УДК 004.056

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГЕТЕРОГЕННОЙ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ

В. П. Кочин[1)], **А. В. Шанцов**[2)]

[1)] *Белорусский государственный университет,*
г. Минск, Республика Беларусь, kochyn@bsu.by
[2)] *Белорусский государственный университет,*
г. Минск, Республика Беларусь, downseason@mail.ru

Определена необходимость применения гетерогенных платформ виртуализации. Выделены основные преимущества в использовании гетерогенных платформ виртуализации. Рассмотрена проблематика обеспечения требуемого уровня защищенности ресурсов гетерогенной платформы. Определена необходимость применения формализованных подходов к процессам обеспечения информационной безопасности. Предложен алгоритм и математическая модель обеспечения информационной безопасности гетерогенных платформ виртуализации.

Ключевые слова: информационная безопасность; облачные вычисления; гетерогенная платформа виртуализации.

MATHEMATICAL MODEL OF ENSURING INFORMATION SECURITY OF A HETEROGENEOUS VIRTUALIZATION PLATFORM

V. P. Kochyn[a)], **A. V. Shantsov**[b)]

[a)] *Belarusian State University,*
Minsk, Republic of Belarus, kochyn@bsu.by
[b)] *Belarusian State University,*
Minsk, Republic of Belarus, downseason@mail.ru

This paper justifies the necessity of employing heterogeneous virtualization platforms, highlighting their principal advantages. It examines the challenges associated with ensuring the required security level for the resources within such heterogeneous environments. The study underscores the need for formalized approaches to information security management. In response to these challenges, we propose a novel algorithm and develop a mathematical model designed to ensure the information security of heterogeneous virtualization platforms.

Keywords: information security; cloud computing; heterogeneous virtualization platform.

1. Введение

Технологии виртуализации прочно вошли в основу современной вычислительной инфраструктуры, обеспечивая эффективное использование ресурсов, снижение затрат и высокую отказоустойчивость. Вместе с тем, увеличение масштабов и сложности виртуализированных сред обуславливает потребность в формализации управленческих процессов, в особенности – механизмов обеспечения информационной безопасности (ИБ) в облачной среде. Пренебрежение регламентами значительно увеличивает риски неоптимального расходования ресурсов, снижения производительности и возникновения угроз ИБ [1].

Внедрение гетерогенных платформ виртуализации открывает широкие возможности для повышения гибкости, отказоустойчивости и общей эффективности управления ИТ-инфраструктурами. Однако для реализации всех преимуществ подобных платформ необходима тщательная формализация процессов управления, среди которых важную роль играет формализация процессов обеспечения защищенности виртуальных машин (ВМ) и платформы в целом.

2. Преимущества применения гетерогенных платформ виртуализации

Внедрение гетерогенных платформ виртуализации позволяет достичь значительного повышения гибкости, устойчивости и безопасности обработки ресурсов. Гетерогенная платформа виртуализации включает в себя две и более подсистемы виртуализации, построенные на различных гипервизорах, объединенных в единый вычислительный кластер [2]. Использование гетерогенных платформ имеет ряд существенных преимуществ, в том числе в аспекте ИБ.

1. Повышение гибкости и совместимости. Использование разнородных гипервизоров, архитектур и аппаратных решений в рамках единой инфраструктуры обеспечивает:

интеграцию унаследованных и современных информационных систем с учётом требований безопасности;

адаптацию под специфические задачи и сервисы за счёт выбора наиболее релевантных и безопасных технологических решений для каждого конкретного случая.

2. Минимизация рисков зависимости от единственного вендора (vendor lock-in). Эксплуатация множества платформ виртуализации (таких как VMware ESXi, Microsoft Hyper-V, KVM, Xen, OpenStack) способствует:

снижению зависимости от конкретного поставщика, что уменьшает риски, связанные с уязвимостями в продуктах одного вендора;

повышению гибкости при изменениях в лицензионной политики или стратегии вендора;

обеспечению возможности миграции между платформами без необходимости полной реконфигурации инфраструктуры.

3. Повышение устойчивости и отказоустойчивости. Гетерогенная архитектура снижает системные риски, связанные с отказами на уровне гипервизора или системного ПО. Так, уязвимость или сбой одной платформы не приводит к полному отказу системы, поскольку иная подсистема остаётся работоспособной. Кроме того, появляется возможность изоляции критичных подсистем на различных гипервизорах, что повышает общий уровень безопасности архитектуры и снижает риски распространения атак.

4. Поддержка безопасных гибридных и мультиоблачных стратегий. Гетерогенные платформы являются фундаментом для построения сложных сред, объединяющих частные и публичные облака, а также периферийные вычисления. Это позволяет:

размещать рабочие нагрузки (ВМ, контейнеры) в оптимальной среде в зависимости от требований к безопасности, производительности, а также требований нормативных правовых актов;

осуществлять централизованное управление и оркестрацию с помощью кросс-платформенных инструментов (Kubernetes, Terraform, Ansible, OpenStack), абстрагирующихся от особенностей нижележащих гипервизоров.

5. Усиление защиты за счёт разнородности среды. Разнообразие программных и аппаратных платформ затрудняет для злоумышленников проведение масштабных атак, поскольку требует разработки различных эксплуатационных методов для каждого типа гипервизора, что в свою очередь позволяет:

осуществить изоляцию критически важных ресурсов на отдельных гипервизорах с уникальными настройками безопасности;

снизить риски «горизонтального перемещения» злоумышленников в случае компрометации одного из компонентов среды;

реализовать принцип комплексной защиты [3], где каждая платформа может быть настроена согласно определенных требований к обеспечению ИБ.

3. Математическая модель обеспечения информационной безопасности гетерогенной платформы

Одновременное использованием разнородных гипервизоров в гетерогенных платформах виртуализации формирует расширенную и многокомпонентную поверхность для потенциальных атак. Неоднородность гетерогенных платформ влечет за собой существенные риски ИБ, включая усложнение управления уязвимостями, несогласованность политик безопасности, трудности в мониторинге и аудите безопасности. Таким

образом, несмотря на все преимущества, гетерогенные платформы порождают комплексные риски ИБ.

Для управления рисками ИБ необходимо использовать математическое моделирование процессов обеспечения ИБ в гетерогенных средах, направленное на решения следующих задач.

1. Формализация и автоматизация политик безопасности. Создание строгих математических моделей позволяет перейти от эвристических правил к детерминированным алгоритмам принятия решений, что минимизирует человеческий фактор – частую причину уязвимостей и ошибок конфигурации.

2. Оптимизация обнаружения инцидентов ИБ. Моделирование позволяет выявлять характерные для кибератак аномалии в поведении ВМ и гипервизоров в условиях высокой сложности и неоднородности инфраструктуры, повышая точность и скорость детектирования угроз [4].

3. Сокращение времени реагирования на киберинциденты. Алгоритм обеспечения безопасности обеспечивает не только своевременное обнаружение, но и автоматизацию ответных мер, таких как изоляция скомпрометированной ВМ или ее миграция на защищенный узел, что критически важно для снижения ущерба [5].

4. Повышение отказоустойчивости и живучести системы. Применение различных платформ виртуализации и возможности динамической балансировки ВМ обеспечивают высокую отказоустойчивость гетерогенной платформы в целом.

Таким образом, актуальность исследований в данной области обусловлена их высокой прикладной значимостью для построения защищенной от кибератак ИТ-инфраструктуры, функционирующей на гетерогенной платформе виртуализации.

Формализация процессов обеспечения ИБ гетерогенных платформ заключается в разработке строгих детерминированных алгоритмов и критериев, регламентирующих обеспечение защищенности ресурсов платформы. Такой подход обеспечивает автоматизацию операций управления, что является необходимым условием для поддержания безопасности в масштабируемых гетерогенных системах. Критерии алгоритмического выбора интегрируют комплекс требований к обеспечению защищенности, включая данные от антивирусных систем, данные систем IPS/IDS, системы EDR, мониторинг аномалий в API-вызовах и прочее, в зависимости от конкретного ресурса.

Обозначим:

$P = \{p_1, p_2\}$ – набор платформ виртуализации;

$V = \{v_1, v_2, ..., v_n\}$ – множество ВМ;

$R = \{AV, IDS, EDR, ...\}$ – параметры состояния защищенности ВМ.

Каждая ВМ характеризуется вектором защищенности:

$$\vec{r}_i(t) = \left(r_i^{AV}(t), r_i^{IDS}(t), r_i^{EDR}(t), ...\right), \quad (1)$$

где $\vec{r}_i(t)$ – вектор защищенности ВМ в момент времени t; $r_i^{AV}(t)$, $r_i^{IDS}(t)$, $r_i^{EDR}(t)$ – значение параметров антивирусной системы, системы обнаружения вторжений и системы анализа телеметрии в момент времени t соответственно.

Зададим условия компрометации ВМ:

$$C(v_i) = \begin{cases} k, \text{ если } |\vec{r}_i(t)| \geq \delta^i_{trigger}, \\ 0, \text{ если } |\vec{r}_i(t)| < \delta^i_{trigger}, \end{cases} \quad (2)$$

где $C(v_i)$ – индикатор компрометации ВМ v_i; $\delta^i_{trigger}$ – значение порога риска для v_i; k – значение индикатора компрометации ВМ ($k \in N$).

Для каждой ВМ v_i платформы p_j значение порога риска $\delta^i_{trigger}$ может задаваться как согласно политик безопасности и являться равным для всех ВМ, так и различаться внутри одной платформы, учитывая специфику ВМ. Значение индикатора компрометации k устанавливается для каждой ВМ согласно критичности обрабатываемых ресурсов и влияния компрометации ВМ на другие ВМ и платформу в целом.

Определим значение уровня риска платформы виртуализации p_j в момент времени t:

$$S_j(t) = \sum_{i=1}^{n} C(v_i), \quad (3)$$

где $S_j(t)$ – значение уровня риска платформы p_j; n – количество ВМ на платформе p_j.

Для каждой платформы виртуализации в соответствии с требованиями политик безопасности определяется пороговое значение риска платформы $\theta^j_{security}$ в зависимости от которого определяется текущее состояние защищенности платформы виртуализации p_j в целом.

В зависимости от соотношения $S_j(t)$ и $\theta^j_{security}$ определяются дальнейшие меры по поддержанию состояния защищенности платформы p_j согласно алгоритму обеспечения безопасности. Алгоритм предусматривает проведения независимой оценки состояния защищенности для каждой платформы p_j, входящей в состав гетерогенной платформы виртуализации. Алгоритм обеспечения ИБ представлен на рисунке и включает следующие этапы.

1. На первом этапе осуществляется расчет векторов защищенности $\vec{r}_i(t)$ для каждой ВМ v_i согласно формуле (1).

2. Согласно формуле (2) рассчитываются значения индикаторов компрометации ВМ $C(v_i)$.

3. При наличии одного и более $C(v_i) > 0$ соответствующие ВМ считаются скомпрометированными, в дальнейшем необходимо выполнить расчет уровня риска платформы и осуществить миграции ВМ. В противном случае осуществляется возврат к шагу 1.

4. Рассчитывается уровень риска $S_j(t)$ для платформы виртуализации p_j согласно формуле (3).

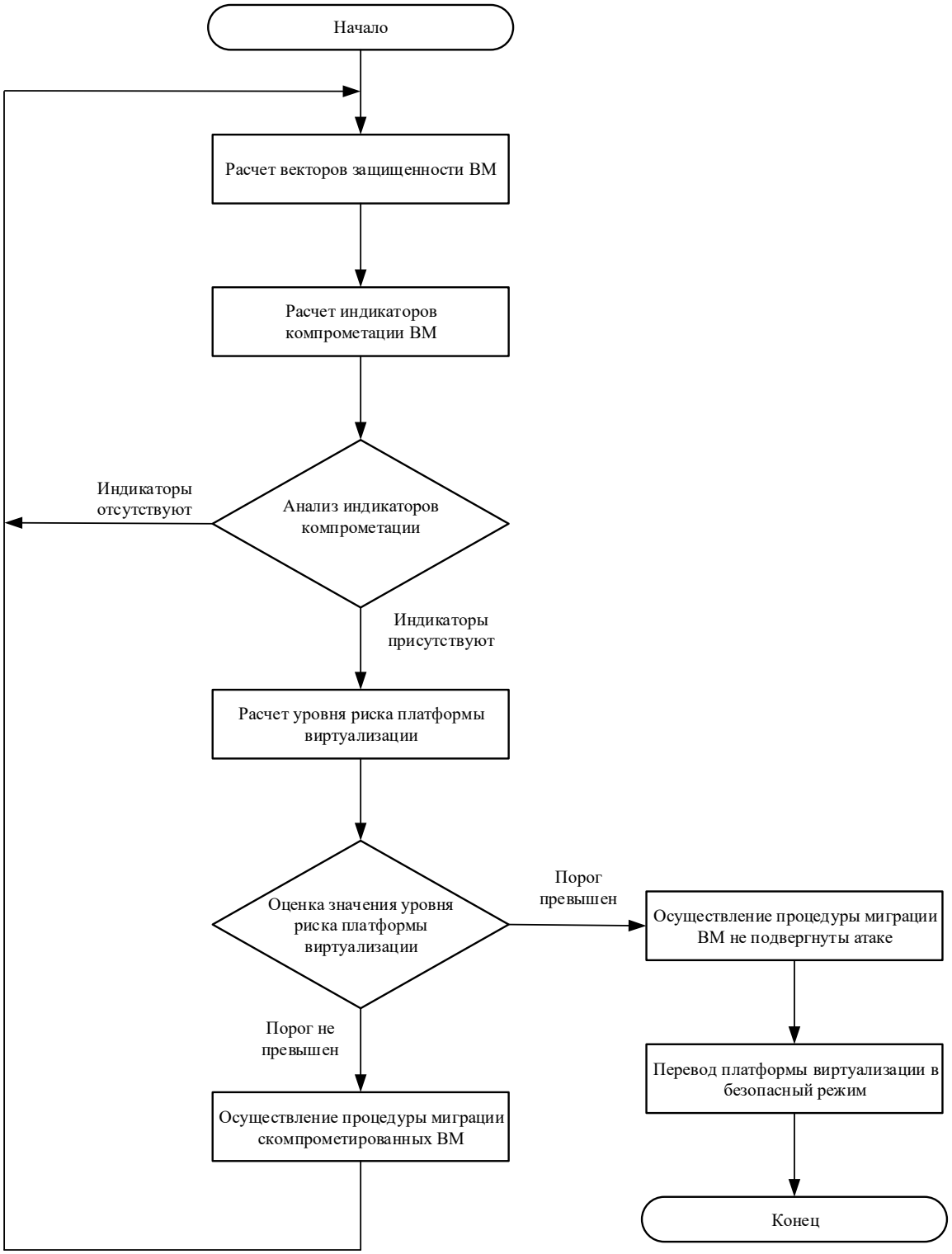
5. Рассчитанный уровень риска $S_j(t)$ сравнивается с установленным пороговым значением риска платформы $\theta^j_{security}$.

6. В случае если пороговое значение не превышено, т.е. $S_j(t) < \theta^j_{security}$, выполняются процедуры по изоляции с последующим переносом скомпрометированных ВМ [6]. Платформа p_j остается в работоспособном состоянии. Осуществляется возврат к шагу 1 алгоритма.

7. В случае если пороговое значение достигнуто или превышено, т.е. $S_j(t) \geq \theta^j_{security}$, платформа считается скомпрометированной. Осуществляется миграция ВМ, не подвергнутых кибератаке (индикатор компрометации $C(v_i) = 0$) на нескомпрометированную платформу виртуализации.

8. Скомпрометированная платформа переводится в защищенный режим:
осуществляется изоляция сетевой инфраструктуры платформы;
запрещается запуск новых ВМ на платформе;
снимается дамп событий платформы виртуализации;
для ресурсов платформы устанавливается режим доступа «только чтение».

9. Скомпрометированная платформа предоставляется подразделению кибербезопасности [7] для осуществления процедур реагирования на киберинциденты. После устранения последствий кибератаки платформа возвращается к нормальному функционированию.



Алгоритм обеспечения ИБ гетерогенной платформы виртуализации

4. Заключение

В данной статье продемонстрированы ключевые преимущества внедрения гетерогенных платформ виртуализации, их потенциал для повышения гибкости, отказоустойчивости и безопасности современной ИТ-инфраструктуры. Проведенный анализ показывает, что интеграция разнородных гипервизоров в единую гетерогенную платформу позволяет минимизировать риски зависимости от вендора, поддерживает реализацию гибридных и мультиоблачных стратегий и создает существенные препятствия для кибератак за счет разнородности среды.

Вместе с тем присущая таким платформам архитектурная сложность и расширенная поверхность атаки формируют значительные риски ИБ. Для нейтрализации данных рисков в работе аргументирована необходимость применения формализованного, модельно-ориентированного подхода к управлению ИБ. Предложенные математическая модель и алгоритм формируют основу для автоматизации процессов управления ИБ. Практическая значимость исследования заключается во вкладе в построение защищенных от кибератак ИТ-инфраструктур, функционирующих на основе гетерогенных платформ.

Библиографические ссылки

1. *Кочин В. П., Шанцов А. В.* Комплексная система защиты информации облачных ресурсов // Комплексная защита информации : материалы XXVI научно-практической конференции. Минск, 2021. С. 332–334.

2. *Кочин В. П., Шанцов А. В.* Гибридный режим функционирования облачных платформ// Информационно-коммуникационные технологии. Достижения, проблемы, инновации : материалы II научно-практической конференции, Полоцк, 30–31 марта 2022 г. / Полоцк : Полоцкий государственный университет. 2022. С. 189–193.

3. *Кочин В. П., Шанцов А. В.* Особенности построения комплексной системы защиты информации облачных ресурсов // Научная конференция студентов и аспирантов Белорусского государственного университета : материалы 78-й научной конференции студентов и аспирантов. Минск : БГУ, 2021. – С. 103–106.

4. Handbook for Computer Security Incident Response Teams (CSIRTs) / M. West-Brown [et al.]. Pittsburgh, PA : Carnegie Mellon Software Engineering Institute, 2003. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305 (date of access: 08.09.2025).

5. *Zimmerman C.* Ten strategies of a world-class cybersecurity operations center. Bedford : MITRE, 2014.

6. *Алексанков С. М.* Модель динамической миграции виртуальных машин с гибридным подходом // Научно-технический вестник информационных технологий, механики и оптики. 2017. № 4. С. 725–732.

7. *Кочин В. П., Шанцов А. В.* Методика создания и структура корпоративного подразделения информационной безопасности // Цифровая трансформация. 2022. № 3. С. 65–72.