УДК 004.45

ЗАХИЩЕНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ

[1]Романов О.І., [1]Нестеренко М.М., [2]Фесьоха Н.О.

[1] *Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського*

[2] *Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут*

E- mail: a_i_romanov@gmail.com, nikolaiy.nesterenko@gmail.com, nadya_viti@i.ua

Protection of information systems in the use of virtualization technologies

Information technology is rapidly evolving, bringing to life many useful tools for work, science. One of the most promising technologies in the computer world is virtualization.

Інформаційні технології стрімко розвиваються, приносячи в повсякденність безліч корисних засобів для роботи, науки. Однією з перспективних технологій в комп'ютерному світі є віртуалізація.

Віртуалізація в інформаційних технологіях (ІТ) - процес подання набору обчислювальних ресурсів або сутностей, який дає певні переваги перед звичайною конфігурацією.

Аналітична компанія *Gartner* в своєму щорічному списку топ-10 стратегічних технологій 2019 виділяє підвищене питання інформаційній безпеці (ІБ).

Отже постає питання: як впливають технології віртуалізації на ІБ. Підвищується, знижується або залишається на попередньому рівні. Існування різних видів віртуалізації не дозволяє дати однозначну відповідь.

Віртуалізація комп'ютера - найбільш поширений вид віртуалізації. Виділяють технології програмної і апаратної віртуалізації. Програмна віртуалізація несе в собі ряд особливостей, що створюють серйозні проблеми ІБ: гіпервізор і хостова ОС представляють єдину точку відмови; реалізація гіпервізора у вигляді програмного модуля більш вразлива до атак, ніж апаратно-програмна реалізація; за технологією *Trusted Platform Module* (*TPM*) відомі рішення з програмною віртуалізації не забезпечені захистом на апаратному рівні.

Більш сучасні технології апаратної віртуалізації вирішують ряд зазначених проблем ІБ. Для підвищення захищеності компанія *Intel* впровадила в одному зі своїх чіпсетів технологію безпеки *LaGrande / TXT*, що використовує специфікацію *TPM* 1.2. Дана технологія дозволяє контролювати цілісність програмно-апаратного середовища комп'ютера. Аналогічні механізми безпеки забезпечує технологія *AMD-V*, в якій реалізований спеціальний захищений режим запуску монітора віртуальних машин.

Віртуалізація мереж являє собою перетворення елементарних мережевих ресурсів типу фрейму, пакета, сесії і управління ними. При цьому можуть використовуватися канальний, мережевий, транспортний і сесійний рівні моделі OSI.

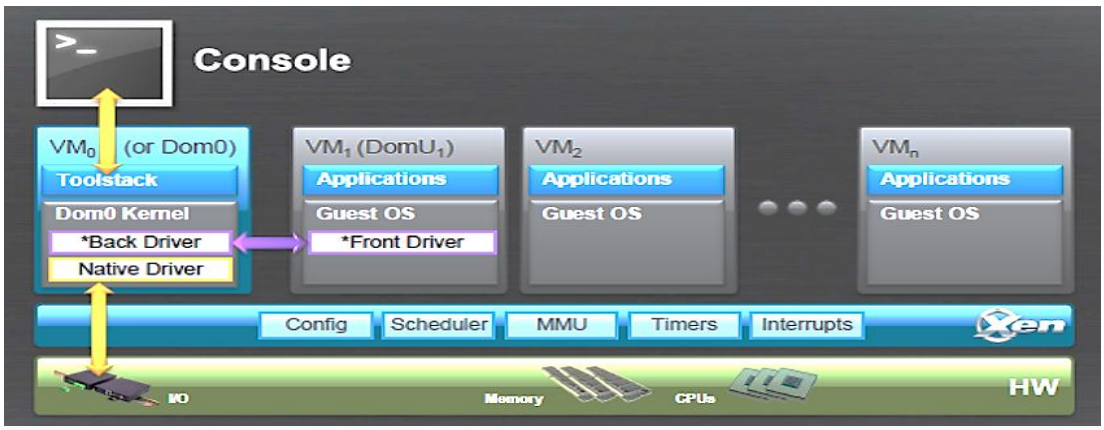

Рис. 1. Гіпервізор Xen типу 1.

Віртуалізація мереж можлива за технологією віртуальної приватної мережі (ВПМ) і за технологією віртуальної локальної обчислювальної мережі (ВЛВС). ВПМ має глобальний характер застосування, так як працює на мережевому рівні, в ВЛВС - тільки локальний. Основними цілями віртуалізації мереж є: поділ і управління потоками інформації, мережева ізоляція, сегментування мережі, а також захист інформації при її передачі по мережі.

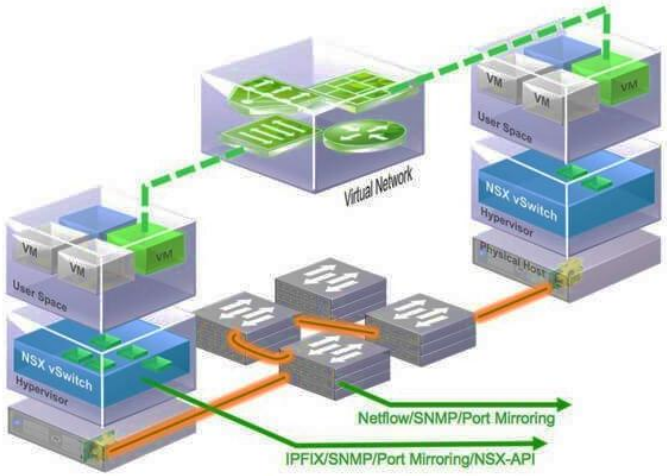

Рис. 2. Віртуалізація мережі.

При віртуалізації додатку формується кілька незалежно працюючих додатків (з контекстами) або його користувальницькі представлення (термінальні сесії, профілі користувачів). Віртуалізація додатків має мету: відокремити додатки від операційної системи, зробити їх мобільними і надати можливість для їх виконання в різних середовищах. Віртуалізація представлень - підхід, при якому додаток виконується на віддаленому сервері, а його користувальницький інтерфейс відображається локально. Віртуалізація представлень широко використовується в сучасних додатках для управління клієнтськими додатками і захисту конфіденційних даних.

Віртуалізація мереж на базі загальноприйнятих (*IPSec, SSL*) і приватних протоколів - склала, самостійний напрям мережевої безпеки. Віртуалізація представлень за допомогою термінальної сесії - доцільний метод ізоляції сервера додатків і робочої станції користувача. Ізоляція користувача і сервера важлива при їх локалізації в двох зонах, протилежних за умовами ІБ. При термінальній сесії на сервер передаються тільки коди натиснутих клавіш робочої станції, а з сервера - растри призначеного для користувача інтерфейсу. Важливо, що між сервером і робочою станцією немає обміну програмним кодом, що виключає ризик передачі шкідливих програм.

Ізоляцію бази даних та процесів між віртуальними машинами забезпечують нові продукти компанії *IBM, Intel, Microsoft, AMD, Citrix (Zen), VMware*. Гарантована ізоляція дає можливість їх використання для розділення операційних середовищ за рівнем конфіденційності інформації, обраних в системі.

Технологія апаратної віртуалізації, що використовує модуль *TPM* і специфікації *TCG* для реалізації довіреного середовища, дозволяє створювати безпечні розділи з перевіркою ідентичності і цілісності віртуальної машини і усіх задіяних в ній програмно-апаратних компонент. Поки що тільки компанії *Parallels і Microsoft* поставляють на ринок продукти віртуалізації, що застосовують ці технології захисту. Компанія *Parallels* працює над використанням *Intel VT- x* і *TXT* для створення монітора віртуальних машин з гарантованим захистом від вірусів. Компанія *Microsoft* використовує технологію апаратного захисту у рамках *Windows Server 2008 і Hyper - V Server.*

Компанії *Microsoft і Citrix* застосовують технологію апаратної віртуалізації *Intel* для контролю середовища користувача, завантаження образів ОС і додатків з корпоративного сервера. Усі необхідні застосування і ОС знаходяться на одному сервері - їх легко контролювати і захищати. При цьому реалізується контроль призначеного для користувача доступу до додатків за допомогою регульованого переліку додатків для конкретного облікового запису.

Одним з головних напрямів застосування технології віртуалізації в завданнях ІБ є забезпечення доступності інформації і безперервності процесів (*BCP, DRP*). Данні задачі вирішуються за допомогою віртуалізації серверів і систем зберігання даних. Віртуалізація економить значні інвестиції в порівнянні з фізичним дублюванням і резервуванням устаткування.

Незважаючи на нові можливості у сфері ІБ, застосування технології віртуалізації несе в собі нові загрози.

Досить порівняти надійність ізоляції віртуальних машин з варіантом фізично ізольованих комп'ютерів. Навіть у нових технологіях апаратної віртуалізації частина механізму віртуалізації реалізується програмним забезпеченням гіпервізора. Незважаючи на оптимізацію об'єму коду гіпервізора і пильну увагу розробників до усунення можливих вразливостей, існує вірогідність наявності прихованих або функціональних вразливостей гіпервізора і можливості проведення проти нього атаки.

Знижує захищеність і простота переносимості віртуальних систем на інші фізичні платформи, використання віртуальних машин в архітектурі "хмарних обчислень".

Системи з віртуалізацією комп'ютерів мають одну точку відмови - ОС і ПО віртуалізації хост-комп’ютера. Такий недолік не дозволяє використати програмну віртуалізацію в завданнях забезпечення безперервності процесів, там, де потрібна висока готовність і доступність інформації. Важливою особливістю застосування технології віртуалізації вважається розробка життєвого циклу інформації, що захищається, при міграції віртуальних хостів і балансування навантаження. У останніх технологічних рішеннях міграція віртуальних машин і даних залишається однією з базових функцій. Нерегульована міграція даних обмеженого доступу недопустима, оскільки здатна привести до порушень її конфіденційності, цілісності і доступності, а в цілому - до зростання ризиків ІБ.

Отже: сама по собі віртуалізація ІТ-обладнання (процесорних систем, комп'ютерів, систем зберігання даних і тому подібне), а також програмних застосувань і ресурсів не є механізмом ІБ. Віртуалізація мережевого ресурсу (*IP*-пакет), протоколу (*IPSec, SSL*), що включає криптографічні методи захисту, вважається механізмом забезпечення безпеки, який дозволяє створювати нові технології мережевого захисту. За винятком віртуалізації представлень, технологія

віртуалізації додатків не призводить до підвищення рівня ІБ, оскільки віртуалізовані застосування не мають гарантованої взаємної ізоляції по міграції програмного коду. Віртуалізація представлень - наприклад, режим термінального доступу - забезпечує межу між клієнтом і сервером, що захищає від проникнення шкідливого програмного коду.

Іншим аспектом ІБ є гарантована ізоляція процесів і цих віртуальних машин один від одного. Проте гарантія ізоляції віртуальних машин за даними не може бути стовідсотковою, оскільки пов'язана з потенційними вразливостями гіпервізора. В порівнянні з фізично ізольованими хостами (відсутність віртуалізації) рівень ризиків ІБ вищий при використанні технологій апаратної віртуалізації і істотно вищий - при реалізації технологій програмної віртуалізації. Для зниження ризиків ІБ у рамках застосування апаратної віртуалізації повинна працювати технологія апаратного захисту на основі модуля *TPM* і специфікації *TCG*.

Використання технологій віртуалізації в ІС вимагає розробки регламенту по захисту інформації, залученої в процеси міграції віртуальних машин. Рекомендується застосування технології віртуалізації для забезпечення безперервності процесів (*BCP*, *DRP*) за рахунок резервування обладнання і програмного забезпечення їх віртуальними аналогами. Для вирішення подібних завдань найбільшою мірою підходить технологія апаратної віртуалізації.

Література

1. Романов О.І., Нестеренко М.М., Фесьоха Н.О. Віртуалізація як спосіб організації інфраструктури інформаційно-телекомунікаційних мереж// Збірник матеріалів Міжнародно наково-технічної конференції «Перспективи телекомунікацій»/Збірник тез конференції (ISSN print 2663-502X). К.: КПІ ім. Ігоря Сікорського, 2019
2. Y. Li, W. Li, and C. Jiang, "A Survey of Virtual Machine System: Current Technology and Future Trends", in Proceedings of the Third International Symposium on Electronic Commerce and Security, 2010.
3. J. E. Smith, and R. Nair, "The Architecture of Virtual Machines", Computer, vol. 38, No. 5, pp. 32-38, 2005.
4. S. Nanda, and T. Chiueh, "A Survey on Virtualization Technologies", Experimental Computer Systems Lab, SUNY Stony Brook, SUNY RPE Report TR-179, 2005.
5. О. С. Головня, "Систематизація технологій віртуалізації", Інформаційні технології в освіті, № 12, с. 127-133, 2012.
6. О. С. Головня, Технології віртуалізації у навчанні операційних систем бакалаврів інформатики: Методичні рекомендації для викладачів вищ. навч. закл.. Житомир: Рута, 2017, с. 15-20.
7. O. S. Holovnia, "Criteria for selecting virtualization software in teaching unix-like operating systems", Information technologies in education, No. 24, p. 119-133, 2015.
8. F. Giraldeau, M. R. Dagenais, and H. Boucheneb, "Teaching operating systems concepts with execution visualization", in 121st ASEE Annual Conference and Exposition, Indianapolis, IN, USA, 2014.
9. A. Garmpis, and N. Gouvatsos, "Innovative teaching methods in Operating Systems: The Linux case", in Innovative approaches in Education: Design and Networking, 2012.
10. О гипервизорах, виртуализации систем и о том, как это работает в облачной среде. [Электронный ресурс] - Режим доступа: https://www.ibm.com/developerworks/ru/library/cl-hypervisorcompare.