предложена многоуровневая архитектура защиты, реализующая принцип эшелонированной

обороны на всех этапах жизненного цикла контейнера.

Сравнительный анализ инструментов защиты показал, что эффективная защита контейнерных сред требует сочетания статических методов (сканирование образов, контроль политик допуска) и динамических методов (runtime-мониторинг, сетевая микросегментация). Полученные результаты могут быть использованы при проектировании конвейеров DevSecOps для контейнеризированных приложений; дальнейшие исследования целесообразно направить на автоматизацию реагирования на инциденты в средах Kubernetes.

Список литературы

1. Дарвиш Г., Хаммуд Ж., Воробьева А. А. Повышение безопасности Kubernetes с использованием машинного обучения: проактивный подход к обнаружению аномалий / Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24, № 6. С. 1007–1015.
2. Липатова С. Е., Белов Ю. С. Практики обеспечения кибербезопасности в Kubernetes / E-Scio. 2022. № 1 (64). С. 490–498.
3. Дарвиш Г., Хаммуд Ж., Воробьева А. А. Повышение эффективности обнаружения DoS-атак в Kubernetes: подход на основе машинного обучения с интеграцией метрик уровня узлов и приложений для мультифреймворковых сред / Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 5. С. 910–922.
4. Безопасное хранение файлов с применением криптоконтейнеров / С. М. Арванова, М. З. Хачмахова, А. А. Нотов, А. А. А. Заммиев / EUROPEAN RESEARCH FORUM: сборник статей IV Международной научно-практической конференции, Петрозаводск, 13 мая 2021 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская Ирина Игоревна), 2021. – С. 24-29.
5. NIST Special Publication 800-190. Application Container Security Guide. Gaithersburg: National Institute of Standards and Technology, 2017. doi: 10.6028/NIST.SP.800-190.

6. Крутяков Д. В. Роль контейнеризации и оркестрации (Docker и Kubernetes) в современной разработке программного обеспечения / Вестник науки. 2026. № 2 (95). Т. 1. С. 724–729.

7. Red Hat, Inc. The State of Kubernetes Security Report, 2024 Edition [Электронный ресурс]. URL: <https://www.redhat.com/en/blog/state-kubernetes-security-2024> (дата обращения: 10.09.2026).

8. OWASP Foundation. Docker Security Cheat Sheet [Электронный ресурс]. URL: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html (дата обращения: 10.09.2026).

УДК 004.056.53:004.738.5

ОЦЕНКА ЗАЩИЩЁННОСТИ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ МЕТОДОЛОГИИ OWASP: ПРАКТИЧЕСКИЙ ПОДХОД

Арванова Саният Мухамедовна

старший преподаватель

Колякова Амина Владимировна

Курданов Халид Солтанович

Залиханов Къурман Русланович

студенты бакалавриата

Научный руководитель: Ксенофонтов Александр Семенович,

к.ф.-м.н., доцент

ФГБОУ ВО «Кабардино-Балкарский государственный университет

имени Х. М. Бербекова», город Нальчик

***Аннотация.** Статья посвящена разработке практического подхода к оценке защищённости веб-приложений на основе методологии Open Web Application Security Project (OWASP). Рассмотрена эволюция перечня OWASP Top Ten и структура актуальной редакции 2021 года. Предложена последовательность этапов практической оценки защищённости в соответствии с руководством OWASP Web Security Testing Guide — от сбора информации о приложении до формирования итогового отчёта. Проведён сравнительный анализ типовых уязвимостей веб-приложений (инъекции, межсайтовый скриптинг, небезопасная десериализация, слабая аутентификация) и соответствующих им защитных мер. Показано, что выход категории нарушения контроля доступа на первое место в редакции 2021 года отражает смещение угроз в сторону ошибок бизнес-логики. Сформулированы практические рекомендации по внедрению регулярной оценки защищённости в процесс разработки программного обеспечения.*

The article addresses the development of a practical approach to web application security assessment based on the Open Web Application Security Project

(OWASP) methodology. The evolution of the OWASP Top Ten list and the structure of the current 2021 edition are considered. A sequence of practical assessment stages is proposed in accordance with the OWASP Web Security Testing Guide, from information gathering to the final report. A comparative analysis of typical web application vulnerabilities (injections, cross-site scripting, insecure deserialization, weak authentication) and the corresponding protective measures is carried out. It is shown that the Broken Access Control category taking first place in the 2021 edition reflects a shift of threats toward business logic errors. Practical recommendations for integrating regular security assessment into the software development process are formulated.

Ключевые слова: *информационная безопасность; OWASP; веб-приложения; уязвимости; тестирование на проникновение; OWASP Top Ten; защита информации*

Keywords: *information security; OWASP; web applications; vulnerabilities; penetration testing; OWASP Top Ten; data protection*

Веб-приложения остаются одной из наиболее массовых целей кибератак: через них злоумышленники получают доступ к персональным данным пользователей, платёжной информации и внутренним ресурсам организаций. Разнородность технологий разработки и высокая скорость выпуска новых версий приводят к тому, что значительная часть уязвимостей остаётся необнаруженной вплоть до эксплуатации в производственной среде.

Наиболее распространённой методологической основой для оценки защищённости веб-приложений является перечень OWASP Top Ten, разрабатываемый некоммерческой организацией Open Web Application Security Project (OWASP) на основе статистики реальных сканирований и опроса профессионального сообщества. Помимо перечня категорий риска, OWASP публикует практическое руководство по тестированию — OWASP Web Security Testing Guide (WSTG), формализующее последовательность этапов оценки.

Целью настоящей работы является разработка практического подхода к оценке защищённости веб-приложений на основе методологии OWASP, объединяющего систематизацию категорий уязвимостей и последовательность этапов

тестирования.

Для достижения поставленной цели решались следующие задачи:

- рассмотреть структуру и эволюцию перечня OWASP Top Ten как основы оценки защищённости веб-приложений;
- разработать последовательность этапов практической оценки защищённости на основе методологии OWASP WSTG;
- провести сравнительный анализ типовых уязвимостей веб-приложений;
- сформулировать практические рекомендации по внедрению регулярной оценки защищённости в процесс разработки.

1. Методология OWASP как основа оценки защищённости

Перечень OWASP Top Ten впервые опубликован в 2003 году и с тех пор обновлялся семь раз — в 2004, 2007, 2010, 2013, 2017 и 2021 годах. Каждая новая редакция отражает изменение ландшафта угроз: в редакции 2021 года категория нарушения контроля доступа (Broken Access Control) впервые заняла первое место, что связано с ростом доли ошибок бизнес-логики и авторизации в общем числе выявляемых недостатков [1].

Актуальная редакция OWASP Top Ten (2021) включает десять категорий риска, охватывающих как технические уязвимости (инъекции, небезопасная десериализация), так и организационные недостатки (отсутствие журналирования, неверная конфигурация безопасности) [2, 3]. Обобщённая структура категорий представлена в таблице 1.

Таблица 1 – Отдельные категории риска OWASP Top 10 (редакция 2021 года)

Категория OWASP Top 10 (2021)	Краткое описание
A01: Нарушение контроля доступа	доступ к ресурсам без надлежащей проверки прав пользователя
A02: Криптографические сбои	использование слабых алгоритмов, хранение данных без шифрования
A03: Инъекции	внедрение постороннего кода через непроверенные входные данные (SQL, OS, LDAP)
A05: Неверная конфигурация безопасности	избыточные права доступа, настройки по умолчанию
A07: Ошибки идентификации и аутентификации	слабые пароли, отсутствие защиты от перебора

2. Этапы практической оценки защищённости веб-приложения

Практическая оценка защищённости веб-приложения строится в соответствии с руководством OWASP Web Security Testing Guide [4] и включает последовательность взаимосвязанных этапов — от сбора информации о приложении до формирования итогового отчёта. Предлагаемая последовательность этапов представлена на рисунке 1.

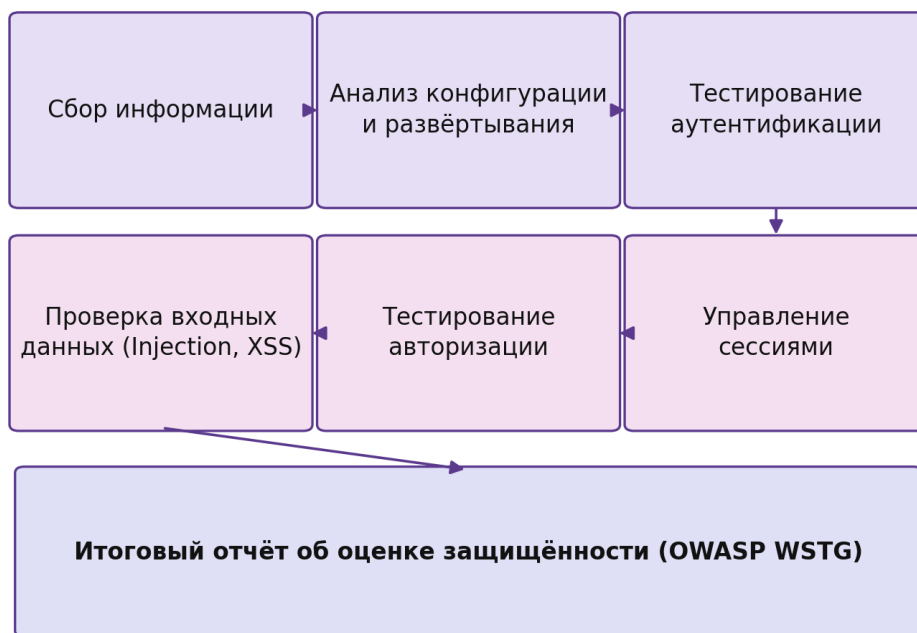


Рисунок 1 – Этапы практической оценки защищённости веб-приложения по методологии OWASP WSTG

На этапе сбора информации определяются технологический стек приложения, точки входа и внешние зависимости. Далее анализируется конфигурация развёртывания — версии программного обеспечения, настройки заголовков безопасности HTTP, параметры TLS. Тестирование аутентификации и авторизации проверяет устойчивость к перебору учётных данных, корректность разграничения прав доступа между ролями пользователей [5, 6].

Отдельное внимание уделяется проверке входных данных на предмет инъекций (SQL-инъекции, межсайтовый скриптинг) и корректности управления пользовательскими сессиями — параметрам сроков действия токенов, механизмам их обновления и инвалидации. Результаты каждого этапа фиксируются в итоговом отчёте с указанием уровня критичности выявленных недостатков в

соответствии с шкалой OWASP Risk Rating.

3. Сравнительный анализ типовых уязвимостей и защитных мер

На основе анализа практических работ по тестированию веб-приложений [2, 5] сопоставлены наиболее распространённые категории уязвимостей и соответствующие им защитные меры, применяемые на практике. Результаты сопоставления приведены в таблице 2.

Таблица 2 – Сопоставление уязвимостей веб-приложений и защитных мер

Уязвимость	Рекомендуемая защитная мера
SQL-инъекция	параметризованные запросы, ORM, входная валидация
Межсайтовый скриптинг (XSS)	экранирование вывода, политика Content Security Policy
Небезопасная десериализация	проверка типов, ограничение допустимых форматов данных
Слабая аутентификация	многофакторная аутентификация, ограничение частоты попыток входа
Раскрытие чувствительных данных	шифрование при хранении и передаче (TLS), минимизация данных

4. Результаты и обсуждение

Ранжирование категорий OWASP Top 10 по степени приоритета, установленное редакцией 2021 года на основе анализа более 500 000 приложений и экспертного голосования профессионального сообщества [1], представлено на рисунке 2.

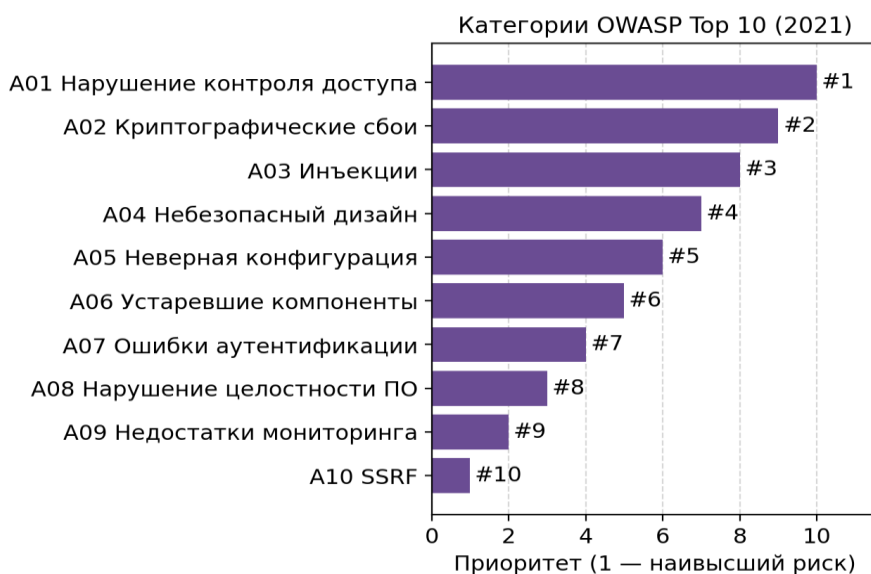


Рисунок 2 – Ранжирование категорий OWASP Top 10 (редакция 2021 года) по уровню приоритета

Выход категории нарушения контроля доступа на первое место подтверждает смещение фокуса атак с чисто технических уязвимостей кода в сторону ошибок бизнес-логики и авторизации, которые автоматизированные сканеры выявляют существенно хуже, чем инъекции или использование устаревших компонентов. Это обосновывает необходимость сочетания автоматизированного сканирования с ручным тестированием на основе методологии OWASP WSTG, а также регулярного пересмотра политик доступа на этапе проектирования приложения [3].

Заключение

В результате проведённого исследования систематизирована структура методологии OWASP как основы оценки защищённости веб-приложений, рассмотрена эволюция перечня OWASP Top Ten и предложена последовательность этапов практической оценки на основе руководства OWASP WSTG.

Сопоставление типовых категорий уязвимостей с соответствующими защитными мерами показало, что эффективная оценка защищённости требует сочетания автоматизированного сканирования и ручного анализа бизнес-логики приложения. Полученные результаты могут быть использованы при построении процесса регулярного аудита безопасности веб-приложений в организациях; дальнейшие исследования целесообразно направить на адаптацию методологии OWASP к оценке защищённости API и микросервисных архитектур.

Список литературы

1. Керим А. Г. Сравнительный анализ версий OWASP Top Ten: эволюция угроз веб-безопасности [Электронный ресурс] / КиберЛенинка. 2025. URL: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-versiy-owasp-top-ten-evolyutsiya-ugroz-veb-bezopasnosti> (дата обращения: 10.09.2026).
2. Путятю М. М., Макарян А. С., Лещенко В. В., Немчинова В. О. Анализ типовых уязвимостей при построении веб-приложений / Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2022. № 3 (306). С. 77–85.

3. Булатова, Э. И. Разработка мобильных приложений как драйвер цифрового предпринимательства / Э. И. Булатова, Л. А. Иванова, С. М. Арванова / Экономика и управление: проблемы, решения. – 2025. – Т. 4, № 10(163). – С. 164-170. – DOI 10.36871/ek.up.p.r.2025.10.04.017.

4. OWASP Foundation. OWASP Web Security Testing Guide (WSTG) [Электронный ресурс]. URL: <https://owasp.org/www-project-web-security-testing-guide/> (дата обращения: 10.09.2026).

5. Когай Д. В., Анисимова Э. С. Атаки на API: анализ уязвимостей и методы защиты REST-сервисов / Молодой учёный. 2026. № 18 (621). С. 79–81.

6. OWASP Foundation. OWASP Top Ten Web Application Security Risks [Электронный ресурс]. URL: <https://owasp.org/www-project-top-ten/> (дата обращения: 10.09.2026).

УДК 004.75:004.732

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ API В АРХИТЕКТУРЕ МИКРОСЕРВИСОВ И МЕТОДЫ ИХ МИТИГАЦИИ

Арванова Саният Мухамедовна

старший преподаватель

Колякова Амина Владимировна

Хежев Дамир Муратович

Карданова Фатимат Мухамедовна

студенты бакалавриата

Научный руководитель: Тхайцухов Арсен Амерханович,

доцент

ФГБОУ ВО «Кабардино-Балкарский государственный университет

имени Х. М. Бербекова»,

город Нальчик

***Аннотация.** Статья посвящена анализу угроз безопасности программных интерфейсов (API) в архитектуре микросервисов. Рассмотрены особенности угроз, обусловленные децентрализованным характером аутентификации и авторизации в распределённых системах. Систематизированы категории угроз в соответствии с актуальным перечнем OWASP API Security Top 10 (2023), включая нарушение авторизации объектного и функционального уровня, некорректное использование токенов JWT и подделку запросов на стороне сервера (SSRF). Предложена архитектура защиты межсервисного взаимодействия, объединяющая шлюз API, сервис идентификации на основе протокола OAuth 2.0 и инфраструктуру service mesh с взаимной TLS-аутентификацией. Систематизированы методы митигации типовых угроз. Показано, что уязвимости уровня бизнес-логики занимают первые позиции актуального перечня и требуют целенаправленного анализа модели авторизации на этапе проектирования сервиса.*

The article addresses the analysis of application programming interface (API) security threats in a microservices architecture. The specifics of threats caused by the decentralized nature of authentication and authorization in distributed systems are

considered. Threat categories are systematized in accordance with the current OWASP API Security Top 10 (2023) list, including broken object- and function-level authorization, improper use of JWT tokens, and server-side request forgery (SSRF). A protection architecture for inter-service communication is proposed, combining an API gateway, an OAuth 2.0-based identity service, and a service mesh infrastructure with mutual TLS authentication. Mitigation methods for typical threats are systematized. It is shown that business logic vulnerabilities occupy the top positions of the current list and require targeted analysis of the authorization model at the service design stage.

Ключевые слова: *информационная безопасность; API; микросервисы; OWASP; OAuth 2.0; JWT; service mesh; кибербезопасность*

Keywords: *information security; API; microservices; OWASP; OAuth 2.0; JWT; service mesh; cybersecurity*

Микросервисная архитектура предполагает декомпозицию приложения на множество независимо развёртываемых сервисов, взаимодействующих между собой преимущественно через программные интерфейсы (API). Такой подход повышает гибкость разработки и масштабируемость систем, однако существенно расширяет поверхность атаки: каждый программный интерфейс представляет собой потенциальную точку входа для злоумышленника.

В отличие от атак на монолитные веб-приложения, атаки на API получают прямой доступ к бизнес-логике сервисов в обход пользовательского интерфейса. По данным профильных исследований, более 80% корпоративного сетевого трафика в настоящее время приходится именно на вызовы API, при этом число инцидентов, связанных с эксплуатацией их уязвимостей, продолжает расти.

Целью настоящей работы является анализ основных классов угроз безопасности API в архитектуре микросервисов и систематизация методов их митигации на основе актуального перечня OWASP API Security Top 10.

Для достижения поставленной цели решались следующие задачи:

- рассмотреть особенности угроз безопасности API, обусловленные микросервисной архитектурой;
- систематизировать категории угроз в соответствии с перечнем OWASP

API Security Top 10 (2023);

– разработать архитектуру защиты межсервисного взаимодействия на основе шлюза API и service mesh;

– сформулировать методы митигации типовых угроз безопасности API.

1. Особенности угроз безопасности API в микросервисной архитектуре

В микросервисной архитектуре аутентификация и авторизация не могут выполняться централизованно на уровне единственного приложения, как в монолитных системах: каждый сервис является отдельным автономным компонентом, а взаимодействие между сервисами происходит преимущественно по протоколу REST с использованием токенов формата JWT [1, 2].

Наиболее распространённым классом уязвимостей API являются нарушения авторизации: нарушение авторизации объектного уровня (Broken Object Level Authorization, BOLA), при котором сервис не проверяет права текущего пользователя на доступ к запрошенному объекту, и нарушение авторизации функционального уровня (BFLA), при котором пользователь с обычными правами получает доступ к административным маршрутам [3]. Отдельную угрозу представляет некорректное использование JWT: предсказуемые или бессрочные токены, использование алгоритма подписи «none» [4, 5].

Обобщённая классификация категорий угроз в соответствии с перечнем OWASP API Security Top 10 (2023) [6] с указанием типичных проявлений представлена в таблице 1.

Таблица 1 – Категории угроз безопасности API (OWASP API Security Top 10, 2023)

Категория угрозы	Типичное проявление
API1: Нарушение авторизации объектного уровня (BOLA)	доступ к чужим данным через подмену идентификатора ресурса в запросе
API2: Нарушение аутентификации	предсказуемые токены, отсутствие защиты от перебора
API5: Нарушение авторизации функционального уровня (BFLA)	доступ обычного пользователя к административным маршрутам
API4: Неограниченное потребление ресурсов	отсутствие лимитов на частоту запросов и размер данных
API7: Подделка запросов на стороне сервера (SSRF)	обращение сервиса к внутренней инфраструктуре по URL, заданному злоумышленником

2. Архитектура защиты межсервисного взаимодействия

Для митигации рассмотренных угроз предлагается архитектура защиты API, построенная на принципе многоуровневой обороны и включающая централизованный шлюз API (API Gateway), сервис идентификации и распределённую инфраструктуру service mesh. Обобщённая схема архитектуры представлена на рисунке 1.

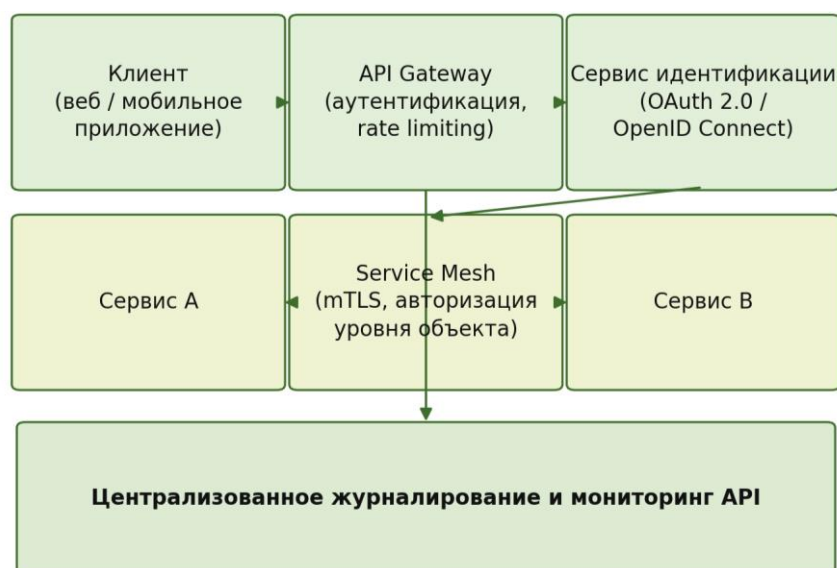


Рисунок 1 – Архитектура защиты межсервисного взаимодействия в микросервисном приложении

Шлюз API выступает единой точкой входа для внешних запросов, обеспечивая базовую аутентификацию, ограничение частоты запросов (rate limiting) и валидацию структуры запроса по схеме OpenAPI. Сервис идентификации реализует протокол OAuth 2.0 совместно с OpenID Connect: для клиентских приложений применяется Authorization Code Flow с PKCE, а для межсервисного взаимодействия — поток Client Credentials [5].

Внутри кластера сервисов инфраструктура service mesh обеспечивает взаимную TLS-аутентификацию (mTLS) между сервисами и применение политик авторизации на уровне отдельного объекта: каждый сервис сверяет идентификатор запрашиваемого ресурса с субъектом токена перед выполнением операции, что предотвращает эксплуатацию уязвимости BOLA [3, 7].

3. Методы митигации типовых угроз

На основе анализа практических рекомендаций [3, 4, 5] систематизированы

методы митигации для наиболее распространённых категорий угроз безопасности API. Результаты систематизации приведены в таблице 2.

Таблица 2 – Методы митигации типовых угроз безопасности API

Угроза	Метод митигации
BOLA / нарушение авторизации объектного уровня	проверка прав на уровне каждого объекта; модели RBAC и ABAC
Небезопасное использование JWT	явное указание алгоритма подписи, ограничение срока действия access-токена, ротация refresh-токенов
Неограниченное потребление ресурсов	лимиты на размер тела запроса, глубину вложенности JSON, частоту запросов на шлюзе
SSRF	белый список разрешённых внешних адресов, проверка IP-адреса после разрешения DNS

4. Результаты и обсуждение

Ранжирование категорий актуального перечня OWASP API Security Top 10 (2023) по степени риска представлено на рисунке 2.

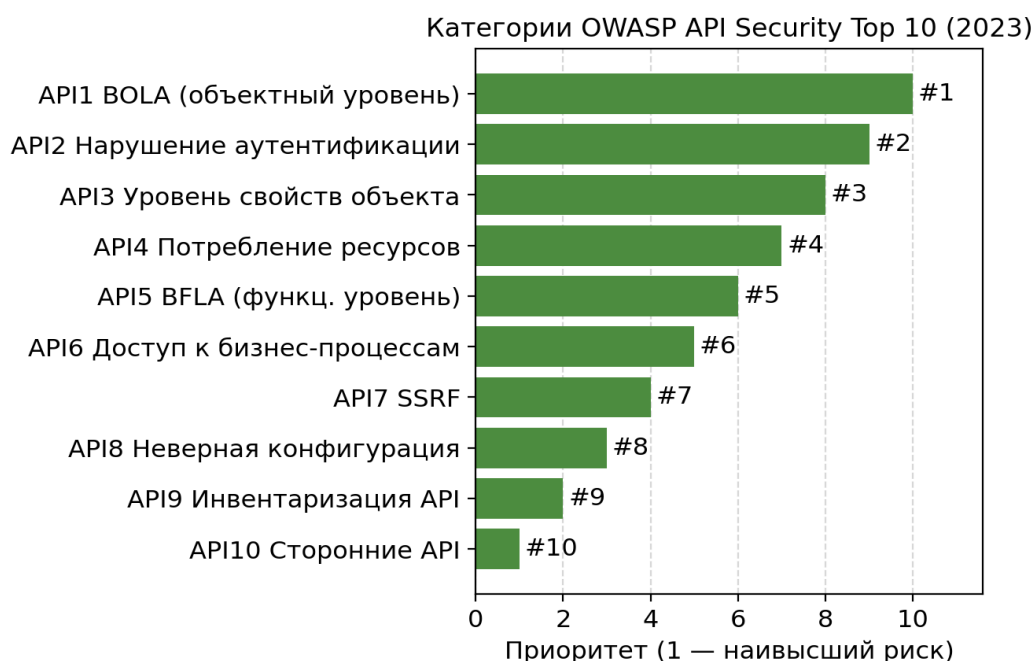


Рисунок 2 – Ранжирование категорий OWASP API Security Top 10 (редакция 2023 года)

Расположение уязвимостей уровня бизнес-логики (BOLA, BFLA) на первых позициях перечня подтверждает вывод о том, что подобные недостатки практически не выявляются средствами автоматизированного сканирования и требуют целенаправленного анализа модели авторизации на этапе

проектирования сервиса [3]. Совместное применение шлюза API, протокола OAuth 2.0 и инфраструктуры service mesh формирует многоуровневую защиту, охватывающую как внешний периметр системы, так и внутреннее взаимодействие сервисов, что существенно затрудняет реализацию рассмотренных угроз.

Заключение

В результате проведённого исследования систематизированы особенности угроз безопасности API, обусловленные микросервисной архитектурой, а также классификация категорий угроз в соответствии с перечнем OWASP API Security Top 10 (2023). Предложена архитектура защиты межсервисного взаимодействия, объединяющая шлюз API, сервис идентификации на основе OAuth 2.0 и инфраструктуру service mesh.

Систематизация методов митигации показала, что защита API требует сочетания мер инфраструктурного уровня (ограничение частоты запросов, mTLS, сегментация сети) и мер уровня приложения (проверка прав на уровне объекта, корректное использование JWT). Полученные результаты могут быть использованы при проектировании систем безопасности микросервисных приложений; дальнейшие исследования целесообразно направить на автоматизацию обнаружения аномального поведения клиентов API на основе методов машинного обучения.

Список литературы

1. Имамбердиев Ф. Ф. Сквозная аутентификация микросервисных приложений / Молодой учёный. 2023. № 14 (461). С. 9–12.
2. Jones M., Bradley J., Sakimura N. JSON Web Token (JWT): RFC 7519 / IETF. 2015. URL: <https://datatracker.ietf.org/doc/html/rfc7519>.
3. Когай Д. В., Анисимова Э. С. Атаки на API: анализ уязвимостей и методы защиты REST-сервисов / Молодой учёный. 2026. № 18 (621). С. 79–81.
4. Арванова, С. М. Анализ угроз информационной безопасности при удаленной работе / Прикладные цифровые технологии и системы XXI века: экономика, менеджмент, управление персоналом, информационная безопасность,

право : Материалы IV Межрегиональной научно-практической конференции, Владимир, 12 декабря 2024 года. – Владимир: Российская академия народного хозяйства и государственной службы при Президенте РФ, 2025. – С. 209-214.

5. Долгов А. Т., Яковлева В. Д. Анализ уязвимостей и обеспечение безопасности использования JWT в веб-разработке / Студент и наука: актуальные вопросы современных исследований. Пенза: Наука и Просвещение (ИП Гуляев Г. Ю.), 2025. С. 40–43.

6. OWASP Foundation. OWASP API Security Top 10 – 2023 [Электронный ресурс]. URL: <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>.

7. Дарвиш Г., Хаммуд Ж., Воробьева А. А. Повышение безопасности Kubernetes с использованием машинного обучения: проактивный подход к обнаружению аномалий / Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24, № 6. С. 1007–1015.

ЭКОНОМИЧЕСКИЕ НАУКИ

УДК 330

СТРАТЕГИИ МИНИМИЗАЦИИ БЮДЖЕТНЫХ РИСКОВ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

Косых Елизавета Александровна

магистрант

Научный руководитель: Спесивцев Валерий Анатольевич,

к.э.н., доцент

Липецкий филиал,

Финансовый университет при Правительстве РФ,

город Липецк

***Аннотация.** В данной статье анализируются подходы к снижению бюджетных угроз в секторе государственного и муниципального администрирования. В условиях высокой макроэкономической волатильности традиционные методы контроля становятся неэффективными, поэтому предлагается внедрение комплексной адаптивной стратегии. Важным элементом является цифровая трансформация — переход к единым информационным системам с визуализацией данных в реальном времени. Сравнительный анализ, представленный в статье, демонстрирует преимущества гибкого управления.*

This article analyzes approaches to reducing budgetary threats in the sector of public and municipal administration. In conditions of high macroeconomic volatility, traditional control methods become ineffective, so the introduction of a comprehensive adaptive strategy is proposed. An important element is digital transformation — the transition to unified information systems with real-time data visualization. The comparative analysis presented in the article demonstrates the advantages of flexible management.

Ключевые слова: бюджетные риски, государственное управление, муниципальное управление, риск-менеджмент, сценарное моделирование, rolling forecast, бюджетная прозрачность, внутренний аудит, финансовая устойчивость

Keywords: budgetary risks, public administration, municipal administration, risk management, scenario modeling, rolling forecast, budget transparency, internal audit, financial stability

В современных реалиях работа с бюджетными рисками в госсекторе требует перехода от разрозненных мер к комплексной, адаптивной управленческой стратегии. Финансовое планирование на уровне муниципалитетов и регионов сегодня происходит в условиях высокой макроэкономической турбулентности, жестких нормативных рамок и масштабных социальных обязательств.

«Бюджетные угрозы многогранны: это не только риск кассовых разрывов или превышения лимитов, но и непредсказуемость трансфертов, законодательные новации, а также уязвимости в самой архитектуре бюджетного процесса» [2]. Грамотный риск-менеджмент позволяет трансформировать эти угрозы в контролируемые параметры, обеспечивая стабильность государственных услуг и предсказуемость финансовой политики. Процесс управления бюджетными рисками может быть представлен в виде схемы (рис. 1).

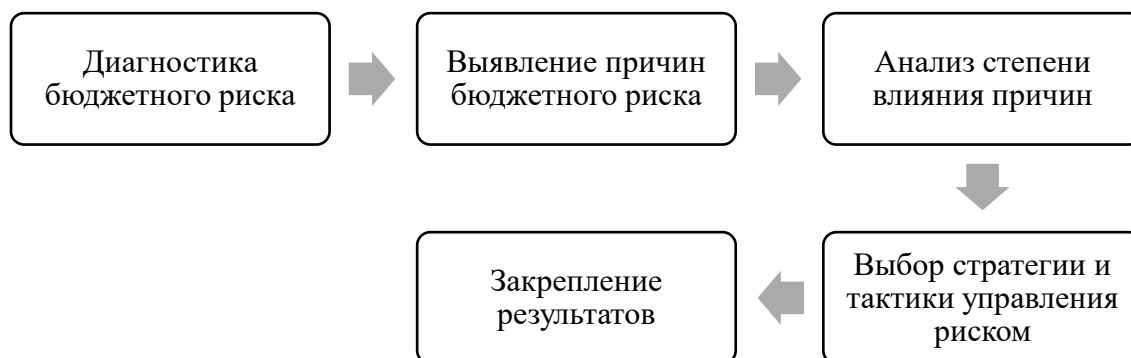


Рисунок 1 - Этапы управления бюджетным риском

В основе современных стратегий управления бюджетным процессом лежат принципы комплексности и персональной ответственности. Модель

всеобъемлющего риск-менеджмента выходит далеко за рамки классического финансового надзора, охватывая все этапы: от планирования расходных статей и проведения тендерных процедур до финальной ревизии. Базовым механизмом здесь выступает реестр рисков, где каждой потенциальной угрозе присваивается индекс критичности, а за контроль над ней закрепляется ответственный сотрудник.

Особое внимание уделяется прогностическим технологиям. «Использование сценарного моделирования, стресс-тестов и вероятностных расчетов позволяет оценить устойчивость бюджета к внешним шокам — например, к резкому падению налоговых доходов или сокращению федеральных субсидий» [5]. Применение количественных методов позволяет трансформировать гипотетические риски в точные расчетные показатели.

На смену жестким годовым планам приходит динамическое бюджетирование (rolling forecast). Поскольку статичный бюджет теряет актуальность практически сразу после принятия, практика регулярного обновления прогнозов на горизонте 6–12 месяцев становится стандартом. Такой подход позволяет своевременно выявлять признаки дефицита и гибко маневрировать ресурсами, направляя их на приоритетные социальные задачи.

Фундаментом финансовой устойчивости является формирование «подушек безопасности» и инструментов для покрытия непредвиденных обязательств. Успех этих мер определяется четкостью нормативной базы: важно детально прописать условия использования резервов и алгоритмы их распределения. Создание специализированных фондов для нейтрализации конкретных угроз существенно повышает уровень доверия со стороны общества.

Современные системы управления бюджетом опираются на интеграцию данных в единую цифровую среду. Такая платформа должна объединять сведения о доходах, расходах и индикаторах риска, визуализируя их через интерактивные дашборды. Ключевое требование — обеспечение высокого качества и оперативности данных для всех уровней управления, а также предоставление доступа общественности через открытые интерфейсы.

Эффективность риск-менеджмента невозможна без развития культуры прозрачности. «Публикация бюджетной отчетности, привлечение независимых аудиторов и участие гражданских институтов в мониторинге закупок создают надежный барьер против коррупции и конфликтов интересов. Регулярный внешний контроль и открытость процессов исполнения бюджета не только повышают качество управления, но и минимизируют вероятность манипуляций, укрепляя доверие граждан к государственным институтам» [4].

Финансы сегодня — это не просто учет, а сервисная функция, опирающаяся на культуру взаимного доверия и четких правил. Внедрение единых стандартов контроля и автоматизация согласований позволяют исключить «серые зоны» и ускорить работу бюджетных подразделений. Особое место в этой системе занимает жесткий внутренний аудит и разграничение полномочий, направленные на предотвращение злоупотреблений. При этом развитие команды становится перманентным процессом: через тренинги и симуляции сценарного планирования сотрудники учатся управлять рисками в режиме реального времени.

Меняется и сама парадигма бюджетного менеджмента. Финансовый руководитель сегодня — это стратегический партнер, который видит связь между цифрами и достижением общественно значимых результатов. Умение выстраивать диалог с различными группами интересов — от внутренних департаментов до гражданского общества — становится ключевой компетенцией. Такой подход превращает бюджет из статичного документа в адаптивный инструмент, способный эффективно реагировать на вызовы времени.

Рассматривая современные тренды, важно не забывать о традиционных методах. Хотя их часто считают менее гибкими, они по-прежнему находят применение в гибридных моделях управления. Например, бюджетирование, опирающееся на данные прошлых периодов, нередко упускает из виду системные риски, консервируя неэффективные статьи расходов. Попытки контролировать бюджет без учета общей стратегии приводят к потере связи между инвестициями и доходами. Централизованный подход, лишенный обратной связи от подразделений, страдает от бюрократических задержек и не отражает реальное положение дел.

Если мониторинг ограничивается только финансовой отчетностью, организация теряет способность предвидеть риски. Дополнительными барьерами выступают слабая цифровизация, ведущая к ошибкам в данных, и недостаточная прозрачность процессов, что негативно сказывается на уровне доверия и качестве внешнего контроля.

Ниже представлена сравнительная таблица современных и традиционных подходов к управлению бюджетными рисками.

Таблица 1 - Сравнение современных и традиционных подходов к управлению бюджетными рисками

Критерии сопоставления	Современные подходы к управлению бюджетными рисками	Старые/традиционные подходы
Целевые ориентиры	Обеспечение финансовой стабильности, прозрачность процессов и сглаживание негативных экономических колебаний.	Фокус на сохранении привычных объемов трат и поверхностный контроль расходов.
Прогнозирование	Сценарное моделирование, стресс-тест, вероятностный прогноз	Опора на исторические данные и стандартное планирование на годовой цикл.
Бюджетное планирование	Rolling forecast, адаптивное бюджетирование	Инкрементальное/линейное бюджетирование
Управление рисками	Системный подход: создание реестров, назначение ответственных лиц и работа профильных комитетов.	Фрагментарный учет рисков, отсутствие единой методологии и системности.
Информационные системы	Автоматизированные системы, дашборды с КРІ и интеграция данных в реальном времени.	Использование разрозненных файлов, ручная обработка информации и низкая скорость подготовки отчетов.
Резервные фонды	Наличие четких регламентов использования и формирование фондов финансовой устойчивости.	Отсутствие строгих правил расходования резервов, не-системный подход.
Взаимодействие с участниками	Открытость бюджетных данных, вовлечение общественности и регулярные независимые проверки.	Закрытость процессов, минимальное участие внешних стейкхолдеров.
Контрольные механизмы	Разграничение полномочий, независимый аудит и многоуровневый внутренний контроль.	Централизация управления, недостаточный надзор и слабая прозрачность операций.
Культура и навыки	Обучение по риск-менеджменту, кризисные	Ограниченное обучение, традиционные процедуры

	тренировки	
Эффективность внедрения	Быстрая адаптация, гибкость, существенные улучшения за счет цифровизации	Медленная адаптация, сопротивление изменениям, затянутые процессы

«Для минимизации рисков в бюджетной сфере органов власти необходима системная работа по укреплению доходной базы, рациональному управлению обязательствами и обеспечению открытости бюджетного процесса» [3]. Ключевыми инструментами здесь становятся многолетнее планирование и сценарный анализ, подкрепленные современными ИТ-решениями и регулярным мониторингом угроз.

Эффективность системы защиты бюджета напрямую зависит от качества кадрового потенциала, строгого аудита и слаженной работы всех уровней власти. В конечном итоге, ключевой целью является сохранение социальной стабильности: бюджет должен оставаться устойчивым даже при воздействии внешних негативных факторов, обеспечивая при этом бесперебойное предоставление государственных услуг.

Сегодня управление бюджетными рисками в органах власти требует перехода к адаптивным методам работы. Успех здесь зависит не только от цифровизации процессов, но и от изменения внутренних установок: развития культуры ответственности и тесного диалога между всеми ветвями власти и населением. Переход к такой модели позволяет отойти от тактики «латания дыр» и создать надежный финансовый фундамент, гарантирующий бесперебойное оказание услуг гражданам, невзирая на любые внешние потрясения.

Список литературы

1. Бюджетный кодекс Российской Федерации от 31.07.1998 № 145-ФЗ (ред. от 26.06.2026).
2. Алексеева, И. В. Механизм нейтрализации угроз стратегии устойчивого развития экономических субъектов государственного сектора / И. В. Алексеева / Современная экономика: проблемы и решения. — 2025. — № 9. — С. 40-54. — ISSN 2078-9017. — Текст: электронный / Лань: электронно-библиотечная

система. — URL: <https://e.lanbook.com/journal/issue/375933> (дата обращения: 08.09.2026). — Режим доступа: для авториз. Пользователей.

3. Алимова, М. С. Анализ и прогнозирование расходов на национальную экономику и национальную оборону Российской Федерации в рамках реализации бюджетного процесса: монография / М. С. Алимова. — Орел: ОГУ имени И.С. Тургенева, 2025. — 103 с. — ISBN 978-5-9929-1759-8. — Текст: электронный / Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/510763> (дата обращения: 08.09.2026). — Режим доступа: для авториз. Пользователей.

4. Государственный контроль в финансово-бюджетной сфере: учебное пособие / под редакцией Р. Е. Артюхина, Э. А. Исаева. — Москва: Прометей, 2023. — 648 с. — ISBN 978-5-00172-401-8. — Текст: электронный / Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/323891> (дата обращения: 09.09.2026). — Режим доступа: для авториз. Пользователей.

5. Янов В. В. Бюджетные риски на стадии исполнения бюджета муниципального образования: монография/В. В. Янов, М. А. Каючкина. — Тольятти: Изд-во ПВГУС, 2023. — 120 с.

ПОЛИТОЛОГИЧЕСКИЕ НАУКИ

УДК 327

МНОВЕКТОРНАЯ ДИПЛОМАТИЯ ГВИНЕИ КАК СТРАТЕГИЯ АДАПТАЦИИ МАЛОГО ГОСУДАРСТВА К ФОРМИРУЮЩЕМУСЯ МНОГОПОЛЯРНОМУ МИРУ

Курума Юнуса

аспирант

Российский университет дружбы народов (РУДН),

г. Москва, Россия

Аннотация. *Статья ставит вопрос немного иначе, чем это обычно делается в работах о внешней политике Гвинеи: не что такое мновекторность гвинейской дипломатии, а зачем она понадобилась малому государству именно сейчас, когда однополярный порядок заметно слабеет. На материале политического перехода 2021–2026 гг. показано, как переходное правительство в Конакри одновременно выстраивает три параллельные линии (с Экономическим сообществом западноафриканских государств, с Россией и с Китаем), не выбирая между ними, а используя саму возможность выбора как рычаг переговорной силы. Опорой служат теория ролевой социализации малых государств и концепция «государства-убежища» (shelter theory). Центральный эмпирический сюжет: поэтапное, а не единовременное восстановление членства Гвинеи в ЭКО-ВАС, частичное снятие санкций в феврале 2024 г. и полное лишь в январе 2026 г. Такая растянутость во времени трактуется в статье не как слабость гвинейской дипломатии, а как признак смены её роли: страна перестаёт быть объектом чужих решений и становится стороной, диктующей часть условий собственного возвращения. Чтобы проверить этот тезис, гвинейский случай сопоставлен с казахстанской моделью мновекторности, более зрелой*

институционально, но построенной, по сути, на той же логике. Вывод осторожен: многополярность действительно расширяет для малых государств пространство манёвра, но превратить это пространство в устойчивую внешнеполитическую линию способны лишь те государства, чьи институты выдерживают испытание временем.

This article asks a slightly different question than is usual in the literature on Guinean foreign policy: not what Guinea's multivector diplomacy looks like, but why a small state would need it now, as unipolarity visibly erodes. Drawing on the 2021–2026 political transition, it shows how the transitional government in Conakry builds three parallel lines of engagement (with the Economic Community of West African States, with Russia, and with China) without choosing among them, treating the very possibility of choice as a source of bargaining leverage. The analysis rests on role socialization theory and the concept of shelter theory. Its central empirical episode is the staged, rather than one-off, restoration of Guinea's ECOWAS membership: partial sanctions relief in February 2024, full reinstatement only in January 2026. That drawn-out timeline is read here not as a sign of Guinean weakness but as evidence of a changing role: the country stops being an object of decisions made elsewhere and becomes a party that dictates part of the terms of its own return. To test this claim, the Guinean case is set against Kazakhstan's more institutionally mature multivector model, built, at bottom, on the same logic. The conclusion is cautious: multipolarity does widen the room for maneuver open to small states, but only those whose institutions hold up over time manage to turn that room into a stable foreign policy line.

Ключевые слова: *многополярность; малые государства; многовекторная дипломатия; Республика Гвинея; ЭКОВАС; теория ролевой социализации; Казахстан*

Keywords: *multipolarity; small states; multivector diplomacy; Republic of Guinea; ECOWAS; role socialization theory; Kazakhstan*

Введение

Формирование многополярного мироустройства сегодня редко оспаривается даже теми, кто скептически относится к самому этому термину: сила

действительно перераспределяется от узкого круга центров к более широкому набору государственных и региональных акторов, и касается это не только крупных держав. Концепция внешней политики Российской Федерации прямо называет становление многополярного мира объективной тенденцией мирового развития [1], но для малых государств из этой тенденции следует не только выгода. Круг потенциальных партнёров расширяется, однако вместе с ним растёт и сложность: приходится одновременно поддерживать отношения с несколькими центрами силы, интересы которых зачастую расходятся.

Гвинея, переживающая после смены власти в сентябре 2021 г. затяжной политический переход, позволяет увидеть эту сложность в действии. Страна оказалась под санкционным давлением региональной организации почти сразу после смены власти, но переходное правительство не свернуло внешнюю активность, а, напротив, расширило её: параллельно выстраивались отношения с Экономическим сообществом западноафриканских государств (ЭКОВАС), с Россией и с Китаем. Ниже эта стратегия рассматривается как форма адаптации малого государства к складывающемуся многополярному порядку, а гвинейский опыт сопоставляется с казахстанской моделью многовекторности, которую в литературе принято считать примером успешной ролевой социализации среднего государства.

Многополярность и малые государства: теоретическая рамка

Раскрыть логику такого поведения помогают две смежные теоретические рамки. Первая, теория ролевой социализации малых государств, описывает внешнюю политику не как разовый выбор курса, а как процесс, в котором государство постепенно осваивает и переопределяет свою роль во взаимодействии с разными партнёрами. Вторая, концепция «государства-убежища» (shelter theory), объясняет, зачем малые государства вообще ищут такие роли: не располагая достаточными ресурсами, они компенсируют структурный дефицит, встраиваясь в более крупные политические, экономические и военно-политические структуры [2]. Там, где доминирует один центр силы, выбор «убежища», как правило, невелик и во многом предопределён; по мере становления многополярности число

таких убежищ растёт, а вместе с ним расширяется и пространство манёвра малого государства.

Наиболее подробно эта логика прослежена на постсоветском материале. С. Уиллардсон и А. Карибаева показывают на примере Казахстана, что многовекторность Астаны, вопреки распространённому мнению, не сводится к пассивному балансированию между Россией, Китаем и Западом: это активный, длящийся процесс ролевой социализации, в котором государство поочерёдно осваивает и закрепляет за собой разные роли в зависимости от партнёра [3, с. 4]. Настоящая статья переносит эту же оптику на существенно менее консолидированный африканский случай, проверяя, работает ли она там, где государственность значительно менее устойчива.

Гвинея и ЭКОВАС: от санкционного давления к переговорной реинтеграции

После сентября 2021 г. ЭКОВАС ответило на смену власти в Конакри пакетом экономических и финансовых санкций, и на протяжении нескольких лет Гвинея заметно ощущала себя именно объектом регионального давления, а не стороной переговоров. Показательно, однако, что снятие этого давления произошло не одним решением, а растянулось на два этапа: в феврале 2024 г. организация частично сняла финансово-экономические санкции, а полное восстановление членства состоялось лишь в январе 2026 г. Если бы речь шла о простом возвращении блудного члена организации, логичнее было бы одно решение и одна дата; двухэтапность больше похожа на след переговорного процесса, в котором переходное правительство добивалось собственных условий возвращения, а не принимало чужие.

Похожая картина уже описана применительно к другим африканским посредническим площадкам. Т. Тьеку и А. Якохене, изучая практику Африканского союза, ЭКОВАС и ООН в Западной Африке, показывают, что переговорные механизмы урегулирования в регионе держатся не только на формальных процедурах, но и на неформальных нормах, складывающихся из повторяющегося взаимодействия одних и тех же акторов, то есть на своего рода

«сообществах практики» [4]. Гвинейский случай хорошо укладывается в эту рамку: растянутое во времени восстановление членства в ЭКОВАС стало результатом накопленного опыта взаимодействия переходных властей с региональными посредниками не меньше, чем результатом формальных договорённостей.

Россия как исторический и актуальный вектор диверсификации

Пока шли переговоры с ЭКОВАС, Гвинея не сворачивала и другие направления, из которых самое давнее и, пожалуй, наименее подверженное конъюнктуре: отношения с Россией. Н. Гришина прослеживает их шестидесятилетнюю историю и показывает, что основы сотрудничества в горнорудной отрасли и в подготовке национальных кадров были заложены ещё в советский период [5, с. 35]. Для многовекторной стратегии Гвинеи — это важная деталь: речь не о партнёрстве, которое приходится выстраивать заново под текущую политическую конъюнктуру, а о ресурсе, уже встроенном в институциональную память двусторонних отношений и потому доступном почти в любой момент, включая период санкционного давления со стороны ЭКОВАС.

Китай и экономическое измерение многовекторности

Второй внерегиональный вектор, Китай, присутствует в гвинейской экономике не столько дипломатически, сколько инфраструктурно: главным примером служит мегапроект «Симанду», один из крупнейших в мире проектов освоения месторождений железной руды. Строительство железной дороги и создание экспортных мощностей ориентированы прежде всего на китайский рынок сырья, и, по оценке Всемирного банка, реализация проекта такого масштаба способна заметно изменить структуру экспортных доходов страны [6]. Здесь стоит заметить противоречие, которое обычно ускользает из поля зрения: дипломатическая многовекторность Гвинеи (одновременные отношения с ЭКОВАС, Россией и Китаем) вовсе не означает такой же многовекторности в экономике. В горнодобывающей сфере страна фактически зависит от одного крупного покупателя, и получается, что многовекторность Гвинеи шире и разнообразнее на уровне дипломатии, чем на уровне реальной экономической зависимости.

Сравнение с Казахстаном: масштаб ресурсной базы и

институциональная зрелость

Сопоставление с Казахстаном интересно именно различиями, а не только сходством. Казахская модель многовекторности, которую С. Уиллардсон и А. Карибаева называют примером успешной ролевой социализации среднего государства [3, с. 7], опирается на несравнимо большую ресурсную базу и выстраивалась гораздо дольше, в условиях относительно консолидированной государственности. Гвинея реализует похожую по логике стратегию в куда менее благоприятных условиях: институты переходного периода нестабильны, а десятилетиями отработанных механизмов принятия внешнеполитических решений попросту нет.

Общее у обоих случаев, впрочем, важнее различий: многовекторность используется не как декларация, а как инструмент расширения переговорной позиции перед более крупными партнёрами. Расходятся страны в другом: способна ли государственная машина превратить многовекторность из ситуативного манёвра в устойчивую, предсказуемую линию.

Заключение

Гвинейский случай показывает, что в условиях складывающейся многополярности многовекторная дипломатия действительно может расширить пространство манёвра переходного правительства и изменить международную роль страны: из объекта регионального давления она постепенно превращается в сторону, которая сама формирует условия собственной реинтеграции. Поэтапное возвращение в ЭКОВАС, сохранение исторически прочных связей с Россией и развитие экономического партнёрства с Китаем в совокупности говорят именно об этом.

Но сопоставление с Казахстаном одновременно ограничивает оптимизм: устойчивость подобной стратегии в конечном счёте определяется не числом партнёров, а способностью государства превратить ситуативную многовекторность в последовательный внешнеполитический курс. Многополярный мир расширяет набор доступных малым государствам «убежищ», однако само по себе это расширение не заменяет институциональной прочности, без которой

дипломатический суверенитет остаётся скорее декларацией, чем фактом.

Список литературы

1. Об утверждении Концепции внешней политики Российской Федерации: Указ Президента Российской Федерации от 31.03.2023 № 229 [Электронный ресурс]. URL: <http://kremlin.ru/acts/bank/49090> (дата обращения: 20.09.2026).
2. Panke D., Thorhallsson B. Foreign Policy of Small States / The Oxford Handbook of Foreign Policy Analysis / ed. by J. Kaarbo, C. G. Thies. Oxford: Oxford University Press, 2024.
3. Willardson S. L., Karibayeva A. Role socialization: Kazakhstan and the nature of the multivector foreign policy role / International Politics. 2025. P. 1–26. DOI: 10.1057/s41311-025-00718-5.
4. Tieku T. K., Yakohene A. B. Exploring Communities of Practice from an Informality Perspective: Insights from the AU, ECOWAS, and UN in West African Mediation Theaters / Global Studies Quarterly. 2024. Vol. 4. No. 1. Art. ksad074. DOI: 10.1093/isagsq/ksad074.
5. Гришина Н. В. 60 лет торгово-экономических связей СССР/России с Гвинеей и Мавританией / Учёные записки Института Африки РАН. 2020. № 4 (53). С. 33–42.
6. Guinea Economic Update. 2nd ed. Washington, D.C.: World Bank Group, 2025.

**«НАУЧНЫЕ ИССЛЕДОВАНИЯ: ПРОБЛЕМЫ И
ПЕРСПЕКТИВЫ В УСЛОВИЯХ ФОРМИРОВАНИЯ
МНОГОПОЛЯРНОГО МИРА»**

XXII Международная научно-практическая конференция

Научное издание

ООО «НИЦ ЭСП» в ЮФО

(Подразделение НИЦ «Иннова»)

353445, Россия, Краснодарский край, г.-к. Анапа,

ул. Весенняя, 8, оф. 1

Тел.: 8-800-201-62-45; 8 (861) 333-44-82

Подписано в печать 22.09.2026 г. Формат 60х84/16. Усл. печ. л. 2,33
Бумага офсетная. Печать: цифровая. Гарнитура шрифта: Times New Roman
Тираж 50 экз. Заказ 149.