DOI 10.37882/2223-2966.2025.11.25

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВ ВИРТУАЛЬНЫХ МАШИН В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

MODERN APPROACHES TO ENSURING THE SECURITY OF VIRTUAL MACHINE IMAGES IN CLOUD INFRASTRUCTURES

V. Pakholiuk
I. Krepak

Summary. The article addresses current challenges and approaches to ensuring the security of virtual machine (VM) images in cloud infrastructures. Special attention is given to issues of integrity verification, provenance control, and protection against malicious code during the storage and operation of VM images. A model of a VM image security management system is presented, incorporating mechanisms for authentication, access control, data filtering, and change tracking. The paper also proposes directions for improving the efficiency of monitoring and automating the security assessment of virtual environments. The study is intended for researchers and practitioners in the fields of information security and cloud computing.

Keywords: cloud computing, virtual machine, VM image, security, integrity control, access management.

Пахолюк Владимир Всеволодович
Финансовый университет при Правительстве Российской Федерации, г. Москва
vova05.qwerty@mail.ru
Крепак Иван Павлович
Финансовый университет при Правительстве Российской Федерации; Руководитель группы информационной безопасности, ООО «Клиника Будь Здоров», г. Москва
krepak.2311@yandex.ru

Аннотация. В статье рассматриваются современные проблемы и подходы к обеспечению безопасности образов виртуальных машин (ВМ) в облачных инфраструктурах. Особое внимание уделяется вопросам целостности, контроля происхождения и защиты от вредоносного кода в процессе хранения и эксплуатации образов. Представлена модель системы управления безопасностью образов ВМ, включающая механизмы аутентификации, контроля доступа, фильтрации данных и отслеживания изменений. Предложены направления повышения эффективности мониторинга и автоматизации проверки безопасности виртуальных сред. Работа ориентирована на исследователей и практиков в области информационной безопасности и облачных вычислений.

Ключевые слова: облачные вычисления, виртуальная машина, образ ВМ, безопасность, контроль целостности, управление доступом.

Введение

Стремительное развитие облачных вычислений оказало глубокое влияние на архитектуру и принципы организации современных информационных систем. Использование облачных технологий позволило предприятиям и исследовательским организациям значительно повысить гибкость масштабирования ресурсов, оптимизировать затраты на эксплуатацию инфраструктуры и обеспечить непрерывность сервисов [1]. Однако, вместе с этим усложнилась задача обеспечения информационной безопасности виртуализированных сред, в которых традиционные методы защиты оказываются недостаточными [3].

Одним из наиболее критичных, и в то же время уязвимых элементов облачной экосистемы являются образы виртуальных машин (Virtual Machine Images, ВМ-образы), представляющие собой самодостаточные шаблоны программно-аппаратной среды, включающие операционные системы, прикладные модули и параметры конфигурации. Данные образы формируют исходное состояние развёртываемых виртуальных машин и, следовательно, определяют уровень защищённости всего виртуального окружения.

В отличие от обычных установочных пакетов, образы виртуальных машин представляют собой готовые к исполнению экземпляры, которые могут содержать скрытые уязвимости, фрагменты вредоносного кода, устаревшие компоненты или конфиденциальную информацию [2]. Любое несанкционированное изменение такого образа потенциально ведёт к масштабным инцидентам, включая утрату целостности данных, нарушение доступности сервисов и компрометацию всей облачной инфраструктуры.

Настоящая работа направлена на анализ рисков, связанных с эксплуатацией и распространением образов виртуальных машин, а также на систематизацию современных методов их защиты, обеспечивающих комплексное управление безопасностью на уровне облачных платформ.

Архитектура и функциональная роль виртуальных машин в облачных инфраструктурах

Виртуальная машина представляет собой изолированное вычислительное окружение, функционирующее поверх гипервизора и обеспечивающее независимое выполнение программных компонентов. Каждый экземпляр виртуальной машины создаётся на основе заранее подготовленного образа, определяющего начальное состояние операционной системы, установленных приложений и параметров безопасности.

Образы виртуальных машин выступают фундаментальным структурным элементом облачных экосистем, определяя целостность и доверенность инфраструктуры в целом. В публичных, гибридных и корпоративных облачных хранилищах, данные образы часто используются множеством пользователей и организаций, что повышает риск распространения компрометированных или модифицированных экземпляров. Таким образом, контроль их подлинности и актуальности становится неотъемлемым аспектом управления информационной безопасностью облака [4].

Основные угрозы информационной безопасности и уязвимости образов виртуальных машин

С точки зрения информационной безопасности, образы виртуальных машин подвержены комплексу типовых угроз [5], каждая из которых может иметь значительные последствия для функционирования облачной среды:

1. Нарушение целостности — несанкционированные изменения файлов образа вследствие вредоносных действий, ошибок обновлений или внутренних сбоев системы хранения.

Рис. 1. Схематическое представление архитектуры облачной платформы с репозиторием образов ВМ и модулями обеспечения безопасности

2. Компрометация конфиденциальных данных — сохранение в образе служебных ключей, паролей, временных файлов или пользовательских артефактов, что создаёт риск их утечки при совместном использовании образа.
3. Внедрение вредоносного программного обеспечения — преднамеренное включение в образы троянов, эксплойтов или программ-шпионов, распространяемых под видом легитимных шаблонов.
4. Несоблюдение лицензионных ограничений — наличие в составе образов нелицензионного или неправомерно используемого программного обеспечения.
5. Использование устаревших версий — эксплуатация образов, не содержащих актуальных обновлений безопасности, что делает их уязвимыми к известным атакам.

Наибольшую проблему представляют дормантные образы — неактивные шаблоны, хранящиеся в репозиториях без регулярной проверки. Их эксплуатация без предварительного анализа способна привести к повторному внедрению известных уязвимостей в систему.

Современные подходы к обеспечению безопасности образов виртуальных машин

Современные механизмы защиты ориентированы на создание комплексной системы управления жизненным циклом образов, включающей следующие направления:

1. Механизмы аутентификации и контроля доступа — каждому образу назначается ответственный владелец, который управляет правами на чтение, модификацию и распространение. На практике применяются модели ролевого разграничения доступа (RBAC), электронная подпись образов, а также многофакторная аутентификация при загрузке в репозиторий.
2. Проверка целостности и интеллектуальная фильтрация содержимого — при публикации и извлечении образов выполняется их автоматизированный анализ, направленный на удаление потенциально опасных данных и выявление признаков заражения. Используются криптографические хэш-функции, цифровые сертификаты доверия и базы данных сигнатур угроз.
3. Отслеживание происхождения и истории изменений (provenance tracking) — Каждое действие с образом фиксируется в виде метаданных: источник, время, операция и хэш состояния. Такая прослеживаемость обеспечивает аудит, позволяет выявлять источники инцидентов и предотвращает умышленные модификации образов.

Дополнительно применяются методы автоматического сканирования репозиториев, регулярного патчинга и удалённого обновления образов. Это формирует устойчивую среду доверия и снижает вероятность распространения уязвимых экземпляров.

Модель интегрированной системы безопасности

Эффективная стратегия защиты образов виртуальных машин реализуется посредством интегрированной системы, сочетающей профилактические и реактивные компоненты [6]. Такая система включает:

Рис. 2. Диаграмма классификации угроз безопасности образов виртуальных машин

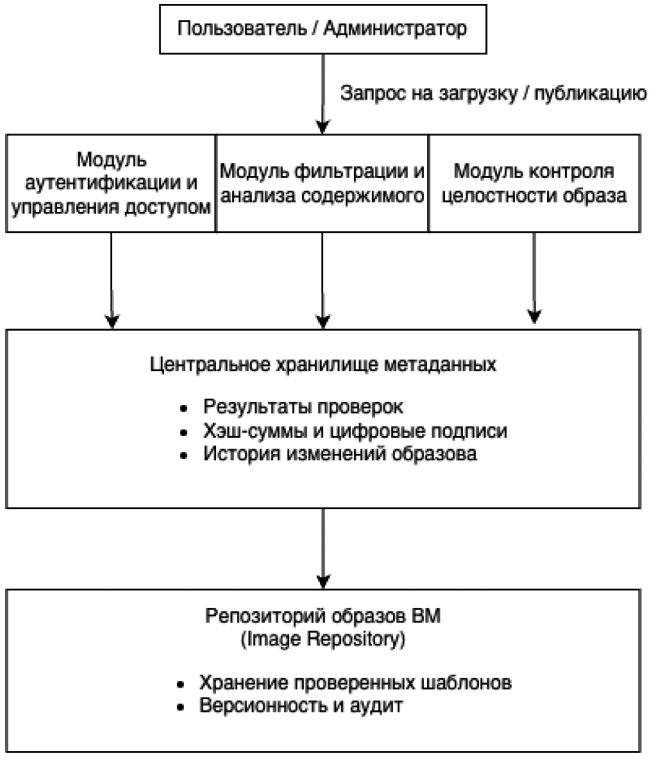

Рис. 3. Модель взаимодействия модулей системы безопасности образов виртуальных машин: аутентификация, фильтрация и контроль целостности, объединённые через центральное хранилище метаданных

— модуль идентификации и аутентификации пользователей;
— подсистему верификации цифровых подписей и контроля версий образов;
— сервис автоматического удаления конфиденциальных артефактов;
— механизм планового антивирусного сканирования и анализа уязвимостей;
— журнал событий и систему уведомлений о нарушениях целостности.

Для повышения производительности подобные решения применяют технологии дедупликации и контент-адресуемого хранения, позволяющие минимизировать объём обрабатываемых данных за счёт исключения повторяющихся элементов и анализа лишь изменённых сегментов образов.

Результаты и обсуждение

Практическое внедрение комплексных систем управления безопасностью образов виртуальных машин демонстрирует значительное снижение вероятности эксплуатации уязвимостей и распространения вредоносных элементов. По оценкам экспериментальных моделей, интеграция механизмов фильтрации и контроля целостности позволяет сократить количество потенциально небезопасных образов в репозитории на 10–15 % по сравнению с исходным состоянием.

Наличие системы отслеживания происхождения повышает прозрачность процессов администрирования и способствует формированию доказательной базы при аудите. Автоматизация обновлений и патч-менеджмента обеспечивает поддержание актуальности программных компонентов без существенного увеличения административных затрат.

Тем не менее, эффективность подобных систем во многом зависит от регулярности обновления баз угроз и своевременности коррекции фильтрующих правил. Пренебрежение этими мерами может привести к накоплению нераспознанных уязвимостей и снижению точности детектирования инцидентов.

Заключение

Безопасность образов виртуальных машин представляет собой фундаментальное условие устойчивости и надёжности облачных инфраструктур. Учитывая возрастающую сложность угроз информационной безопасности, обеспечение доверенной среды требует интеграции многоуровневых механизмов защиты — контроля целостности, управления доступом, прослеживаемости изменений и автоматического обновления компонентов.

Перспективными направлениями дальнейших исследований являются разработка интеллектуальных систем анализа образов на основе машинного обучения, внедрение динамического мониторинга поведения виртуальных экземпляров и создание единых отраслевых стандартов сертификации безопасных образов.

Комплексная автоматизация процессов обеспечения безопасности позволит минимизировать человеческий фактор, повысить уровень доверия пользователей и обеспечить устойчивое развитие облачных технологий в долгосрочной перспективе.

ЛИТЕРАТУРА

1. Armbrust M. et al. A View of Cloud Computing. Communications of the ACM, 2010.
2. Ghosh A. et al. Security of Virtual Machine Images in Cloud Computing. IEEE Cloud Computing, 2015.
3. Иванов С.А., Петрова Е.Ю. Безопасность виртуализации и облачных систем. Журнал «Информационная безопасность», 2021.
4. Козлов А.В., Смирнова Т.М. Управление безопасностью образов виртуальных машин в облаке. Труды конференции «Информационные технологии», 2019.
5. Николаев Д.Р., Сидорова Н.В. Классификация угроз виртуализации в облачных средах. Журнал «Проблемы кибербезопасности», 2020.
6. Лебедев М.Ю., Орлова А.Г. Интегрированные системы обеспечения безопасности виртуальных инфраструктур. Сборник «Современные тенденции ИБ», 2022.

Журнал «Современная наука: актуальные проблемы теории и практики»