Т. А. Митюшкина, Ю. М. Туманов

МОДЕЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВЫПОЛНЯЕМОГО НА СРЕДСТВЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ВХОДЯЩЕМ В СОСТАВ ГРИД-СЕТИ

На данный момент не существует единой методики развертывания сред облачных вычислений (ОВ). Однако можно выделить три подхода к построению сред ОВ: использование мэйнфреймов в качестве основы для облачных вычислений, применение предварительно собранной и протестированной инфраструктуры для частных ОВ и использование кластерных технологий [1].

Каждый из подходов предполагает концентрацию большого количества вычислительных ресурсов на стороне поставщика услуг ОВ, что влечет за собой ограничения в наращивании вычислительных мощностей. В связи с этим поставлена задача рассмотреть возможные способы развертывания сред облачных вычислений с применением нового подхода, сохранив при этом преимущества, характерные для существующих решений, такие как доступность, эластичность, экономичность и масштабируемость.

На основании проведенного анализа существующих решений в области построения сред ОВ был сделан вывод о возможности и целесообразности их развертывания с использованием технологии Грид-сетей. Такая реализация позволит пользователям Грид-сети, имея гетерогенные СВТ, предоставлять часть ресурсов для выполнения вычислительных заданий, которыми являются процессы, выполняемые в средах ОВ. Число задействованных СВТ в идеальном случае ограничено лишь их количеством на планете, вследствие чего возникает возможность практически бесконечного наращивания вычислительных мощностей.

Однако современные реализации Грид-сетей направлены на решение строго определенных задач. Для выполнения же произвольных заданий предлагается использовать технологию «толстого клиента», которая позволит объединить несколько физических вычислительных узлов в один логический, вычислительные ресурсы которого будут использованы для выполнения заданий.

В настоящее время к услугам ОВ обращается все большее количество пользователей. Причин этому много, основные — удобство использования и доступность данных из любой точки мира. Несмотря на растущую популярность ОВ, по-прежнему мало внимания уделяется вопросам безопасности. Технология облачных вычислений предполагает концентрацию большого объема данных в едином пространстве, что в случае успешной атаки нарушителя может повлечь компрометацию всей информации. Таким образом, на плечи поставщиков услуг ОВ ложится не только ответственность за предоставление бесперебойного доступа к услугам, но и защита пользовательских данных, размещенных на удаленных серверах [2].

Общая схема работы предлагаемого подхода к развертыванию сред ОВ с применением Грид-сети

Управляющей частью разрабатываемой среды ОВ является координатор ОВ. Он выполняет функции поиска и выделения ресурсов, распределения заданий между вычислительными узлами и обработки результатов выполнения заданий.

Вычислительным узлом является СВТ пользователя, на котором установлено ПО, состоящее из клиента Грид-сети и клиента ОВ. В функции клиента ОВ входит предоставление ресурсов среде ОВ, обеспечение целостности и конфиденциальности обработки данных при выполнении задания. Клиент Грид-сети (клиент ГС) осуществляет возможность работы клиента ОВ и служит связующим звеном между клиентом ОВ и координатором ОВ.

Функциональные возможности и алгоритм работы клиента ОВ

Клиент ОВ обладает следующими функциональными возможностями: проведение аутентификации, расшифрование кода задания, выполнение задания, формирование ЭЦП, зашифрование результата выполнения задания, отправка результата клиенту ГС, формирование сообщений об ошибках, возникающих в процессе работы клиента ОВ, и отправка их клиенту ГС. На рис. 1 представлен алгоритм работы клиента ОВ.

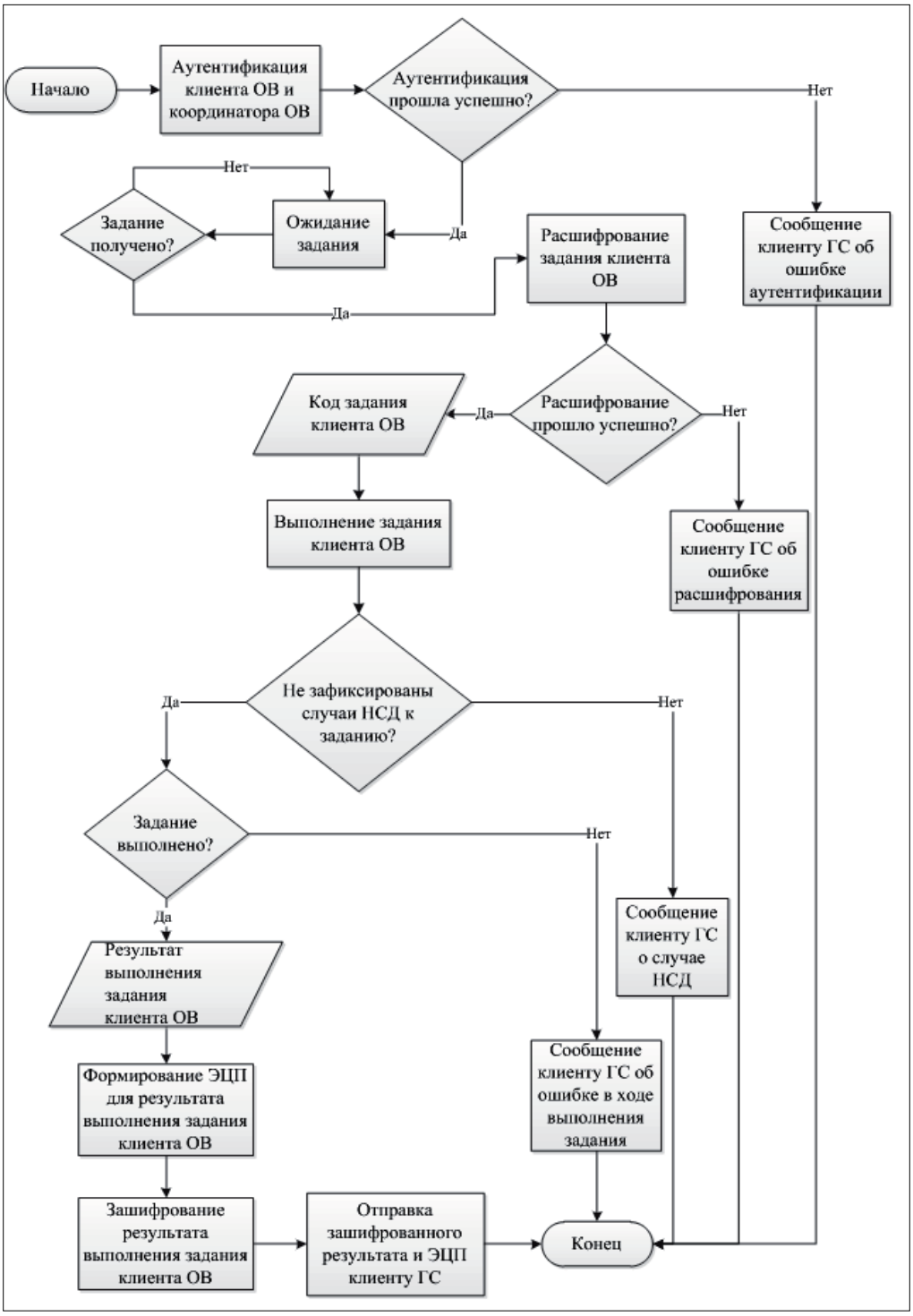

Рис. 1. Алгоритм работы клиента ОВ

Модель клиента ОВ

На рис. 2 представлена модель клиента ОВ.

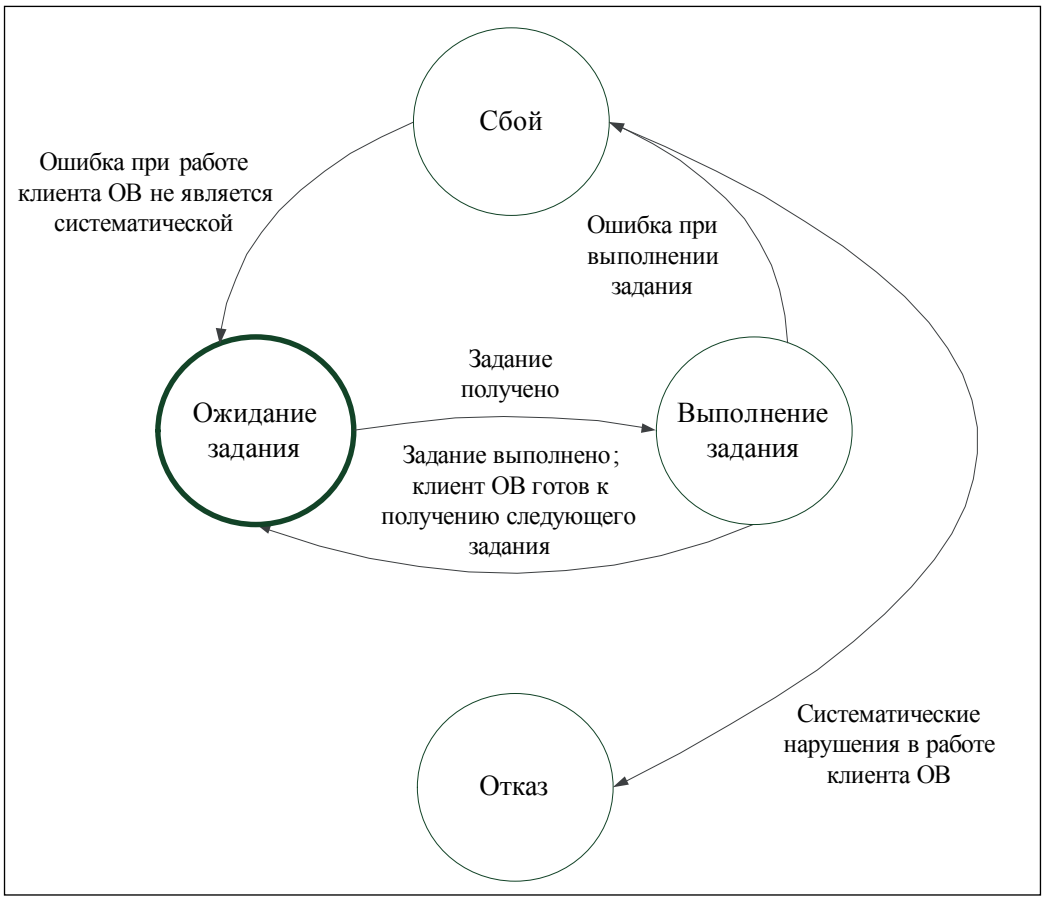

Рис. 2. Модель клиента ОВ

Механизмы обеспечения безопасности клиента ОВ

Двусторонняя аутентификация клиента ОВ и координатора ОВ происходит в момент подключения к сети клиента ОВ. Без успешно пройденной процедуры аутентификации клиенту ОВ не может быть выдано задание на выполнение. Аутентификация производится путем обмена сертификатами, изданными доверенным УЦ. Необходимость проведения аутентификации заключается в возможности противодействовать таким образом атаке типа «человек посередине» [3].

В случае неуспешной аутентификации со стороны клиента ОВ считается, что ключи данного клиента скомпрометированы и выдавать ему вычислительное задание небезопасно. Данный клиент ОВ исключается из состава вычислительных узлов среды ОВ по крайней мере до получения нового сертификата. В случае неуспешной аутентификации со стороны координатора ОВ клиент ОВ не может принимать от него задания на выполнение.

Результат выполнения задания и код задания не должны передаваться по каналам связи в открытом виде. Для шифрования используется технология «цифрового конверта», которая предполагает генерацию отправляющей стороной сеансового секретного ключа для зашифрования данных и зашифрование этого сеансового ключа на открытом ключе получателя. Преимуществами такого подхода являются высокая скорость шифрования из-за использования симметричных криптоалгоритмов, решение проблемы безопасного распределения секретных ключей, отсутствие проблемы хранения секретных ключей клиентов ОВ на координаторе ОВ [4].

Применение технологии «цифрового конверта» не дает получателю информации о том, кто именно отправил сообщение. Для решения задачи установления отправителя (в данном случае клиента ОВ) применяется ЭЦП на основе использования хэш-функции. Во-первых, при отправке по каналу передачи данных подписанного значения функции хэширования от результата выполненного задания сам результат не передается по каналу в открытом виде. Во-вторых, проверив подпись, получатель удостоверится в авторстве сообщения.

Еще одним преимуществом использования ЭЦП является возможность проверки целостности результата вычислительного задания путем сравнения двух значений хэш-функции — полученного от подписывающего и взятого от результата, пришедшего получателю [5].

Предлагаемый подход к развертыванию сред ОВ с использованием Грид-сетей преследует те же цели, что и иные существующие подходы. Однако появляется преимущество в возможности наращивания вычислительных мощностей за счет привлечения большого числа пользователей Грид-сети.

СПИСОК ЛИТЕРАТУРЫ:

1. *Черняк Л.* От мэйнфреймов к облакам [Электронный ресурс]: Лекционные курсы / Л. Черняк. URL: https://sites.google.com/site/moiknigiilekcii/lekcii/informatika/ lekcia-no25/cloud/otmejnfrejmovkoblakam (дата обращения: 07.06.2012).
2. Облачные вычисления. Размышления на тему безопасности [Электронный ресурс]: Cloudzone.Ru – В мире технологий облачных вычислений. URL: http://cloudzone.ru/articles/analytics/5.html (дата обращения: 07.06.2012).
3. *Копытин Д.* Безопасность при межпроектном взаимодействии [Электронный ресурс]: MsMaxGroup / Д. Копытин. URL: http://www.msmax.kz/index.html?id=595 (дата обращения: 07.06.2012).
4. *Берд К.* Цифровой конверт: тайна электронной переписки [Электронный ресурс]: Популярная механика / К. Берд. URL: http://www.popmech.ru/article/572-tsifrovoy-konvert/ (дата обращения: 07.06.2012).
5. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Т. 2. Средства защиты в сетях. М.: Горячая линия — Телеком, 2008. — 558 с.