УДК 004.056.3

Д. С. Антропов[1]✉, Ю. Н. Ханбекова[1]

Система теневого копирования операционных систем Linux

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: a.Danila2001@yandex.ru

Аннотация. В статье рассматривается концепция разработки и практической реализации метода теневого копирования в операционных системах семейства Linux, ориентированного на повышение уровня информационной безопасности в условиях современных киберугроз. Предложенное решение основано на использовании технологий контейнеризации (Docker), а также механизмах автоматизированной маршрутизации и фильтрации сетевого трафика для создания изолированных вычислительных сред. Эти среды предназначены для безопасного анализа поведения вредоносных объектов и расследования инцидентов без воздействия на продуктивную инфраструктуру. Описан процесс формирования цифрового двойника системы, в котором реализуется возможность детального поведенческого анализа подозрительной активности. Разработанный испытательный стенд поддерживает модульную архитектуру, включает средства мониторинга, логирования и управления сетевыми политиками, что позволяет гибко конфигурировать сценарии анализа. Методика направлена на повышение эффективности цифровой криминалистики, обеспечение непрерывности работы систем и развитие адаптивных механизмов реагирования на потенциальные угрозы.

Ключевые слова: теневое копирование, виртуализация, linux, мониторинг, подотчетность, контроль целостности

D. S. Antropov[1]✉, J. N. Khanbekova[1]

Shadow copy system of linux operating systems

[1]National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: a.Danila2001@yandex.ru

Abstract. The article explores the concept of developing and practically implementing a shadow copying method in Linux-based operating systems, aimed at enhancing information security in the face of modern cyber threats. The proposed solution is based on the use of containerization technologies (Docker), as well as automated routing and network traffic filtering mechanisms to create isolated computing environments. These environments are designed for the safe analysis of malicious behavior and incident investigation without affecting the production infrastructure. The article describes the process of forming a digital twin of the system, which enables detailed behavioral analysis of suspicious activity. The developed testbed features a modular architecture, integrates monitoring, logging, and network policy management tools, and allows for flexible configuration of analysis scenarios. The methodology is aimed at improving the effectiveness of digital forensics, ensuring system continuity, and developing adaptive response mechanisms to potential threats.

Key words: shadow copying, virtualization, linux, monitoring, accountability, integrity control

Введение

Современные информационные технологии стали неотъемлемой частью функционирования организаций, обеспечивая устойчивость, гибкость и рост

бизнес-процессов. Вместе с тем, по мере увеличения масштабов и сложности IT-инфраструктуры возрастает и уязвимость к внешним и внутренним угрозам – от сбоев в работе систем до целенаправленных кибератак. Это требует постоянного совершенствования методов защиты и анализа инцидентов, особенно в средах с открытым исходным кодом, таких как Linux. Таким образом, применение изолированных модельных сред с технологиями теневого копирования позволяет решать возникающие проблемы благодаря безопасному анализу атак, восстановлению хода событий и разработке защитных мер.

С научной точки зрения, такие подходы углубляют цифровую криминалистику и повышают эффективность обнаружения угроз. Исследования [1, 2] подчеркивают важность интеллектуальной поддержки в принятии технических решений [3] и акцентируют внимание на мониторинге процессов. Развитие теневого копирования открывает перспективы для автоматизации расследований и реконструкции действий злоумышленников.

Для бизнеса эффективное расследование киберинцидентов – это способ минимизировать репутационные и финансовые потери. Цифровые двойники и моделирование инцидентов в Linux-средах становятся важным инструментом для анализа и быстрого реагирования на атаки. Работы [4, 5] также рассматривают защиту компонентов виртуальных машин, особенно в виртуализированных инфраструктурах.

С государственной стороны, законодательство требует строгих мер по мониторингу и реагированию на инциденты. ФСТЭК предписывает организациям использовать технологии идентификации атак и контроля доступа. Исследования подтверждают важность изолированных сред и цифровых двойников для повышения безопасности сетей и соответствия нормативам.

В связи со сформулированной проблематикой предметной области возникает актуальность разработки решений, позволяющих провести новые исследования в области теневого копирования при помощи контейнеризации и виртуализации [6–10].

Постановка задачи

Целью данной работы является обеспечение доступности, неотказуемости и подотчетности операционных систем Linux посредством расследования киберинцидентов в изолированной модельной среде, созданной с использованием теневого копирования. Разработка предложенного метода позволит создать среду, в которой можно безопасно анализировать последствия атак, выявлять уязвимости и разрабатывать эффективные стратегии защиты.

Предлагаемое решение

В качестве решения теневого копирования семейства ОС Linux предлагается метод защиты информационных систем, который включает в себя автоматизированное развертывание и управление приложениями, в том числе фильтрацию и маршрутизацию сетевого трафика в случае киберинцидентов, а также систему мониторинга.

Метод автоматизированного развертывания элементов инфраструктуры представляет собой структурированную последовательность взаимосвязанных процедур, направленных на корректную и безопасную инициализацию, конфигурирование и дальнейшее развертывание компонентов информационной системы. На рис.1 приведена блок-схема метода, иллюстрирующая этапы автоматизированного развертывания в рамках предлагаемой модели защиты.

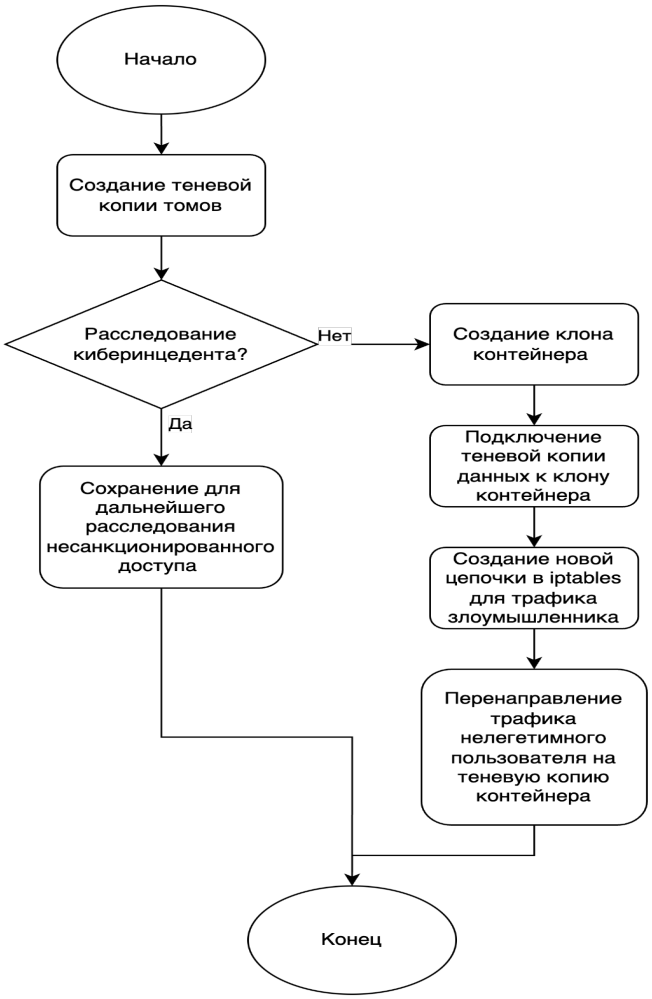

Рис. 1. Блок-схема метода теневого копирования

Проектирование метода теневого копирования начинается с подробного анализа требований к безопасности и надежности системы. Первоначально определяются ключевые аспекты: уровень защиты данных, необходимый уровень мониторинга, допустимые задержки в обработке запросов и методы выявления подозрительной активности. Это позволяет сформировать полноценную модель будущей системы.

На первом этапе осуществляется создание последней актуальной версии оригинального контейнера, в котором был зафиксирован подозрительный или критический инцидент. Это необходимо для предотвращения дальнейших изменений и фиксации состояния системы на момент обнаружения аномалии.

На следующем этапе выполняется создание клонированного контейнера на основе ранее созданного снапшота. Здесь возможны два параллельных направления: либо создается полноценный клон контейнера для идентичного воспроизведения среды, либо происходит клонирование только данных с последующим формированием нового контейнера, включающего теневую копию этих данных.

Затем происходит развертывание двух изолированных сред в случае продолжения наблюдения за злоумышленником. Клон контейнера может использоваться для оперативного восстановления или повторного воспроизведения инцидента, в то время как контейнер с теневой копией данных применяется для углубленного анализа поведения вредоносных запросов в условиях полной изоляции от основной инфраструктуры.

На заключительном этапе производится запуск соответствующих контейнеров и включение систем мониторинга и логирования. В зависимости от цели анализа данные об активности в теневой среде используются для обнаружения уязвимостей, анализа векторов атаки и принятия решений о последующих мерах реагирования, включая блокировку, отчетность или автоматическое обновление политик безопасности.

Критически важным является выбор подходящей схемы маршрутизации сетевого трафика. Предлагаемая система обеспечивает четкое разделение потоков данных, направляя запросы легитимных пользователей к основному серверу, а подозрительные – в специально выделенную изолированную среду. Подобный подход снижает риски атак на основной сервер и позволяет локализовать угрозы без влияния на работоспособность системы в целом. При проектировании учитываются не только текущие угрозы, но и перспективы дальнейшего развития системы. Архитектура является масштабируемой, гибкой и легко адаптируемой к изменяющимся условиям безопасности. Также реализованы механизмы автоматизированного создания и управления теневыми копиями для оперативного выявления и анализа потенциальных угроз в режиме реального времени.

Неотъемлемой частью является минимизация задержек при перенаправлении трафика, что достигается за счет оптимизации правил iptables и эффективного использования сетевых пространств. Учитываются также сценарии с множественными параллельными инцидентами, требующие одновременного запуска нескольких теневых копий. Предусмотрена возможность расширения логики фильтрации на основе контекстного анализа запросов и поведения пользователей. Такое проектное решение обеспечивает не только реагирование на угрозы, но и устойчивость инфраструктуры к целенаправленным атакам и внутренним нарушениям.

Архитектура системы включает пять логических зон: клиентскую часть, управляющую зону и зону анализа, а также хранилища данных и логов.

Реализация системы представлена в виде графического пользовательского интерфейса программы Docker Manager, разработанной на языке Python с применением библиотек docker, tkinter и json.

Docker Manager предлагает три основных блока функционала:

1. Управление контейнерами:

a. просмотр текущих контейнеров в удобной табличной форме;

b. возможность обновления информации о контейнерах;

c. создание «теневой копии» контейнеров с новыми томами, сетевыми настройками и образами;

d. подробный просмотр информации о контейнерах с помощью команды docker inspect;

e. удаление контейнеров.

2. Управление томами:

a. отображение списка существующих Docker-томов;

b. обновление информации о доступных томах;

c. создание копий томов при генерации теневой копии контейнеров;

d. получение детальной информации о томах через docker inspect;

e. удаление томов.

3. Управление сетями:

a. просмотр доступных Docker-сетей;

b. возможность обновления списка сетей;

c. автоматический подбор свободной подсети в заданном диапазоне с последующим созданием новой сети;

d. получение подробной информации о сети через docker inspect;

e. удаление сетей.

Процесс создания теневой копии контейнера является ключевой функцией разработанной системы. Он включает создание нового образа с помощью команды docker commit, формирование новых Docker-сетей и томов с копированием данных и запуск нового контейнера с уникальными параметрами.

Началом процесса является выбор исходного контейнера и назначение уникального имени для нового образа. Важной составляющей процесса является создание копий данных оригинального контейнера, особенно если это предусмотрено тестируемым сценарием. При наличии томов у исходного контейнера производится создание новых томов с переносом необходимых данных.

Для реализации описанного метода были использованы технологии Docker и Docker Compose, которые обеспечивают не только надежную контейнеризацию, но и гибкость управления инфраструктурой. Docker Compose позволяет организовать автоматизированный запуск связанного набора сервисов, включая базы данных, маршрутизаторы и вспомогательные компоненты мониторинга. Это существенно упрощает воспроизводимость среды, снижает трудозатраты при развертывании и минимизирует ошибки конфигурации.

Настройка сетевого взаимодействия между компонентами производится с использованием технологии Docker Bridge, позволяющей формировать изолированные виртуальные сети. Управление маршрутизацией и фильтрацией трафика реализуется посредством iptables, с применением механизмов NAT и MASQUERADE. Это дает возможность контролировать направление сетевого трафика, организовывать сокрытие внутренних адресов, а также избирательно перенаправлять потоки данных для анализа (рис. 2, 3). Такая конфигурация обеспечи-

вает высокий уровень изоляции, надежности и безопасности взаимодействия между узлами в тестируемой инфраструктуре.

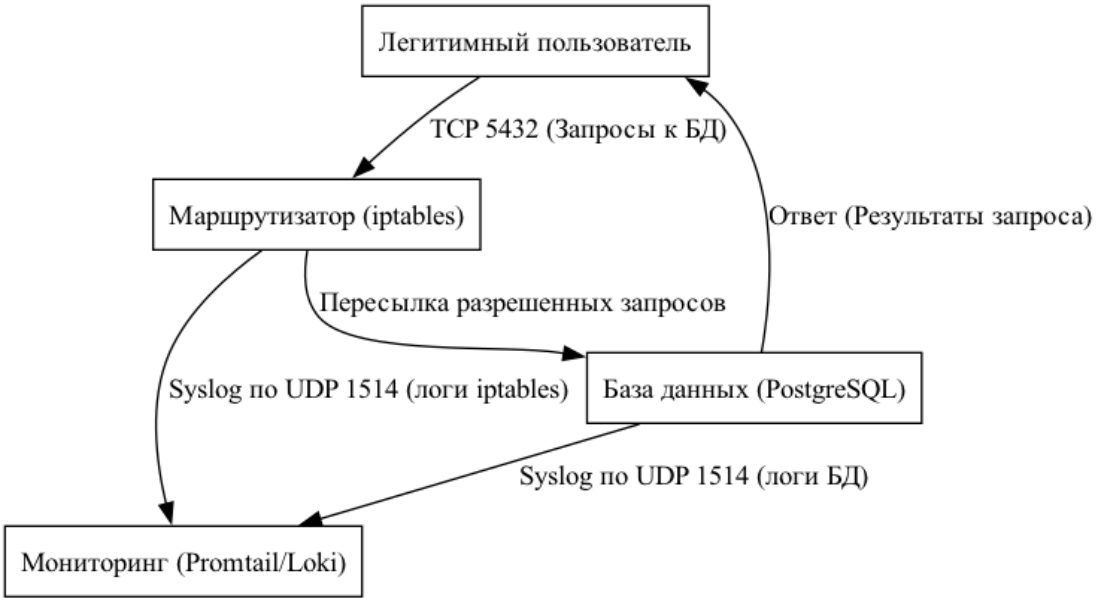

Рис. 2. Схема действий легитимного пользователя

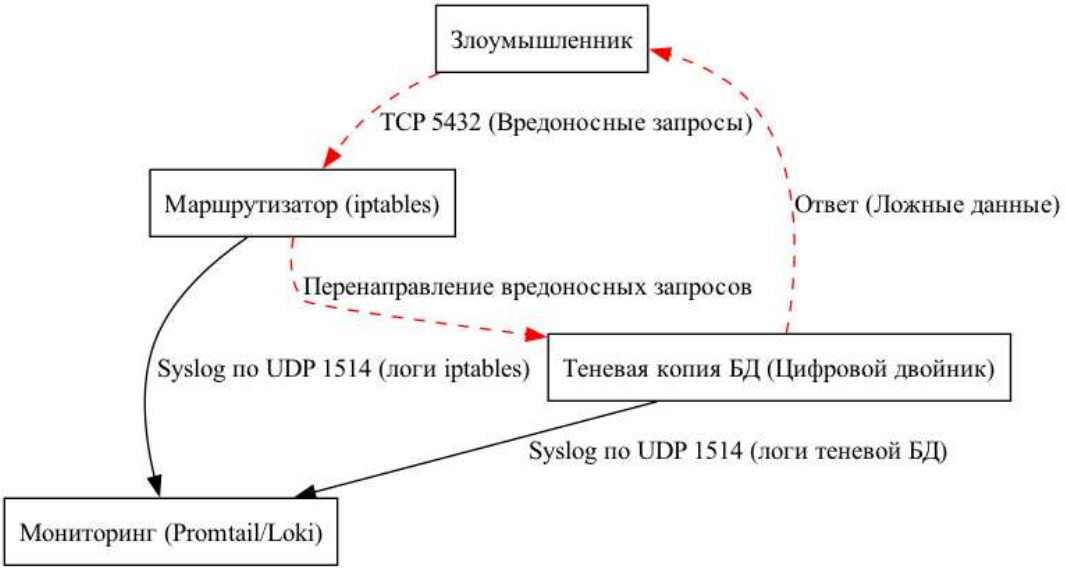

Рис. 3. Схема действий злоумышленника

Предусмотрено два сценария использования теневого копирования:

1) создание полной копии сервера с реальными данными для внутренних тестов и анализа несанкционированного доступа к системе без влияния на основной сервер;

2) создание копии сервера с фиктивными данными для анализа действий злоумышленников в реальном времени, предотвращения атак и минимизации ущерба от инцидентов.

В разработанном стенде реализован второй сценарий с созданием цифрового двойника, мониторингом и сбором метрик и логов. Стенд включает два сетевых пространства:

1) основное пространство с маршрутизатором, базой данных PostgreSQL и контейнером для клонирования.

2) мониторинговое пространство с инструментами Promtail, Loki и Grafana для анализа логов.

Ключевым компонентом также является маршрутизатор, который обеспечивает маршрутизацию и фильтрацию трафика, разграничивая доступ легитимных пользователей и злоумышленников, и ведет логирование для последующего анализа.

Для контроля сетевого трафика используется инструмент tcpdump, который позволяет перехватывать и анализировать входящие запросы к базе данных.

Разработанная система демонстрирует модульность и гибкость за счет четкой структуризации компонентов и возможности их независимого управления через графический интерфейс. Функциональные блоки по работе с контейнерами, томами и сетями обеспечивают удобство эксплуатации и прозрачность процессов клонирования. Благодаря использованию технологий Docker и iptables реализована изоляция, контроль и фильтрация трафика, что делает систему надежным инструментом для анализа киберинцидентов и управления инфраструктурой в условиях повышенных требований к безопасности.

Заключение

В рамках данной работы была предложена разработка системы теневого копирования операционных систем Linux, которая была успешно реализована в виде программного обеспечения. Использование технологий теневого копирования и создание цифровых двойников в изолированных средах представляет собой перспективный подход к повышению уровня информационной безопасности семейства операционных систем Linux. Эти методы позволяют эффективно анализировать киберинциденты, восстанавливать хронологию атак, своевременно выявлять уязвимости и разрабатывать надежные механизмы защиты, исключая риск воздействия на рабочие системы.

С научной точки зрения предложенное решение способствует дальнейшему развитию цифровой криминалистики и совершенствованию методов мониторинга и реагирования на угрозы. Внедрение данных технологий обеспечивает глубокий анализ текущих инцидентов, а также помогает прогнозировать и предотвращать возможные атаки.

С точки зрения бизнеса данный подход гарантирует непрерывность работы организаций, минимизирует риски киберугроз и защищает финансовую и персональную часть и репутацию компаний.

Таким образом, предложенный метод теневого копирования способствует повышению устойчивости систем и обеспечивает их доступность, неотказуемость и подотчетность в условиях современных информационных угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Интеллектуальная поддержка при принятии технических решений в информационной инфраструктуре предприятия // Защита информации. Инсайд. – 2020. – № 4. – С. 68-73.

2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия = Comprehensive Methodology of Intelligently Adaptive Management of an Enterprise Information Infrastructure / Е. А. Басыня. - Текст : непосредственный // Защита информации. Инсайд = Zasita informacii. Inside. - 2021. - № 5 (101). - С. 16-25.

3. Басыня Е. А., Худяков Д. С. Комплексный мониторинг информационной инфраструктуры предприятия // Защита информации. Инсайд. – 2020. – № 6. – С. 28-33.

4. Денис О. Контроль целостности компонентов виртуальных машин, созданных на базе гипервизора KVM // Безопасность информационных технологий. – 2020. – Т. 27. – № 2. – С. 118-131.

5. Zhang K., Wang X. Peeping Tom in the Neighborhood: Keystroke Eavesdropping on Multi-User Systems // USENIX Security Symposium. – 2009. – Т. 20. – С. 23.

6. Smith J., Brown A., Davis L. Enhancing Security in Linux Virtualization // International Journal of Cybersecurity. – 2022. – Т. 8. – № 5. – С. 112-120.

7. Уймин А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения // Радиотехнические и телекоммуникационные системы. – 2023. – № 3. – С. 44-52.

8. Уймин А. Г., Никитин О. Р. Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников // I-methods. – 2023. – Т. 15. – № 2. – С. 4.

9. Zakirova A. B. et al. Intelligent support in making technical decisions in the enterprise information infrastructure // Journal of Theoretical and Applied Information Technology. – 2021. – Т. 99. – № 13. – С. 3144-3154.

10. Лычкина Н. Н., Павлов В. В. Концепция цифрового двойника и роль имитационных моделей в архитектуре цифрового двойника. – 2023.