В. В. Макаров, А. Б. Вавренюк, В. А. Шурыгин, О. К. Курышева

РАЗРАБОТКА АРХИТЕКТУРЫ ЗАЩИЩЕННОГО ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА, В КОТОРОМ ПРИЛОЖЕНИЯ ФУНКЦИОНИРУЮТ В ВИРТУАЛЬНОЙ СРЕДЕ

В связи с тенденцией развития виртуализации возникают вопросы, связанные с выбором платформы для построения систем на базе виртуализации и облачных вычислений. Такие системы должны обеспечивать безопасную работу тысяч пользователей на общем для них оборудовании.

Несмотря на то что в мире уже существуют такие крупные облачные провайдеры, как Amazon, Azure и RackSpace, не существует готовой системы виртуализации, которая включала бы все компоненты для обеспечения возможности безопасной работы и которую можно было бы использовать без доработок. Существующие решения компаний VMware, Red Hat, Microsoft и Citrix находятся в зачаточном состоянии и не предоставляют все требуемые средства защиты информации в комплекте, предлагая использовать сторонние разработки. В то же время в последние годы российские компании, вводящие в эксплуатацию частные облачные инфраструктуры, столкнулись с проблемой аттестации своих объектов информатизации по требованиям безопасности.

Основной причиной этого является отсутствие готовой системы, включающей все компоненты, необходимые для функционирования виртуализации, которая соответствовала бы требованиям ФСТЭК РФ [1]. Из-за отсутствия такового каждая аттестация объекта информатизации, включающая виртуальную инфраструктуру, является уникальным проектом.

Целостный программно-технический комплекс (ПТК), обслуживающий все задачи виртуализации, должен включать не только серверы виртуализации и управления виртуальными машинами, но и систему мониторинга, средство управления пользователями, выделенную систему хранения данных. В случае, когда при проектировании ПТК наличие этих элементов уже заложено в архитектуру, становится намного проще защитить систему, чем при интеграции серверов виртуализации с множеством сторонних систем.

В программно-техническом комплексе, в котором приложения функционируют в виртуальной среде, защищаемыми активами являются данные, находящиеся внутри виртуальных машин пользователей, а также конфигурационные файлы системы виртуализации, которые требуются для запуска виртуальных машин с подключенными образами дисков. Данные пользователей можно получить двумя способами: получив доступ непосредственно к виртуальной машине как к обычной рабочей станции, например, по сети, или получив доступ к образу диска виртуальной машины с сервера виртуализации. Первый способ является стандартным и относится также к любой инфраструктуре без системы виртуализации, второй применим только к виртуальной среде.

Владельцами активов в данной постановке задачи являются пользователи виртуальных машин и администраторы ПТК. Потенциальными нарушителями (источниками угроз) могут быть как пользователи и администраторы, умышленно или случайно порождающие угрозы для активов, так и внешние лица, не имеющие права доступа к ПТК. Таким образом, требуется минимизировать риски для активов, которые возникают в связи с угрозами, порождаемыми источниками угроз.

В разрабатываемом ПТК используется система виртуализации на базе QEMU и KVM, программных средств с открытым исходным текстом, что упрощает процедуру проведения контроля отсутствия недекларированных возможностей. В качестве операционной системы для всех элементов ПТК используется Red Hat Enterprise Linux 6.

При разработке структуры программно-технического комплекса решим следующие задачи:

- определение списка задач, решаемых в рамках проектируемой системы;
- определение списка элементов (серверов, решающих разные функциональные задачи) ПТК, решающих определенные ранее задачи;

- определение и обоснование количества локальных вычислительных сетей и их разделения для взаимодействия между разными подсистемами.

В рамках проектируемого комплекса решаются следующие задачи:

- запуск и функционирование виртуальных машин;
- хранение образов дисков виртуальных машин (шифрование, ограничение доступа, контроль целостности);
- управление виртуальными машинами (создание, удаление, управление правами доступа, выделение дополнительных аппаратных ресурсов);
- работа пользователей в виртуальных машинах (запуск, выключение виртуальных машин, доступ к гостевым операционным системам и данным);
- управление пользователями (добавление, удаление пользователей, выдача прав доступа к системе);
- контроль состояния системы (мониторинг общего состояния комплекса и мониторинг безопасности).

Определим, какие элементы потребуется использовать для решения указанных задач:

- запуск и функционирование виртуальных машин должны производиться на серверах, оснащенных процессорами, поддерживающими аппаратную виртуализацию (Intel-VT или AMD-V). В зависимости от размера комплекса таких серверов может быть от одного до нескольких тысяч;
- для хранения образов дисков виртуальных машин воспользуемся выделенной системой хранения данных;
- управление виртуальными машинами и работа пользователей в виртуальных машинах обеспечивается разработкой специального ПО. Средство управления виртуальными машинами администратором и средство управления виртуальными машинами пользователями являются разными элементами ПТК для решения задачи использования различных серверов и сетей для этих двух элементов;
- для управления пользователями требуется выделенный элемент системы для создания единой базы всех пользователей и дальнейшей аутентификации пользователей всех элементов в соответствии с записями и правами в базе;
- контроль состояния системы производится средствами специализированной системы мониторинга, разработка которой должна быть проведена в процессе разработки ПТК.

Для распределения элементов по сегментам и определения числа локальных вычислительных сетей разделим решаемые задачи на три группы: задачи функционирования системы виртуализации, задачи администрирования и задачи использования.

К задачам функционирования относятся запуск и функционирование виртуальных машин, а также хранение образов дисков виртуальных машин. Эти задачи должны решаться без участия пользователей по отлаженным схемам функционирования. Вмешательство пользователя в функционирование этой части ПТК влечет за собой возможные нарушения в работе.

К задачам администрирования относятся управление виртуальными машинами, пользователями и контроль состояния системы. К этим функциям должны иметь доступ только администраторы.

К задачам использования относится использование виртуальных машин пользователями. Пользователи не должны иметь доступа к задачам администрирования и напрямую к образам дисков виртуальных машин. Пользователи обращаются к данным виртуальных машин, получая к ним доступ по протоколу доставки виртуального рабочего стола (VNC, Spice).

Таким образом, ПТК можно разделить на три сегмента, создав для каждого сегмента свою локальную вычислительную сеть:

- внешний сегмент, через который пользователи взаимодействуют со своими виртуальными машинами;

- сеть управления, в которой располагается средство управления виртуальными машинами администратора, сервер каталогов, через который происходит аутентификация пользователей, и сервер мониторинга;
- сеть данных, через которую происходит доступ гипервизора к образам дисков виртуальных машин.

Создание выделенной сети данных позволяет изолировать систему хранения данных от нарушителей во внешней сети и повысить скорость обмена данными, так как для взаимодействия между серверами с гипервизорами и системой хранения данных может использоваться протокол Fibre Channel с пропускающей способностью до 10 Гб/с.

Разделение внешнего сегмента и сети управления позволяет решить многие вопросы безопасности системы, так как при такой архитектуре доступ к административным функциям ПТК будут иметь только доверенные администраторы. Пользователи внешнего сегмента имеют право лишь на запуск и выключение виртуальных машин, могут получать к ним доступ по протоколу Spice, подключаясь к серверам виртуализации напрямую. Межсетевой экран, функционирующий во внешнем сегменте, ограничивает доступ пользователей к другим функциям системы.

Таким образом, в целях безопасности интерфейс пользователей для получения доступа к виртуальными машинам и интерфейс администратора для управления виртуальными машинами разделяются по разным серверам и сетям. Серверы виртуализации являются единственными элементами, входящими во все три сегмента, на этих серверах настраивается межсетевой экран iptables, а также ограничивается доступ по используемым протоколам (SSH, Spice, FTP) для разных сегментов. Используемые серверы должны иметь две сетевые платы для подключения к внешний сети и сети управления, а также плату для подключения к СХД по протоколу Fibre Channel. Управление сетями доступно только сетевому администратору.

Структурная схема программно-технического комплекса представлена на рис. 1.

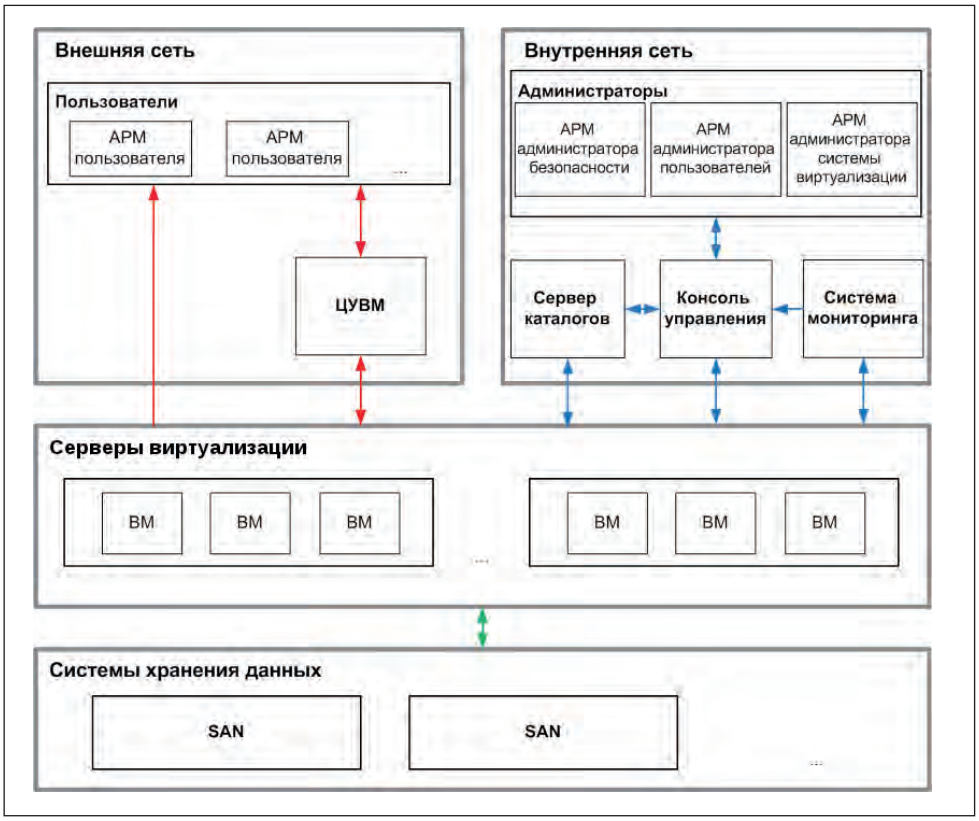

Рис. 1. Структурная схема ПТК

Основываясь на руководящих документах ФСТЭК РФ [1], опишем детали реализации каждого элемента и связи между ними.

Сервер виртуализации включает систему виртуализации QEMU, KVM, средство управления виртуальными машинами libvirt и серверную часть реализации протокола доставки виртуального рабочего стола Spice.

Сервер виртуализации подключается к системе хранения данных, на которой хранятся образы дисков виртуальных машин и конфигурационные файлы, посредством Fibre Channel. Использование выделенной системы хранения данных (например, SAN) позволит запускать виртуальные машины на любом из серверов при полной загрузке вычислительных ресурсов той машины, на которой обычно функционирует виртуальная машина. Также при больших объемах данных специализированная система хранения данных будет лучше справляться с большим количеством операций ввода-вывода. Контроль целостности данных и задача шифрования данных решаются встроенными средствами системы хранения данных.

Для управления виртуальными машинами требуется разработка специального программного обеспечения. Администратор системы виртуализации должен иметь доступ к функциям управления виртуальными машинами пользователей и общими настройками ПТК. Для этого в ПТК должна быть предусмотрена Консоль администратора.

В существующих системах средство управления виртуальными машинами всегда имеет абсолютные права доступа к серверам виртуализации. Пользователи, подключаясь к средству управления, авторизуются во внутренней базе пользователей средства, после чего само программное обеспечение решает, права доступа к каким функциям есть у данного конкретного пользователя. Таким образом, получив доступ к средству управления, используя его уязвимости, можно получить права администратора на серверах виртуализации. Такой подход к проектированию средств управления виртуальными машинами требует создания профиля защиты и отдельной сертификации как серверов виртуализации, так и средства управления виртуальными машинами. Данный процесс можно упростить, используя нижеописанную архитектуру при проектировании средства управления.

Средство управления имеет двухзвенную архитектуру. В качестве сервера используется стандартное средство virsh, разработанное на базе библиотеки libvirt. Virsh функционирует на серверах виртуализации и выполняет команды пользователей, передаваемые со средства управления виртуальными машинами. В качестве клиента реализуется программное средство, имеющее веб-интерфейс, что позволит администратору подключаться к системе без установки дополнительных приложений кроме веб-браузера на рабочую станцию администратора. Подключение администратора к веб-интерфейсу средства производится по протоколу HTTPS (имя пользователя, пароль, запрос на доступ к виртуальной машине). Аутентификация пользователя производится в соответствии с правами пользователя в базе пользователей.

После получения запроса от пользователя средство управления виртуальными машинами преобразует его в формат libvirt и направляет запрос на серверы с гипервизорами от имени пользователя, авторизуясь на сервере виртуализации с использованием имени пользователя и пароля, только что введенного пользователем. Это позволит упростить задачу контроля безопасности средства управления виртуальными машинами, так как сервер, на котором установлено средство, не будет содержать никакой информации кроме способа преобразования запроса в формат libvirt, а также списка IP-адресов серверов виртуализации. Все данные, подлежащие защите, находятся на серверах виртуализации и в системах хранения данных. Управление виртуальными машинами производится через libvirt непосредственно на серверах виртуализации, а средство управления предназначено для обеспечения безопасного доступа администратора к функциям libvirt.

Средство управления виртуальными машинами пользователей является аналогом средства управления виртуальными машинами администратора, но имеет функции только для запуска,

выключения виртуальных машин, а также подключения к запущенным машинам с использованием протокола Spice. Таким образом, разница между средствами состоит лишь в количестве команд, которые средство умеет переводить из языка взаимодействия пользователей в язык запросов libvirt. Разработка средства с веб-интерфейсом для доступа пользователей позволяет исключить необходимость производить установку клиента на рабочие станции пользователей.

Соединение с виртуальными машинами по протоколу Spice осуществляется с серверами виртуализации, минуя средство управления виртуальными машинами пользователей. Таким образом, трафик пользователей, работающих с виртуальными машинами, не проходит через средство, что позволяет увеличить пропускную способность канала связи при подключении к нескольким серверам виртуализации. Это ограничение существенно в связи с тем, что для передачи виртуального рабочего стола передается заметный объем трафика.

Используя протокол Spice, пользователи будут видеть рабочий стол своей виртуальной машины, иметь возможность работать с данными внутри своей виртуальной машины. Но они не будут иметь возможность подключить внешнее записывающее устройство (flash-карту, диск) для извлечения данных из виртуальной машины. Это позволяет обеспечить сохранность данных и предотвратить угрозы со стороны доверенных пользователей. Как правило, работая с данными, требующими защиты, пользователям также не нужен доступ к сети Интернет. При необходимости объединить виртуальные машины пользователей в виртуальную локальную вычислительную сеть это делается администратором, имеющим соответствующие права на серверах виртуализации.

Для хранения базы пользователей, имеющих доступ к системе виртуализации, используется сервер каталогов OpenLDAP или другое сертифицированное средство, работающее с использованием протокола LDAP.

Система предусматривает разделение пользователей на следующие роли:

- администратор системы виртуализации, имеющий доступ к созданию, удалению, изменению конфигурации виртуальных машин, добавлению новых серверов в ПТК и их настройке;
- администратор безопасности, отвечающий за безопасность системы и работающий с системой мониторинга ПТК для обеспечения быстрого реагирования на события, затрагивающие безопасность системы;
- администратор пользователей, отвечающий за создание, удаление пользователей и выдачу им прав доступа в соответствии с требованиями;
- пользователь ПТК, имеющий право включать и выключать виртуальные машины, которые ему создал администратор системы, получать доступ к данным внутри этих виртуальных машин.

ПТК должен обеспечивать централизованное хранение базы пользователей. Это позволит при добавлении нового элемента в ПТК не дублировать все учетные записи пользователей и их права в базу нового сервера. Использование сервера, работающего по протоколу LDAP, позволяет организовать аутентификацию пользователей всех средств (средство управления виртуальными машинами, Консоль администратора, операционная система серверов виртуализации, пользователи libvirt) в соответствии с единой базой пользователей. Используя Консоль администратора, уполномоченный сотрудник создает пользователь и выдает им права доступа к виртуальным машинам.

Для оптимизации создаваемой структуры ПТК объединим консоли администратора системы виртуализации, администратора пользователей и администратора безопасности в единый веб-интерфейс. В зависимости от роли подключающегося к консоли администратора ему будет предложен для исполнения набор функций, соответствующий его роли. Объединение пользовательских интерфейсов администраторов позволит не дублировать функционал разных подсистем и предоставить пользователям единый интерфейс для подключения к ПТК.

Система мониторинга разрабатывается на базе низкоуровневых интерфейсов, предоставляемых операционной системой и библиотекой libvirt. Существующие системы ориентированы на

решение задачи мониторинга потребления ресурсов, доступности подсистем, но не решают задачу комплексного мониторинга. Для получения информации о событиях, угрожающих безопасности системы виртуализации, используются программные средства autitd и syslog, которые позволяют контролировать события безопасности на уровне ядра. Мониторинг средств управления виртуальными машинами проводить не требуется, так как задачи управления выполняются на серверах виртуализации. В проектируемом ПТК необходимо проводить агентский мониторинг, для чего на серверы виртуализации следует устанавливать агенты мониторинга. Этот подход позволит уменьшить нагрузку на сервер мониторинга и количество передаваемых по сети данных, что будет эффективным в случаях, когда число серверов виртуализации станет значительным.

При разработке средства мониторинга также необходимо определить состав событий и действий, за которыми требуется производить контроль. Этот состав на данный момент еще не определен в руководящих документах Гостехкомиссии России по виртуализации, но его можно сформировать, основываясь на существующих документах по защите средств автоматизации. Данная работа уже проведена компанией «Крок» [3]. На основе этой информации можно составить список событий.

Разработку средства мониторинга целесообразно проводить на языке программирования Python. Python является скриптовым языком. Это упрощает процедуру проведения контроля отсутствия недекларированных возможностей в разрабатываемом программном обеспечении за счет отсутствия зависимости от среды сборки и компилятора.

При проектировании ПТК также должно учитываться, что количество серверов может быть большим (до 100–1000 машин). В связи с этим пропускная способность сети должна быть соответствующей для отображения пользователям графического интерфейса виртуальных машин.

Данный ПТК спроектирован для решения задачи управления, разграничения прав доступа и полноценного мониторинга системы виртуализации масштаба Центра обработки данных. ПТК включает в себя серверы виртуализации, системы хранения данных, средства мониторинга, управления пользователями, администрирования и предоставления доступа пользователям к системе виртуализации. В целях безопасности работа с ПТК производится в трех различных сетях, в зависимости от роли работающего пользователя.

СПИСОК ЛИТЕРАТУРЫ:

1. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (Общие положения и Часть 1). Введен 19.06.2002. – 58 с.
2. IBM Corporation. KVM security. 2010. URL: http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaat/liaatsecurity_pdf.pdf (дата обращения: 15.10.2012).
3. Компания КРОК. Защита в виртуальной среде. Чеклист угроз. 2012. URL: http://habrahabr.ru/company/croc/blog/140044/ (дата обращения: 15.10.2012).