УДК 004.75

О возможности внедрения технологии облачных вычислений в ведомственных (корпоративных) распределенных автоматизированных информационных системах

© В.С. Заборовский[1], А.А. Лукашин[2], В.Ю. Скиба[3]

[1] Санкт-Петербургский политехнический университет, Санкт-Петербург, 195251, Россия
[2] ЦНИИ Робототехники и технической кибернетики, Санкт-Петербург, 194064, Россия
[3] МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Несмотря на все преимущества технологии облачных вычислений, в ведомственных (корпоративных) распределенных автоматизированных информационных системах (РАИС) она практически не используется. Рассмотрен один из подходов к внедрению технологии облачных вычислений в ведомственные (корпоративные) РАИС, позволяющий достичь требуемого уровня обеспечения безопасности информации.

Ключевые слова: *облачные вычисления, распределенные автоматизированные информационные системы, защита информации, межсетевые экраны.*

Современные вычислительные технологии, основанные на виртуализации и сетецентрическом взаимодействии, получили название «облачные вычисления» (ОВ).

Несмотря на многочисленные предложения как технических, так и программных средств, ОВ в настоящее время практически не применяются в различных ведомствах или в крупных корпорациях, в которых созданы свои собственные ведомственные (корпоративные) распределенные автоматизированные информационные системы (РАИС).

Ведомственные (корпоративные) РАИС, как правило, объединяют в единый контур большое число разнородных территориально распределенных объектов и включают разнообразные средства вычислительной техники, различное телекоммуникационное оборудование, общесистемное и прикладное программное обеспечение [0].

Внедрение в таких РАИС технологий ОВ в полном объеме сдерживает наличие:

собственных центров обработки данных на региональном или территориальном уровне;

собственной ведомственной (корпоративной) информационно-телекоммуникационной сети, объединяющей все центры обработки данных и локальные сети головных, региональных и территориальных офисов, филиалов и подразделений;

заказного специализированного программного обеспечения;

требований по защите информации (по обеспечению информационной безопасности);

региональных и территориальных подразделений по информационным технологиям.

Рассмотрим один из подходов к внедрению технологии ОВ в ведомственные (корпоративные) РАИС, позволяющий достичь требуемого уровня обеспечения безопасности информации.

Применение технологии ОВ позволяет создавать надежные и масштабируемые информационные системы, реализующие информационные сервисы различных классов. Среда облачных вычислений включает не только средства виртуализации вычислительных ресурсов, но и систему централизованного управления этими ресурсами и информационными сервисами, которые данные ресурсы используют (рис. 1).

Рис. 1. Компоненты облачной инфраструктуры

Применение облачных вычислений для развития автоматизированных информационных систем обладает следующими преимуществами по сравнению с существующими решениями на базе сетевых технологий класса «клиент — сервер».

- Автоматизация процессов конфигурации ресурсов. Пользователь среды ОВ имеет возможность самостоятельно обеспечить себя вычислительными ресурсами, такими как серверы или сетевое хранилище.
- Доступ по сети. Сервис предоставляется по сети передачи данных и доступен пользователю с помощью различных платформ — мобильных устройств, персональных компьютеров, рабочих станций и пр.
- Разделяемые ресурсы. Вычислительные ресурсы среды ОВ разделяются между различными потребителями и предоставляются с помощью модели «аренды» физических и виртуализованных сервисов.
- Масштабируемость. Среда ОВ эффективно масштабируема. Для потребителя среда ОВ выглядит как набор ресурсов, которые можно использовать исходя из текущих потребностей в удобное для этого время.
- Сбалансированность. Среда ОВ контролирует и оптимизирует расход ресурсов. Примером балансировки нагрузки может служить миграция виртуальных машин между вычислительными узлами или передача потоков данных сразу с нескольких серверов распределенного хранилища.

Переход к модели ОВ может быть весьма перспективным решением, позволяющим повысить надежность и эффективность работы не только небольших предприятий и организаций, но и больших корпораций и ведомств (рис. 2).

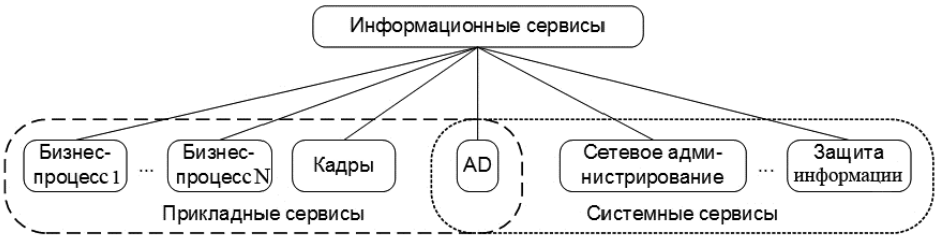

Рис. 2. Сервисы информационной системы

Развитие ведомственных (корпоративных) РАИС на базе среды ОВ может дать следующие преимущества с точки зрения технологии реализации сервисов.

- Переход к технологии виртуализации ресурсов позволит всем сервисам функционировать в единой среде выполнения, что упрощает управление работой и настройкой РАИС в целом.
- Горизонтальное масштабирование ресурсов или включение нового виртуального сервера без остановки других приложений.
- Создание единого центра управления и его резервного образа, повышающего надежность функционирования РАИС.
- Возможность использования единой системы мониторинга как серверов, так и виртуальных машин, на которых функционируют сервисы предприятия, организации или ведомства.
- Сокращение затрат на обслуживание вычислительного парка серверов предприятия, организации или ведомства.
- Снижение расходов на электроэнергию за счет распределения виртуальных машин по узлам виртуализации. Незадействованные серверы могут быть выключены или находиться в состоянии ожидания до момента, когда потребуются их вычислительные мощности.
- Облегчение администрирования виртуальных серверов за счет использования единых программных платформ виртуальных машин и единого механизма обновлений.
- Возможность автоматического запуска копии виртуальной машины с информационными сервисами предприятия, организации или ведомства в случае аварии на функционирующей виртуальной машине или повышенной нагрузки на информационный сервис.
- Возможность «сохранения» состояния виртуального сервиса, например, перед внесением изменений в конфигурацию приложений или установкой новой версии программного обеспечения.
- Перемещение виртуальных серверов на другие вычислительные узлы виртуализации без времени простоя, что обеспечивает возможность проведения сервисных работ с оборудованием без потерь для пользователей информационных сервисов.
- Обеспечение гибких механизмов защиты информации за счет интеграции средств защиты с программными сервисами среды облачных вычислений.

Переход к облачной инфраструктуре в РАИС стал возможным благодаря высокому качеству существующих каналов передачи данных. Он позволит снизить расходы на управление серверной инфраструктурой региональных и территориальных филиалов и подразделений.

Концепция интеграции облачных технологий в вычислительную инфраструктуру представлена в виде метода интеграции и применяемой технологии. Методом является виртуализация вычислительных ресурсов без радикального изменения аппаратной платформы [0]. Технология интеграции — сетецентрические средства управления и защиты виртуализованных ресурсов в рамках выделенных зон с данной политикой безопасности [0].

У вычислительной инфраструктуры любой уже работающей РАИС есть сложившийся парк серверов и программных сервисов. Целью внедрения среды облачных вычислений является не замена существующей программной или аппаратной платформы РАИС, а дополнение и усовершенствование существующей инфраструктуры за счет построения сервисов управления вычислительными ресурсами и интеграции облачных технологий в информационные процессы таможни. Такой подход позволит снизить зависимость от аппаратной платформы, оптимизировать использование существующих информационных систем и повысить защищенность программных сервисов.

В настоящее время уже существует эффективный и надежный опыт переноса информационных сервисов в виртуальную инфраструктуру. Однако возможности технологий виртуализации шире достигнутых результатов, поэтому перспективным направлением развития является включение виртуальных средств в единую среду управления.

Допустим, что часть сервисов РАИС уже перенесена в виртуальную инфраструктуру, построенную с использованием технологий *VMware*, в частности, с использованием гипервизоров *VMware ESX*. Задачи проекта интеграции облачной платформы — построение системы управления существующими виртуализованными информационными ресурсами РАИС, создание шаблонов виртуальных машин и унификации программной платформы. При необходимости расширения функциональности и разработки специализированных решений могут быть использованы гипервизоры других типов, в том числе *XEN, XEN Cloud Platform, KVM,* что позволит снизить совокупную стоимость владения и обеспечить надежную систему управления виртуальными ресурсами.

Предлагаемая облачная система может быть развернута с использованием аппаратных платформ и программных сервисов производителей серверных решений, в том числе *Hewlett Packard*, *IBM*, *SuperMicro*, без необходимости поставки дополнительного парка серверов. Такой подход позволяет снизить стоимость интеграции новых технологий в инфраструктуру РАИС.

В процессе интеграции могут быть реализованы различные варианты технологий мониторинга и управления, позволяющие интегрировать с существующими в инфраструктуре РАИС решениями, в том числе на базе *OpenView*. В частности, возможен одновременный мониторинг программных и аппаратных компонент РАИС с помощью сервисов облачной среды и *OpenView* как в виртуальном, так и в аппаратном окружении.

Программные и аппаратные средства защиты информации, поставляемые в рамках проекта, могут быть применены как в виртуализованных сегментах, так и в программных компонентах, развернутых на аппаратных решениях без использования технологий виртуализации. Существуют отечественные межсетевые экраны серии ССПТ, разрабатываемые НПО РТК, которые прозрачно интегрируются в системы виртуализации и классические вычислительные сети. Благодаря использованию единой системы защиты появляется возможность использования единого сервиса управления политикой доступа, что облегчает администрирование системы защиты и снижает ее стоимость.

Рассмотрим *концептуальные аспекты внедрения облачных технологий.* Как правило, ведомственная (корпоративная) РАИС обладает сложной структурой и большим набором функций, для реализации которых используются гетерогенные вычислительные ресурсы. Для повышения надежности, масштабируемости и защищенности предоставляемых сервисов в рамках существующей инфраструктуры РАИС может быть создана защищенная среда ОВ, на виртуальных машинах которой развернуты ее программные компоненты сервисов.

В общем случае в состав среды ОВ входят:

1) аппаратная платформа. Среда ОВ может быть развернута как на существующих вычислительных ресурсах, что обеспечивает плавный переход к облачной инфраструктуре, так и на аппаратной платформе вновь создаваемого центра обработки данных (ЦОД);

2) средства виртуализации. В качестве технологии виртуализации может быть обеспечена поддержка следующих типов гипервизоров:

VMWare ESX(i);

KVM (kernel virtual machine);

XEN;

XEN Cloud platform;

3) средства управления и мониторинга. Средства мониторинга предназначены для наблюдения за состоянием и сигнализации о нештатных событиях в аппаратно-программном облачном комплексе. Средствами управления служат программные сервисы, обеспечивающие управление виртуальными машинами с использованием концепции облачных вычислений. Наиболее перспективна платформа *OpenStack* — разработка мирового уровня с участием отечественных и зарубежных специалистов. Данная система обеспечит:

управление жизненным циклом виртуальных машин;

хранилище с программными сервисами ФТС;

единый интерфейс доступа к распределенному хранилищу данных;

программный, командный и графический интерфейсы доступа к управлению виртуальными машинами;

4) система хранения данных. Она предназначена для размещения и надежного хранения пользовательских данных. Данный программный компонент является сервисом среды облачных вычислений, построенным на платформе *OpenStack Swift*. Сервис хранения обеспечивает надежное хранение данных, копии которых находятся на разных серверах системы. Также сервис обеспечивает программный интерфейс REST для доступа к данным;

5) сервис защиты. Он предназначен для обеспечения функций разграничения доступа к информационным сервисам, функционирующим в виртуальной среде, и представляет собой совокупность элементов:

подсистемы межсетевого экранирования (на базе МСЭ серии ССПТ);

сервиса управления доступом;

подсистемы криптографической защиты каналов передачи данных (например, на базе КШ Континент).

Как происходит *защита информации* при использовании облачных технологий?

Основным элементом при реализации РАИС на базе технологии ОВ является подсистема межсетевого экранирования (рис. 3). Она обеспечивает многоуровневую защиту, включающую:

уровень защиты сервиса;

уровень защиты среды облачных вычислений;

уровень защиты сегмента РАИС.

Уровень защиты сервиса обеспечивается межсетевым экраном, функционирующим в среде облачных вычислений, т. е.запущенным в виде виртуальной машины в гипервизоре каждой физической машины ЦОД. Защита уровня сервиса обеспечивает контроль доступа на уровне пользователя и работает в совокупности с системой авторизации РАИС (доменная структура), персональными межсетевыми экранами, установленными на автоматизированных рабочих местах пользователей. Межсетевые экраны уровня сервиса могут быть доработаны в соответствии с требованиями протокола сетевого взаимодействия конкретного сервиса, т. е.могут обеспечивать фильтрацию специализированных протоколов.

Уровень защиты среды облачных вычислений обеспечивается кластером аппаратных межсетевых экранов, включенных в режиме горячего резервирования, и предназначен для контроля доступа в виртуальную среду на основании списков контроля доступа, содержащих адресную информацию [0]. Актуализация списков может проводиться как в ручном, так и в автоматизированном режимах.

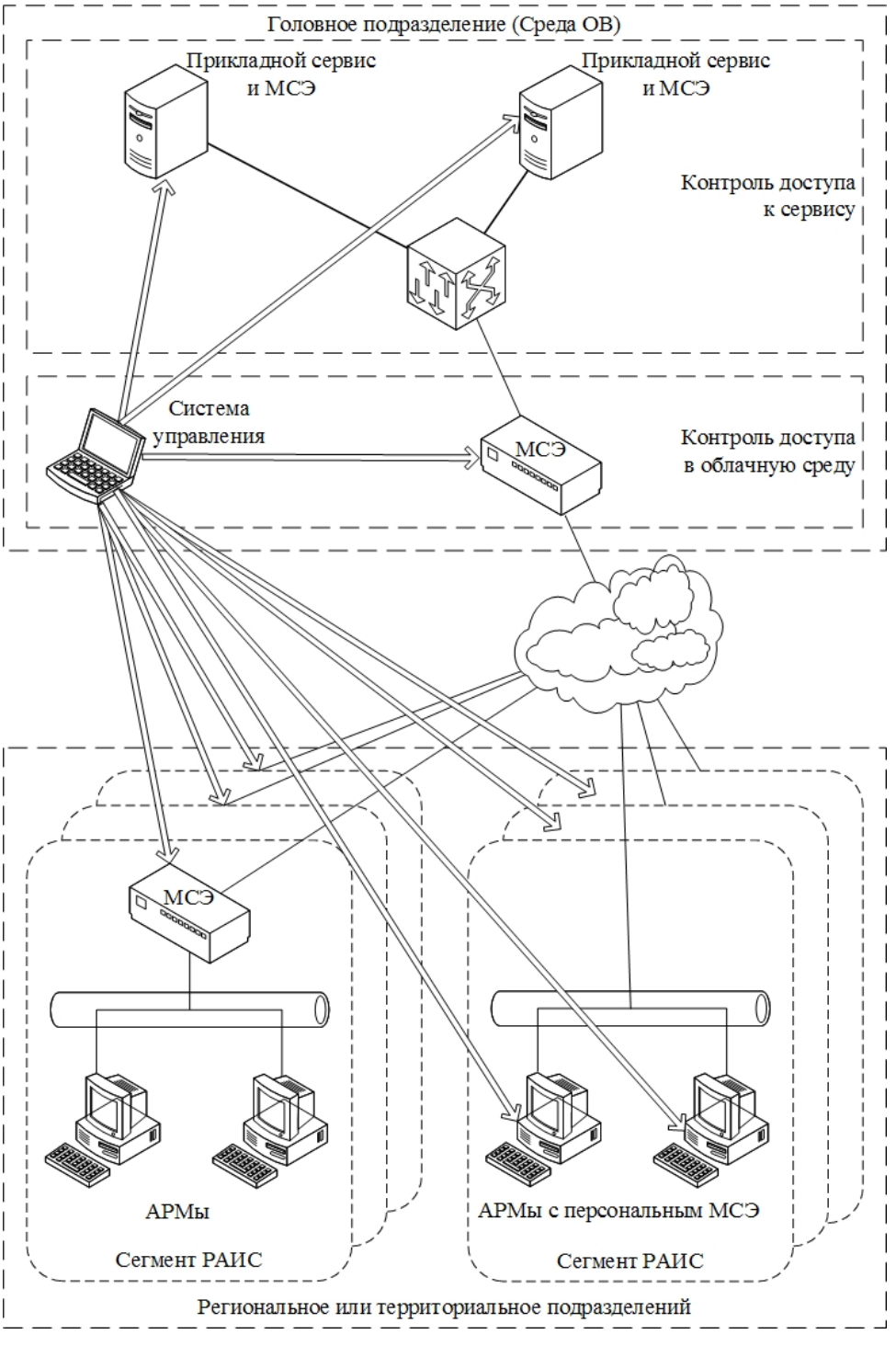

Рис. 3. Защита информации в РАИС на базе технологии ОВ

Уровень защиты сегмента РАИС обеспечивается аппаратными или персональными межсетевыми экранами. В зависимости от структуры сети, требований к надежности возможно использование кластера повышенной надежности, отдельно установленных аппаратных межсетевых экранов, персональных межсетевых экранов, установленных на автоматизированных рабочих местах пользователей. Уровень защиты сегмента РАИС позволяет сегментировать существующую сеть с целью уменьшения аттестуемого сегмента.

Управление подсистемой межсетевого экранирования обеспечивается за счет единого центра управления, который, в том числе, решает следующие задачи:

генерация правил фильтрации и их загрузка в межсетевые экраны;

мониторинг работоспособности и сигнализация о возникновении инцидентов.

Более детально сетецентрический подход к контролю доступа в среде облачных вычислений, модель осуществления контроля с помощью оценки функции риска, а также методы реализации сетецентрической модели в среде ОВ, использующие группировку виртуальных межсетевых экранов, интегрированных в средства виртуализации, и управляемые с помощью сервиса политики безопасности, рассмотрены в работах В.С. Заборовского и А.А. Лукашина [0, 0].

Таким образом, ОВ могут применяться и в ведомственных (корпоративных) РАИС, в которых предъявляются усиленные требования по защищенности информации. Это позволит существенно сэкономить ресурсы, необходимые для обеспечения функционирования РАИС. При этом можно говорить о гибком перераспределении ресурсов и кадров между центральными, региональными и территориальными подразделениями ведомства (корпорации). Реализация ведомственных (корпоративных) РАИС с использованием технологий ОВ позволит обеспечить централизованное управление процессами обеспечения безопасности распределенной обработки информации и необходимый уровень контроля доступа к физическим ресурсам РАИС одновременно с максимально эффективным использованием физических, вычислительных, информационных и логических ресурсов РАИС, что в конечном счете приведет к снижению совокупной стоимости создания, развития и функционирования РАИС.

В этом случае структурно-функциональная схема ведомственной (корпоративной) РАИС по-прежнему будет частным случаем структурно-функциональной схемы РАИС, предложенной В.Ю. Скибой [0], в которой все функциональные подсистемы будут иметь централизованные информационные ресурсы.

ЛИТЕРАТУРА

[1] Скиба В.Ю. Структурно-функциональная схема распределенной АИС в защищенном исполнении. *Вопросы защиты информации*, 2009, № 3(86), с. 35–38.

[2] Заборовский В.С., Лукашин А.А., Купреенко С.В., Мулюха В.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений. *Вестник Уфимского авиационного технического университета. Управление, вычислительная техника и информатика*, 2011, № 5 (45).

[3] Заборовский В.С., Лукашин А.А. Сетецентрическая модель и методы контроля доступа к информационным ресурсам в среде облачных вычислений. *Научно-технические ведомости СПбГПУ. Информатика, телекоммуникации, управление*, 2012, № 2 (145), с. 91–95.

[4] Заборовский В.С., Лукашин А.А. Система контроля доступа в среде облачных вычислений. *Научно-технические ведомости СПбГПУ. Информатика, телекоммуникации, управление*, 2012, № 4 (152), с. 7–12.

Статья поступила в редакцию 26.07.2013

Ссылку на эту статью просим оформлять следующим образом:

Заборовский В.С., Лукашин А.А., Скиба В.Ю. О возможности внедрения технологии облачных вычислений в ведомственных (корпоративных) распределенных автоматизированных информационных системах. *Инженерный журнал: наука и инновации*, *2013, вып. 3*. URL: http://engjournal.ru/catalog/it/network/652.html

Заборовский Владимир Сергеевич — заведующий кафедрой «Телематика» Санкт-Петербургского политехнического университета, д-р техн. наук. Автор более 100 научных работ в области телематики и информационной безопасности. e-mail: vlad@neva.ru

Лукашин Алексей Андреевич — научный сотрудник ЦНИИ Робототехники и технической кибернетики, кандидат технических наук. Автор более 10 научных работ в области сетевых технологий, контроля доступа и защиты информации.
e-mail: lukash@neva.ru

Скиба Владимир Юрьевич — д-р техн. наук, профессор кафедры предпринимательства и внешнеэкономической деятельности МГТУ им. Н.Э. Баумана. Автор свыше 100 научных работ, в том числе 2 монографий и 3 учебных пособий в области разработки систем защиты информации и информационной безопасности предприятий и организаций. e-mail: skiba@eecommission.org