УДК 004.056.53

Прокофьева Арина Сергеевна

Студент

РГУ нефти и газа (НИУ) имени И. М. Губкина

Прокофьева Мария Сергеевна

Студент

РГУ нефти и газа (НИУ) имени И. М. Губкина

ОЦЕНКА ЭФФЕКТИВНОСТИ СКАНЕРОВ БЕЗОПАСНОСТИ КОНТЕЙНЕРНЫХ ОБРАЗОВ (TRIVY, CLAIR, ANCHORE) В СРЕДЕ ОС АЛЬТ ПО МЕТОДИКЕ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ФСТЭК РОССИИ

Аннотация. Рассмотрена задача оценки эффективности открытых сканеров безопасности контейнерных образов Trivy, Clair и Anchore (Grype + Syft) в отечественной операционной системе ОС Альт применительно к требованиям Методики анализа защищённости информационных систем, утверждённой ФСТЭК России 25 ноября 2025 г. (раздел СКО.1.4). Разработана воспроизводимая методика количественной оценки, основанная на эталонном контейнерном образе с верифицированным набором уязвимостей из Банка данных угроз безопасности информации (БДУ ФСТЭК) и международных баз CVE, а также на взвешенной интегральной оценке, учитывающей класс защищённости информационной системы по Приказу ФСТЭК России № 118. На виртуальном стенде под управлением ОС Альт проведено 18 сканирований; рассчитаны полнота (Recall), точность (Precision), производительность и доля выявленных уязвимостей из БДУ ФСТЭК. Установлено, что Trivy обеспечивает наилучшее сочетание полноты обнаружения (Recall = 87,5 %), приемлемой точности (Precision = 77,8 %) и минимального времени сканирования (8,2 с) и является единственным из рассмотренных инструментов со встроенной поддержкой формата OVAL и БДУ ФСТЭК, что соответствует пороговому

требованию раздела СКО.1.4.

Clair занимает промежуточное положение, а Grype непригоден для образов ОС Альт без доработки баз уязвимостей. Сформулированы рекомендации и матрица выбора сканера в зависимости от класса защищённости информационной системы.

Ключевые слова: контейнерная безопасность; сканер уязвимостей; Trivy; Clair; Anchore; ОС Альт; Podman; ФСТЭК России; БДУ ФСТЭК; СКО.1.4; OVAL; полнота обнаружения; точность.

Prokofieva A.S.

Student

Gubkin Russian State University of Oil and Gas

Prokofieva M.S.

Student

Gubkin Russian State University of Oil and Gas

EVALUATION OF THE EFFECTIVENESS OF CONTAINER IMAGE SECURITY SCANNERS (TRIVY, CLAIR, ANCHORE) IN THE ALT OS ENVIRONMENT ACCORDING TO THE FSTEC INFORMATION SYSTEM SECURITY ANALYSIS METHODOLOGY

Abstract. The paper addresses the evaluation of the effectiveness of open-source container image security scanners Trivy, Clair and Anchore (Grype + Syft) within the Russian ALT operating system, with respect to the requirements of the Information System Security Analysis Methodology approved by FSTEC of Russia on 25 November 2025 (section SCO.1.4). A reproducible quantitative assessment methodology is proposed; it relies on a reference container image with a verified set of vulnerabilities from the Russian Data Security Threats Database (BDU FSTEC) and international CVE databases, and on a weighted integral score that accounts for the protection class of the information system. On a virtual test bench

running ALT OS, 18 scans were performed; recall, precision, performance and the share of detected BDU FSTEC vulnerabilities were calculated. Trivy is shown to provide the best balance of detection completeness (Recall = 87.5 %), acceptable precision (77.8 %) and minimal scanning time (8.2 s), and is the only tool with built-in OVAL/BDU FSTEC support, meeting the SCO.1.4 threshold. Recommendations and a scanner-selection matrix by protection class are formulated.

Keywords: container security; vulnerability scanner; Trivy; Clair; Anchore; ALT OS; Podman; FSTEC of Russia; BDU FSTEC; SCO.1.4; OVAL; recall; precision.

ВВЕДЕНИЕ

В условиях активного импортозамещения информационных технологий и перехода государственных и критически важных информационных систем (ИС) Российской Федерации на отечественное программное обеспечение существенно возрастает роль средств контейнеризации. Контейнерные технологии (Docker, Podman, Kubernetes и их аналоги) обеспечивают высокую масштабируемость, портативность и скорость развёртывания приложений, однако одновременно расширяют поверхность атаки за счёт уязвимостей в образах контейнеров, ошибок конфигурации среды выполнения и отсутствия контроля зависимостей [27; 28]. Областью настоящего исследования является обеспечение информационной безопасности контейнерных сред в отечественных операционных системах, в которую предполагается привнести новое прикладное знание о применимости открытых средств анализа защищённости.

Систематизация рисков и уязвимостей контейнеров выполнена в обзоре [28], где предложена их таксономия по фазам жизненного цикла (образ, хост, межконтейнерное взаимодействие, сеть и оркестрация, среда выполнения). В руководстве NIST SP 800-190 образы контейнеров выделены как один из наиболее частых векторов компрометации [27]. Вопросы контейнерной

безопасности и классификации угроз на этапе развёртывания образов рассматривались в отечественных работах [5; 18], а сравнительный анализ сканеров уязвимостей в условиях импортозамещения – в работах [3; 16; 17]. Нормативную основу формируют требования ФСТЭК России к средствам контейнеризации и к защите информации в ИС [10; 11], развитые в Методике анализа защищённости информационных систем [4].

Вместе с тем в открытых источниках отсутствуют верифицированные данные о полноте, точности и производительности популярных open-source-сканеров безопасности именно в среде ОС Альт с учётом Банка данных угроз безопасности информации (БДУ ФСТЭК). Этот пробел приобретает практическую значимость в связи со вступлением в силу Методики [4], которая впервые на нормативном уровне вводит отдельный класс работ по анализу средств контейнеризации (СКО), а подраздел СКО.1.4 прямо требует выявления образов, содержащих известные уязвимости. Отсутствие таких данных создаёт риски несоответствия результатов сканирования требованиям регулятора и появления ложных отрицательных срабатываний в аттестуемых системах. Специфика ОС Альт (использование Podman в режиме без привилегий суперпользователя, собственные репозитории, интеграция с БДУ ФСТЭК) требует отдельной адаптации инструментов, изначально ориентированных на зарубежные дистрибутивы [9; 25]. Восполнение указанного пробела и составляет предмет актуальности настоящей работы.

Объект исследования – процессы выявления уязвимостей в контейнерных образах в рамках анализа защищённости информационных систем.

Предмет исследования – открытые сканеры безопасности контейнерных образов Trivy, Clair и Anchore и методика оценки их эффективности в среде ОС Альт по требованиям ФСТЭК России.

Цель работы – оценка эффективности сканеров безопасности контейнерных образов Trivy, Clair и Anchore в операционной системе Альт по требованиям Методики анализа защищённости информационных систем

ФСТЭК России. Для достижения цели поставлены следующие задачи:

1) проанализировать нормативно-правовую базу и методические документы ФСТЭК России в части анализа защищённости средств контейнеризации;
2) изучить архитектуру, возможности и особенности работы сканеров Trivy, Clair и Anchore, а также критерии оценки их эффективности;
3) разработать методику и тестовую среду для сравнительного анализа сканеров в ОС Альт с опорой на БДУ ФСТЭК;
4) выполнить экспериментальное сканирование контейнерных образов и проанализировать результаты по метрикам полноты, точности, производительности и соответствия требованиям раздела СКО.1.4.

Научная новизна работы заключается в разработке методики адаптивной оценки сканеров безопасности контейнерных образов в условиях импортозамещения, учитывающей требования ФСТЭК России к средствам контейнеризации. В отличие от известных сравнительных исследований, методика основана на эталонном тестовом образе с верифицированным набором уязвимостей из БДУ ФСТЭК, использует формализованные критерии соответствия разделу СКО.1.4 и допускает варьирование весовых коэффициентов в зависимости от класса защищённости информационной системы.

Для сравнительного анализа отобраны три открытых сканера, представляющих различные архитектурные подходы: монолитный (Trivy), микросервисный (Clair) и SBOM-ориентированный (Anchore в открытой реализации Grype + Syft). Коммерческие и облачные инструменты (Docker Scout, Snyk) исключены как недопустимые для изолированных защищённых ИС; Dependency-Track ориентирован на анализ зависимостей приложений, а не на послойное сканирование образов; Docker Bench Security проверяет лишь конфигурацию хоста. Все отобранные инструменты распространяются по открытым лицензиям и развёртываются в изолированной среде ОС Альт без доступа к внешним сетям.

ЛИТЕРАТУРНЫЙ ОБЗОР

Контейнер – изолированная исполняемая единица, разделяющая ядро хостовой ОС; образ контейнера – неизменяемый послойный шаблон, из которого создаётся контейнер. Сканер безопасности образов – средство статического анализа, сопоставляющее программные компоненты образа с базами уязвимостей. СКО – класс работ по анализу средств контейнеризации в Методике [4]; БДУ ФСТЭК – Банк данных угроз безопасности информации; OVAL – открытый формат описания уязвимостей, используемый для интеграции с БДУ; SBOM – реестр программных компонентов образа. Полнота (Recall) и точность (Precision) – метрики качества обнаружения, определяемые ниже формулами (1)–(2).

Контейнерные технологии повышают эффективность ИС за счёт низких накладных расходов и высокой плотности размещения, однако совместное использование ядра хоста формирует общую поверхность атаки. По данным исследований, контейнеризация снижает потребление ресурсов по сравнению с виртуальными машинами на 50–70 % [18; 27], но привносит риски уязвимых образов, привилегированного запуска, слабой сетевой изоляции и недостаточной защиты среды выполнения [28]. Сопоставление преимуществ и рисков приведено в таблице 1.

Таблица 1 – Преимущества и риски контейнерных технологий

Аспект	Преимущества	Риски и угрозы безопасности
Ресурсы и производительность	Низкие накладные расходы, высокая плотность размещения	Общий доступ к ядру хоста, атаки на cgroups
Портативность и изоляция	Единое окружение dev/test/prod	Выход за пределы контейнера, привилегированный доступ
Масштабируемость	Быстрое развёртывание микросервисов	Распространение угроз через оркестратор
Безопасность по умолчанию	Возможность неизменяемой инфраструктуры	Уязвимые образы, секреты в открытом виде

Нормативно-правовая база безопасности средств контейнеризации в Российской Федерации опирается на Федеральный закон № 149-ФЗ [15] и специализированные документы ФСТЭК России. Приказ ФСТЭК России от

04.07.2022 № 118 устанавливает требования к средствам контейнеризации и вводит шесть классов защиты [11], а Приказ от 11.04.2025 № 117 распространяет процессный подход к защите информации на широкий круг ИС, включая их контейнерные компоненты [10]. Ключевым методическим документом является Методика анализа защищённости информационных систем [4; 6; 7], выделяющая этапы внешнего (С1) и внутреннего (С2) анализа и отдельный класс работ СКО. Дифференциация требований по классам защиты обобщена в таблице 2.

Таблица 2 – Требования по классам защиты и уровню доверия средств контейнеризации

Класс защиты	**Уровень доверия**	**Основные требования (примеры)**
1 (высший)	1	Полный набор мер, включая сертифицированные средства обнаружения уязвимостей образов, строгая изоляция, аудит всех событий
2–3	2–3	Расширенный контроль целостности и конфигурации, обязательное сканирование образов перед развёртыванием
4–6 (низший)	4–6	Базовые меры (идентификация, регистрация событий), хостовая ОС соответствующего класса

Подраздел СКО.1.4 является центральным для оценки сканеров: он обязывает выявлять образы, содержащие известные уязвимости ПО в соответствии с БДУ ФСТЭК. Формально требование считается выполненным, если средство сканирования обеспечивает выявление не менее 80 % известных уязвимостей по идентификаторам БДУ (Recall ≥ 0,8), позволяет фильтровать результаты по записям БДУ и документировать дефекты с привязкой к идентификаторам угроз. Пороговое значение устанавливается оператором с учётом класса защищённости и может ужесточаться [4].

Операционная система семейства ОС Альт реализует контейнеризацию преимущественно на базе Podman, работающего без привилегированного демона и в режиме без привилегий суперпользователя (rootless), что соответствует принципу минимальных привилегий Приказа № 118 [11; 25].

ОС Альт предоставляет официальный реестр образов registry.altlinux.org, а в состав дистрибутива включён сканер Trivy с поддержкой формата OVAL для интеграции с БДУ ФСТЭК; в релизе «Альт СП 10» реализован встроенный механизм проверки образов по базам CVE и БДУ с блокировкой запуска скомпрометированных образов [8; 9; 2]. Ключевые особенности платформы обобщены в таблице 3.

Таблица 3 – Особенности реализации контейнеризации и сканирования уязвимостей в ОС Альт

Аспект	**Реализация в ОС Альт**	**Преимущества для безопасности**
Менеджер контейнеров	Podman (без привилегированного демона)	Минимизация эскалации привилегий (Приказ № 118)
Режим работы	Непривилегированный (rootless), subuid/subgid	Изоляция процессов, принцип минимальных привилегий
Реестр образов	Официальный registry.altlinux.org	Контроль поставки и совместимость образов
Сканер уязвимостей	Trivy + встроенный механизм (CVE + БДУ)	Покрытие требований СКО.1.4, поддержка OVAL
Дополнительные меры	Проверка целостности с блокировкой образов	Предотвращение эксплуатации уязвимых образов

Trivy – открытый универсальный сканер компании Aqua Security, написанный на Go и распространяемый единым статическим бинарным файлом. Имеет монолитную модульную архитектуру (CLI, модули сканеров, базы Trivy DB, детекторы, репортер) и выполняет статический анализ образов без их запуска [20; 29; 30; 31]. Принцип работы Trivy показан на рисунке 1.

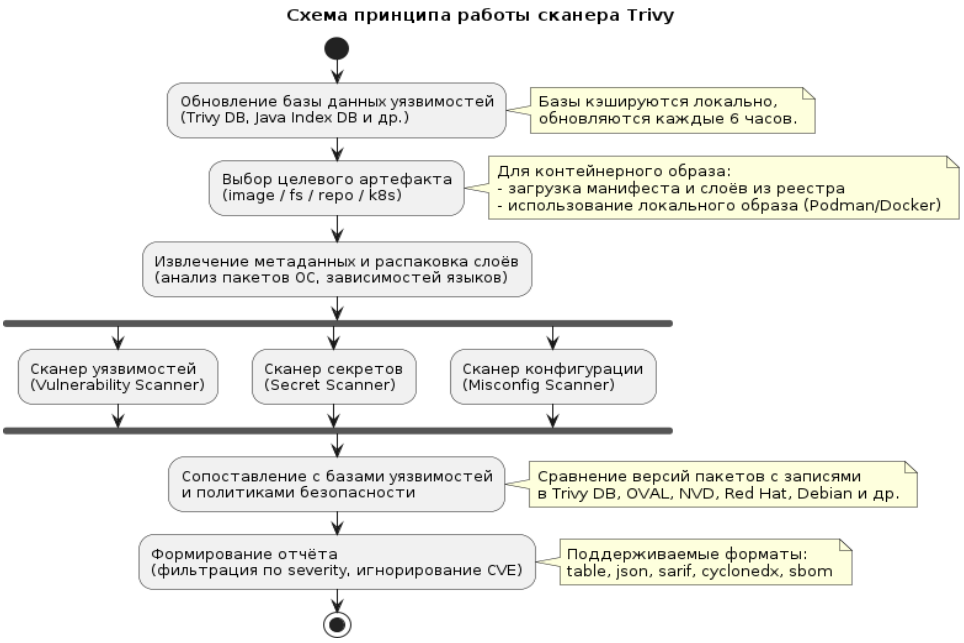

Рисунок 1 – Архитектура и принцип работы сканера Trivy (выполнено автором с использованием PlantUML)

Clair – открытый сканер уязвимостей контейнерных образов (CoreOS / Red Hat, проект Quay), построенный по микросервисной архитектуре на основе библиотеки ClairCore. Ключевые компоненты – Indexer, Matcher, Updater, API-сервер и PostgreSQL; процесс работы делится на индексацию, сопоставление и уведомление [22; 23; 24; 32]. Архитектура Clair приведена на рисунке 2.

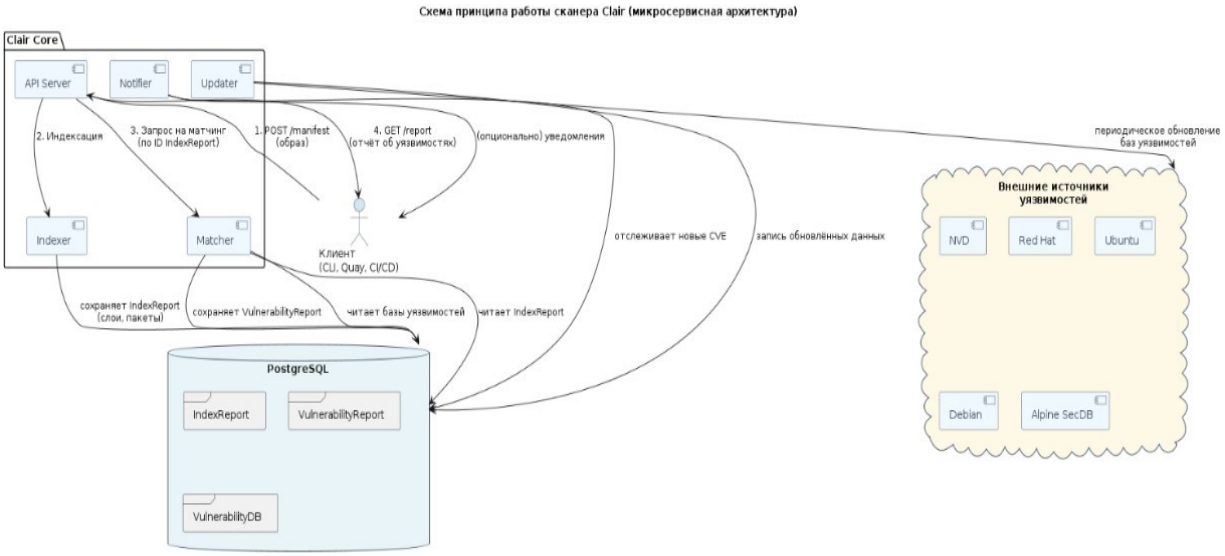

Рисунок 2 – Архитектура и принцип работы сканера Clair (выполнено автором с использованием PlantUML)

Anchore в открытой реализации представлен компонентами Syft (каталогизатор, формирующий SBOM) и Grype (движок сопоставления уязвимостей) и реализует SBOM-first-подход с политико-ориентированной оценкой рисков [19; 21]. Схема работы Anchore приведена на рисунке 3.

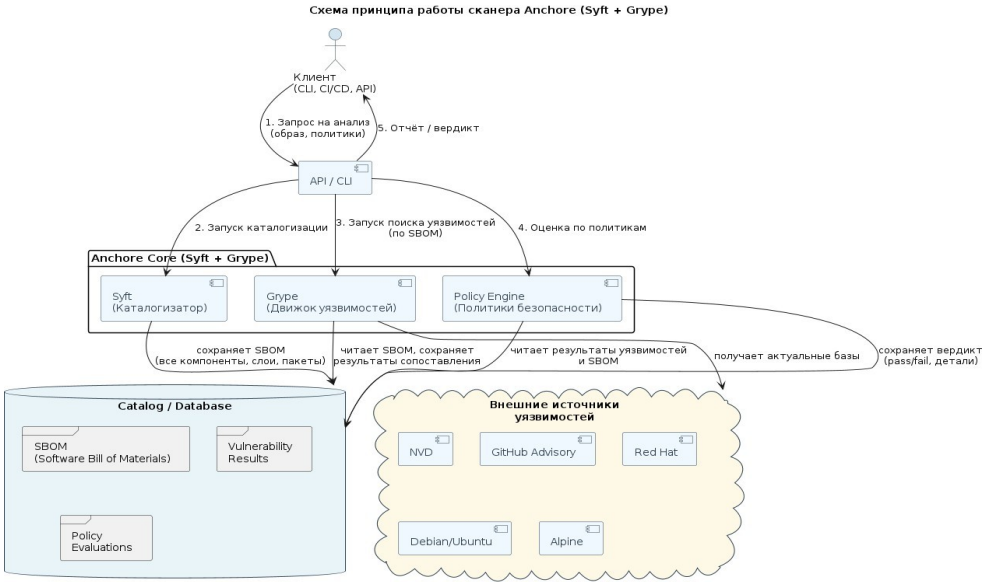

Рисунок 3 – Архитектура и принцип работы сканера Anchore (Syft + Grype) (выполнено автором с использованием PlantUML)

Сопоставление функциональных возможностей сканеров, поддерживаемых баз уязвимостей, форматов образов и интеграций приведено в таблице 4. Особое внимание уделено поддержке ОС Альт, БДУ ФСТЭК и соответствию разделу СКО.1.4.

Таблица 4 – Сравнительный анализ функциональных возможностей сканеров

Характеристика	**Trivy**	**Clair**	**Anchore**
Архитектура	Монолитная (standalone / client-server)	Микросервисная (Indexer + Matcher)	Модульная (SBOM-first: Syft → Grype)
Поддержка rootless / Podman	Полная, нативная	Полная	Полная
Поддержка ОС Альт / registry.altlinux.org	Полная (в репозиториях)	Ручная настройка	Ручная настройка
Поддержка БДУ ФСТЭК (OVAL)	Да, встроенная	Нет	Нет
Генерация SBOM	Да (CycloneDX, SPDX)	Нет	Да (подробный)
Поиск секретов	Да	Нет	Да
Оценка по политикам	Базовая	Отсутствует	Расширенная, гибкая
Соответствие СКО.1.4 Методики ФСТЭК	Высокое	Среднее	Высокое*

* при отсутствии встроенной поддержки БДУ ФСТЭК. Trivy выделяется простотой развёртывания, нативной поддержкой ОС Альт и прямой интеграцией с БДУ ФСТЭК; Clair выигрывает в крупных enterprise-окружениях с Quay, но уступает по гибкости; Anchore обеспечивает наибольшую глубину анализа за счёт SBOM и политик, но не имеет встроенной поддержки БДУ.

Оценка эффективности проводится по пяти критериям: полнота обнаружения (Recall), точность (Precision), уровень ложных срабатываний, производительность и поддержка БДУ ФСТЭК (таблица 5). Расчётные метрики определяются формулами (1)–(3):

Таблица 5 – Критерии и метрики оценки эффективности сканеров

Критерий	**Метрика**	**Формула / ед. измерения**
Полнота обнаружения	Recall	TP / (TP + FN) × 100 %
Точность	Precision	TP / (TP + FP) × 100 %
Ложные срабатывания	FP per image, FPR	FP / (TP + FP) × 100 %
Производительность	Время, CPU, RAM	с, %, МБ
Покрытие БДУ ФСТЭК	Доля выявленных уязвимостей БДУ	%

$$Recall = TP / (TP + FN) \times 100\ \% \quad (1)$$

$$Precision = TP / (TP + FP) \times 100\ \% \quad (2)$$

$$FPR = FP / (TP + FP) \times 100\ \% \quad (3)$$

где TP – истинно положительные (верно обнаруженные уязвимости), FP – ложные положительные, FN – ложные отрицательные (пропущенные) результаты. Для систем различных классов защищённости вводится взвешенная интегральная оценка эффективности (4):

$$E = w_1 \cdot Recall + w_2 \cdot Precision + w_3 \cdot БДУ + w_4 \cdot V_{норм} \quad (4)$$

$$V_{норм} = (t_{max} - t) / (t_{max} - t_{min}) \quad (5)$$

где t – время сканирования оцениваемого инструмента, t_{min} и t_{max} – минимальное и максимальное время среди сравниваемых сканеров. Весовые коэффициенты $w_1 \ldots w_4$ определяются классом защищённости ИС: для

высших классов (1–2) приоритетны полнота и поддержка БДУ ($w_1 = 0,4$; $w_3 = 0,3$; $w_2 = 0,2$; $w_4 = 0,1$); для низших (4–6) повышается значимость производительности. Приведённые значения получены экспертным методом и согласуются с подходом [12]; допускается их корректировка под конкретную модель угроз.

Гипотезы исследования. На основе анализа сформулированы три гипотезы. H1: в среде ОС Альт пороговое требование СКО.1.4 (Recall ≥ 0,8) выполняется сканером Trivy и не выполняется сканерами Grype и Clair. H2: только Trivy обладает встроенной поддержкой формата OVAL и БДУ ФСТЭК и обеспечивает 100 % покрытие подмножества уязвимостей БДУ эталонного образа. H3: ранжирование сканеров по полноте обнаружения устойчиво (Trivy
> Clair > Grype) и воспроизводится во всех прогонах.

МЕТОДЫ ИССЛЕДОВАНИЯ

Тип исследования – экспериментальное сравнительное, проводимое на цифровом двойнике инфраструктуры [14], что обеспечивает изоляцию и воспроизводимость конфигураций. Исследование сочетает количественную оценку (метрики Recall, Precision, FPR, производительность) и качественный анализ соответствия нормативным требованиям.

Характеристика выборки. В качестве объектов сканирования использованы базовые образы alt:p10 и nginx:latest, а также эталонный образ vulnerable-test:latest с заранее известным набором из 8 уязвимостей (ground truth), сформированным на базе alt:p10 путём установки устаревших версий пакетов. Перечень эталонных уязвимостей приведён в таблице 6. Каждое сканирование повторялось трижды (n = 3); общий объём эксперимента составил 3 сканера × 2 образа × 3 повторения = 18 сканирований.

Таблица 6 – Перечень уязвимостей эталонного образа vulnerable-test:latest

Пакет	Версия	Уязвимости	Кол-во
curl	7.71.0-alt1	CVE-2020-8231, CVE-2020-8284, CVE-2020-8285	3
openssl	1.1.1k-alt1	CVE-2021-23840, CVE-2021-23841, БДУ-2021-04567	3
libxml2	2.9.7-alt1	CVE-2019-19956, CVE-2020-7595	2
Итого	–	в том числе 3 уязвимости из БДУ ФСТЭК	8

Методы сбора данных. Стенд развёрнут средствами Oracle VirtualBox под управлением ОС Альт (alt-workstation-11.1-x86_64) с характеристиками: 4 ядра (Intel Core i5-8250U), 8 ГБ ОЗУ, 50 ГБ дискового пространства, сетевой адаптер NAT. Схема стенда приведена на рисунке 4. Podman настроен в режиме rootless (активация user namespaces, диапазоны subuid/subgid, fuse-overlayfs, podman system migrate), активирован сокет Podman; права доступа к каталогам образов и логов установлены в 755, к файлам – 644.

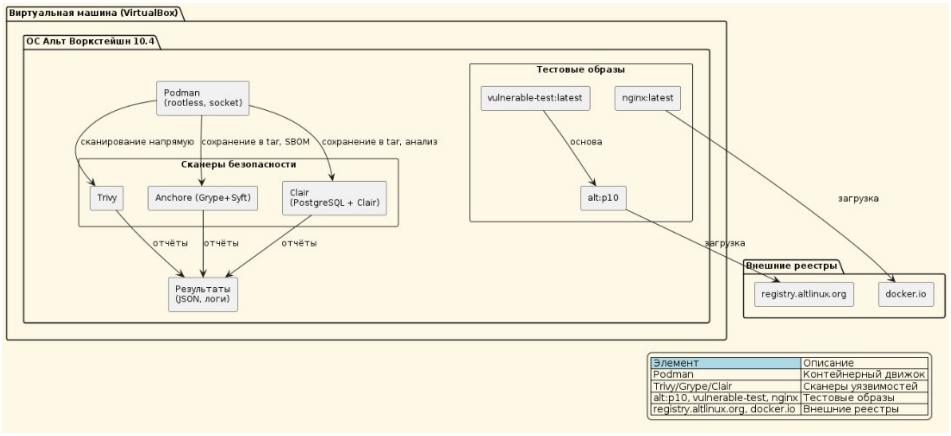

Рисунок 4 – Схема экспериментального стенда (выполнено автором с использованием PlantUML)

Установка сканеров выполнена согласно методике: Trivy установлен из официального репозитория ОС Альт (базы загружаются из российского реестра altlinux.space/trivy/trivy-db, обеспечивающего данные БДУ ФСТЭК и поддержку OVAL); Grype и Syft установлены официальными скриптами; Clair v4 развёрнут в контейнере Podman с СУБД PostgreSQL 13-alpine в изолированной сети clair-net, для управления использована утилита clairctl. Проверка показала, что Grype и Clair не имеют встроенной поддержки OVAL и БДУ ФСТЭК.

Процедура проведения исследования включает восемь последовательных этапов:

1. подготовка тестовой среды и проверка соответствия политикам безопасности ОС Альт;
2. установка и настройка сканеров Trivy, Grype + Syft и Clair, обновление

баз уязвимостей;

3. формирование базовых образов и эталонного образа с документированным перечнем уязвимостей;
4. проведение сканирований всех образов каждым сканером с фиксацией времени, потребления ОЗУ и загрузки CPU; каждый эксперимент повторяется трижды;
5. сбор отчётов и классификация результатов эталонного образа на TP, FP и FN;
6. расчёт метрик эффективности (Precision, Recall) и производительности (время, RAM, CPU) с усреднением по повторениям;
7. оценка поддержки БДУ ФСТЭК и соответствия требованиям раздела СКО.1.4;
8. сравнительный анализ результатов и формирование рекомендаций.

Методы обработки данных. Воспроизводимость обеспечена скриптами автоматизации (trivy-batch.sh, grype-batch.sh, clair-batch.sh, collect-metrics.sh, run-experiments.sh); скрипт grype-batch.sh дополнительно сохраняет образ в tar-архив и генерирует SBOM средствами Syft. Метрики производительности фиксировались утилитой /usr/bin/time и посекундным журналом загрузки CPU и ОЗУ (CSV). Классификация уязвимостей TP/FP/FN выполнена автоматизированным скриптом на языке Python путём сопоставления идентификаторов CVE/БДУ из JSON-отчётов с эталонным перечнем; для верификации проведена ручная проверка 20 % результатов каждого прогона. По итогам трёх повторений вычислены среднее арифметическое и стандартное отклонение, 95 %-ные доверительные интервалы (по t-критерию Стьюдента), а для сравнения сканеров по полноте применён непараметрический парный критерий Уилкоксона. Интегральная эффективность рассчитывается по формулам (4)–(5).

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

По итогам полного цикла экспериментов получен массив из 18 сканирований. Количество уязвимостей, выявленных каждым сканером в базовых образах, приведено в таблице 7.

Таблица 7 – Количество выявленных уязвимостей в базовых образах

Образ	Trivy	Grype (Anchore)	Clair
alt:p10	12	0	8
nginx:latest	162	162	145

Для образа alt:p10 Grype не обнаружил ни одной уязвимости, что обусловлено отсутствием в его базах данных сведений о пакетах ALT Linux; Trivy и Clair, напротив, выявили уязвимости, что подтверждает необходимость поддержки отечественных дистрибутивов. Для популярного образа nginx:latest все три сканера обнаружили более 140 уязвимостей; расхождения (162 против 145) объясняются различиями в используемых базах и алгоритмах сопоставления.

Классификация результатов сканирования эталонного образа vulnerable-test:latest (8 известных уязвимостей) приведена в таблице 8.

Таблица 8 – Классификация результатов сканирования эталонного образа

Сканер	TP (из 8)	FP	FN
Trivy	7	2	1
Grype (Anchore)	3	0	5
Clair	6	1	2

На основе данных таблицы 8 по формулам (1)–(2) рассчитаны метрики полноты и точности (таблица 9).

Таблица 9 – Метрики эффективности сканеров

Сканер	Precision, %	Recall, %
Trivy	77,8	87,5
Grype (Anchore)	100,0	37,5
Clair	85,7	75,0

Trivy демонстрирует наилучшую полноту (Recall = 87,5 %), обнаружив 7 из 8 уязвимостей при точности 77,8 % (два ложных срабатывания) и

единственным превышает пороговое значение СКО.1.4. Grype показывает абсолютную точность (100,0 %) при крайне низкой полноте (37,5 %), что делает его непригодным для образов ОС Альт без доработки баз. Clair занимает промежуточное положение (Recall = 75,0 %, Precision = 85,7 %).

Рассчитаны 95 %-ные доверительные интервалы (t-критерий Стьюдента, n = 3). Для Trivy: Recall – [84,5 %; 90,5 %] (среднее 87,5 %, SD = 1,0 %), Precision – [72,1 %; 83,5 %]; для Clair: Recall – [70,8 %; 79,2 %], Precision – [82,1
%; 89,3 %]. По парному критерию Уилкоксона различия между Trivy и Grype по полноте статистически значимы ($p < 0,05$); между Trivy и Clair значимость не достигается из-за ограниченного объёма выборки, однако направление различий устойчиво. Показатели производительности приведены в таблице 10.

Таблица 10 – Метрики производительности сканеров (среднее по 3 прогонам)

Сканер	Время, с	Пиковая RAM, МБ	Загрузка CPU, %
Trivy	8,2 ± 0,5	450	35
Grype (Anchore)	12,5 ± 1,2	320	28
Clair	45,3 ± 3,8	680	42

Trivy показывает наименьшее время сканирования (8,2 с) благодаря монолитной архитектуре и кэшированию баз; Grype затрачивает дополнительное время на генерацию SBOM (12,5 с); Clair является самым медленным (45,3 с) из-за индексации и сопоставления в PostgreSQL. Критически важная для аттестуемых ИС поддержка БДУ ФСТЭК обобщена в таблице 11.

Таблица 11 – Поддержка БДУ ФСТЭК

Сканер	Поддержка OVAL	Поддержка БДУ ФСТЭК	Доля уязвимостей БДУ
Trivy	Да (встроенная)	100 %	3 из 3 (100 %)
Grype (Anchore)	Нет	0 %	0 из 3 (0 %)
Clair	Да (заруб. дистрибутивы)	0 %	0 из 3 (0 %)

Trivy – единственный из рассмотренных сканеров со встроенной поддержкой формата OVAL, что позволяет использовать БДУ ФСТЭК в

качестве источника данных; в эксперименте он выявил все 3 уязвимости БДУ эталонного образа. Grype и Clair не поддерживают БДУ ФСТЭК, что ограничивает их применение в российских защищённых ИС.

Процесс сканирования формально описывается конвейером $M = D \cdot P \cdot E$, где E – извлечение из образа списка программных компонентов, P – сопоставление с базой уязвимостей с учётом дистрибутивно-зависимых исправлений (backport), D – фильтрация и ранжирование результатов. Расхождения между сканерами объясняются различным покрытием баз для ALT Linux (Trivy включает данные ALT, Grype – нет) и различиями алгоритмов сопоставления: Trivy учитывает дистрибутивный контекст, тогда как Grype работает по фиксированным CPE без адаптации к бэкпортам.

Для поддержки выбора инструмента в зависимости от класса защищённости ИС предложена матрица принятия решений (таблица 12).

Таблица 12 – Матрица принятия решений для выбора сканера

Класс ИС (Приказ № 118)	**Приоритетные метрики**	**Рекомендованный сканер**
1–2 (высший)	Полнота + поддержка БДУ ФСТЭК	Trivy
3	Баланс полноты и точности	Trivy или Clair*
4–6 (низший)	Производительность + точность	Clair или Trivy

* применение Clair требует дополнительной настройки OVAL-фидов для отечественных дистрибутивов.

Верификация методики. Воспроизводимость подтверждена низкой вариативностью результатов по трём прогонам (число найденных уязвимостей: Trivy – 7, 7, 8; Grype – 3, 3, 4; Clair – 6, 6, 7; SD ≈ 0,6). Корректность автоматической классификации TP/FP/FN подтверждена ручной проверкой 20 % результатов (полное совпадение). Соблюдены требования раздела СКО.1.4: применение отечественной ОС, проверка образов на известные уязвимости и подтверждённая работа Trivy с OVAL-фидами. Следует отметить, что объём выборки (n = 3) является малым для строгого статистического вывода, поэтому приведённые доверительные

интервалы и p-значения носят иллюстративный характер; вместе с тем направление различий (Trivy > Clair > Grype по полноте) устойчиво воспроизводится во всех прогонах.

ЗАКЛЮЧЕНИЕ

В работе разработана и апробирована воспроизводимая методика количественной оценки эффективности открытых сканеров безопасности контейнерных образов Trivy, Clair и Anchore в операционной системе Альт по требованиям Методики анализа защищённости информационных систем ФСТЭК России. На виртуальном стенде выполнены 18 сканирований; рассчитаны полнота, точность, производительность и доля выявленных уязвимостей из БДУ ФСТЭК. Главным результатом является методика адаптивной оценки, опирающаяся на эталонный образ с верифицированным набором уязвимостей и взвешенную интегральную оценку, учитывающую класс защищённости ИС.

Результаты проверки гипотез. Гипотеза H1 подтверждена частично: пороговое требование СКО.1.4 (Recall ≥ 0,8) выполнено только сканером Trivy (87,5 %), тогда как Clair (75,0 %) и Grype (37,5 %) ему не соответствуют. Гипотеза H2 подтверждена полностью: только Trivy обладает встроенной поддержкой OVAL/БДУ ФСТЭК и обеспечил 100 % покрытие подмножества уязвимостей БДУ эталонного образа. Гипотеза H3 подтверждена: ранжирование Trivy > Clair > Grype по полноте устойчиво воспроизводится во всех прогонах.

Таким образом, Trivy является наиболее сбалансированным инструментом, сочетающим высокую полноту, приемлемую точность, лучшую производительность и единственную встроенную поддержку БДУ ФСТЭК, что делает его оптимальным выбором для аттестуемых ИС. Clair применим ограниченно – в средах без строгого требования соответствия БДУ либо при интеграции дополнительных OVAL-фидов. Grype непригоден для образов ОС Альт без существенной доработки баз и оправдан лишь для

зарубежных дистрибутивов при отсутствии регуляторных ограничений. Практическая значимость работы состоит в применимости методики и рекомендаций при выборе инструментов анализа защищённости средств контейнеризации в государственных и критически важных ИС; теоретическая – в формализации критериев соответствия разделу СКО.1.4.

Направления дальнейшего исследования: расширение тестового набора до нескольких десятков образов различных дистрибутивов и типов приложений с общим числом уязвимостей не менее 50–100; увеличение числа прогонов до 10–30 для получения статистически значимых выводов; разработка и подключение OVAL-фидов БДУ ФСТЭК для Clair и Grype; интеграция апробированной методики в конвейеры CI/CD аттестуемых информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Лапин, В. Г. Требования по безопасности информации к средствам контейнеризации / В. Г. Лапин, Е. А. Кеньков, М. А. Лапина, Д. А. Кужева
   // Прикаспийский журнал: управление и высокие технологии. – 2025. – № 1 (69). – URL: https://cyberleninka.ru/article/n/trebovaniya-po-bezopasnosti-informatsii-k-sredstvam-konteynerizatsii (дата обращения: 19.05.2026). – Текст : электронный.
2. Листовка по продукту «Альт СП» : [сайт]. – URL: https://gosinform.ru/wp-content/uploads/2025/11/Листовка-по-продукту-Альт-СП.pdf (дата обращения: 24.03.2026). – Текст : электронный.
3. Меньшенин, А. Е. Комплекс мер для повышения уровня информационной безопасности с использованием сканера анализа безопасности / А. Е. Меньшенин, С. А. Стрельников // Развитие науки в XXI веке: вызовы, достижения и перспективы : сб. науч. тр. по материалам III Междунар. науч.-практ. конф., Анапа, 1 авг. 2025 г. – Анапа : НИЦ ЭСП в ЮФО, 2025. – С. 70–75. – EDN ORDWXK.
4. Методика анализа защищённости информационных систем : методический документ : утв. ФСТЭК России 25 нояб. 2025 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-noyabrya-2025-g (дата обращения: 24.03.2026). – Текст : электронный.
5. Молодцова, Ю. В. Классификация угроз на этапе развёртывания контейнерных образов на объектах критической информационной инфраструктуры / Ю. В. Молодцова, Д. А. Печёнов // Правовая информатика. – 2026. – № 1. – С. 52–59.
6. Обзор Методики анализа защищённости информационных систем : [сайт]. – Аттестация.ру, 2025. – URL: https://attestation.ru/article/1173/ (дата обращения: 24.03.2026). – Текст : электронный.
7. Обзор новой методики анализа защищённости ИС : [сайт]. – КСБ-Софт,

2025. – URL: https://ksb-soft.ru/blog/obzor/obzor-novoy-metodiki-analiza-zashchishchennosti-is/ (дата обращения: 24.03.2026). – Текст : электронный.

8. ОС Альт (ранее Альт Линукс, ALT Linux) : [сайт] // TAdviser. – URL: https://www.tadviser.ru (дата обращения: 24.03.2026). – Текст : электронный.
9. Отечественная операционная система «Альт СП» релиз 10 отвечает новым требованиям ФСТЭК России по защите средств виртуализации и контейнеризации : [сайт] // BaseALT. – URL: https://www.basealt.ru (дата обращения: 24.03.2026). – Текст : электронный.
10. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : приказ ФСТЭК России от 11.04.2025 № 117 : [зарегистрирован в Минюсте России 16.06.2025 № 82619]. – URL: https://fstec.ru (дата обращения: 24.03.2026). – Текст : электронный.
11. Требования по безопасности информации к средствам контейнеризации (выписка) : утв. приказом ФСТЭК России от 04.07.2022 № 118 // База данных «Гарант». – URL: https://base.garant.ru/405955413/ (дата обращения: 24.03.2026). – Текст : электронный.
12. Уймин, А. Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2023. – № 7 (600). – С. 22–29. – DOI 10.33285/2782-604X-2023-7(600)-22-29. – EDN WXXUPK.
13. Уймин, А. Г. Оценка безопасности Wine с использованием методологии STRIDE: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164–170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP.

14. Уймин, А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения / А. Г. Уймин // Радиотехнические и телекоммуникационные системы. – 2023. – № 3 (51). – С. 44–52. – DOI 10.24412/2221-2574-2023-3-44-52. – EDN QUSITK.
15. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ : [ред. от 08.08.2024] // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1). – Ст. 3448.
16. Фролов, А. Ю. Сравнительный анализ сканеров уязвимостей для аудита программного обеспечения и инфраструктуры в условиях импортозамещения / А. Ю. Фролов, Е. Н. Пальчун // Известия Тульского государственного университета. Технические науки. – 2024. – № 4. – С. 231–233. – DOI 10.24412/2071-6168-2024-4-231-232. – EDN ZXUOGK.
17. Цабей, А. А. Сравнительный анализ сканеров по методам поиска уязвимостей в системе безопасности / А. А. Цабей, Д. Н. Титов // Интеллектуальный потенциал Сибири : материалы 32-й Регион. науч. студ. конф. : в 5 ч., Новосибирск, 20–25 мая 2024 г. – Новосибирск : НГТУ, 2024. – С. 521–524. – EDN BNZOTB.
18. Цыбенко, О. С. Контейнерная безопасность / О. С. Цыбенко // E-Scio. – 2023. – № 5 (80). – С. 158–165.
19. Anchore Enterprise Architecture : [сайт]. – URL: https://docs.anchore.com/current/docs/overview/architecture/ (дата обращения: 24.03.2026). – Text : electronic.
20. Aqua Trivy: Vulnerability and Misconfiguration Scanning : [сайт] // Aqua Security. – URL: https://www.aquasec.com/products/trivy/ (дата обращения: 24.03.2026). – Text : electronic.
21. Architecture | Anchore Open Source : [сайт]. – URL: https://oss.anchore.com/docs/architecture/ (дата обращения: 24.03.2026). – Text : electronic.

22. Chapter 1. Clair security scanner : [сайт] // Red Hat Documentation. – URL: https://docs.redhat.com/en/documentation/red_hat_quay/3.11/html/vulnerability_reporting_with_clair_on_red_hat_quay/clair-vulnerability-scanner (дата обращения: 24.03.2026). – Text : electronic.
23. Clair Documentation. Architecture and Concepts : [сайт] // Quay GitHub. – URL: https://quay.github.io/clair/ (дата обращения: 24.03.2026). – Text : electronic.
24. Clair in DevSecOps: A Comprehensive Tutorial : [сайт] // DevSecOps School. – 2025. – URL: https://devsecopsschool.com/blog/clair-in-devsecops-a-comprehensive-tutorial/ (дата обращения: 24.03.2026). – Text : electronic.
25. Podman : [сайт] // ALT Linux Wiki. – URL: https://www.altlinux.org/Podman (дата обращения: 24.03.2026). – Text : electronic.
26. Project Clair : [сайт]. – URL: https://clairproject.org/ (дата обращения: 24.03.2026). – Text : electronic.
27. Souppaya, M. Application Container Security Guide : NIST Special Publication 800-190 / M. Souppaya, J. Morello, K. Scarfone. – Gaithersburg, MD : National Institute of Standards and Technology, 2017. – URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf (дата обращения: 24.03.2026). – Text : electronic.
28. Sroor, M. A Systematic Mapping Study on Risks and Vulnerabilities in Software Containers / M. Sroor, T. Das, R. Mohanani, T. Mikkonen // arXiv preprint arXiv:2512.11940v1 [cs.SE]. – 2025. – URL: https://arxiv.org/pdf/2512.11940 (дата обращения: 24.03.2026). – Text : electronic.
29. Trivy Documentation. Overview : [сайт]. – URL: https://trivy.dev/docs (дата обращения: 24.03.2026). – Text : electronic.
30. Trivy Documentation. Vulnerability Scanning : [сайт]. – URL: https://trivy.dev/docs/v0.57/guide/scanner/vulnerability/ (дата обращения: 24.03.2026). – Text : electronic.

31. Trivy Project Principles : [сайт]. – URL: https://trivy.dev/docs/latest/community/principles/ (дата обращения: 24.03.2026). – Text : electronic.
32. What is ClairV4 : [сайт] // Clair Documentation. – URL: https://quay.github.io/clair/whatis.html (дата обращения: 24.03.2026). – Text : electronic.