DOI 10.37882/2223–2966.2022.06.19

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ

Карпов Дмитрий Анатольевич
К.т.н., МИРЭА — Российский Технологический Университет
Воробьева Ирина Алексеевна
Соискатель, МИРЭА — Российский Технологический Университет
irina2803v@mail.ru

Аннотация. Технологии виртуализации являются динамичной областью, которая все еще развивается и повсеместно внедряется как для решения задач бизнеса, так и для бытового использования. Виртуализация упрощает создание динамически масштабируемых архитектур, а также дает возможность переносить виртуальные машины для балансировки нагрузки, что позволяет запускать различные операционные системы на одном физическом компьютере. Однако, уязвимости в различных развертываниях виртуальных машин постоянно растут, они появляются из-за ошибок в программном коде продуктов, плохих конфигураций или аспектов, которые не были приняты во внимание во время их проектирования или разработки.

Ключевые слова: виртуализация, гипервизор, угрозы информационной безопасности, защита информации.

PROBLEMS OF DATA PROTECTION IN VIRTUAL INFRASTRUCTURE IN ACCORDANCE WITH THE LEGISLATION OF THE RUSSIAN FEDERATION

D. Karpov
I. Vorobieva

Summary. Virtualization technologies are a dynamic area that is still evolving and being implemented everywhere for both business and home use. Virtualization simplifies the creation of dynamically scalable architectures, as well as the ability to move virtual machines for load balancing, allowing you to run different operating systems on the same physical machine. However, vulnerabilities in various virtual machine deployments are constantly growing, they appear due to errors in the product code, poor configurations, or aspects that were not taken into account during their design or development.

Keywords: virtualization, hypervisor, information security threats, information protection.

Технологическое развитие сетей изменило перспективы сетевой безопасности. В настоящее время большинство организаций и предприятий имеют распределенную структуру, располагая офисы в различных географических точках. Сети являются критическим фактором для компаний, потому что с их помощью можно передавать информацию в режиме реального времени, снижать затраты для компании, преодолевать барьер локальных соединений, позволяя подключать персонал и офисы в других зданиях, городах и странах [1–2].

Согласно законодательству Российской Федерации в автоматизированных системах государственных учреждениях использование средств криптографической защиты информации (СКЗИ) для защиты информации конфиденциального характера является обязательным [3–6]. СКЗИ, применяемые в государственных учреждениях, должны использовать утвержденные государственным стандартом Российской Федерации криптографические алгоритмы и иметь сертификаты соответствия [7–11].

Технологическая инфраструктура, особенно связанная с информационно-коммуникационными технологиями, стала необходимой для любого предприятия, независимо от того, к какому сектору оно принадлежит. Виртуализация сегодня является одной из наиболее часто используемых технологий из-за их гибкости и масштабируемости для сервисов и приложений [12]. Технологии виртуализации содержат компоненты защиты, однако они неспособны нейтрализовать весь спектр угроз, в частно-

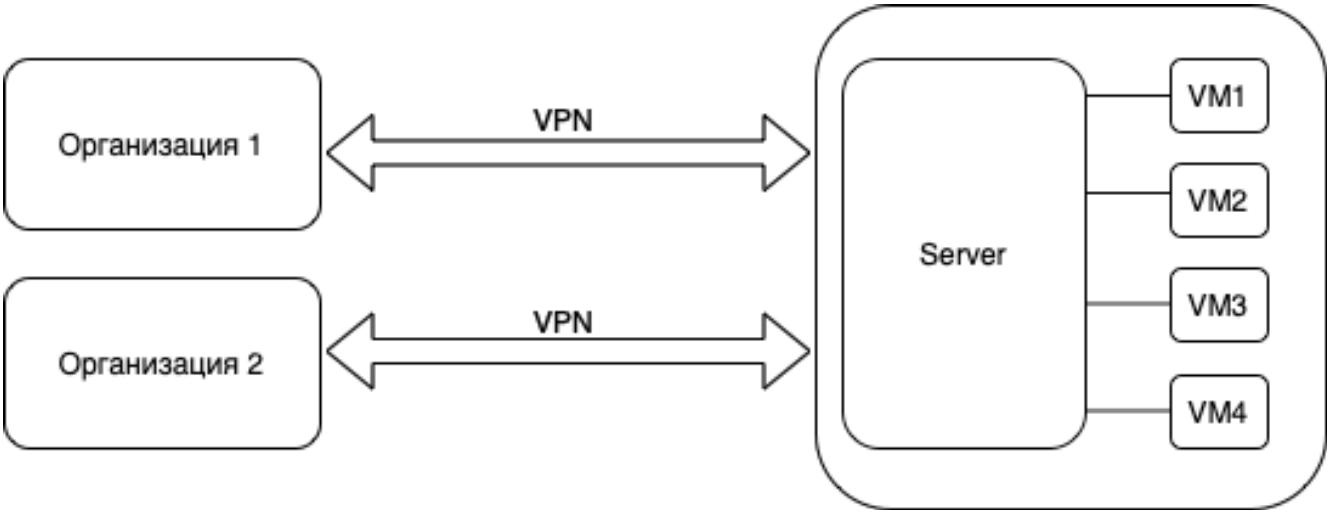

Рис. 1. Пример виртуальной архитектуры

сти, несанкционированный доступ к информации при ее передаче по недоверенным каналам связи (рис. 1).

Классифицируя угрозы ИБ применительно к конкретной архитектуре виртуальной инфраструктуры, можно выделить три группы угроз:

- Угрозы для платформы виртуальной среды.
- Угрозы, вызванные проблемами конфигурации виртуальной среды.
- Стандартные угрозы реальной среды в виртуальном пространстве.

Кроме того, можно выделить и проклассифицировать способы реализации угроз в виртуальных средах, среди которых:

- Атака на гипервизор с виртуальной машины — выполняется с использованием уязвимостей хост-операционной системы, в которой работает гипервизор. Как только злоумышленник берет под контроль операционную систему, гипервизор скомпрометирован. Атака, где взят под контроль гипервизор, называется гиперджекинг [13].
- Атака миграции — происходит в сети во время миграции виртуальной машины из одного места в другое. Данная атака имеет успех благодаря легкости перемещения виртуальных машин, будь то резервное копирование, распространение обновлений, обмен изображениями и т.д.

Конкретный случай такого типа атаки происходит из-за функциональности, предоставляемой некоторыми гипервизорами. Это называется live-миграцией, она позволяет переносить виртуальную систему с одного гипервизора на другой (даже между гипервизорами на разных физических компьютерах) без выключения системы. Эта функция упрощает управление и может использоваться, среди прочего, для балансировки рабочей нагрузки сервера. Механизм связи, используемый для передачи состояния от одного гипервизора к другому, должен быть аутентифицированным, конфиденциальным и устойчивым к изменениям.

- Атака на виртуальную машину с другой виртуальной машины –гостевая операционная система используется для получения несанкционированного доступа к гипервизору или другим виртуальным машинам. Поскольку несколько виртуальных машин используют одни и те же физические ресурсы, если злоумышленник может найти, как отображаются ресурсы, на которых он работает, он может напрямую атаковать физические ресурсы. Злонамеренное изменение виртуальной памяти может повлиять на общие физические ресурсы и атаковать другие виртуальные машины и гипервизор. Учитывая сложность этого типа атаки, чаще всего происходит сбой гостевой операционной системы, тем самым достигая отказа в обслуживании.
- Гипервизор как вредоносный код и руткит. Гипервизор может использоваться каким-то вредоносным кодом или руткитом для установки себя в качестве гипервизора под операционной системой (которая является жертвой атаки). Обнаружение вредоносного кода в этом случае очень сложно, так как вредоносное ПО может перехватывать все операции операционной системы.
- Атака отката виртуальной машины подразумевает использование функциональности гипервизоров для создания снимков с текущим состоянием процессора, дисков и памяти.

Злоумышленник может заменить систему старым снимком, чтобы удалить часть или всю запись о том, что

произошло между моментом создания снимка и текущим моментом системы.

Для защиты от этих угроз можно использовать сертифицированные программные СЗИ, которые обеспечат надежную изоляцию виртуальных машин и проверку на отсутствие злонамеренного кода в гипервизоре. К числу таких средств защиты информации относятся Security Code vGate for VMware Infrastructure и ПК СВ «Брест».

Security Code vGate for VMware Infrastructure — это программное обеспечение, которое позволяет предотвращать утечки через специфичные каналы среды виртуализации. В том числе и через каналы обмена трафиком с другими виртуальными машинами. Также vGate производит разделение объектов инфраструктуры на логические группы и сферы администрирования через мандатное и ролевое управление доступом. Разграничение доступа к элементам, находящимся внутри защищаемого периметра, реализуется на основе заданных ACL и параметров соединения [14]. Усиленная аутентификация совместно с разделением ролей и делегированием полномочий позволяют усилит защиту управления виртуальной инфраструктурой. Управление виртуальной инфраструктурой и параметрами безопасности предоставляется только аутентифицированным пользователям, при этом процедура аутентификации осуществляется по протоколам, нечувствительным к атакам типа «man-in-the-middle» и перехватам паролей. Кроме того, в vGate содержатся средства мониторинга событий ИБ и средства создания структурированных отчетов.

Программный комплекс управления защищённой средой виртуализации «Брест» — это комплексное решение позволяющее создавать и администрировать виртуальные IT-структуры с применением СЗИ из состава операционной системы Astra Linux и обеспечивающее работу виртуальных машин в условиях дискреционного и мандатного управления доступом. В версии «Брест» реализована поддержка FreeIPA для задания политик доступа и управления идентификацией пользователей [15–16]. Astra Linux использует 256 уровней доступа и 64 категории доступа, разграничивающий допуск к операциям и файлам.

Однако все эти средства защиты информации не способны обеспечить конфиденциальность и защитить информацию покидающую виртуальную машину. Несмотря на то, что трафик может изолироваться применением технологии виртуальных локальных сетей (VLAN) это не является защитой информации с точки зрения законодательства Российской Федерации (VLAN можно рассматривать лишь как средство понижения актуальности угроз). Поэтому для обеспечения безопасной обработки информации в виртуальной инфраструктуре необходимо дополнить используемые средства защиты виртуальных машин, даже если информация она не покидает сети владельца виртуального хостинга.

ЛИТЕРАТУРА

1. И.А. Мандыч, А.В. Быкова. Трудности и перспективы развития высокотехнологичных проектов в эпоху цифровой трансформации экономики // Российский технологический журнал. — 2021. — No 9(2). — С. 88–95.
2. Красимир Шишманов Особенности развития информационных систем малых предприятий // Шишманов Красимир // Российский технологический журнал. — 2016. — № Том 4 No 5. — С. 63–69.
3. Указ Президента РФ от 6 марта 1997 г. No 188 «Об утверждении перечня сведений конфиденциального характера» // ГАРАНТ: [Электронный ресурс] — URL: https://base.garant.ru/10200083/#ixzz5OGPzHs6K (дата обращения: 29.03.2022).
4. Федеральный закон «О персональных данных» от 27.07.2006 No 152-ФЗ // КонсультантПлюс: [Электронный ресурс] — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 20.03.2022).
5. Федеральный закон от 27 июля 2006 г. No 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) // ГАРАНТ: [Электронный ресурс] — URL: https://base.garant.ru/12148555/#ixzz5OGYA43bX (дата обращения: 20.03.2022).
6. Указ Президента РФ от 3 апреля 1995 г. No 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» // ГАРАНТ: [Электронный ресурс] — URL: https://base.garant.ru/10104146/#ixzz5OGcX8k1S (дата обращения: 20.03.2022).
7. Приказ ФСБ РФ от 9 февраля 2005 г. No 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // ГАРАНТ: [Электронный ресурс] — URL: https://base.garant.ru/187947/#ixzz5OGelok00 (дата обращения: 20.03.2022).
8. Приказ ФСТЭК России от 25 декабря 2017 г. No 239 // ФСТЭК России: [Электронный ресурс] — URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-gn-239 (дата обращения: 07.04.2022).
9. Приказ ФСТЭК России от 21 декабря 2017 г. No 235 // ФСТЭК России: [Электронный ресурс] — URL: https://fstec.ru/en/288-tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/prikazy/1606-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 07.04.2022).

10. Приказ ФСТЭК России от 18 февраля 2013 г. No 21 // ФСТЭК России: [Электронный ресурс] — URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/692-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 08.04.2022).
11. Приказ ФСТЭК России от 11 февраля 2013 г. No 17 // ФСТЭК России: [Электронный ресурс] — URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 08.04.2022).
12. Cloud Computing Models for Business // I.A. Vorobeva, A.V. Panov, A.A. Safronov, A.I. Sazonov // International Journal of Emerging Technology and Advanced Engineering.— 2022.— Volume 12 Issue 1.— C. 163–172.
13. F. Bazargan, C. Yeun y J. Zemerly // «State-of-the-Art of Virtualization, its Security Threats and Deployment Models» // International Journal for Information Security Research, 2013.
14. vGate // Код Безопасности: [Электронный ресурс] — URL: https://www.securitycode.ru/products/vgate/ (дата обращения: 07.04.2022).
15. Операционные системы и средства виртуализации // Astra Linux: [Электронный ресурс] — URL: https://astralinux.ru/products/ (дата обращения: 07.04.2022).
16. Система виртуализации Astra Linux. Программный комплекс «Средства виртуализации «Брест» // Astra Linux: [Электронный ресурс].— URL: https://astralinux.ru/products/ (дата обращения: 07.04.2022).

© Карпов Дмитрий Анатольевич, Воробьева Ирина Алексеевна (irina2803v@mail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»

МИРЭА — Российский технологический университет