

строительное регулирование требуется разработка национальных стандартов на разборные строительные конструкции, создание нормативной базы для материальной паспортизации зданий и установление процедур сертификации пригодности материалов к повторному использованию. Без этих мер положения стратегии останутся преимущественно декларативными, а инвестиционная практика сохранит линейный характер.

#### СПИСОК ЛИТЕРАТУРЫ

1 **Benachio, G. L. F.** Circular economy in the construction industry: A systematic literature review and future research agenda / G. L. F. Benachio, M. do C. D. Freitas, S. F. Tavares // Journal of Cleaner Production. – 2024. – Vol. 435. – Art. no. 140524. – DOI: 10.1016/j.jclepro.2024.140524.

2 **Захаренко, З. Н.** Экономика строительства объектов инфраструктуры железнодорожного транспорта : учеб.-метод. пособие / З. Н. Захаренко. – Гомель : БелГУТ, 2023. – 325 с.

3 Национальная стратегия развития экономики замкнутого цикла (циркулярной экономики) Республики Беларусь на период до 2035 года : утв. постановлением Совета Министров Респ. Беларусь 29 мая 2024 г. № 393 // Национальный правовой Интернет-портал Республики Беларусь. – URL: <https://pravo.by/document/?guid=3871&p0=C22400393> (дата обращения: 08.05.2026).

Получено 26.06.2026

---

ISSN 2227-1155. Сборник студенческих научных работ.  
Вып. 31. Гомель, 2026

---

УДК 004.8:004.056

*В. Ю. АШУРКО, М. Е. ГОНЧАРОВ (ЭМ-31)*

Научные руководители: старшие преподаватели *С. В. КИСЕЛЕВА,*  
*В. Е. МИНИН*

### **ФРЕЙМВОРК ATOMIC RED TEAM ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ**

Рассматривается, как работает открытый фреймворк Atomic Red Team и как его применять для проверки систем защиты. Описаны структура атомарных тестов, способы безопасного запуска и встраивание фреймворка в рабочие процессы учебной лаборатории кибербезопасности. Предложены простые метрики для оценки качества детектирования, даны рекомендации по минимизации рисков при тестировании и сравнение с альтернативными решениями.

Современные корпоративные инфраструктуры стали сложными и распределенными. Обычные проверки безопасности, такие как периодические аудиты или сканирование уязвимостей, уже не показывают, как система

поведет себя при реальной атаке. Хакеры действуют поэтапно и стараются оставаться максимально незамеченными, поэтому компаниям нужно регулярно проверять, срабатывают ли их средства защиты и мониторинга на известные техники проникновения.

Для этого в индустрии закрепились практики Threat Emulation и Purple Teaming: команды кибербезопасности сами имитируют предполагаемые действия злоумышленников, чтобы найти слабые места в своих системах мониторинга и реагирования на проникновение. Базовым стандартом для классификации техник атак стала матрица MITRE ATT&CK, но нужен практический инструмент для реализации подобных атак. Именно таким инструментом и является фреймворк Atomic Red Team (сокр. ART). ART упрощает работу командам кибербезопасности: он содержит библиотеку готовых, воспроизводимых тестов, напрямую привязанных к техникам MITRE ATT&CK.

Главная идея ART – атомарность. Каждый тест – это небольшой, самостоятельный сценарий, который имитирует одну конкретную технику атаки (например, запуск скрипта, добавление ключа в автозагрузку или скачивание файла из интернета). Все тесты описаны в файлах формата YAML. Все тесты можно хранить в Git, отслеживать изменения и запускать автоматически.

В структуре каждого YAML-файла есть несколько обязательных блоков: метаданные – идентификатор техники из mitre att&ck, тактика, уровень сложности; пререквизиты – какие программы, права или настройки нужны для запуска; команды выполнения – непосредственные действия, имитирующие атаку; ожидаемые артефакты – что должно появиться в системе (файлы, ключи реестра, процессы); команды очистки – инструкции для отката изменений после теста.

Изначально фреймворк разрабатывался под Windows, поэтому его ядро выполнено на PowerShell. Для Linux и macOS существуют Bash-скрипты и Python-обертки, но поддержка в них неравномерная и в основном идет от пользователей. Во фреймворке присутствуют техники, завязанные на работе со специфичными для Windows механизмами (реестр, WMI, PowerShell-модули), на Unix-системах они просто не запустятся без серьезной адаптации.

Работа с ART строится по принципу Purple Teaming. Процесс можно разбить на пять шагов:

- 1 Выбрать техники, которые актуальны для конкретной инфраструктуры (исходя из отчетов по угрозам или истории инцидентов).

- 2 Загрузить подходящие тесты из репозитория ART и проверить, соответствуют ли они текущей конфигурации системы.

- 3 Запустить тесты в изолированной среде и зафиксировать телеметрию.

- 4 Проверить, записала ли система защиты эти действия (EDR, SIEM, NDR и другие), и настроить правила, если этого не произошло.

- 5 Задokumentировать результаты и использовать их для дальнейшего

улучшения систем защиты и мониторинга.

Чтобы оценивать прогресс объективно, удобно отслеживать три метрики:

1 Покрытие (Coverage Rate) – доля техник АТТ&СК, которые уже протестированы в конкретной среде. Начинать лучше с самых опасных или часто используемых техник, а не пытаться запустить все тесты сразу.

2 False Positive Rate (FPR) – процент нормальных событий, которые система защиты по ошибке приняла за атаку. Высокий FPR ведет к «усталости от предупреждений»: аналитики начинают игнорировать уведомления систем безопасности, что может привести к печальным последствиям.

3 Mean Time to Detect (MTTD) – среднее время от запуска теста до появления алерта (предупреждения) в SIEM. Чем меньше это время, тем быстрее специалисты упразднят атаку. Сам фреймворк не улучшает метрики автоматически. Прогресс появляется только если команда регулярно разбирает алерты, дорабатывает правила и убирает лишний шум. Выбор инструмента для эмуляции угроз зависит от бюджета, опыта команды и зрелости процессов. В таблице 1 приведено сравнение популярных подходов.

Открытое ПО обеспечивает полный контроль и не требует лицензионных отчислений, но за его использование нужно платить временем и техническими компетенциями. Коммерческие платформы работают «из коробки», снижают операционные риски, но привязывают организацию к вендору. На практике команды часто комбинируют подходы: ART используют для быстрых проверок конкретных техник, а коммерческие инструменты – для автоматических кампаний и управленческих отчетов.

Имитация атаки всегда несет риски. Можно случайно нарушить работу сервиса, спровоцировать блокировку легитимных процессов или оставить после теста артефакты, которые повлияют на следующие проверки. Поэтому важно соблюдать несколько базовых правил.

1 Изоляция: тестировать только на специально подготовленных стендах (виртуальные машины со снапшотами, отдельные сегменты сети).

2 Проверка требований: перед запуском убеждаться, что у теста есть нужные зависимости и права.

**Таблица 1 – Сравнительный анализ открытых и коммерческих решений для эмуляции угроз**

| Характеристика | Atomic Red Team (open-source)              | MITRE Caldera (open-source)           | Коммерческие платформы (Pentera, SafeBreach) |
|----------------|--------------------------------------------|---------------------------------------|----------------------------------------------|
| Лицензия       | MIT                                        | Apache 2.0                            | Проприетарная, подписка                      |
| Гибкость       | Высокая: редактирование YAML, открытый код | Средняя: работа через ability-профили | Ограничена логикой вендора                   |

*Окончание таблицы 1*

| Характеристика     | Atomic Red Team (open-source)                      | MITRE Caldera (open-source)                     | Коммерческие платформы (Pentera, SafeBreach) |
|--------------------|----------------------------------------------------|-------------------------------------------------|----------------------------------------------|
| Стоимость          | Нет лицензий; траты на инфраструктуру и экспертизу | Нет лицензий; нужна настройка сервера и агентов | Подписка SaaS/On-premise; поддержка включена |
| Скорость внедрения | Средняя: требует ручной подготовки тестов          | Низкая: сложная архитектура, долгая настройка   | Высокая: готовые сценарии и автоматизация    |
| Поддержка          | Сообщество, документация                           | Сообщество, официальная документация MITRE      | SLA 24/7, регулярные обновления базы ТТР     |

Обязательная очистка: после каждого теста выполняется блок cleanup, который удаляет временные файлы и откатывает изменения. Если тест упал – стенд восстанавливается из снапшота. Принцип наименьших привилегий: не запускать тесты под учетными записями с избыточными правами.

В производственной среде запускать модифицирующие тесты можно только с согласования ответственных лиц и в специально выделенные окна обслуживания. В остальное время лучше ограничиваться пассивной проверкой или тестами, которые не меняют состояние системы.

Атомарные тесты удобно встраивать в пайплайны непрерывной интеграции и доставки. Например, при каждом обновлении инфраструктуры Jenkins или GitLab CI может автоматически запускать набор тестов ART и проверять, сработали ли правила SIEM. Это реализует принцип «security as code»: безопасность проверяется на каждом этапе, а не раз в квартал.

В контексте работы учебной лаборатории кибербезопасности фреймворк помогает решать три задачи:

- калибровка правил корреляции SIEM;
- проверка автоматического реагирования (SOAR);
- тренировка аналитиков на реалистичных, но безопасных сценариях.

Главная техническая проблема здесь – дрейф окружений. Обновления операционной системы, новые версии софта или изменения в сети могут сломать старые YAML-тесты. Чтобы избежать ложных негативных результатов, нужно автоматически проверять совместимость тестов с новыми версиями систем, отслеживать успешность запусков и вовремя обновлять описания в репозитории. Без автоматизации поддержка библиотеки тестов быстро превращается в ручную и ресурсоемкую задачу.

Atomic Red Team – это практичный и доступный инструмент для регулярной проверки систем защиты. Он не заменяет полноценные пентесты или аудиты, но позволяет быстро и дешево проверять, срабатывают ли правила детекти-

рования на известные техники атак. Успешное использование ART зависит от дисциплины: четкой изоляции стендов, обязательной очистки после тестов и регулярной настройки детекторов на основе полученных данных.

Внедрение фреймворка в CI/CD-пайплайны и рабочие процессы делает проверку безопасности непрерывной частью жизненного цикла инфраструктуры. В дальнейшем ожидается более тесная интеграция ART с платформами Threat Intelligence и системами автоматизированного реагирования, что позволит командам безопасности быстрее адаптироваться к новым векторам атак.

#### СПИСОК ЛИТЕРАТУРЫ

- 1 What Is AIOps? // Gartner. – URL: <https://www.gartner.com/en/information-technology/glossary/a-i-o-p-s> (date of access: 02.04.2026).
- 2 Purple Teaming: A Methodology for Improving Detection // SANS Institute. – URL: <https://www.sans.org/blog/purple-teaming/> (date of access: 02.04.2026).
- 3 Atomic Red Team Documentation // Red Canary. – URL: <https://github.com/redcanaryco/atomic-red-team> (date of access: 02.04.2026).
- 4 Data Sources and Components // MITRE. ATT&CK Framework. – URL: <https://attack.mitre.org/resources/data-sources/> (date of access: 02.04.2026).
- 5 Atomic Test Structure and Best Practices // Red Canary. – URL: <https://github.com/redcanaryco/atomic-red-team/wiki/Atomic-Test-Structure> (date of access: 02.04.2026).
- 6 Cybersecurity Framework 2.0: Detect and Respond Functions / NIST. – Gaithersburg : NIST, 2024. – 78 p.
- 7 Data Breach Investigations Report (DBIR) 2024. – Verizon Business, 2024. – 112 p.
- 8 **Chen, M.** Alert Fatigue in Security Operations: Causes and Mitigations / M. Chen, Wang Y. // Journal of Cybersecurity. – 2023. – Vol. 9, № 1. – P. 45–62.
- 9 Validating Detection Rules with Atomic Red Team // Elastic. – URL: <https://www.elastic.co/guide/en/security/current/atomic-red-team.html> (date of access: 02.04.2026).
- 10 DevSecOps Guideline // OWASP. – URL: <https://owasp.org/www-project-devsecops-guideline/> (date of access: 02.04.2026).
- 11 Caldera: Open Source Adversary Emulation Platform // MITRE. – URL: <https://caldera.mitre.org/> (date of access: 02.04.2026).
- 12 Market Guide for Security Validation Platforms. – Gartner Research, 2023.
- 13 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. – International Organization for Standardization, 2022. – URL: <https://www.iso.org/standard/27001> (date of access: 02.04.2026).
- 14 Security Operations Center Best Practices for Threat Simulation // Microsoft. – URL: <https://learn.microsoft.com/en-us/security/operations/> (date of access: 30.03.2026).
- 15 SecOps and Continuous Security Testing Principles // CNCF. – URL: <https://www.cncf.io/blog/> (date of access: 02.04.2026).
- 16 Measuring Security Control Effectiveness: Metrics and KPIs. – SANS Reading Room, 2023.

Получено 11.06.2026