Конференции «Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации» 5 лет

УДК 004.056.53

Задачи защиты систем виртуализации

Дюсметова А. А.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Постановка задачи. *Виртуализация, будучи ключевым компонентом современных IT-решений, представляет собой сложную систему, в которой различные элементы взаимосвязаны и взаимодействуют друг с другом. Это делает виртуальные инфраструктуры особенно уязвимыми к разнообразным атакам и угрозам, комплексный анализ которых позволит выявить и классифицировать основные задачи защиты систем виртуализации.* ***Целью работы*** *является идентификация уязвимых мест во всей виртуальной инфраструктуре для оценки текущего уровня безопасности и разработки рекомендаций для улучшения защиты виртуальных систем.* ***Используемые методы:*** *решение поставленной задачи основано на анализе виртуальной инфраструктуры, разделенной на сегменты, каждый из которых требует индивидуального подхода к обеспечению безопасности. Подход с разделением инфраструктуры на зоны способствует направленной защите и оптимизации ресурсов безопасности, позволяя эффективно распределять их в зависимости от важности и рисков каждой зоны.* ***Результат:*** *проведенный анализ угроз демонстрирует, что каждая составляющая виртуальной системы подвержена рискам атак или несанкционированного доступа к хранимой и передаваемой информации. Угрозы могут быть направлены как на аппаратную, так и на программную часть инфраструктуры и имеют разнообразный характер.*

Ключевые слова: *виртуализация, гипервизор, аутентификация, виртуальная машина, защита данных, конфиденциальность, целостность*

Актуальность темы

Актуальность данной темы обусловлена тем, что виртуализация позволяет объединить различные вычислительные ресурсы в централизованную инфраструктуру, что значительно упрощает администрирование и масштабирование [1]. Этот подход повышает эффективность использования оборудования, снижает эксплуатационные расходы, упрощает резервное копирование и восстановление информации. В дополнение к этому изоляция виртуальных машин (ВМ) и приложений создает барьер для распространения атак: в случае взлома воздействие ограничивается только одним приложением на одной операционной системе. При разграничении виртуальной инфраструктуры обеспечивается доступ к системе для пользователей без раскрытия им критической информации. В случае заражения ВМ ее можно оперативно вернуть к состоянию до компрометации, что ускоряет восстановление работоспособности [2]. Более того, виртуализация позволяет сократить количество физического оборудования, что упрощает инфраструктуру, снижая затраты на эксплуатацию и улучшая физическую безопасность – меньше устройств означает меньше потенциальных точек доступа, а также меньшую потребность в центрах обработки данных. В совокупности эти аспекты делают виртуализацию привлекательной для компаний, стремящихся к обеспечению повышенной безопасности обрабатываемой информации и оптимизации

Библиографическая ссылка на статью:
Дюсметова А. А. Задачи защиты систем виртуализации // Вестник СПбГУТ. 2024. Т. 2. № 4. С. 9. EDN: NJYZEU
Reference for citation:
Dyusmetova A. Virtualization System Protection Task // Herald of SPbSUT. 2024. Vol. 2. Iss. 4. P. 9. EDN: NJYZEU

EDN: NJYZEU
URL: https://vestnik-sut.ru/2024-4/C09.pdf

управления ресурсами. Однако с широким распространением виртуальных сред появляется и новый уровень угроз, что делает вопрос безопасности виртуализации критически важным.

К мерам защиты виртуальных инфраструктур (как отдельных ВМ, так и гипервизоров) относится предохранение от несанкционированного доступа к информации, утечки данных, различных атак, использующих уязвимости или вредоносный код. Эти меры помогают поддерживать безопасность данных и ресурсов, что особенно важно в виртуализированных средах, где любое нарушение может затронуть множество систем и сервисов одновременно [3]. На рисунке 1 представлен пример схемы виртуальной инфраструктуры, где за внешним периметром сети администрирования находится рабочее место администратора виртуальной инфраструктуры (АВИ), внутри периметра средство защиты информации (СЗИ) обеспечивает доступ только доверенным лицам, за средством защиты и соответственно во внутреннем периметре находятся гипервизоры (ESXi серверы) и ВМ.

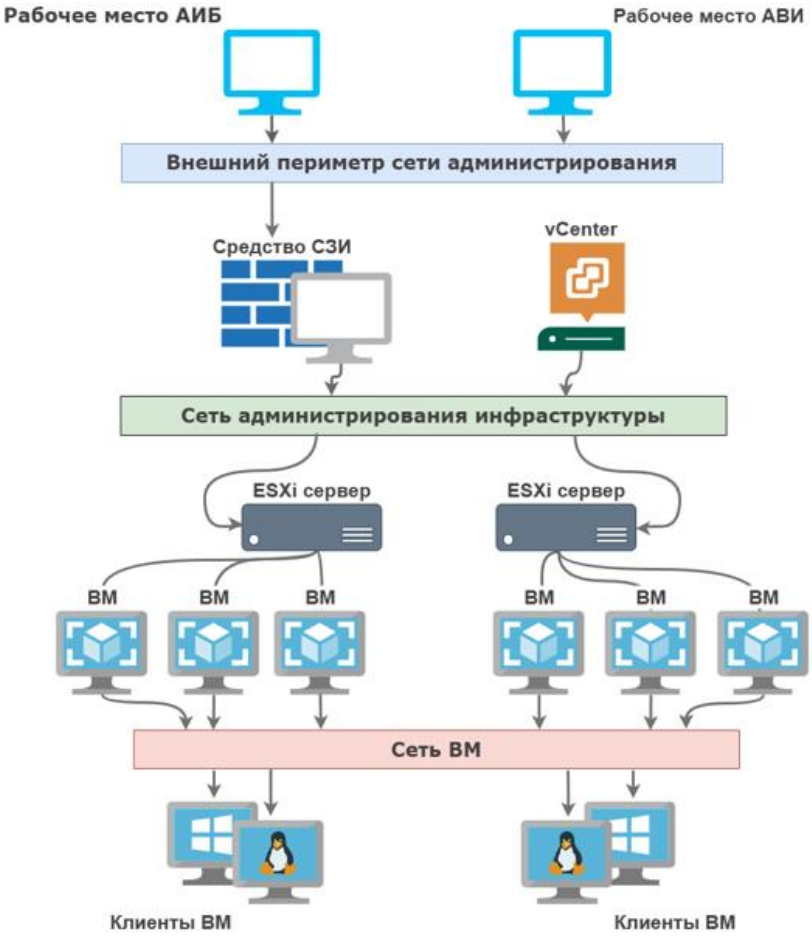

Рис. 1. Схема виртуальной инфраструктуры

Задачи защиты систем виртуализации

Задачи защиты систем виртуализации подразделяются на:
– противодействие нарушению работы аппаратных компонентов;
– обеспечение управления доступом и разграничения доступа;
– обеспечение целостности и конфиденциальности данных;
– обеспечение отказоустойчивости и резервирования;
– обеспечение защиты сетевой инфраструктуры;
– контроль виртуальной инфраструктуры.

В данной работе исследуются способы защиты, не требующие дополнительного функционала от платформ виртуализации: рассматривается подход, основанный на применении принципов безопасности.

Нарушения работы аппаратных компонентов

Сбой в работе сервера или компьютера, связанный с его аппаратными частями, может привести к нарушению функционирования всех запущенных на нем ВМ. Аппаратные сбои, такие как отказы процессоров, памяти или дисков, могут иметь разрушительные последствия для виртуализированных систем. Поскольку данные системы тесно связаны между собой (рисунок 2), нарушение работы основы повлечет за собой сбой всей системы.

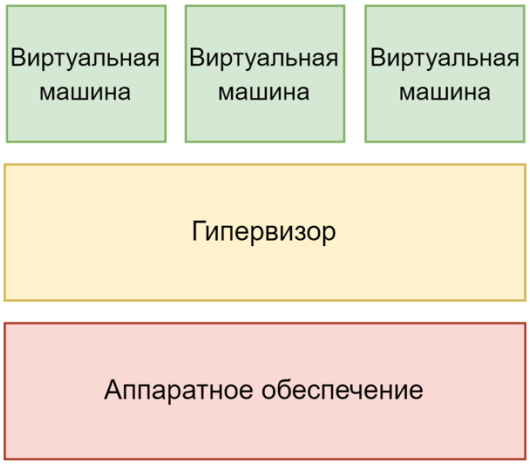

Рис. 2. Схема виртуализации для гипервизора, исполняемого на аппаратном уровне

Также ВМ, работающие на сервере виртуализации, могут быть связаны виртуальными каналами передачи данных, которые эмулируют реальные телекоммуникационные сети. При переносе вычислительных ресурсов в виртуальное пространство важно сохранить все коммуникации на прежнем уровне, обеспечивая соответствие существующим условиям коммутации и маршрутизации, а также эффективную фильтрацию трафика [4].

Одним из основных рисков остается использование плохо защищенных ВМ с некорректными настройками безопасности. Уязвимости, такие как слабые пароли или отсутствие актуальных патчей, делают их легкой мишенью для злоумышленников. Также важно учитывать риски сетевых атак между ВМ, так как вирусные заражения или другие формы атак могут быстро распространяться по всей инфраструктуре, нарушая работу системы.

Для предотвращения таких угроз требуется внедрение сетевой изоляции, регулярный мониторинг и контроль за настройками безопасности ВМ.

Управление доступом и контроль

Одной из ключевых задач защиты систем виртуализации является обеспечение строгого управления доступом к виртуальным ресурсам, часто содержащим конфиденциальную информацию. Для предотвращения несанкционированного доступа, способного привести к утечкам данных или нарушению их целостности, используется многоуровневая аутентификация, включающая двухфакторные механизмы, смарт-карты или токены (рисунок 3) [5]. Эти меры позволяют минимизировать вероятность несанкционированного доступа даже при компрометации учетных записей.

Ролевой доступ обеспечивает пользователям доступ только к тем ресурсам, которые необходимы для выполнения их обязанностей. Для повышения контроля над действиями пользователей важно внедрить систему мониторинга и аудита, которая фиксирует все операции и позволяет проводить их анализ в случае инцидентов. Особое внимание уделяется защите консолей управления, поскольку их компрометация может привести к полному контролю злоумышленника над инфраструктурой [6].

Рис. 3. Схема работы с токеном

Обеспечение целостности и конфиденциальности данных

Некачественное разграничение доступа или нарушение правил безопасности может привести к утечке данных и компрометации всей инфраструктуры. Несанкционированный доступ к сети хранения образов ВМ создает серьезные риски, позволяя злоумышленникам получить доступ к критически важным данным и управлению системой, что может привести к сбоям и утечкам.

Помимо этого, несанкционированный доступ к консоли управления ВМ или их настройкам создает угрозу перехвата управления. Злоумышленники, получившие доступ к конфигурациям, могут изменить настройки или получить доступ к конфиденциальным данным, что ставит под угрозу безопасность всей виртуальной среды.

Виртуализированные среды часто содержат конфиденциальные данные, включая персональную информацию. Для их защиты необходимо строгое разграничение прав доступа, шифрование информации и соблюдение требований законодательства по защите персональных данных. Нарушение конфиденциальности данных может повлечь за собой юридические и репутационные риски, поэтому важно уделять внимание обеспечению безопасности на каждом этапе управления данными.

Образы ВМ, содержащие конфиденциальные данные, могут быть подвержены несанкционированному копированию или искажению, что создает угрозу безопасности [4].

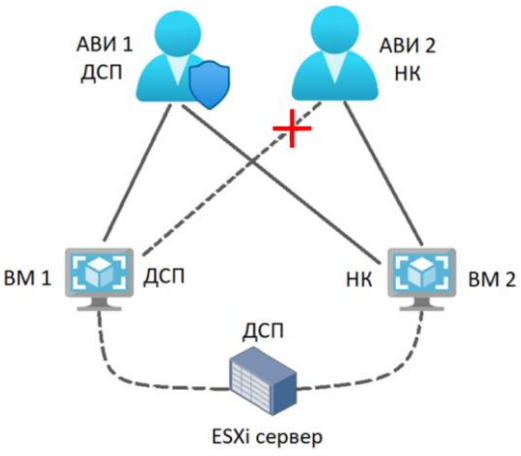

Рис. 4. Пример обеспечения конфиденциальности данных

Пример разграничения конфиденциальной информации представлен на рисунке 4: администратор виртуальной инфраструктуры (АВИ) с уровнем доступа «для служебного пользования» (ДСП) имеет доступ к информации с таким же уровнем и уровнем ниже, но АВИ с уровнем «неконфиденциально» (НК) не имеет доступа к информации уровнем выше. Уничтожение или повреждение носителей данных с образами ВМ может привести к потере информации и отказу в доступе к ВМ. Чтобы минимизировать такие риски, важно использовать надежное резервное копирование и механизмы контроля целостности данных, такие как хэш-суммы и цифровые подписи.

Уровни конфиденциальности, их количество и характеристика определяются лицом, ответственным за безопасность или администрирование виртуальной инфраструктуры. Например, уровни могут разделиться следующим образом: неконфиденциальная информация, конфиденциальная информация, информация для служебного пользования, секретная информация и совершенно секретная информация. ВМ, содержащие данные разных уровней конфиденциальности, должны быть изолированы друг от друга для предотвращения утечек информации в случае компрометации одной из них. При миграции данных между ВМ необходимо применять шифрование, чтобы исключить риск перехвата.

Отказоустойчивость и резервирование

Необходимость в отказоустойчивости становится критически важной в условиях высокой зависимости организаций от виртуальных систем [6]. Сбои в сетевых коммуникациях, оборудовании или программном обеспечении могут вывести из строя всю инфраструктуру [2]. Для обеспечения непрерывности работы применяются механизмы резервирования сетей. Дублирование серверов (рисунок 5), сетевых путей и хранилищ позволяет свести к минимуму влияние аппаратных неисправностей.

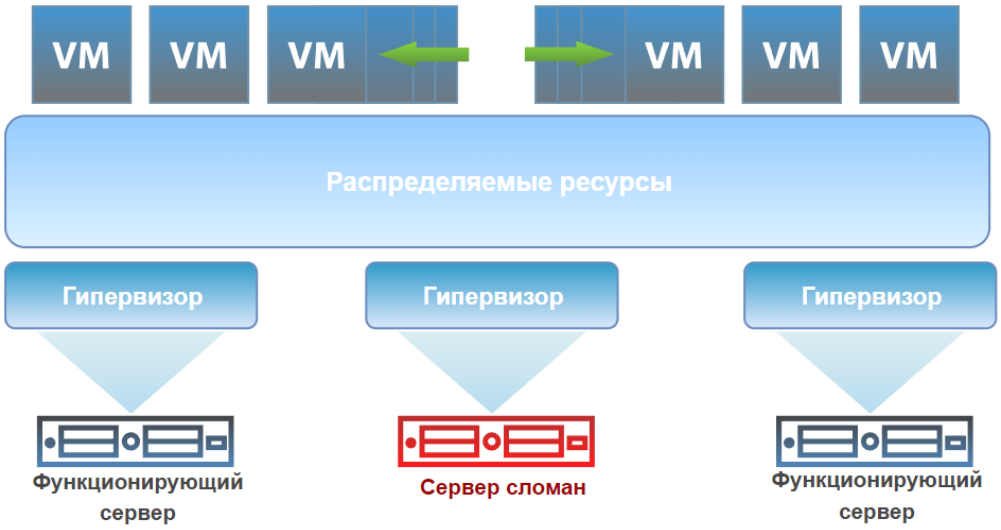

Рис. 5. Пример резервирования серверов

Регулярное резервное копирование данных помогает избежать их утраты и обеспечивает возможность восстановления в случае повреждений. Планирование включает разработку сценариев восстановления инфраструктуры после критических инцидентов, таких как аварии или атаки. Системы мониторинга в реальном времени позволяют оперативно выявлять неисправности и предотвращать их распространение.

Защита сетевой инфраструктуры

Виртуальные сети, обеспечивающие взаимодействие между ВМ, также нуждаются в надежной защите. Одной из основных мер является изоляция сетевых сегментов, которая предотвращает несанкционированный доступ к чувствительным данным. Виртуальные межсетевые экраны играют важную роль в блокировке негативного трафика. Фильтрация трафика позволяет ограничить доступ к критически

важным ресурсам, что дополнительно защищает инфраструктуру от атак. Вредоносное программное обеспечение, распространяющееся через виртуальные сети, представляет значительную угрозу, поэтому важно использовать антивирусные решения и разграничение трафика между ВМ [7].

Контроль виртуальной инфраструктуры

Эффективное управление виртуальной инфраструктурой подразумевает не только контроль ее безопасности, но и предотвращение неконтролируемого роста числа ВМ. Создание избыточного количества ВМ может привести к повышенной нагрузке на оборудование и усложнению управления системой. Важной задачей является управление развертыванием новых ВМ с применением систем автоматизации, которые позволяют отслеживать ресурсы и их использование. Также необходимо планировать нагрузку на оборудование, чтобы избегать избыточного потребления ресурсов и поддерживать стабильную работу всей инфраструктуры. Использование систем управления жизненным циклом ВМ упрощает контроль над всеми этапами их работы, от развертывания до завершения.

Заключение

Виртуальные среды обеспечивают гибкость и масштабируемость, но при этом они уязвимы для различных видов атак и технических сбоев, поскольку множество ВМ работают на общем аппаратном оборудовании под управлением гипервизора. Последний является одной из ключевых точек безопасности, поэтому основное внимание уделяется его защите, а также поддержанию его надежной изоляции от других элементов системы.

Таким образом эффективная защита ВМ предполагает не только обеспечение их изоляции друг от друга и от гипервизора, но и контроль доступа, регулярное обновление программного обеспечения и мониторинг безопасности. Использование многоуровневой аутентификации, разграничения доступа, разделения сети на сегменты позволяет сократить риск несанкционированного доступа. Важнейшим элементом обеспечения безопасности является управление доступом и аудит всех действий в виртуализированной среде. Виртуальные сети, которые связывают ВМ, также подвержены угрозам. Защита сетевой инфраструктуры требует применения механизмов шифрования, изоляции сетевых сегментов и регулярного мониторинга трафика. Важнейшим элементом обеспечения безопасности является управление доступом и аудит всех действий в виртуализированной среде.

Литература

1. Virtualization Security – защита виртуализации // Cloud Networks. 2023. URL: https://cloudnetworks.ru/inf-bezopasnost/virtualization-security (дата обращения 02.11.2024)

2. Средство защиты информации vGate R2. Руководство администратора // Код безопасности. 2021. URL: https://www.securitycode.net/upload/iblock/522/vGate%20R2%20vSphere%20-%20Руководство%20администратора%20-%20Установка,%20настройка%20и%20эксплуатация.pdf (дата обращения 02.11.2024)

3. Безопасность Виртуализации. Ч. 1 // Habr.com. 2014. URL: https://habr.com/ru/articles/243845 (дата обращения 02.11.2024)

4. Угрозы ИБ систем виртуализации и современные средства защиты // Information Security. 2014. URL: https://lib.itsec.ru/articles2/Oborandteh/ugrozy-ib-sistem-virtualizatsii-i-sovremennye-sredstva-zaschity (дата обращения 02.11.2024)

5. Курносов К. В. Методика оценки безопасности информационных систем, построенных с использованием технологий виртуализации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22. № 1. С. 37–44. DOI: 10.21293/1818-0442-2019-22-1-37-44. EDN: SXRVUE

6. Печенкина А. В., Селифанов В. В. Системы обеспечения безопасности, применяемые при использовании технологии виртуализации // Интерэкспо Гео-Сибирь. 2019. № 2. С. 150–158. DOI: 10.33764/2618-981X-2019-6-2-150-158. EDN: OULNUQ

7. Иващенко В. В., Газизов А. Р. Угрозы и методы обеспечения информационной безопасности виртуальных сред // Вестник науки. 2018. Т. 3. № 7. С. 88–91. EDN: YLJDNB

Статья поступила 15 ноября 2024 г.
Одобрена после рецензирования 24 декабря 2024 г.
Принята к публикации 27 декабря 2024 г.

Материалы статьи были представлены на V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей «Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации» (ПКМ-2024).

Информация об авторе

Дюсметова Азалия Айдаровна – студент 1-го курса магистратуры (группа ИКТБ-47м) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.
E-mail: dusmetova.aa@sut.ru

Virtualization System Protection Task

Dyusmetova A.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Problem Statement. *Virtualization, being a key component of modern IT solutions, is a complex system in which various elements are interconnected and interact with each other. This makes virtual infrastructures particularly vulnerable to a variety of attacks and threats, a comprehensive analysis of which will identify and classify the main tasks of protecting virtualization systems.* ***Purpose.*** *The goal is to identify vulnerabilities in the entire virtual infrastructure in order to assess the current level of security and develop recommendations for improving the protection of virtual systems.* ***Methods used:*** *solving the problem is based on the analysis of a virtual infrastructure divided into segments, each of which requires an individual approach to security. The approach of dividing infrastructure into zones contributes to the targeted protection and optimization of security resources, allowing them to be effectively distributed depending on the importance and risks of each zone.* ***Results.*** *The threat analysis demonstrates that each component of the virtual system is subject to the risks of attacks or unauthorized access to stored and transmitted information. Threats can be directed at both the hardware and software parts of the infrastructure and are of a diverse nature.*

Key words: *virtualization, hypervisor, authentication, virtual machine, data protection, confidentiality, integrity*

Information about Author

Dyusmetova Azaliya – 1st Year Master's Student (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E-mail: dusmetova.aa@sut.ru