УДК: 004.451.1

Виртуализация подсистемы прерываний микропроцессоров «Эльбрус»

С.А. Рыбаков[1,2], Р.В. Деменко[1]

[1]АО «МЦСТ», Москва, Россия
[2]МИРЭА – Российский технологический университет (РТУ МИРЭА), Москва, Россия

В новых поколениях микропроцессоров семейства «Эльбрус» появилась аппаратная поддержка виртуализации [1], в том числе для подсистемы прерываний [2]. Реализованные в аппаратуре механизмы доставки виртуальных прерываний необходимо поддержать в программном обеспечении.

Рассмотрим работу ПО с виртуальными прерываниями на примере связки QEMU (Quick Emulator [2]) и KVM (Linux Kernel Virtual Machine [3]). QEMU – пользовательское приложение, которое эмулирует для гостевой ОС процессорные ядра, оперативную память и устройства ввода-вывода. Для каждого виртуального процессорного ядра QEMU запускает собственный поток исполнения, виртуальные компоненты ввода-вывода также выделены в отдельный поток. KVM представляет собой гипервизор, реализованный в виде модуля ядра Linux. Взаимодействие QEMU и KVM осуществляется через системные вызовы IOCTL (Input/Output Control).

При наличии аппаратной поддержки виртуализации код гостевой ОС исполняется непосредственно на физическом оборудовании. В этом случае QEMU задействует KVM, который сохраняет рабочее состояние (контекст) хоста и запускает исполнение виртуальной машины (рис.1).

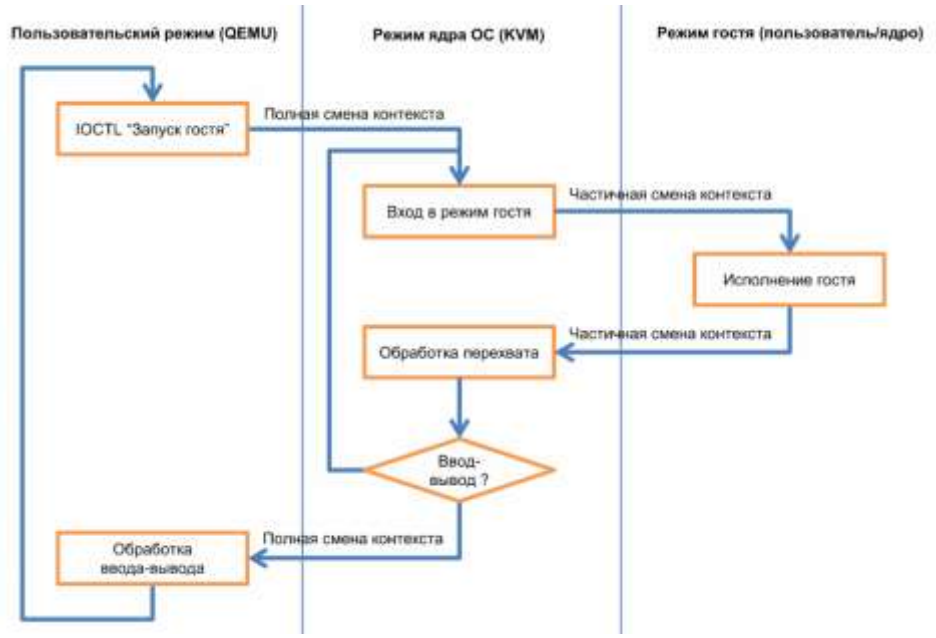

Рис. 1 Цикл запуска виртуальной машины

Работа гостевой ОС продолжается до первого перехвата – принудительного возврата в контекст гипервизора. Причиной перехвата может быть обращение гостя к привилегированным ресурсам (к примеру, регистрам ввода-вывода) или истечение выделенного виртуальной машине кванта времени. В случае перехвата KVM анализирует ее причину: если необходима эмуляция ввода-вывода, KVM возвращает управление QEMU (дополнительная смена контекста). Таким

образом, перехваты можно разделить на две группы: легковесные (обрабатываемые в KVM), и тяжеловесные (с выходом в QEMU).

Доставка и обработка виртуальных прерываний подразумевает обращения гостевой ОС к привилегированным регистрам контроллера прерываний EPIC. Без аппаратной поддержки виртуализации подсистемы прерываний эти обращения требуют перехвата (рис.2), что значительно снижает эффективность виртуальных машин.

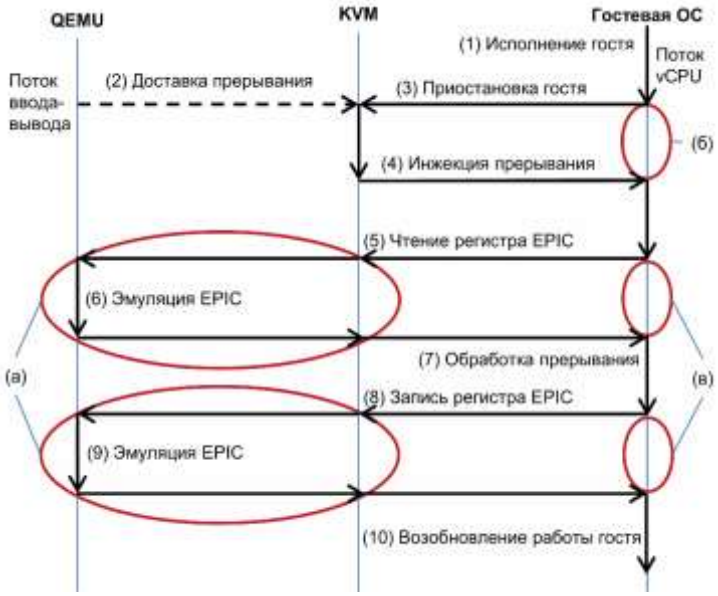

Рис. 2 Доставка и обработка гостевого прерывания

Для повышения эффективности виртуальных машин и уменьшения времени реакции на прерывания при исполнении гостевой ОС были реализованы следующие оптимизации:

а) модель контроллера прерываний была перенесена из QEMU в KVM, что позволило уйти от тяжеловесных перехватов с выходом QEMU (если аппаратная поддержка подсистемы прерываний не используется, т.е. необходима эмуляция);
б) был реализован алгоритм доставки прерываний гостевому ядру без перехвата (аппаратная поддержка);
в) гостю был обеспечен доступ к регистрам программируемого контроллера прерываний без перехватов (аппаратная поддержка)

Программно-аппаратные решения, реализованные в новом поколении микропроцессоров семейства «Эльбрус», позволили значительно снизить накладные расходы, связанные с перехватом при доставке и обработке виртуальных прерываний.

Литература

1. *Знаменский Д.В.* Выбор вариантов реализации средств аппаратной поддержки виртуализации архитектуры Эльбрус. – «Вопросы радиоэлектроники», сер. ЭВТ. – 2014. – вып. 3.
2. *Деменко Р.В., Трофимов В.Б.* Аппаратная поддержка виртуализации системы прерываний в микропроцессорах семейства «Эльбрус» // Вопросы радиоэлектроники. — 2018. — No 3. — (ЭВТ)
3. *Bellard F. QEMU,* a Fast and Portable Dynamic Translator // ATEC '05: Proceedings of the annual conference on USENIX Annual Technical Conference. – 2005.
4. *Kivity A.* KVM: The linux virtual machine monitor // In Proc. of the 2007 Ottawa Linux Symposium (OLS). — 2007. — С. 225—230.