DOI:

Гипергивергентные информационные системы с виртуализацией на основе программно-аппаратного комплекса виртуализации «Горизонт-ВС»

И. Коптелов[1], С. Назаров, д. т. н.[2], М. Ермолова[3]

УДК 004.946 | ВАК

Начало 2010-х годов ознаменовалось появлением конвергентных инфраструктур. Термин был предложен компанией Hewlett-Packard. В терминологии Gartner этот тип инфраструктуры называется интегрированной системой, а в компании Cisco Systems – системой унифицированных вычислений (UCS). В любом случае – это готовое решение от производителя, цель которого – ускорить развертывание инфраструктуры с нескольких месяцев до нескольких дней. Дальнейшее развитие конвергентных систем привело к гиперконвергентным инфраструктурам. Помимо упрощения архитектуры, в гиперконвергентной системе более простая модель администрирования. Вместо группы IT-администраторов для управления массивом данных, виртуализацией и серверным оборудованием, гиперконвергентной системой управляет одна команда (иногда один системный администратор). В статье рассматривается возможность построения гиперконвергентной инфраструктуры на примере модернизации вычислительной инфраструктуры таможенных постов Московской областной таможни на основе программного обеспечения (ПО) отечественного производства и отечественной платформы виртуализации «Горизонт-ВС».

КОНВЕРГЕНТНЫЕ И ГИПЕРКОНВЕРГЕНТНЫЕ ИНФРАСТРУКТУРЫ

Интенсивное развитие IT-технологий приводит к постоянному появлению новых эффективных решений. Одно из таких решений последних лет – конвергентные инфраструктуры. Понятие «конвергентность» (от лат. con вместе и vergere – сближаться) означает склонность к чему-либо, сближение с чем-либо. Например, в больших технических системах – это постепенное сближение различных устройств этой системы и их слияние в одну единую систему, доказавшую свою пригодность и эффективность.

Созданная ИТ-инфраструктура предприятия, как правило, постоянно дорабатывается, модернизируется по различным причинам – завершается срок службы отдельных устройств, планируется переход на более совершенное оборудование, новое программное обеспечение. Новые проекты, переход на выпуск новых продуктов и др. предъявляют зачастую более сложные требования к инфраструктуре предприятия. Приходится вводить дополнительное разнообразное оборудование и новое программное обеспечение, которое не всегда легко согласуется с имеющимся, необходимо уделять много внимания разрешению частных текущих проблем, в результате усложняется поддержка нормальной работоспособности системы. Встает вопрос о полной перестройке ИТ-инфраструктуры. Ответом на эти проблемы стало предложенное многими компаниями решение, получившее название **«конвергентная инфраструктура» (Converged Infrastructure, CI)**.

Основная идея нового метода – замена выделенного сервера виртуализованными, которые запускаются на общедоступном оборудовании. Для построения конвергентных решений можно использовать типовое оборудование x86, при этом допускается простое подключение специализированных аппаратных компонентов.

[1] ООО «Инновационный центр «Баррикады», и. о. генерального директора, koptelov@gorizont-vs.ru, igor.koptelov@mail.ru.

[2] ЗАО «МНИТИ», главный специалист, профессор, действительный член Международной академии информатизации, nazarov@mniti.ru, s_nazarov@mail.ru.

[4] ООО «Инновационный центр «Баррикады», исполнительный директор, МГТУ им. Н.Э. Баумана, ассистент, ermolova@gorizont-vs.ru, ermolova.88@mail.ru.

Создается возможность просто и легко наращивать архитектуру системы, добавлять новые функции для ее поддержки и при этом сохранять затраты на невысоком уровне. Управление инфраструктурой ведется централизованно. Это также дополнительно сокращает затраты, связанные с администрированием и настройкой [1].

Конвергентные инфраструктуры стремительно развиваются, и сегодня основные игроки ИТ-рынка включили CI в свои производственные программы. В августе 2012 года компанией IBM анонсировано семейство систем Pure Systems. Эта линейка продуктов IBM с предварительно сконфигурированными на заводе компонентами и серверами называется «Экспертная интегрированная система» [2]. Центральным элементом PureSystems является IBM Flex System Manager в совокупности с «шаблонами экспертизы» для автоматизированной конфигурации и управления системой. PureSystems может содержать четыре разные операционные системы (AIX, IBM i, Linux, Windows) и пять гипервизоров (Hyper-, KVM, PowerVM, VMware, Xen) в двух разных архитектурах набора команд: Power ISA и x86 [3]. PureSystems продается как система, главная идея которой объединение разрозненных аппаратных и программных компонентов в единый комплекс и предоставление заказчику всего, что необходимо для работы: вычислительной мощности, ресурсов хранения, сетевой поддержки, средств виртуализации, программного администрирования, единой консоли управления.

Дальнейшее развитие IT-технологий привело к появлению гиперковергентных инфраструктур (Hiper Converged Infrastructure, HCI). Последние позволяют добиться более плотной интеграции большего числа компонентов с применением программных средств. И в конвергентной, и в гиперконвергентной инфраструктуре все элементы совместимы друг с другом. Это позволяет упростить процесс развертывания такой инфраструктуры для компаний, которым необходимо осуществить виртуализацию настольных систем. Несмотря на свою эффективность и инновационность, технологии CI и HCI имеют определенные отличия в возможностях использования и в целевом назначении. **HCI-инфраструктура** строится на базе конвергентной, сохраняя все компоненты конвергентной инфраструктуры, но добавляются дополнительные программные компоненты, такие как ПО для резервного копирования, возможности мгновенных снимков, функционал дедупликации данных, промежуточное сжатие, оптимизация работы глобальной вычислительной сети и многое другое. **Конвергентная инфраструктура** в первую очередь опирается на аппаратные средства, а программно-определяемый ЦОД адаптируется под любое аппаратное обеспечение. В гиперконвергентной инфраструктуре эти две возможности объединены.

Гибкость HCI-инфраструктуры делает ее более масштабируемой и рентабельной по сравнению с конвергентной, поскольку в ней присутствует возможность добавления вычислительных устройств и устройств хранения по мере необходимости. Стоимость начальных капиталовложений для обеих инфраструктур высокая, но в долгосрочной перспективе стоимость вложенных средств окупается. CI-системы обычно состоят из нескольких физических модулей, объединяемых в горизонтально масштабируемый кластер. Каждый из них содержит вычислительное ядро, ресурсы хранения, сетевые компоненты и гипервизор. Отдельное устройство имеет от одного до четырех узлов, каждый из которых представляет собой самостоятельный сервер с процессором и памятью в общем шасси.

Гиперконвергентные кластеры обычно содержат от 4 до 64 узлов, хотя некоторые производители не указывают пределов масштабируемости. Для того чтобы узлы могли совместно использовать ресурсы хранения, применяется программное обеспечение для создания виртуальной сети хранения или кластерная файловая система. Во многих продуктах используется виртуальное устройство хранения (Virtual Storage Appliance, VSA) для объединения ресурсов хранения в общий пул. Другой подход состоит в использовании платформы VMware EVO : RAIL, в которой функции хранения и управления интегрированы в соответствующий гипервизор [4].

Позволяя избавиться от выделенной сети хранения, гиперконвергентная инфраструктура реализует виртуальную сеть хранения (Virtual SAN, VSAN). Виртуальное устройство хранения предоставляет функции контроллера хранения для гипервизора в кластере. Ресурсы хранения физического узла предоставляются VSA (Virtual Storage Appliance). Крупным поставщиком гиперконвергентной инфраструктуры является компания VMware. Как в случае с традиционными инфраструктурами, стоимость гиперконвергентной инфраструктуры может варьироваться в зависимости от используемого гипервизора. Инфраструктура на VMware vSphere или Microsoft Hyper-V может стоить достаточно дорого, более дешевые решения поставляют компании Nutanix и Simplivity [5].

В целом рынок гипергивергентных систем интенсивно растет. Проявляют к ним интерес и отечественные интеграторы и поставщики подобных решений, а также крупные государственные компании и предприятия. Отечественный рынок ИТ-инфраструктуры быстро меняется. По состоянию на 2017 год гиперконвергентные системы заменили привычные серверы и системы хранения в 20% российских компаний. За следующие три года 10% бюджетов на серверы и СХД достанутся производителям гиперконвергентных решений. Таковы результаты исследования TAdviser «Актуальные тенденции рынка гиперконвергентной инфраструктуры» [6]. Аналитики ожидают

рост рынка на 25–30% в год, который сдерживается тем, что значительная часть ИТ-специалистов не знакома с подобными решениями. Тем не менее спрос на HCI в России есть. Интерес к гиперконвергентным решениям проявляют российские банки. Из свежих примеров – развертывание VDI на базе Dell EMC VxRail в СКБ-банке. В числе российских заказчиков гиперконвергентных систем есть предприятия промышленности, розничной торговли и госсектора. В частности, в администрации Екатеринбурга осуществляется проект миграции ЦОДа классической архитектуры на гиперконвергентную. Программное обеспечение «Росплатформы» используется в Федеральной налоговой службе, Министерстве транспорта РФ, на судостроительном заводе «Янтарь» и ряде российских университетов [7].

ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ВИРТУАЛИЗАЦИИ «ГОРИЗОНТ-ВС» ДЛЯ ПОСТРОЕНИЯ ГИПЕРКОНВЕРГЕНТНЫХ ИНФРАСТРУКТУР

Цели модернизации вычислительных структур

Рассмотрим возможности построения гиперконвергентных систем на основе программно-аппаратного комплекса виртуализации (ПАК) «Горизонт-ВС», используемого в составе вычислительной инфраструктуры Московской областной таможни, которая подвергается модернизации в соответствии с техническим заданием, утвержденным Заказчиком. Основными целями модернизации являются:

- создание виртуальной вычислительной инфраструктуры таможенных постов, обеспечивающее снижение операционных затрат при эксплуатации за счет использования меньшего количества аппаратных компонентов;
- централизация управления всеми ИТ-ресурсами таможенных постов Московской областной таможни (МОТ);
- импортозамещение системного программного обеспечения (ПО) и ПО виртуализации иностранного производства;
- повышение надежности обработки и хранения информации;
- обеспечение масштабируемости и распределения загрузки вычислительной мощности аппаратной составляющей таможенных постов.

Пользователи модернизируемой системы – сотрудники таможенных постов, обеспечивающие ее администрирование и эксплуатацию. Вычислительная инфраструктура МОТ построена по иерархической схеме «звезда» на базе 21 таможенного поста с единым центром. Техническая инфраструктура создана на базе bare-metal серверов IBM. Идея bare-metal состоит в использовании выделенных серверов для создания облачной среды. Словосочетанию bare-metal еще нет адекватного перевода на русский язык (в некоторых источниках встречается «голое железо» или «чистое железо») [8]. В среде bare metal виртуальные машины инсталлируются непосредственно на аппаратуру. Серверы bare-metal не содержат гипервизор, и не виртуализированы, но могут быть предоставлены в пользование клиенту через модель услуг, подобную облаку. Облако в этом случае обеспечивает замену виртуальной облачной среды на среду с выделенными серверами, что дает возможность «сэкономить» ресурсы на виртуализации.

Технологии виртуализации и защита информации

Одним из наиболее эффективных способов модернизации вычислительной инфраструктуры является создание изолированных сред, использующих совместные ресурсы, к которым можно отнести технологии виртуализации. Все сервисы и услуги из реальных сетей перемещаются в виртуальные корпоративные или публичные облака. Наличие гипервизора позволяет повысить общую безопасность виртуализированных систем, поскольку гипервизор является прослойкой между аппаратным слоем и слоем гостевых операционных систем (ОС). В гипервизоре возможно реализовать дополнительные функции обеспечения безопасности, не реализованные в аппаратном слое. Однако виртуальная среда несет и новые угрозы информационной безопасности, которые часто не учитываются. Поэтому необходим комплексный подход к их защите с применением методов, разработанных именно для виртуальных сред.

Важно отметить появление **нового управляющего слоя для виртуальной инфраструктуры**, который достаточно часто не защищается специализированными средствами. Угрозы безопасности для виртуальных инфраструктур можно классифицировать следующим образом:

- атака на гипервизор с виртуальной машины;
- атака на гипервизор из физической сети;
- атака на диск виртуальной машины;
- атака на средства администрирования виртуальной инфраструктуры;
- атака на виртуальную машину с другой виртуальной машины;
- атака на сеть репликации виртуальных машин;
- неконтролируемый рост числа виртуальных машин.

Одной из ключевых проблем использования технологий виртуализации является легитимность защиты информации, которая обрабатывается в виртуальной среде. Согласно российскому законодательству организации обязаны обеспечить надлежащую защиту конфиденциальной информации, в том числе с применением сертифицированных средств защиты.

Для модернизации вычислительной инфраструктуры таможни предлагается использовать системы аппаратной виртуализации, имеющие следующие преимущества по сравнению с программной:

- упрощение разработки платформ виртуализации за счет предоставления аппаратных интерфейсов управления и поддержки виртуальных гостевых систем;
- возможность увеличения быстродействия платформ виртуализации;
- возможность независимого запуска нескольких виртуальных платформ с возможностью переключения между ними на аппаратном уровне;
- независимость гостевой системы от архитектуры хостовой платформы и реализации платформы виртуализации.

Одним из требований к модернизации вычислительной инфраструктуры является наличие у системы виртуализации сертификата на соответствие руководящим документам:

- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля;
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности.

Следует отметить, что ядра сертифицированных операционных систем (ОС семейства МСВС и ОС специального назначения Astra Linux Specail Edition) собраны без поддержки гипервизора Xen. Это исключает возможность их использования в автоматизированных системах, обрабатывающих информацию ограниченного доступа, и режим паравиртуализации для повышения производительности гостевых операционных систем. Системы виртуализации зарубежной разработки – VMware vSphere, Citrix XenServer и Microsoft Hyper-V – имеют сертификат на соответствие только требованиям технических условий (ТУ) и не могут быть сертифицированы по требованиям руководящих документов российских регуляторов, так как их исходные коды являются закрытыми. Включенные в реестр российского ПО «Р-Виртуализация» и «Скала-Р» обладают высокими техническими характеристиками, но не имеют сертификатов ФСТЭК по требованиям безопасности информации, и, следовательно, не удовлетворяют требованиям руководящих документов. ROSA Virtualization имеет сертификат только на соответствие ТУ и руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля, что также не соответствует требованиям на модернизацию системы.

Программно-аппаратный комплекс «Горизонт-ВС»

Полностью удовлетворяет требованиям Задания на модернизацию инфраструктуры МОТ программно-аппаратный комплекс (ПАК) «Горизонт-ВС» [9], а также программные комплексы «Виртуализации и управления» и ПК «Брест» только при условии установки в ОССН Astra Linux Special Edition релиза «Смоленск». Согласно требованиям, на модернизацию вычислительной инфраструктуры МОТ подсистема виртуализации должна устанавливаться непосредственно на аппаратное обеспечение и не содержать в своем составе ОС общего назначения. Использование гипервизора первого типа снижает расходы на закупку и обслуживание, а также формирует защищенный слой виртуализации между аппаратной платформой и устанавливаемыми гостевыми ОС.

ПАК «Горизонт-ВС» является гипервизором 1-го типа и устанавливается непосредственно на аппаратную платформу. Механизм создания замкнутой программной среды реализован непосредственно в ПАК «Горизонт-ВС», в состав которого входит специализированная сборка ядра Linux, включая модули ядра, на основе которых и реализован механизм создания замкнутой программной среды. Инсталляция и дальнейшая загрузка ПАК «Горизонт-ВС» производятся с USB-накопителя. После инсталляции и настройки системы автоматически генерируется пара «закрытый и открытый ключ», и инициализируется механизм защиты. В процессе инициализации для всех инсталлируемых на жесткий диск файлов ПАК «Горизонт-ВС» системой автоматически подсчитывается с использованием алгоритма SHA-1 контрольная хеш-сумма, которая подписывается сгенерированным закрытым ключом. После этого подписанная хеш-сумма сохраняется в расширенных атрибутах файловой системы для каждого файла в отдельности.

Поскольку хеш-сумма с электронной подписью сохраняется в атрибутах каждого файла, при копировании и переносе файлов в другие директории подписанная хеш-сумма копируется совместно с файлами. Таким образом, изменение пути файла на возможность проверки перемещенных или скопированных файлов не влияет. Вследствие того, что закрытый ключ, которым были подписаны файлы при инсталляции при ее завершении уничтожается, подписать контрольную сумму какого-либо файла после процедуры инсталляции в ходе эксплуатации изделия не представляется возможным. В связи с этим после инсталляции изделия в среде ПАК «Горизонт-ВС»

невозможно выполнить какой-либо файл, не инсталлированный в ходе процедуры начальной установки, либо измененный в процессе эксплуатации.

Проведенный анализ показал, что ПАК «Горизонт-ВС» и ПК «Брест» обладают схожими функциональными возможностями по формированию замкнутой информационно-вычислительной среды. Однако использование механизма замкнутой программной среды в ПАК «Горизонт-ВС» включается при установке изделия и не требует от администратора дополнительных действий по включению механизма создания замкнутой программной среды и генерации ключей для подписи файлов, не являющихся исполнимыми файлами формата ELF (Executable and Linkable Format – формат исполнимых и компонуемых файлов). Таким образом, выбор ПАК «Горизонт-ВС» значительно снижает вероятность ошибки администратора при установке и настройке безопасного функционирования. Кроме того, ПАК «Горизонт-ВС» позволяет избежать дополнительных затрат на системное программное обеспечение, так как он является гипервизором первого типа и устанавливается непосредственно на аппаратную платформу.

Для обеспечения отказоустойчивости может использоваться кластеризация серверов под управлением «Горизонт-ВС» с использованием функции High-Available (HA) кластер высокой доступности. «Горизонт-ВС» также позволяет кластеризировать системы хранения данных серверов, объединив их в общую разделяемую распределенную СХД. На первом этапе модернизации предлагается установить на имеющиеся на постах МОТ ФТС серверы Aquarius Q51 (на каждом посту развернут один сервер) гипервизор «Горизонт-ВС» и развернуть поверх него две ВМ с серверами АИС «Аист-М», а также «Учет товаров на ВХ» и «Оформление ТПО». Это обеспечит возможность переноса из имеющейся морально устаревшей инфраструктуры программное обеспечение таможенной службы на новую аппаратную платформу.

В имеющейся инфраструктуре реализованы функции информационной безопасности на базе ПО «КриптоПро» с использованием USB смарт-карт. ПО «Горизонт-ВС» обеспечивает прозрачный проброс USB-портов сервера в целевые ВМ, что гарантирует корректную работоспособность используемых средств информационной безопасности в виртуальной среде. В гипервизоре «Горизонт-ВС» реализованы функции виртуальной сетевой инфраструктуры, обеспечивается коммутация Ethernet фреймов ВМ и маршрутизация IP-пакетов. Возможно развертывание виртуальных информационных сетей различной конфигурации, разделение виртуальных коммутаторов на отдельные широковещательные (Broadcast) домены с использованием VLAN (стандарт 802.1q). Также возможно объединение Broadcast-доменов с использованием функций маршрутизации, что позволяет создавать в рамках одного гипервизора виртуальные сетевые структуры различных конфигураций. Виртуальные сети могут быть скоммутированы с физическими внешними сетями передачи данных с использованием физических сетевых (Ethernet) интерфейсов сервера. Средствами «Горизонт-ВС» поддерживаются функции агрегации сетевых каналов связи, что обеспечивает максимальную производительность и отказоустойчивость соединений между виртуальной и физической средой передачи данных.

Этапы модернизации вычислительных структур МОТ

Автоматизацию распределенных территориально систем предлагается провести **в два этапа**. При этом **на первом этапе** модернизации не реализуются функции отказоустойчивости информационных систем при выходе из строя серверов инфраструктуры. Существующие каналы связи между постами не позволяют организовать НА-кластер между серверами этих постов. **На втором этапе** модернизации предлагается оснастить каждый пост двумя дополнительными серверами с установленным гипервизором «Горизонт-ВС» с функциями РСХД и организовать отказоустойчивый кластер с общей разделяемой системой хранения данных на базе локальных дисковых подсистем серверов – участников кластера. Это обеспечит непрерывную работу программного обеспечения серверов и рабочих станций таможенных постов при полном выходе из строя произвольного сервера кластера, либо его отдельных компонентов (дисков HDD, сетевых интерфейсов и т. д.). Отказоустойчивость достигается за счет использования функций НА-кластера «Горизонт-ВС» и функций обеспечения отказоустойчивости РСХД на базе ПО «Горизонт-ВС».

Дополнительные серверы кластера должны быть сопоставимы по основным техническим характеристикам с имеющимся сервером. Каждый сервер кластера должен быть оснащен минимум двумя 10G Ethernet-интерфейсами. Для коммутации серверов между собой должен быть использован 10G Ethernet-коммутатор с функциями агрегации каналов связи. Предлагается перевести все рабочие места пользователей таможенного поста в инфраструктуру VDI (около 48 рабочих мест на пост). Такое решение обладает высокими характеристиками надежности и отказоустойчивости, однако требует серьезных капиталовложений: закупки двух дополнительных серверов на каждый таможенный пост. В связи с этим предлагается архитектура, позволяющая обеспечить отказоустойчивость вычислительной инфраструктуры при условии закупки одного дополнительного сервера. Структурная схема серверной архитектуры типового таможенного поста приведена на рис. 1.

В данной архитектуре предполагается, что два сервера виртуализации, которыми оснащается таможенный

пост, имеют закрепленное за каждым из них определенное функциональное назначение. На одном из них (сервер № 1, рис. 1) в виртуальной среде размещаются серверы приложений ПО таможенного поста («Учет товаров на ВХ», «Оформление ТПО», АИС «Аист-М» и др.), на другом (сервер № 2, рис. 1) – виртуальные машины пользователей VDI данного поста.

На хранилищах «Горизонт-ВС» все диски серверов № 1, 2 (C:/, D:/, F:/) (физические и логические тома) представляют собой файлы (и/или разделы). В свою очередь, хранилища «Горизонт-ВС» разделяются на реплицируемую и нереплицируемую области. Между серверами организуется канал синхронной репликации средствами «Горизонт-ВС». На нереплицируемой области хранилища сервера виртуализации 1 располагаются системные диски серверов № 1, 2 (C:/), другие диски серверов с неизменяемым ПО и данными, а также системные диски ВМ VDI (системные диски ВМ VDI на сервере виртуализации 1 являются актуальными копиями системных дисков ВМ VDI с сервера виртуализации 2. До аварийного переключения эти диски не используются, чтение и запись на них не производятся). На реплицируемой области хранилища серверов виртуализации 1, 2 располагаются диски с изменяемыми данными (редактируемые документы, БД, переносимые профили пользователей и другие файловые информационные объекты, которые изменяются в ходе работы и имеют практическую ценность).

На реплицируемой области хранилища сервера виртуализации 2 располагаются системные диски (C:/), другие диски с неизменяемым ПО и данными ВМ VDI, а также системные диски (C:/) и другие диски с неизменяемым ПО и данными серверов № 1, 2 (системные диски серверов № 1, 2 на сервере виртуализации 2 являются актуальными копиями системных дисков серверов № 1, 2 с сервера виртуализации 1; до аварийного переключения эти диски не используются, чтение и запись на них не производятся).

Профили пользователей Windows ВМ VDI в предлагаемой архитектуре должны быть настроены в Active Directory как переносимые профили (roaming profile) и располагаться на диске F:/ сервера № 2. Для управления

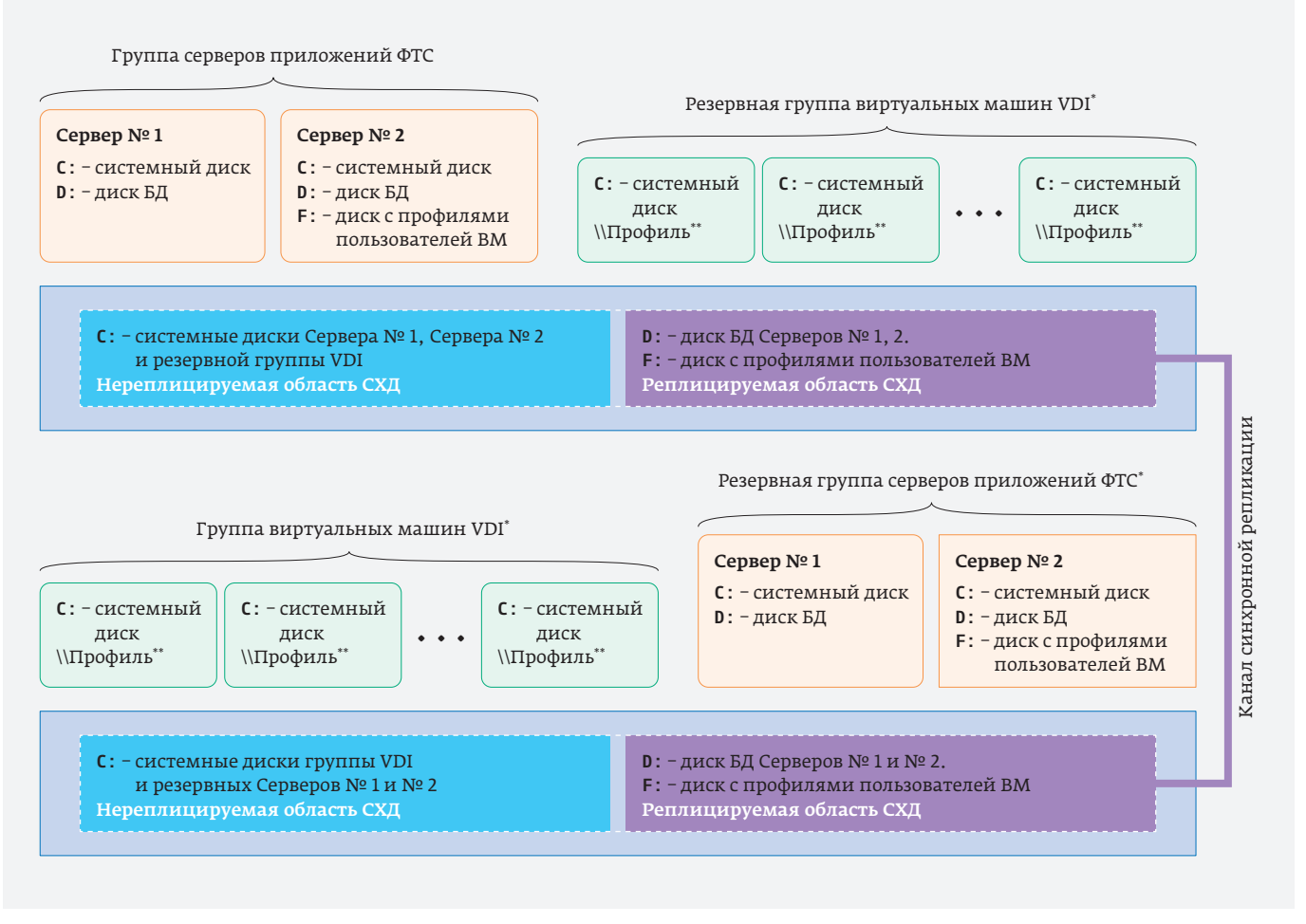

Рис. 1. Схема серверного узла типового таможенного поста

распределенными ресурсами кластера в изделии используются средства менеджера ресурсов.

При выходе из строя одного из серверов виртуализации средствами кластеризации «Горизонт-ВС» обеспечивается включение ВМ вышедшего из строя сервера на работающем сервере (например, при выходе из строя сервера виртуализации 1 серверы № 1 и 2 перезапустятся на сервере виртуализации 2). При этом может наблюдаться общее снижение производительности системы, но работоспособность ВМ VDI и серверов № 1 и 2 сохранится в полном объеме. Поскольку данные, располагающиеся на общем реплицируемом хранилище, всегда находятся в актуальном и консистентном состоянии, при аварийном переключении серверов виртуализации потери данных не произойдет.

Согласно плану модернизации системы, на каждом таможенном посту МОТ должна быть установлена платформа виртуализации «Горизонт-ВС» с последующим подключением к центральному офису МОТ (рис. 2). На каждом таможенном посту МОТ на сервере Aquarius T51 D27 устанавливается защищенная платформа виртуализации «Горизонт-ВС» в следующей конфигурации:

- дисковая подсистема: все SSD-диски объединены в массив, на каждом созданы два логических раздела с файловой системой ext4. Первый раздел содержит системные и конфигурационные файлы гипервизора «Горизонт-ВС». Второй раздел назначен в качестве быстрого хранилища для виртуальных машин, или их отдельных дисков. Шпиндельные диски объединены в массив. Этот раздел используется в качестве медленного хранилища дисков ВМ;
- конфигурация сетевой подсистемы: внутри каждого гипервизора «Горизонт-ВС» настраивается виртуальный маршрутизатор Open vSwitch с подключенным внешним (физическим) и внутренним (виртуальным) портами.

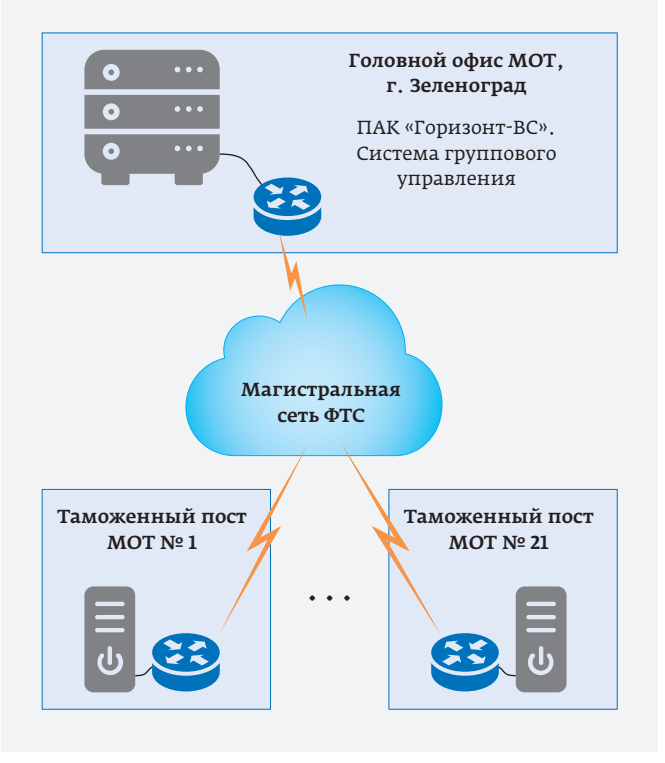

Рис. 2. Схема организации инфраструктуры

Сетевая структура МОТ является маршрутизируемой и имеет узкое место в виде слабых каналов связи со скоростью передачи 10–50 Мбит/с от таможенных постов до центрального управления МОТ. Все серверы с установленным ПАК «Горизонт-ВС» при помощи маршрутизируемых сетей имеют связь с центральным сервером в г. Зеленоград. В центральном управлении МОТ установлен ПАК «Горизонт-ВС» с добавленной ролью администратора и развернутой системой группового управления (СГУ). В СГУ добавлены серверы с установленной платформой виртуализации «Горизонт-ВС» для каждого таможенного поста. Взаимодействие между СГУ и гипервизорами осуществляется по протоколу TCP/IP с указанием IP-адресов или DNS-имен серверов. Запущен постоянный мониторинг состояния гипервизоров.

Стандартная конфигурация подразумевает добавление всех серверов в один логический кластер и использование одного общего хранилища. Однако данная конфигурация в сетевой инфраструктуре МОТ не реализуема, так как каналы связи между сервером с СГУ в головном офисе и серверами виртуализации на таможенных постах обладают низкой пропускной способностью. С целью получения возможности централизованного мониторинга и управления виртуальной инфраструктурой создается следующая конфигурация (рис. 3).

В системе создается 32 логических кластера по именам постов, каждый из которых содержит в себе:

- сервер таможенного поста (с установленным «Горизонт-ВС»);
- описание сетевых параметров (виртуальная сеть) для таможенного поста, с уникальными MAC адресами во всей сети МОТ;
- локальное системное хранилище гипервизора на SSD-дисках;
- локальное хранилище образов (дисков) гипервизора на шпиндельных дисках;
- локальная группа пользователей и пользователи таможенного поста.

Подобное решение обеспечивает:

- централизованный мониторинг и управление системой виртуализации;
- ограничивает возможность ошибок при использовании и администрировании;

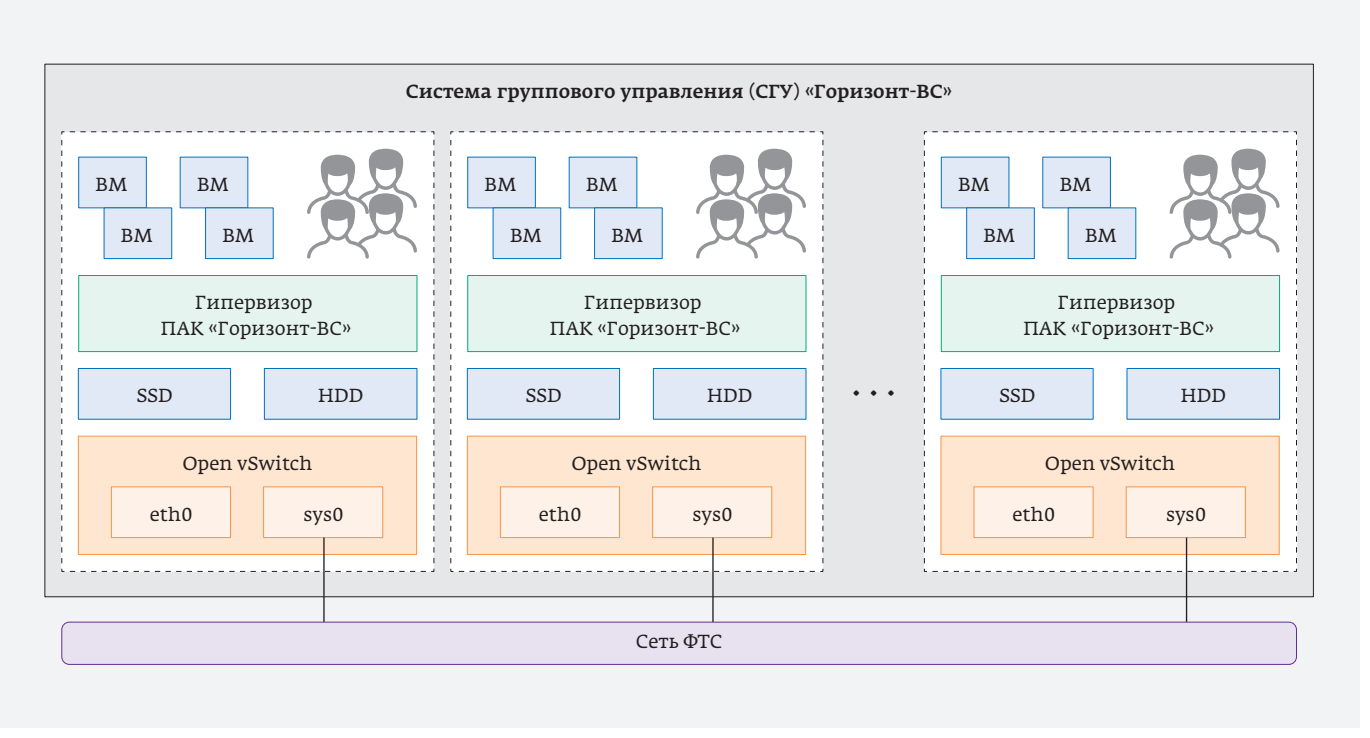

Рис. 3. Конфигурация централизованного управления

- запрещает миграцию дисков и виртуальных машин между постами по медленным каналам связи;
- изолирует ресурсы кластера (сети, гипервизоры, хранилища, группы пользователей);
- позволяет использовать индивидуальные параметры и правила доступа пользователей на каждом посту.

Кроме серверной виртуализации реализуется инфраструктура виртуальных рабочих столов (VDI), что потребует модификации части программного обеспечения СГУ. В стандартной схеме все коммуникации подразумевают использование центрального сервера с СГУ. В условиях МОТ это приведет к коллизиям во время сессии удаленного рабочего стола, увеличению времени отклика и повышенной утилизации пропускной способности каналов. Каждый гипервизор системы содержит настроенный и запущенный брокер подключений. Сведения о локальных брокерах подключений (порт и сетевой адрес) содержатся в СГУ. Тонкие клиенты получают параметры доступа и маршруты от СГУ в центральном офисе. Соединение с ВМ происходит в соответствии с полученным маршрутом через локальный брокер поста (рис. 4).

При отсутствии связи с центральным офисом сотрудники таможенного поста посредством тонких клиентов могут осуществлять подключение к ВМ, запущенным на локальном гипервизоре поста, используя местный сегмент локальной вычислительной сети. При первом обращении к брокеру подключений СГУ (в центральном офисе) полученные данные об авторизации в хэшированном виде сохраняются в локальном брокере подключений поста. Если соединение с СГУ будет отсутствовать, то тонкий клиент запустится с параметрами, хранящимися локально. В качестве аппаратного обеспечения тонких клиентов используются существующие рабочие места, загрузка осуществляется с использованием внешнего накопителя. Существующие данные на рабочем месте остаются на локальных дисках и при необходимости могут быть получены.

Для каждого тонкого клиента подготовлен «золотой» образ рабочего места, соответствующий требованиями к рабочим местам МОТ. Из «золотого» образа созданы ВМ для использования в среде VDI. В соответствии с принятой в МОТ политикой безопасности в СГУ созданы учетные записи сотрудников, а также сконфигурированы индивидуальные права доступа. На каждую ВМ назначены права доступа.

Отказоустойчивость СГУ достигнута путем использования floating IP и запуска нескольких экземпляров СГУ на разных серверах центрального подразделения МОТ. В случае аварии управление переходит к другому экземпляру СГУ, при этом сетевой адрес остается неизменным и «переезжает» к выбранному системой экземпляру. Восстановление происходит автоматически и не требует участия администратора.

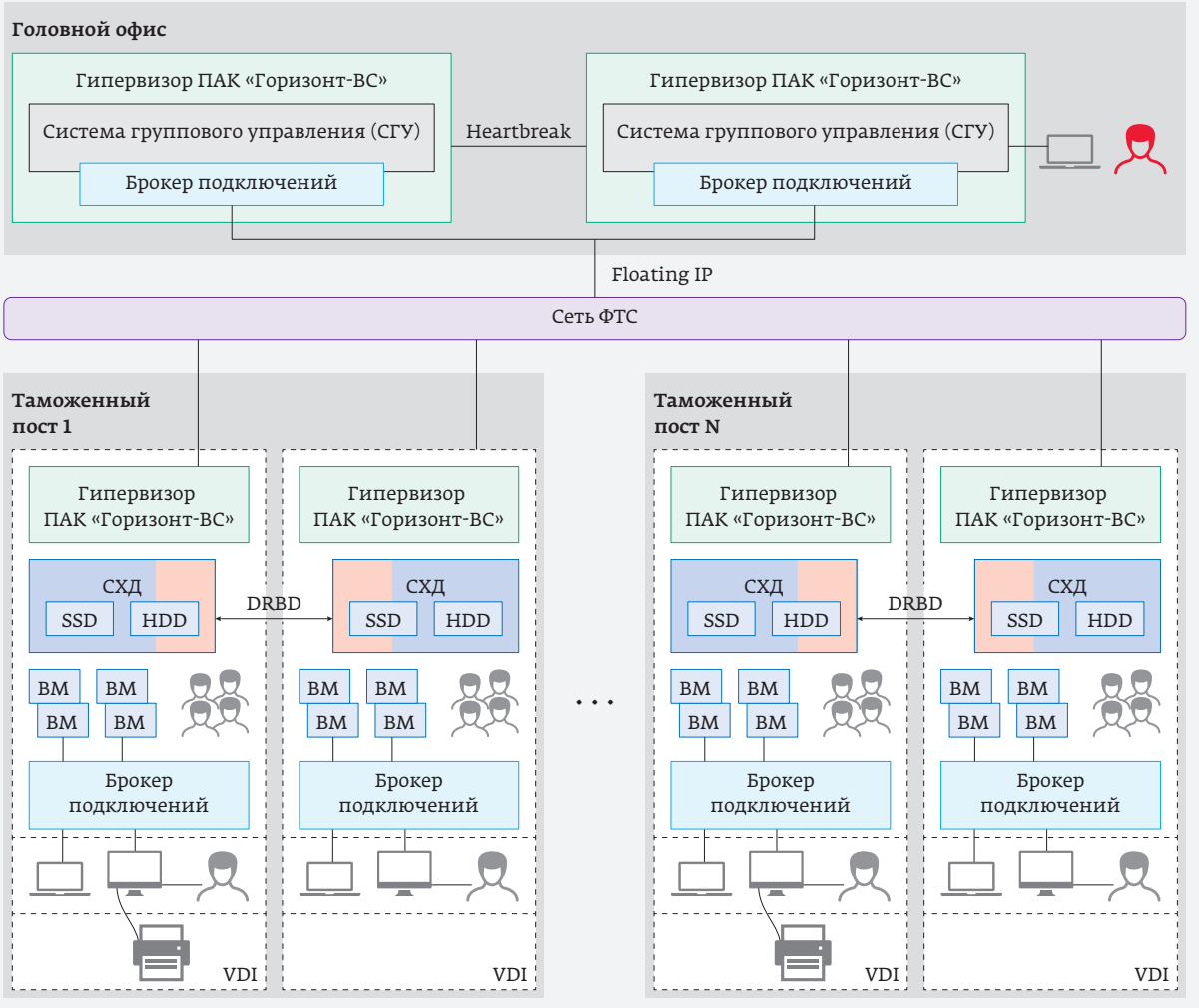

Рис. 4. Схема виртуальных рабочих столов

❊ ❊ ❊

В результате внедрения платформы виртуализации «Горизонт-ВС» ожидается достижение следующих преимуществ в работе московской областной таможни:

- обеспечение функций централизованного администрирования гостевых ОС с использованием единого веб-интерфейса управления;
- общее повышение надежности и отказоустойчивости системы за счет резервирования в облаке «Горизонт-ВС»;
- повышение безопасности функционирования программных приложений, так как «Горизонт-ВС» является сертифицированным средством защиты информации отечественного производства;
- увеличение скорости исполнения программных приложений за счет использования встроенных функций «Горизонт-ВС», обеспечивающих использование быстрых SSD-дисков в качестве кэша для более медленных HDD-дисков серверов с адаптацией к виртуальной среде;
- повышение контроля над производительностью системы с целью упреждающего выявления аномальной активности, в том числе связанной с действием вредоносного ПО;
- получение возможности последующего создания единой системы мониторинга и управления ресурсами.

В перспективе имеется возможность перевода коммуникационных серверов на виртуальную инфраструктуру с созданием единой системы управления как вычислительной инфраструктурой, так и коммуникационной с использованием единой облачной системы управления и возможность переноса в облачную среду централизованных баз данных, что позволит обеспечить отказоустойчивость системы за счет создания кластерной архитектуры и обеспечить управление как централизованными

ресурсами, так и ресурсами таможенных постов с использованием единой системы управления.

ЛИТЕРАТУРА

1. **Черняк Л.** Время конвергентных инфраструктур // Открытые системы. СУБД. 2012. № 4. https://www.osp.ru/os/2012/04/13015754/
2. PureFlex™ System. https://www.ibm.com/ibm/puresystems/ru/ru/pf_pureflex.html.
3. Dsvolk Oracle News. IBM PureSystems. http://dsvolk.blogspot.com/2012/04/ibm-puresystems.html.
4. **Самойленко А.** Решение VMware EVO: RAIL – строительный блок для конвергентной инфраструктуры. https://www.vmgu.ru/press/vmware-evo-rail-appliance.
5. **Ганьжа Д.** Гиперконвергенция: ИТ-инфраструктура на раз, два, три // Журнал сетевых решений/LAN. 2016. № 5. https://www.osp.ru/lan/2016/05/13049349/.
6. Исследование TAdviser: Перспективы российского рынка гиперконвергентной инфраструктуры. http://www.tadviser.ru/index.php/.
7. **Носов Н.** Гиперконвергентная инфраструктура как сервис. http://www.iksmedia.ru/articles/5501575-Giperkonvergentnaya-infrastruktura.html.
8. Что такое «облако в bare metal»? // https://www.xelent.ru/blog/chto-takoe-oblako-v-bare-metal/
9. **Коптелов И., Назаров С., Ермолова М.** Отечественная защищенная платформа виртуализации «Горизонт-ВС» // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2018. № 9. С. 84–90.