УДК: 004.056.5 DOI: 10.53816/23061456_2022_11–12_89

ПОДХОД К БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ В КРИТИЧЕСКИ ВАЖНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

AN APPROACH TO THE SECURE USE OF CONTAINER VIRTUALIZATION IN MISSION-CRITICAL AUTOMATED SYSTEMS

Канд. техн. наук В.М. Зима, канд. техн. наук Р.О. Крюков

Ph.D. V.M. Zima, Ph.D. R.O. Kryukov

Военно-космическая академия им. А.Ф. Можайского

Представлен практический подход к безопасному применению контейнерной виртуализации в критически важных автоматизированных системах (АС), основанный на интеграции системы виртуализации Astra Linux Special Edition и платформы контейнеризации Kubernetes/OpenShift. Рассмотрены проблемы, возникающие с контейнерной виртуализацией в критически важных АС, раскрыта схема интеграции платформы Kubernetes/OpenShift в систему виртуализации Astra Linux SE для безопасного использования преимуществ контейнерной виртуализации, описана архитектура системы виртуализации Astra Linux SE на базе программного комплекса средств виртуализации (ПК СВ) «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift, приведено обоснование предложенного решения в части выполнения нормативных требований по защите информации от несанкционированного доступа.

Ключевые слова: безопасность информации, средства защиты информации от несанкционированного доступа, виртуализация аппаратного обеспечения, виртуализация программного обеспечения, среда виртуализации, защита среды виртуализации.

Abstract: The article presents a practical approach to the safe application of container virtualization in critical automated systems (AS), based on the integration of Astra Linux Special Edition virtualization system and Kubernetes/OpenShift containerization platform. The problems arising with container virtualization in the critical automated systems (AS) are considered, the scheme of integration of the Kubernetes/OpenShift platform into the Astra Linux SE virtualization system to safely use the advantages of container virtualization is revealed, the architecture of the Astra Linux SE virtualization system based on the software virtualization tools package “Brest” and “Brest. VDI”, integrated with the Kubernetes/OpenShift platform, the justification of the proposed solution in terms of compliance with regulatory requirements to protect information from unauthorized access is given.

Keywords: information security, means of protecting information from unauthorized access, virtualization of hardware, virtualization of software, virtualization environment, protection of the virtualization environment.

Введение

В критически важных АС к обязательным компонентам, необходимым для формирования защищенной виртуальной среды на базе операционной системы (ОС) Astra Linux Special Edition (далее — Astra Linux SE), относится программный комплекс средств виртуализации (ПК СВ) «Брест». Для централизованного управления виртуальными машинами (ВМ) и подключениями к ВМ на основе шаблонов и политик безопасности целесообразно использование дополнительного компонента — программного расширения ПК СВ «Брест» — отдельного программного продукта «Брест.VDI».

Astra Linux SE, ПК СВ «Брест» и «Брест. VDI» сертифицированы в системе сертификации МО РФ и ФСТЭК России для возможности использования в АС до класса защищенности 1Б включительно, определяемого в соответствии с РД АС [1].

Система виртуализации Astra Linux SE на базе ПК СВ «Брест» и расширения «Брест.VDI» обеспечивает реализацию классической виртуализации платформ и ресурсов. В терминологии ГОСТ Р 56938 (п. 3.3 [2]) классическая виртуализация платформ и ресурсов называется виртуализацией аппаратного обеспечения и вычислительных систем, под которой понимается технология создания изолированной программной среды (ВМ) со специфическим набором компонентов эмулируемого микропрограммного и аппаратного обеспечения, обеспечивающим работу отдельных операционных систем.

Однако в последнее время все более широкую популярность приобретает виртуализация на уровне ОС или, как ее еще называют, контейнерная виртуализация. В терминологии ГОСТ Р 56938 (п. 3.2 [2]) контейнерная виртуализация называется виртуализацией программного обеспечения (ПО) (программ), под которой понимается технология создания изолированной программной среды (контейнера) со специфическим набором компонентов эмулируемой ОС, обеспечивающим работу отдельных программ. У контейнерной виртуализации, по причине интенсивного развития этой технологии, помимо более высокой производительности появились другие преимущества, связанные с более высокой степенью автоматизации разработки контейнеров приложений, их развертывания, поддержания безотказной работы за счет кластеризации, а также масштабирования. К наиболее апробированным, масштабируемым и автоматизируемым программным платформам контейнерной виртуализации относятся построенные на одной кодовой базе платформы Kubernetes и OpenShift (далее — Kubernetes/OpenShift).

Таким образом для возможности безопасного использования преимуществ контейнерной виртуализации по более высокой степени автоматизации разработки, развертывания, кластеризации и масштабирования контейнеров появилась необходимость интеграции системы виртуализации Astra Linux SE и универсальной платформы контейнеризации Kubernetes/OpenShift с учетом выполнения нормативных требований по защите информации от несанкционированного доступа.

Обоснование выбора системы виртуализации Astra Linux SE на базе ПК СВ «Брест»

С 2011 года ФСТЭК России полностью взял на вооружение общие критерии оценки безопасности информационных технологий (ОКБ, ГОСТ Р ИСО/МЭК 15408 [3–5]), и все новые требования к безопасности средств защиты информации от несанкционированного доступа (СрЗИ) во ФСТЭК издаются в виде профилей защиты (ПЗ), каждый из которых соответствует определенному классу защищенности, которые могут быть уточнены в заданиях по безопасности (ЗБ), ориентированных на конкретную схему нейтрализации угроз и условия эксплуатации [6].

Вместе с тем, в отличие от операционных систем (ОС) со встроенными средствами защиты и средств защиты других типов, например систем обнаружения вторжений, для средств виртуализации отсутствуют утвержденные профили защиты, и эти средства сертифицируют только на соответствие требуемому уровню контроля отсутствия недекларированных возможностей [7] (в системе сертификации МО РФ) или уровню доверия [8] (в системе сертификации ФСТЭК России).

Таким образом, средства виртуализации в критически важных АС должны соответствовать требуемому уровню контроля отсутствия недекларированных возможностей (НДВ) или доверия, и использовать сертифицированные по требуемому классу защищенности СрЗИ.

Для оценки реализуемости требований по защите информации от несанкционированного доступа (НСД) и уровню контроля отсутствия НДВ (доверия) по отношению к средствам виртуализации использовались критерии, представленные в табл. 1.

Таблица 1

Результаты оценки реализуемости требований по защите информации от НСД и уровню контроля отсутствия НДВ (доверия), с учетом введенных критериев, по отношению к средствам виртуализации для АС

Критерии оценки	ПК СВ «Брест»	ПАК «Горизонт-ВС»	ROSA Virtualization	zVirt	«Р-Виртуализация»	TIONIX Cloud
К.СВ.1 — соответствие формальным требованиям для возможности обработки информации соответствующего грифа — наличие сертификатов МО РФ или ФСТЭК России на соответствие требуемому уровню контроля отсутствия НДВ (доверия)	+	+	+	+	+	+
К.СВ.2 — наличие сертификатов МО РФ или ФСТЭК России для возможности обработки информации, содержащей сведения, составляющие государственную тайну — на соответствие 3, 2 или 1 уровню контроля отсутствия НДВ (доверия)	+	+	–	–	–	–
К.СВ.3 — использование средств защиты информации, встроенных в ОС Astra Linux SE, сертифицированных на соответствие требованиям к средствам защиты информации от НСД для построения АС по классу защищенности 1Б [1]	+	–	–	–	–	–
К.СВ.4 — использование отечественных ОС для формирования виртуальной инфраструктуры	+	+	+	+	+	+
К.СВ.5 — возможность масштабирования виртуальных машин (ВМ) — автоматического перераспределения ВМ без остановки в их работе с целью выравнивания нагрузки на физические серверы с гипервизорами	+	+	+	+	+	+
К.СВ.6 — централизованное управление кластерами серверов с гипервизорами, их масштабирование и обеспечение отказоустойчивости — возможность создания кластеров высокой доступности (High Availability) и централизованного управления ими	+	+	+	+	+	+
К.СВ.7 — возможность централизованного управления ВМ и подключениями к ВМ на основе шаблонов и политик безопасности	+	–	–	–	–	+
К.СВ.8 — совместимость с технологиями на базе служб LDAP-совместимых каталогов — поддержка службы каталогов FreeIPA, совместимой со службой каталога Active Directory, для централизованного управления виртуальной инфраструктурой и задания политик безопасности	+	–	+	+	–	–

Примечания: Знак «+» — требование реализуется; Знак «–» — требование не реализуется.

Все имеющиеся в настоящий момент средства виртуализации, сертифицированные в системе сертификации МО РФ или ФСТЭК России, основаны на открытых (Open Source) проектах и используют входящие в состав Linux гипервизор KVM (Kernel-based Virtual Machine), а также эмулятор аппаратного окружения виртуальных машин QEMU:

– программный комплекс средств виртуализации «Брест» для ОС Astra Linux SE (разработчик — компания «РусБИТех-Астра»), основан на открытом проекте OpenNebula и сертифицирован для использования в АС до класса защищенности 1Б включительно в соответствии с РД АС [1];

– программно-аппаратный комплекс (ПАК) виртуализации и защиты виртуальных систем «Горизонт-ВС» (разработчик — компания «ИЦ «Баррикады»), основан на открытом проекте OpenNebula и сертифицирован для использования в АС до класса защищенности 1Б включительно в соответствии с РД АС;

– система управления виртуализацией ROSA Virtualization (разработчик — компания «НТЦ ИТ РОСА»), основана на Open Source проекте oVirt и сертифицирована для использования в АС до класса защищенности 1Г включительно в соответствии с РД АС;

– система управления средой виртуализации zVirt (разработчик — компания «Инфолэнд»), основана на Open Source проекте oVirt и сертифицирована для использования в АС до класса защищенности 1Г включительно в соответствии с РД АС;

– система управления средой виртуализации «Р-Виртуализация» (разработчик — компания «Расплатформа»), основана на Open Source проекте OpenStack и сертифицирована для использования в АС до класса защищенности 1Г включительно в соответствии с РД АС;

– система управления средой виртуализации TIONIX Cloud Platform (разработчик — компания «ТИОНИКС»), основана на Open Source проекте OpenStack и сертифицирована для использования в АС до класса защищенности 1Г включительно в соответствии с РД АС.

Результаты оценки реализуемости требований по защите информации от НСД и уровню контроля отсутствия НДВ (доверия), с учетом введенных критериев, по отношению к средствам виртуализации представлены в табл. 1.

Для формирования виртуальной инфраструктуры, в которой обрабатывается информация до грифа «ДСП» включительно, могут использоваться средства виртуализации ROSA Virtualization, zVirt, «Р-Виртуализация» и TIONIX Cloud Platform. Однако вместе с этими средствами виртуализации должны использоваться СрЗИ [9], сертифицированные по 4 классу в соответствии с профилями защиты ФСТЭК или 5 классу по РД средств вычислительной техники (СВТ) [10]. Например, в системе управления виртуализацией ROSA Virtualization в качестве сертифицированных СрЗИ используются средства защиты, встроенные в ОС ROSA «КОБАЛЬТ», которая сертифицирована на соответствие профилю защиты ОС типа «А» четвертого класса защиты (ИТ.ОС.А4.ПЗ) и 4 уровню контроля отсутствия НДВ.

Для формирования виртуальной инфраструктуры для критически важных АС, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, могут использоваться только ПК СВ «Брест» и ПАК «Горизонт-ВС», которые сертифицированы по 2 уровню контроля отсутствия НДВ.

Для защиты информации от НСД в ПК СВ «Брест» используются СрЗИ, встроенные в ОС Astra Linux SE, которая сертифицирована на соответствие профилю защиты ОС типа «А» второго класса защиты (ИТ.ОС.А2.ПЗ) и 2 уровню доверия.

Для защиты информации от НСД в ПАК «Горизонт-ВС» используются СрЗИ, встроенные в сам комплекс, который дополнительно сертифицирован по 3 классу защищенности информации от НСД по РД СВТ [10].

ПК СВ «Брест» и ПАК «Горизонт-ВС» вместе с сертифицированными СрЗИ обеспечивают выполнение большинства требований приказа ФСТЭК № 17 от 11.02.2013 (с изменениями, внесенными приказом ФСТЭК № 27 от 15.02.2017 [11]) по защите среды виртуализации (табл. 2), а именно — требований ЗСВ.1–ЗСВ.7, ЗСВ.10. Для выполнения требований ЗСВ.9 и ЗСВ.8, не реализуемых ПК СВ «Брест» и ПАК «Горизонт-ВС», необходимо использовать средство антивирусной защиты (САВЗ), например Kaspersky Endpoint Security, и средство резервного копирования, например Bacula из состава Astra Linux SE.

Таблица 2

Группа требований по защите среды виртуализации (ЗСВ)

Условное обозначение меры	Меры защиты	Реализация в ПК СВ «Брест» и «Горизонт-ВС»
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	+
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	–
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	–
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+

Примечания: Знак «+» — требование реализуется ПК СВ «Брест» и «Горизонт-ВС»; Знак «–» — требование не реализуется ПК СВ «Брест» и «Горизонт-ВС».

Однако в ПК СВ «Брест» и ПАК «Горизонт-ВС» не обеспечивается реализация функции централизованного управления ВМ и подключениями к ВМ на основе шаблонов и политик безопасности. Для реализации этой функции компанией «РусБИТех-Астра» было разработано и сертифицировано для обработки информации, содержащей сведения, составляющие государственную тайну, программное расширение ПК СВ «Брест» — отдельный программный продукт «Брест.VDI», основанный на Open Source программной платформе управления ВМ OpenUDS. Поэтому, с учетом наличия программного расширения «Брест.VDI» для ОС Astra Linux SE, оптимальным вариантом построения защищенной виртуальной инфраструктуры для критически важных АС является использование ПК СВ «Брест», специально разработанного для ОС Astra Linux SE.

Интеграция платформы Kubernetes/OpenShift в систему виртуализации Astra Linux SE

Для возможности использования преимуществ контейнерной виртуализации, связанных с более высокой степенью автоматизации разработки, развертывания, кластеризации и масштабирования контейнеров в защищенной виртуальной среде, где вместо контейнеров используются ВМ, был создан открытый проект Kubernetes Virtualization API and Runtime для управления ВМ в среде платформы контейнеризации Kubernetes (kubevirt.io). В результате был разработан Open Source программный пакет Kubevirt, который расширяет функции программной платформы контейнеризации Kubernetes/OpenShift функциями для управления ВМ.

Модули Kubevirt интегрируются как в подсистему управления технологической платформой Kubernetes/OpenShift, функционирующую на узле управления (Master node), так и в подсистемы рабочих узлов (Worker nodes) кластера Kubernetes/OpenShift (рис. 1). В подсистему управления добавляется модуль управления кластером с контейнерами ВМ virt-controller и обработчик запросов virt-api, поступающих через Web- и CLI-пользовательские интерфейсы. В подсистему каждого рабочего узла добавляется обработчик событий virt-handler по управлению объединениями (подами) контейнеров ВМ, и контроллер запуска ВМ virt-launcher.

Технология KubeVirt позволяет управлять ВМ в среде платформы контейнеризации Kubernetes/OpenShift, а расширение Kubevirt обеспечивает возможность запуска платформы контейнерной виртуализации Kubernetes/OpenShift не на основе классических контейнеров (LXC, Docker), а на основе любых ВМ, поддерживаемых кроссплатформенной библиотекой и сервисом управления виртуализацией libvirt, входящей в состав ОС Astra Linux SE.

С учетом того, что libvirt входит в состав ОС Astra Linux SE и используется ПК СВ «Брест» в качестве базового программного интерфейса для создания защищенной виртуальной среды, Open Source программный пакет Kubevirt при условии сертификации вместе с Kubernetes/OpenShift может использоваться для дополнения системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI» платформой контейнеризации Kubernetes/OpenShift для управления ВМ. Это позволит повысить степень автоматизации разработки, развертывания, кластеризации и масштабирования ВМ в защищенной виртуальной среде системы виртуализации Astra Linux SE за счет использования для этого мощного потенциала платформы Kubernetes/OpenShift для управления ВМ по типу контейнерных нагрузок.

При использовании классической контейнерной виртуализации контейнеры задействуют механизмы Linux-ядра, такие как namespaces и cgroups для изоляции процессов и управления ресурсами. Обычно под процессами понимаются запущенные исполняемые файлы, приложения Python и любые другие процессы, например

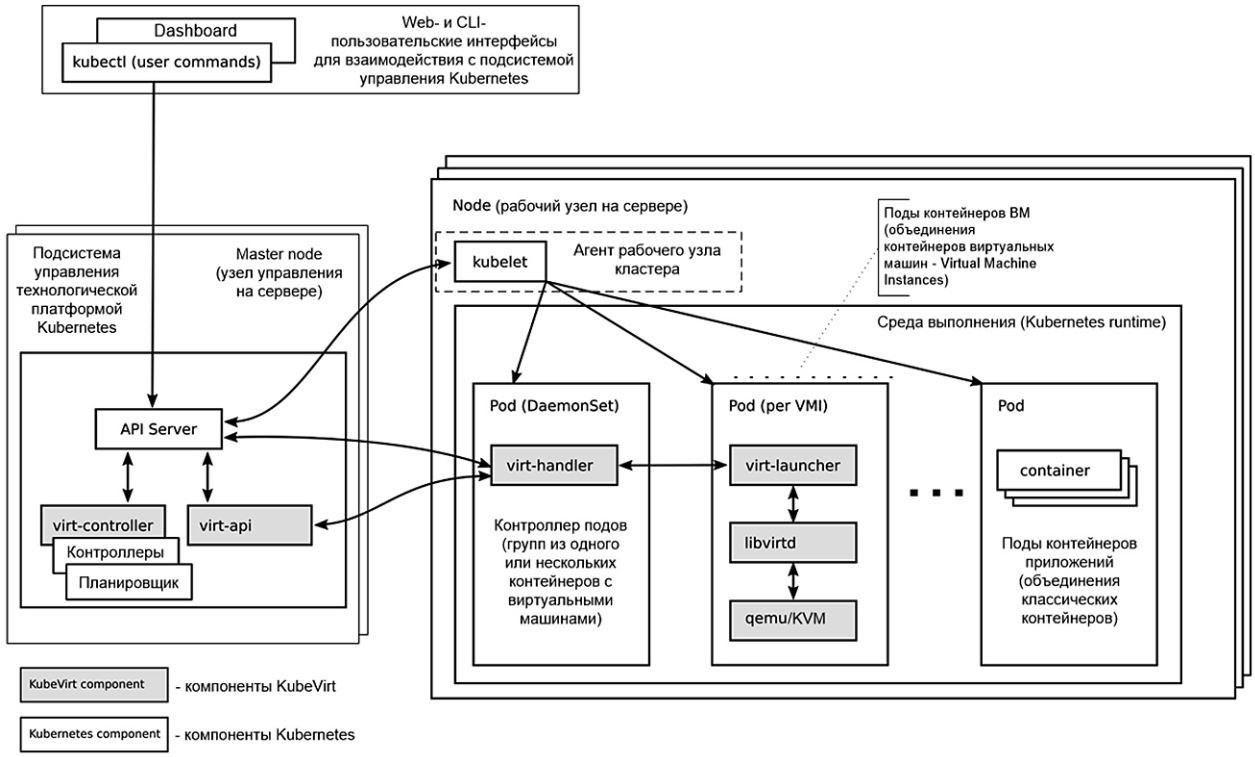

Рис. 1. Схема интеграции платформы Kubernetes/OpenShift в систему виртуализации Astra Linux SE, основанной на средствах виртуализации libvirt/QEMU/KVM

командная оболочка (Shell) Bash. При использовании платформы контейнерной виртуализации Kubernetes/OpenShift с расширением Kubevirt виртуальная машина рассматривается так же как процесс, но только не процесс приложения, а KVM-процесс, отвечающий за выполнение конкретной ВМ (рис. 2).

Поскольку виртуальная машина KVM (ВМ-KVM) или объединение нескольких ВМ-KVM — это Pod в терминологии Kubernetes/OpenShift (т.е. группа из одного или нескольких контейнеров на одном узле), то Pod из ВМ-KVM автоматом наследует всю функциональность Pod'а в Kubernetes/OpenShift. К ВМ-KVM-pod'ам точно так же, как и к обычным Pod'ам, применяются схемы и критерии планировщика Kubernetes/OpenShift для автоматизации развертывания, кластеризации и масштабирования контейнеров, но в данном случае — не контейнеров приложений, а контейнеров виртуальных машин. При этом создание защищенной виртуальной среды обеспечивает система виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI».

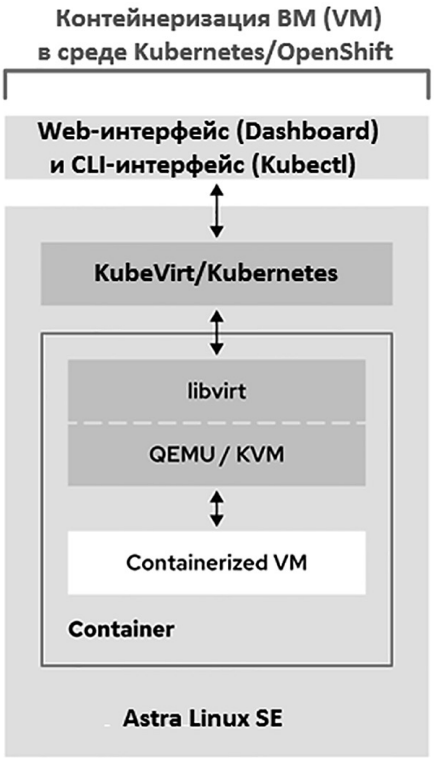

Рис. 2. Общая схема управления виртуальной машиной как контейнером с KVM-процессом в среде платформы Kubernetes/OpenShift при использовании расширения Kubevirt

Архитектура системы виртуализации Astra Linux SE, интегрированной с платформой KUBERNETES/OPENSHIFT

Архитектура системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift с помощью расширения Kubevirt, включает следующие основные составляющие (рис. 3):

– на нижнем уровне — загружаемый модуль ядра KVM и эмулятор аппаратного окружения виртуальных машин QEMU из состава ОС Astra Linux SE;

– на среднем уровне:

1) libvirt — кроссплатформенная библиотека и сервис управления виртуализацией, позволяющие контролировать по сети ВМ на других компьютерах (также входит в состав Astra Linux SE). Сервис libvirtd, входящий в программный пакет libvirt, способен создавать требуемые ВМ и подключать к ним необходимые ресурсы;

2) virt-manager — менеджер ВМ и графическая консоль управления гипервизором KVM на базе Web-интерфейса. Используется для создания и контроля состояния ВМ на уровне отдельных серверов. Virt-manager также предоставляет возможность управления удаленными серверами виртуализации, осуществляет сетевые соединения с удаленными процессами libvirtd из состава программного пакета libvirt;

3) virsh — утилита для командной строки Linux, предназначенная для управления ВМ и гипервизорами KVM. Virsh использует API (Application Programming Interface) libvirt и является альтернативой для графической консоли virt-manager;

– на верхнем уровне — платформа управления виртуальной инфраструктурой OpenNebula, а также платформа контейнерной виртуализации Kubernetes/OpenShift с расширением Kubevirt.

Программные составляющие архитектуры системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift с помощью Kubevirt, функционируют как в пространстве ядра ОС Astra Linux SE, так и в пользовательском пространстве.

В пространстве ядра функционируют основные модули гипервизора KVM, который использует аппаратную поддержку виртуализации

за счет специальной процессорной архитектуры для работы гипервизора (Intel VT — Intel Virtualization Technology, AMD Virtualization — AMD-V или др.):

– аппаратную виртуализацию процессоров и оперативной памяти (Symmetric Multi Processing — SMP, Memory Management Unit — MMU);

– аппаратную виртуализацию ввода-вывода (Input Output Memory Management Unit — IOMMU);

– аппаратную поддержку управления ВМ (Virtual Machine Extensions — VMX).

Программное обеспечение (ПО) KVM состоит из 1 загружаемого модуля ядра, предоставляющего базовый сервис виртуализации, 2 процессорно-специфического загружаемого модуля, использующего возможности конкретного процессора, и 3 компонентов пользовательского режима. Загрузка вышеперечисленных модулей превращает ядро ОС Astra Linux SE в гипервизор. В архитектуре гипервизора KVM виртуальная машина исполняется как обычный процесс, что позволяет задействовать все возможности ядра.

Модуль ядра KVM поддерживает динамическую миграцию, обеспечивая возможность перемещения работающих ВМ между физическими узлами без прерывания обслуживания. Динамическая миграция прозрачна для пользователей: виртуальная машина остается включенной, сетевые соединения активными, пользовательские приложения продолжают работать, в то время как ВМ перемещается на новый физический сервер. Наряду с динамической миграцией гипервизор KVM поддерживает сохранение копии текущего состояния виртуальной машины на диск, позволяя хранить ее и восстанавливать позднее.

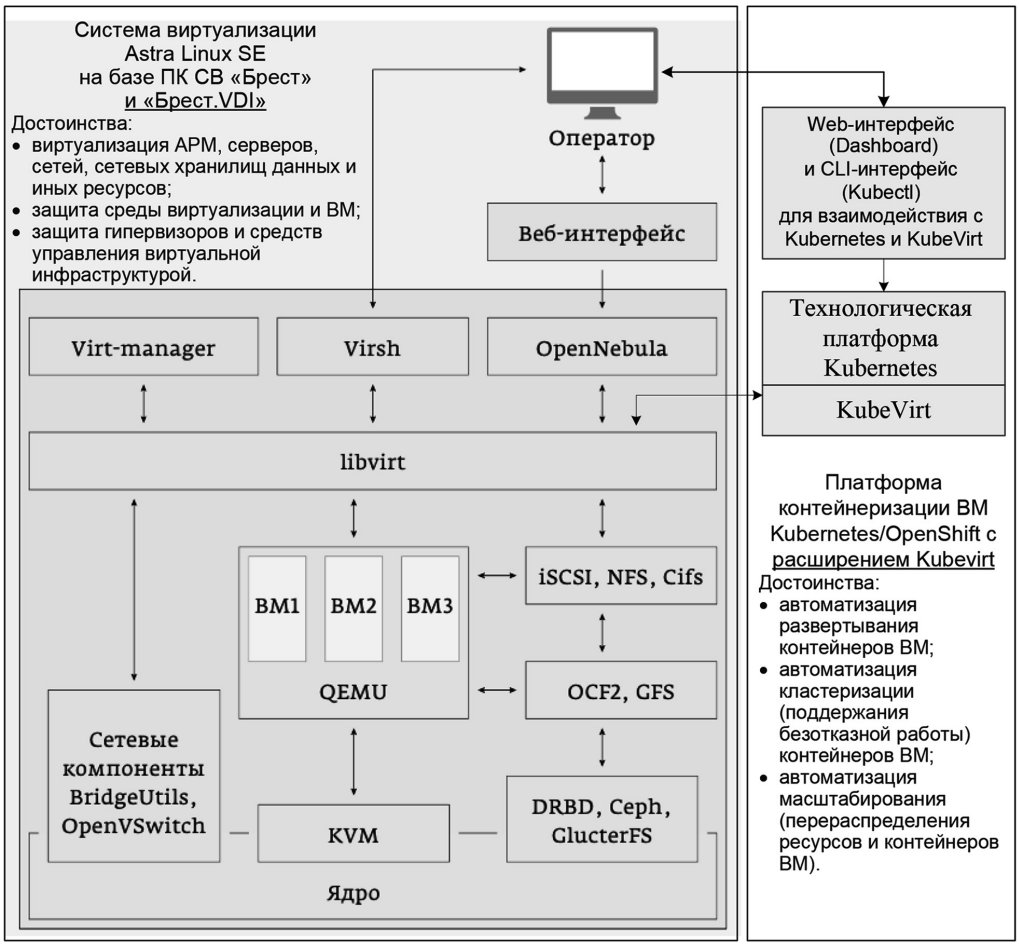

Рис. 3. Архитектура системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift с помощью расширения Kubevirt

Пользовательское пространство архитектуры системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift с помощью Kubevirt, представлено остальными программными составляющими (рис. 3), за исключением сетевых компонентов bridge-utils и OpenvSwitch для формирования сегментируемой и коммутируемой виртуальной сети, а также используемых файловых систем (Ceph — Software-Defined Storage, DRBD — Distributed Replicated Block Device и др.), часть модулей которых для высокой производительности функционирует в пространстве ядра ОС Astra Linux SE.

В пользовательском пространстве ОС Astra Linux SE функционирует и модуль QEMU, который обеспечивает виртуальное аппаратное окружение для гостевых ОС: UEFI/BIOS, шины PCI, шины USB, а также стандартный набор устройств, таких как дисковые контроллеры IDE, SATA, SCSI, сетевые карты и др. Каждая ВМ в окружении QEMU функционирует как изолированный процесс также в пространстве пользователя.

QEMU в качестве эмулятора ВМ может обеспечивать запуск ОС и программ, разработанных для одной аппаратной платформы (например, ARM или MIPS) на аппаратных платформах другого типа (например, на x86-совместимой).

В режиме виртуализации модуль QEMU выполняет гостевой код, который может быть выполнен хостовым процессором, непосредственно на нем, благодаря чему достигается производительность, близкая к производительности хостовой системы.

Таким образом, полноценным гипервизором Astra Linux SE становится только при совместном функционировании модуля ядра KVM с QEMU в пространстве пользователя, эмулирующим устройства ввода-вывода и UEFI/BIOS. Для каждой ВМ запускается отдельный процесс QEMU-KVM. При выключении гостевой системы этот процесс уничтожается или осуществляется выход из него. Помимо потоков виртуальных процессоров существуют специализированные потоки, в которых обрабатываются операции ввода-вывода, такие как передача сетевых пакетов и дисковые операции.

Сетевая виртуальная среда в системе виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift с помощью Kubevirt, реализована на основе модулей bridge-utils и OpenvSwitch, используемых для формирования сегментируемой и коммутируемой виртуальной сети.

Управление гипервизором QEMU/KVM и ВМ реализуется через API библиотеки libvirt с помощью платформы управления виртуальной инфраструктурой OpenNebula и платформы контейнерной виртуализации Kubernetes/OpenShift с расширением Kubevirt, а также графической консоли управления KVM Virt-manager и утилиты командной строки Virsh с функциями поддержки на уровне ОС Astra Linux SE модели дискреционного, мандатного и ролевого разграничения прав доступа.

Функции взаимодействия с различными объектами в libvirt реализованы в драйверах — программных модулях, которые в момент инициализации регистрируются в libvirt. Каждый драйвер регистрирует API-функции, реализованные на API-интерфейсах libvirt. Сервис libvirtd порождает процесс QEMU-KVM, который взаимодействует с модулями ядра и создает ВМ. QEMU взаимодействует с KVM через различные системные вызовы. Для каждой ВМ сервисом libvirtd запускается отдельный процесс QEMU-KVM. Свойства ВМ (количество процессоров, объем памяти, конфигурация устройств ввода-вывода) описываются в отдельных XML-файлах, используемых сервисом libvirtd для формирования списка аргументов, который передается в виде командной строки при запуске процесса QEMU-KVM.

Функции защиты информации, встроенные в ОС Astra Linux SE, реализуются в отношении любых контролируемых ОС субъектов и объектов доступа, включая процессы ВМ, которые могут управляться по типу контейнерных нагрузок, файлы-образы ВМ, специальные файлы эмулируемых устройств для использования ВМ, средства межпроцессного и сетевого взаимодействия, используемые ВМ, и прочее.

Заключение

В статье рассмотрен практический подход к безопасному применению контейнерной виртуализации в критически важных АС, основанный на интеграции системы виртуализации Astra Linux Special Edition и платформы

контейнеризации Kubernetes/OpenShift, раскрыты особенности реализации архитектуры системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI», интегрированной с платформой Kubernetes/OpenShift. На основе изложенного материала целесообразно сформулировать следующие выводы.

1. В критически важных АС к обязательным компонентам, необходимым для формирования защищенной виртуальной среды на базе операционной системы (ОС) Astra Linux Special Edition (далее — Astra Linux SE), относятся ОС Astra Linux SE и программный комплекс средств виртуализации «Брест». Для централизованного управления виртуальными машинами и подключениями к ВМ на основе шаблонов и политик безопасности целесообразно использование дополнительного компонента — программного расширения ПК СВ «Брест» — отдельного программного продукта «Брест.VDI».

2. Для возможности использования преимуществ контейнерной виртуализации, связанных с более высокой степенью автоматизации разработки, развертывания, кластеризации и масштабирования контейнеров в защищенной виртуальной среде, где вместо контейнеров используются ВМ, целесообразно использование Open Source программного пакета Kubevirt, который расширяет функции программной платформы контейнеризации Kubernetes/OpenShift функциями для управления ВМ. Технология KubeVirt позволяет управлять ВМ в среде платформы контейнеризации Kubernetes/OpenShift, а расширение Kubevirt обеспечивает возможность запуска платформы контейнерной виртуализации Kubernetes/OpenShift не на основе классических контейнеров (LXC, Docker), а на основе любых ВМ, поддерживаемых кроссплатформенной библиотекой и сервисом управления виртуализацией libvirt, входящей в состав ОС Astra Linux SE.

3. Функции защиты информации, встроенные в ОС Astra Linux SE, реализуются в отношении любых контролируемых ОС субъектов и объектов доступа, включая процессы ВМ, которые могут управляться по типу контейнерных нагрузок, файлы-образы ВМ, специальные файлы эмулируемых устройств для использования ВМ, средства межпроцессного и сетевого взаимодействия, используемые ВМ, и прочее. Виртуальная инфраструктура, включая контейнеры виртуальных машин при использовании Kubernetes/OpenShift вместе с расширением Kubevirt, представлена в ОС Astra Linux SE в виде тех же сущностей, что и другие функциональные подсистемы, а предусмотренные приказом ФСТЭК № 17 от 14.02.2013 (с изменениями, внесенными приказом ФСТЭК № 27 от 15.02.2017 [11]) меры защиты функциональных подсистем, в т.ч. среды виртуализации, реализуются одними и теми же средствами защиты ОС Astra Linux SE под управлением ПК СВ «Брест», «Брест.VDI» и платформы контейнерной виртуализации Kubernetes/OpenShift с расширением Kubevirt для управления ВМ по типу контейнерных нагрузок.

4.) Open Source программный пакет Kubevirt при условии сертификации вместе с Kubernetes/OpenShift может использоваться для расширения системы виртуализации Astra Linux SE на базе ПК СВ «Брест» и «Брест.VDI» платформой контейнеризации Kubernetes/OpenShift для управления ВМ по типу контейнерных нагрузок и, соответственно, безопасного использования преимуществ контейнерной виртуализации по более высокой степени автоматизации разработки, развертывания, кластеризации и масштабирования контейнеров.

Литература

1. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России. 1992. 29 с.

2. ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. — М.: Стандартинформ, 2018. 36 с.

3. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: Стандартинформ, 2012. 56 с.

4. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. — М.: Стандартинформ, 2013. 161 с.

5. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. — М.: Стандартинформ, 2013. 150 с.

6. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. — М.: Стандартинформ, 2018. 102 с.

7. Руководящий документ. Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Гостехкомиссия России. 1999. 107 с.

8. Приказ ФСТЭК России № 76 от 02.06.2020. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обесечения безопасности информационных технологий». 19 с.

9. Зима В.М., Крюков Р.О. Методика формирования защищенной виртуальной инфраструктуры в сложных автоматизированных системах специального назначения // Труды ВКА им. А.Ф. Можайского. — СПб.: ВКА им. А.Ф. Можайского, 2019. № 667. С. 213–223.

10. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. Гостехкомиссия России. 1992. 29 с.

11. Приказ ФСТЭК России № 17 от 11.02.2013. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с изменениями, внесенными приказом ФСТЭК России № 27 от 15.02.2017. 15 с.

References

1. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection. State Technical Commission of Russia. 1992. 29 p.

2. GOST R 56938-2016. Data protection. Information protection when using virtualization technologies. General provisions. — M.: Standartinform, 2018. 36 p.

3. GOST R ISO/IEC 15408-1-2012. Information technology. Methods and means of ensuring security. Criteria for evaluating information technology security. Part 1. Introduction and general model. — M.: Standartinform, 2012. 56 c.

4. GOST R ISO/IEC 15408-2-2013. Information technology. Methods and means of ensuring security. Criteria for evaluating information technology security. Part 2: Security functional requirements.— M.: Standartinform, 2013. 161 p.

5. GOST R ISO/IEC 15408-3-2013. Information technology. Methods and means of ensuring security. Criteria for evaluating information technology security. Part 3: Security Assurance Requirements.— M.: Standartinform, 2013. 150 p.

6. GOST R 57628-2017. Information technology. Methods and means of ensuring security. Guidance for developing protection profiles and security targets. — M.: Standartinform, 2018. 102 p.

7. Guidance document. Protection against unauthorized access to information. Information security software. Classification by the level of control of the absence of undeclared capabilities. State Technical Commission of Russia. 1999. 107 p.

8. Order of FSTEC of Russia № 76 of 02.06.2020. «Requirements for information security, establishing levels of confidence in the means of technical protection of information and means of ensuring the security of information technologies». 19 p

9. Zima V.M., Kryukov R.O. Methodology for the formation of a secure virtual infrastructure in complex automated systems for special purposes // Proceedings of the VKA named after A.F. Mozhaisky. — St. Petersburg: VKA named after A.F. Mozhaisky, 2019. No. 667. Pp. 213–223.

10. Guidance document. Computer facilities. Protection against unauthorized access to information. Indicators of security from unauthorized access to information. State Technical Commission of Russia. 1992. 29 p.

11. Order of FSTEC of Russia № 17 of 2013. «On Approval of Requirements for Protection of Information Not Constituting State Secrets Contained in State Information Systems» as amended by FSTEC Order № 27 of 15.02.2017. 15 p.