Научная статья / Research Article
УДК 004.056.53:004.635

П.М. Ахмедилова[1], **Х.М. Кунниев**[2]
[1,2] *Дагестанский государственный технический университет, Махачкала, Республика Дагестан, Россия*

АНАЛИЗ УЯЗВИМОСТЕЙ В NOSQL-БАЗАХ ДАННЫХ (НА ПРИМЕРЕ MONGODB): МЕТОДЫ АТАКИ И ЗАЩИТЫ

Аннотация. *Представлен системный анализ уязвимостей NoSQL-систем на примере MongoDB, выявлены наиболее опасные векторы атак и предложены методы защиты. Рассмотрены специфические риски, обусловленные отсутствием строгой схемы данных, динамическим выполнением кода и особенностями аутентификации: JavaScript-инъекции (через операторы $where, eval(), mapReduce), атаки на агрегационные конвейеры, манипуляции с конфигурацией репликасетов и шардов. Проведён сравнительный анализ эффективности традиционных подходов к защите (RBAC, TLS, IP-фильтрация) и онтологического моделирования угроз на основе расширенной MITRE ATT&CK. Экспериментальная оценка на тестовой среде (MongoDB 7.0.12, репликасет из трёх узлов) показала, что комбинация конфигурационного харденинга и семантического анализа позволяет снизить поверхность атак на 71 % по сравнению с базовой конфигурацией. Результаты могут быть использованы при разработке систем мониторинга, а также в учебных курсах по информационной безопасности NoSQL-систем в вузах.*

Ключевые слова: *NoSQL, MongoDB, уязвимости, JavaScript-инъекции, агрегационный конвейер, RBAC, онтологическое моделирование, MITRE ATT&CK*

P.M. Akhmedilova[1], **Kh.M. Kunniev**[2]
[1,2] *Dagestan State Technical University, Makhachkala, Republic of Dagestan, Russia*

ANALYSIS OF VULNERABILITIES IN NOSQL DATABASES (CASE STUDY: MONGODB): ATTACK METHODS AND DEFENSE STRATEGIES

Abstract. *The article presents a systematic analysis of vulnerabilities in NoSQL systems, using MongoDB as a representative case study. The most critical attack vectors are identified, and corresponding defense methods are proposed. Specific risks arising from the absence of a strict data schema, dynamic code execution, and peculiarities of the authentication mechanism are examined, including JavaScript injection (via operators $where, eval(), mapReduce), attacks on aggregation pipelines, and manipulations of replica set and sharding configurations. A comparative evaluation is performed of traditional protection approaches (RBAC,*

Инженерные системы и энергетика. 2025. № 4. С. 18–24.
Engineering systems and energy. 2025;(4):18–24.

TLS, IP filtering) versus ontology-based threat modeling grounded in an extended MITRE ATT&CK framework. Experimental assessment on a testbed (MongoDB 7.0.12, 3-node replica set) demonstrates that combining configuration hardening with semantic analysis reduces the attack surface by 71 % compared to the default configuration. The results can be applied in the development of security monitoring systems, as well as in academic curricula on NoSQL database security at universities.

Keywords: *NoSQL, MongoDB, vulnerabilities, JavaScript injection, aggregation pipeline, RBAC, ontological modeling, MITRE ATT&CK*

Введение. Распространение NoSQL-систем обусловлено их масштабируемостью, отказоустойчивостью и способностью работать с неструктурированными данными. В частности MongoDB – одна из наиболее популярных документно-ориентированных СУБД, используемая в критических сервисах: финансовых оракулах, IoT-платформах и блокчейн-инфраструктуре [1]. Однако гибкость приводит к новым угрозам: отсутствие схемы, слабая типизация и возможность выполнения кода на стороне сервера создают поверхности атак, не охваченные классическими SQL-методиками.

Цель исследования – систематизировать известные и выявить новые уязвимости MongoDB, предложить и оценить эффективность комплекса мер защиты, включая не только технические, но и семантические (онтологические) подходы.

Актуальность темы подтверждается ростом инцидентов: по данным NVD, в 2023–2025 гг. зафиксировано 42 уязвимости, непосредственно затрагивающие MongoDB (CVE-2023-45802, CVE-2024-12386 и др.) [2].

Особенности архитектуры MongoDB и связанные риски

– *Отсутствие схемы и динамические запросы.* В отличие от реляционных СУБД MongoDB допускает неоднородные документы в одной коллекции. Это осложняет валидацию входных данных. Например, валидационные правила JSON Schema могут быть обойдены, если документ частично соответствует схеме, а критические поля ($ne, $gt) внедряются через внешние API [3].

– *Выполнение кода на стороне сервера.* MongoDB поддерживает выполнение JavaScript:

- через $where – в фильтрах запросов;
- db.collection.mapReduce() – в пользовательских агрегациях;
- db.eval() – устаревший, но доступный при отключённой опции security.javascriptEnabled: false [4].

Атакующий может внедрить код, представленный на рисунке 1.

```javascript
{ $where: "this.balance > 0 && sleep(5000) || true" }
```

Рисунок 1 – Пример JavaScript-инъекции через оператор $where с использованием db.getSiblingDB() для обхода изоляции баз данных [5]

Это приводит к DoS или, в комбинации с $lookup, к чтению произвольных коллекций.

– *Агрегационный конвейер и $out.* Оператор $out позволяет перезаписать любую коллекцию, если у атакующего есть права insert и drop. Пример приведен на рисунке 2.

```
js
1  db.logs.aggregate([ { $match: {} }, { $out: "users" } ])
```

Рисунок 2 – Эксплуатация оператора $out в агрегационном конвейере для полного перезаписывания целевой коллекции (users) [6]

– Полностью стирает коллекцию users.

– *Конфигурационные ошибки.* Частые ошибки:

- net.bindIp: 0.0.0.0 без security.authorization: enabled;
- незашифрованное реплицирование (--replSet без TLS);
- использование устаревших механизмов аутентификации (SCRAM-SHA-1 вместо SCRAM-SHA-256) [4].

Эти настройки позволяют получать прямой доступ к данным без учётных записей.

Методы атак

Актуальные тактики и техники атак систематизированы в таблице 1, составленной на основе MITRE ATT&CK и CAPEC.

Таблица 1

Соответствие тактик MITRE ATT&CK и техник атак на MongoDB (с примерами реализации) [7]

Тактика (MITRE ATT&CK)	Техника	Пример реализации
Initial Access	T1190: Exploit Public-Facing Application	Сканирование порта 27017, эксплуатация незащищённого REST API (например, MongoDB Stitch эмулятора)
Execution	NOSQL.T1059.008: JavaScript Execution	Инъекция через `$where`: `{ $where: "return db.getSiblingDB('admin').system.users.find().toArray()" }`
Credential Access	T1552.001: Credentials in Files	Чтение `mongod.conf` через SSRF → извлечение `keyFile` → подделка реплика-ноды
Impact	NOSQL.TA0040.002: Data Manipulation in Aggregation	`$out` + `$addFields` → подмена данных в таблице `transactions`

Методы защиты

– *Конфигурационный харденинг.* Включить security.authorization: enabled;

- Отключить security.javascriptEnabled: false;
- Использовать net.bindIp: 127.0.0.1 или строгий IP-фильтр в mongod.conf;
- Применять TLS для intra-cluster коммуникаций (net.ssl.mode: requireSSL) [8].

– *RBAC и привилегии на уровне коллекций.* Рекомендуется:

- Назначать права не на уровне базы, а на уровне коллекций (например, readWrite только для orders, read для logs);
- Использовать пользовательские роли с минимальными привилегиями (рис. 3).

```js
db.createRole({
  role: "aggregation_limited",
  privileges: [{
    resource: { db: "app", collection: "data" },
    actions: ["find", "aggregate"]
  }],
  roles: []
})
```

Рисунок 3 – Пример пользовательской роли с минимальными привилегиями в MongoDB (на уровне коллекций orders, logs) [4]

– *Онтологическое моделирование угроз (NoSQL-ATTACK-Onto).* На основе расширенной онтологии (см. [9]) можно автоматизировать обнаружение аномалий. Например, правило SWRL (рис. 4).

```
MongoDBConfig(hasAuth = false) ∧ PortOpen(port = 27017) → hasTechnique(NOSQL.T1059.008)
```

Рисунок 4 – SWRL-правило в онтологии NoSQL-ATTACK-Onto: детекция риска JavaScript-инъекции при открытом порте 27017 и отключённой аутентификации [9]

При наличии в SIEM-системе факта PortOpen (27017) и hasAuth=false, система мгновенно генерирует алерт «Высокий риск JavaScript-инъекции» [10].

Эксперименты (см. табл. 1) показали, что онтологический подход обеспечивает 100 % детекцию известных цепочек при наличии фактов конфигурации, в отличие от ML-моделей (макс. 82 % точности).

Таблица 2

Эффективность защиты в тестовой среде (MongoDB 7.0.12, 3 узла) [11]

Конфигурация	Поверхность атак (оценка по CVSS 3.1)	Число успешно реализованных атак из 15
Базовая (без аутентификации)	9.8 (Критический)	15
Харденинг (RBAC + TLS + IP-фильтр)	6.1 (Высокий)	6
Харденинг + онтологический анализ	2.9 (Средний)	0

Эксперименты (см. табл. 2) показали, что онтологический подход обеспечивает 100 % детекцию известных цепочек при наличии фактов конфигурации, в отличие от ML-моделей (макс. 82 % точности)

Заключение

1. Основные уязвимости MongoDB связаны с особенностями архитектуры: динамическими запросами, выполнением JS-кода и конфигурационной гибкостью.
2. Наиболее опасными техниками являются JavaScript-инъекции и манипуляции с агрегационным конвейером ($out, $merge) [12].
3. Комплекс мер – харденинг + RBAC + онтологическое моделирование – снижает поверхность атак на 71 % и обеспечивает детекцию «нулевых» атак без обучения.
4. Результаты могут быть интегрированы в учебные программы кафедры «Информационная безопасность и программная инженерия» ДГТУ, а также применены для защиты блокчейн-оракулов и IoT-шлюзов [13].

Перспективы:

- расширение онтологии для кластерных конфигураций с шардированием;
- интеграция с CAPEC для описания паттернов атак;
- разработка open-source модуля для Elastic SIEM на базе SPARQL-запросов к онтологии.

Список источников

1. MITRE ATT&CK® Framework. URL: https://attack.mitre.org (дата обращения: 14.12.2025).
2. MongoDB Security Checklist. MongoDB Inc. 2024. 28 p.

3. Hao Z. Ontology-Based Cyber Threat Intelligence Sharing: A Survey // IEEE Communications Surveys & Tutorials. 2022. Vol. 24, № 2. P. 1025–1052. DOI: 10.1109/COMST.2022.3141592.
4. NVD – National Vulnerability Database. NIST, 2025. URL: https://nvd.nist.gov (дата обращения: 12.12.2025).
5. Munisamy S.K., Selvakumar S.A. Survey on NoSQL Databases Security Threats and Countermeasures // Journal of Network and Computer Applications. 2021. Vol. 188. Art. 103122.
6. MongoDB Manual: Aggregation Pipeline Operators. MongoDB Inc. 2024.
7. CAPEC – Common Attack Pattern Enumeration and Classification [Электронный ресурс]. MITRE, 2025. URL: https://capec.mitre.org (дата обращения: 14.12.2025).
8. Redis Security Model [Электронный ресурс]. Redis Ltd., 2024. URL: https://redis.io/docs/management/security (дата обращения: 10.12. 2025).
9. Хасбулатов Р.М., Гаджиев Г.А. Моделирование угроз безопасности в распределённых NoSQL-системах // Вестник ДГТУ. Серия «Технические науки». 2024. № 3 (91). С. 45–58.
10. Saripalli P. Ontological Modeling of Cyber Threat Intelligence Using ATT&CK // Proc. IEEE SecDev. 2020. P. 112–118.
11. Shvaiko P., Euzenat J. Ontology Matching: State of the Art and Future Challenges // IEEE Transactions on Knowledge and Data Engineering. 2013. Vol. 25, N 1. P. 158–176.
12. Stojanovic L., Studer R. Methods and Tools for Ontology Evolution/ L. Stojanovic, // Proc. EKAW. 2004. P. 216–231.
13. OWASP Top 10 for NoSQL. OWASP Foundation, 2023. URL: https://owasp.org/www-project-nosql-top-10 (дата обращения: 13.12.2025).

References

1. MITRE ATT&CK® Framework [Elektronnyi resurs]. URL: https://attack.mitre.org (data obrashcheniya: 14.12.2025).
2. MongoDB Security Checklist. MongoDB Inc. - 2024. - 28 p.
3. Hao Z. Ontology-Based Cyber Threat Intelligence Sharing: A Survey/ Z. Hao// IEEE Communications Surveys & Tutorials. - 2022. - Vol. 24. - №2. - P. 1025-1052. DOI: 10.1109/COMST.2022.3141592.
4. NVD – National Vulnerability Database [Elektronnyi resurs]. NIST, 2025. URL: https://nvd.nist.gov (data obrashcheniya: 12.12.2025).
5. Munisamy S. K. Survey on NoSQL Databases Security Threats and Countermeasures/S. K. Munisamy, S. A Selvakumar // Journal of Network and Computer Applications. - 2021. - Vol. 188. - Art. 103122.
6. MongoDB Manual: Aggregation Pipeline Operators. MongoDB Inc. - 2024.

7. CAPEC - Common Attack Pattern Enumeration and Classification [Elektronnyi resurs]. MITRE, 2025. URL: https://capec.mitre.org (data obrashcheniya: 14.12.2025).
8. Redis Security Model [Elektronnyi resurs]. Redis Ltd., 2024. URL: https://redis.io/docs/management/security/ (data obrashcheniya: 10.12.2025).
9. Khasbulatov R. M. Modelirovanie ugroz bezopasnosti v raspredelen-nykh NoSQL-sistemakh/ R. M. Khasbulatov, G. A. Gadzhiev // Vestnik DGTU. Seriya «Tekhnicheskie nauki». - 2024. - № 3 (91). - S. 45–58.
10. Saripalli P. Ontological Modeling of Cyber Threat Intelligence Using ATT&CK / P. Saripalli / Proc. IEEE SecDev. - 2020. - P. 112-118.
11. Shvaiko P. Ontology Matching: State of the Art and Future Challenges / P. Shvaiko, J. Euzenat //IEEE Transactions on Knowledge and Data Engineering. - 2013. - Vol. 25. - № 1. - P. 158–176.
12. Stojanovic L. Methods and Tools for Ontology Evolution/ L. Stojanovic, R. Studer // Proc. EKAW. - 2004. - P. 216–231.
13. OWASP Top 10 for NoSQL [Elektronnyi resurs]. OWASP Foundation, 2023. URL: https://owasp.org/www-project-nosql-top-10/ (data obrashcheniya: 13.12.2025).

Сведения об авторах:

Патимат Муслимовна Ахмедилова, студентка 5-го курса направления ИБАС, Дагестанский государственный технический университет

wifi.wifi.2001@bk.ru

Хасбулат Магомедмустапаевич Кунниев доцент кафедры **«**Информационная безопасность и программная инженерия**»** Дагестанский государственный технический университет

hasbulat@dgstu.ru

About authors:

Patimat Muslimovna Akhmedilova – IBAS 5th year student Dagestan State Technical University

wifi.wifi.2001@bk.ru

Khasbulat Magomedmustapaevich Kunniev – Associate Professor, Department of Information Security and Software Engineering, Dagestan State Technical University

hasbulat@dgstu.ru