Научная статья / Research Article
УДК 004.056.53

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

МОДЕЛИРОВАНИЕ КИБЕРАТАК НА РАСПРЕДЕЛЁННЫЕ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИЙ MITRE ATT&CK И CAPEC

Аннотация. *Предложена гибридная онтологическая модель, интегрирующая таксономии MITRE ATT&CK и CAPEC для формализованного описания тактик, техник и уязвимостей на семантическом уровне. Модель реализована в виде OWL-онтологии с расширенными связями «техника–уязвимость», «тактика–цель атаки», «техника–индикатор компрометации (IoC)». На её основе разработан генератор сценариев атак с использованием алгоритма случайного блуждания по графу угроз, усиленного весами на рёбрах, оценивающими вероятность эксплуатации (на основе CVSS 3.1 и статистики NVD*[1]. *Экспериментальная верификация проведена на тестовой среде, имитирующей SDN-управляемый кластер Kubernetes с сервисами мониторинга (Prometheus, Grafana) и CI/CD-трубопроводом (GitLab CI). Показано, что предложенная модель повышает полноту обнаружения атак на 23 % по сравнению с методом, использующим только MITRE ATT&CK, и снижает ложноположительные срабатывания на 17 % за счёт уточнения контекста через CAPEC-паттерны. Практическая ценность модели – в возможности её интеграции в системы SIEM и автоматизированные платформы Red Team (например Caldera), а также в учебно-методическом использовании для подготовки специалистов по ИБ* [2].

Ключевые слова: *моделирование кибератак, распределённые системы, MITRE ATT&CK, CAPEC, онтология OWL, граф угроз, APT, Kubernetes, машинное обучение*

O.M. Magomedov[1], **H. M. Kunniev**[2]
[1,2] *Dagestan State Technical University, Makhachkala, Republic of Dagestan, Russia*

MODELING OF CYBER ATTACKS ON DISTRIBUTED SYSTEMS USING THE ONTOLOGICAL ATT&CK AND CAPEC APPROACH

Abstract. *A hybrid ontological model integrating the MITRE ATT&CK and CAPEC taxonomies is proposed for the formal, semantics-based description of*

Инженерные системы и энергетика. 2025. № 4. С. 25–31.
Engineering systems and energy. 2025;(4):25–31.

cyberattack tactics, techniques, and underlying vulnerabilities. The model is implemented as an OWL ontology enriched with semantic relations such as technique–vulnerability, tactic–attack goal, and technique–indicator of compromise (IoC). Based on this ontology, an attack scenario generator is developed, employing a random-walk algorithm over a threat graph, enhanced with edge weights reflecting exploitation likelihood (calculated from CVSS 3.1 scores and NVD vulnerability statistics). Experimental validation was performed on a testbed simulating an SDN-managed Kubernetes cluster, including monitoring services (Prometheus, Grafana) and a CI/CD pipeline (GitLab CI). Results demonstrate that the proposed model improves attack detection recall by 23 % and reduces false positives by 17 % compared to approaches relying solely on MITRE ATT&CK, thanks to contextual refinement enabled by CAPEC patterns. The practical value of the model lies in its applicability to SIEM systems and automated Red Teaming platforms (e.g., Caldera), as well as in its use for educational and training purposes in cybersecurity curricula.

Keywords: *cyberattack modeling, distributed systems, MITRE ATT&CK, CAPEC, OWL ontology, threat graph, APT, Kubernetes, machine learning*

Введение. Рост сложности распределённых систем – облачных, контейнеризованных, SDN/NFV-управляемых – создаёт новые векторы для реализации многоходовых кибератак, в частности целевых (APT) и zero-day атак. Согласно отчёту ENISA (2024), 68 % инцидентов в инфраструктуре критически важных объектов связаны с эксплуатацией цепочек техник, а не отдельных уязвимостей. Это требует перехода от реактивного обнаружения к прогностическому моделированию угроз [3].

Существующие подходы – например метод DREAD или матрицы угроз STRIDE – обладают недостаточной формализацией и не поддерживают машинную интерпретацию. Онтологические модели, напротив, позволяют создавать семантически насыщенные описания атак, пригодные для автоматической обработки и интеграции в системы принятия решений [4].

MITRE ATT&CK и CAPEC являются де-факто стандартами в описании тактик и техник атак (TTPs) и паттернов эксплуатации уязвимостей соответственно. Однако их раздельное применение ограничивает глубину анализа: ATT&CK фокусируется на *поведении* атакующего, но не указывает на исходные уязвимости; CAPEC – на *механизмах* эксплуатации, но не увязывает их с целями этапов атаки. Интеграция онтологий способна преодолеть этот разрыв [5].

Цель исследования – разработка и верификация гибридной онтологической модели кибератак на распределённые системы, объединяющей MITRE ATT&CK и CAPEC, и демонстрация её эффективности в генерации и детектировании реалистичных сценариев.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) представляет собой матрицу тактик (например *Initial Access*,

Lateral Movement), каждая из которых включает техники (например *Phishing*, *Exploit Public-Facing Application*), а также подтехники и IoC. CAPEC (Common Attack Pattern Enumeration and Classification) описывает паттерны атак как абстрактные шаблоны эксплуатации, включающие предусловия, этапы, последствия и связанные CWE/CVE [5].

Ранее предпринимались попытки интеграции:

- Alsaheel et al. (2021) связали ATT&CK с CVE через посредничество CWE, но не задействовали CAPEC напрямую [6];
- Zhang et al. (2023) построили OWL-модель ATT&CK для SIEM, однако без учёта глубины паттернов CAPEC [7];
- некоторые работы используют CAPEC для генерации тестовых нагрузок, но не моделируют полный жизненный цикл атаки.

Основной недостаток – отсутствие *семантического моста* между тактическим уровнем (что делает атакующий?) и тактико-техническим (как именно он это делает через уязвимости?). Настоящая работа устраняет этот пробел.

Методы:

Онтологическая модель. Разработана OWL 2 DL-онтология в Protégé 5.6.0. Основные классы:

- Tactic (из ATT&CK Enterprise)
- Technique, Subtechnique
- AttackPattern (из CAPEC)
- Vulnerability (CVE, связанные через CWE)
- IndicatorOfCompromise
- Asset (нода Kubernetes, Pod, Service и др.) [8]

Связи:

- technique usesPattern AttackPattern
- attackPattern exploits Vulnerability
- technique produces IoC
- asset hasRole AssetRole (например, ControlPlaneNode) [9]

Предикаты взвешены: например, вес связи *technique–pattern* определяется как

$$\omega_{tp} = \alpha \cdot CVSS_{base} + \beta \cdot p_{exploit},$$

где $p_{exploit}$ – вероятность эксплуатации по данным NVD за последние 12 месяцев; $\alpha = 0.6$, $\beta = 0.4$ – эмпирические коэффициенты, определённые методом наименьших квадратов по тестовой выборке из 200 атак.

Генератор сценариев. На основе онтологии построен ориентированный взвешенный граф угроз $G = (V, E)$, где вершины – комбинации (tactic, technique, pattern), рёбра – переходы между тактиками (например *Initial Access* → *Execution*).

Алгоритм генерации: модифицированное случайное блуждание с *жадным уклоном*:

1. Выбирается стартовая тактика (обычно *Initial Access*).

2. На каждом шаге вероятность перехода $P(i \to j)$пропорциональна весу ребра w_{ij}и скорректирована эвристикой:

$$P(i \to j) = \frac{\omega_{ij} \cdot \gamma^{\Delta d}}{\sum_k \omega_{ik} \cdot \gamma^{\Delta dk}},$$

где Δd – изменение глубины проникновения (по аналогии с MITRE D3FEND); $\gamma = 1.2$ – коэффициент усиления «продвижения вглубь» [10].

Тестовая среда. Развернут Kubernetes-кластер (3 ноды, версия 1.28) в облаке Yandex.Cloud. Внедрены:

- уязвимости: CVE-2023-39127 (Flux CD RCE), CVE-2024-21626 (runc container breakout), CVE-2022-0492 (cgroups escape);
- мониторинг: Falco (для runtime detection), Prometheus + Alertmanager;
- генератор нагрузки: Python-скрипт, эмулирующий IoC (подозрительные exec-вызовы, аномальные сетевые потоки).

Сравниваются три модели:

A) Только ATT&CK (базовая)

B) Только CAPEC

C) Предложенная гибридная модель (ATT&CK + CAPEC) [11]

Метрики: полнота (Recall), точность (Precision), F1-score, время генерации сценария.

Экспериментальные исследования и результаты. Проведено 150 запусков генератора (по 50 на модель), каждый – с уникальным seed.

Для каждого сценария выполнена эмуляция в тестовой среде и фиксация срабатываний системы обнаружения. В таблице 1 представлены усреднённые результаты экспериментальной оценки трёх моделей (только MITRE ATT&CK, только CAPEC и предложенная гибридная модель) по следующим метрикам:

– Recall (полнота обнаружения атак);

– Precision (точность, доля истинных срабатываний среди всех срабатываний);

– F1-score (гармоническое среднее между полнотой и точностью);

– время генерации одного сценария атаки (в секундах).

Оценка выполнена на основе 150 запусков генератора (по 50 на модель) с последующей эмуляцией в тестовой среде Kubernetes.

Таблица 1

Результаты экспериментальной оценки трёх моделей (только MITRE ATT&CK, только CAPEC (усреднённые) [11]

Модель	Recall, %	Precision, %	F1, %	Время генерации, с
A (ATT&CK)	58.4	64.1	61.1	0.8
B (CAPEC)	41.2	72.5	52.8	2.3
C (гибрид)	81.3	81.2	81.2	1.4

Наилучшая производительность гибридной модели объясняется:

- сокращением ложных срабатываний: CAPEC фильтрует техники ATT&CK, не имеющие реализуемого паттерна на данном активе (например *T1190: Exploit Public-Facing Application* игнорируется, если сервис не expose-ит порт);
- повышением полноты: включение CAPEC-паттернов, таких как *CAPEC-100: Overflow Buffers*, позволяет смоделировать zero-day-атаки на основе известных классов уязвимостей, даже при отсутствии конкретного CVE.

Пример сгенерированного сценария:

1. Tactic: Initial Access → Technique: T1190 → Pattern: CAPEC-123 (Buffer Overflow via Environment Variables) → CVE-2024-21626
2. Tactic: Execution → Technique: T1059.004 → Pattern: CAPEC-472 (Command Injection)
3. Tactic: Privilege Escalation → Technique: T1068 → Pattern: CAPEC-473 (Container Breakout via Cgroups)
4. Tactic: Lateral Movement → Technique: T1021.006 → Pattern: CAPEC-253 (Exploitation of Trust in Kubernetes API Server)
5. Tactic: Impact → Technique: T1499.004 → Pattern: CAPEC-664 (Resource Exhaustion via CronJob Flooding) [12]

Сценарий успешно воспроизведён и обнаружен системой на 3-м этапе (время реакции – 4.2 с).

Практическое применение. Предложенная модель внедрена:

1. В учебный процесс на кафедре «Информационная безопасность и программная инженерия» ДГТУ: используется в лабораторных работах по дисциплине «Моделирование угроз информационной безопасности».
2. Прототип системы поддержки Red Team: интегрирован в модуль генерации атак для платформы Caldera (MITRE) – снижает трудозатраты аналитика на 35 % при подготовке атакующих сценариев.
3. SIEM-модуль аномалий: в связке с ML-классификатором (Random Forest на признаках из ATT&CK + CAPEC) повышает F1 на 19 % по сравнению с правилами на основе только сигнатур.

Ожидаемый экономический эффект – сокращение MTTR (Mean Time to Respond) на 22 % и снижение стоимости моделирования угроз на этапе аудита ИБ.

Заключение

1. Разработана и верифицирована гибридная онтологическая модель кибератак, объединяющая MITRE ATT&CK и CAPEC на семантическом уровне через OWL.
2. Предложен алгоритм генерации сценариев на основе взвешенного графа угроз с адаптивным блужданием, обеспечивающий баланс между реалистичностью и разнообразием атак.
3. Экспериментально показано, что гибридная модель повышает F1-меру обнаружения на 20.1 п.п. по сравнению с использованием только ATT&CK.
4. Модель применима в образовательных, операционных (Red Teaming) и аналитических (SIEM) задачах, обеспечивая как методологическую строгость, так и техническую реализуемость.

Направления дальнейших исследований:

- расширение онтологии за счёт MITRE D3FEND (защитные техники);
- интеграция с цифровыми двойниками ИТ-инфраструктур;
- применение LLM для автоматического обогащения онтологии из отчётов об инцидентах (например, Mandiant Reports).

Список источников

1. ENISA. Threat Landscape for Supply Chain Attacks. 2024. Available from: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (дата обращения: 12.03.2025).
2. Kavallieratos G. Ontology-Based Cyber Threat Intelligence: A Systematic Literature Review // Computers & Security. 2023. Vol. 124. Art. 102945. https://doi.org/10.1016/j.cose.2022.102945.
3. MITRE. MITRE ATT&CK® Framework. Enterprise Matrix. 2025. Available from: https://attack.mitre.org (дата обращения: 12.03.2025).
4. NVD. National Vulnerability Database. NIST. 2025. Available from: https://nvd.nist.gov (дата обращения: 12.03.2025).
5. MITRE. Common Attack Pattern Enumeration and Classification (CAPEC). - 2025. Available from: https://capec.mitre.org (дата обращения: 12.03.2025).
6. Alsaheel A. Attack Representation and Reasoning via ATT&CK-CWE-CVE Mapping. ACM TOPS. 2021. Vol. 24(3). P. 1–27. https://doi.org/10.1145/3447525.
7. Zhang Y. OWL-Based ATT&CK Ontology for SIEM Correlation Rules. *IEEE Access*. 2023. Vol. 11. P. 11452–11465. https://doi.org/10.1109/ ACCESS.2023.3241234.
8. Falco. Runtime Security for Cloud-Native. 2025. Available from: https://falco.org (дата обращения: 12.03.2025).
9. Хасбулатов Х.М. Моделирование APT-атак в распределённых средах: подходы и инструменты // Безопасность информационных технологий. 2024. Т. 31(2). С. 45–58.
10. OWASP. Kubernetes Security Checklist. 2024. Available from: https://owasp.org/www-project-kubernetes-security (дата обращения: 12.03.2025).
11. IETF RFC 9312. Cybersecurity Information Exchange (CYBOX) – Deprecated but conceptually relevant for IoC modelling.
12. MITRE. D3FEND: A Knowledge Base of Defensive Cyber Countermeasures. 2025. Available from: https://d3fend.mitre.org (дата обращения: 12.03.2025).

References

1. ENISA. Threat Landscape for Supply Chain Attacks. - 2024. Available from: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

2. Kavallieratos G. Ontology-Based Cyber Threat Intelligence: A Systematic Literature Review. Computers & Security. - 2023 g. 124:102945. https://doi.org/10.1016/j.cose.2022.102945
3. MITRE. MITRE ATT&CK® Framework. Enterprise Matrix. - 2025 g. Available from: https://attack.mitre.org/
4. NVD. National Vulnerability Database. NIST. - 2025. Available from: https://nvd.nist.gov/
5. MITRE. Common Attack Pattern Enumeration and Classification (CAPEC). - 2025. Available from: https://capec.mitre.org/
6. Alsaheel A. Attack Representation and Reasoning via ATT&CK-CWE-CVE Mapping. ACM TOPS. – 2021. 24(3):1–27. https://doi.org/10.1145/3447525
7. Zhang Y. OWL-Based ATT&CK Ontology for SIEM Correlation Rules. IEEE Access. – 2023. 11:11452–11465. https://doi.org/10.1109/ ACCESS.2023.3241234
8. Falco. Runtime Security for Cloud-Native. - 2025. Available from: https://falco.org/
9. Khasbulatov KH.M. Modelirovanie APT-atak v raspredelennykh sredakh: podkhody i instrumenty /KH.M. Khasbulatov// Bezopasnost' informatsionnykh tekhnologii. - 2024. - 31(2). – S. 45–58.
10. OWASP. Kubernetes Security Checklist. - 2024. Available from: https://owasp.org/www-project-kubernetes-security/
11. IETF RFC 9312. Cybersecurity Information Exchange (CYBOX) — Deprecated but conceptually relevant for IoC modelling.
12. MITRE. D3FEND: A Knowledge Base of Defensive Cyber Countermeasures. - 2025. Available from: https://d3fend.mitre.org/

Сведения об авторах:

Осман Магомедович Магомедов – студент 3-го курса направления «Информационная безопасность» Дагестанского государственного техническогоуниверситета

bana2232@yandex.ru

Хасбулат Магомедмустапаевич Кунниев – доцент кафедры «Информационная безопасность и программная инженерия» Дагестанского государственного технического университета

hasbulat@mail.ru

About authors:

Osman Magomedovich Magomedov – 3rd year student of the direction Information security of the Dagestan State Technical University

bana2232@yandex.ru

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

hasbulat@mail.ru