Некоторые подходы в организации удаленного доступа пользователей к суперкомпьютерным ресурсам

Ю.Ю. Дубенская, А.П. Крюков, А.П. Демичев

НИИЯФ МГУ, Москва

В статье анализируются современные подходы к организации удаленного доступа пользователей к суперкомпьютерным ресурсам, такие как: прямой доступ по защищенному протоколу, доступ с использованием RESTful веб-сервиса, доступ с через веб-интерфейс и доступ через грид. В работе рассматриваются перспективные направления развития методов организации удаленного доступа. Даны характеристики каждого подхода, а также приведены конкретные примеры их использования. Отдельно уделено внимание сравнительному анализу подходов с точки зрения поддерживаемой функциональности, обеспечения информационной безопасности и удобства использования. На основании проведенного анализа исследованы области применимости этих подходов для решения различных вычислительных задач.

1. Введение

В настоящее время во многих областях науки и техники появляется все больше ресурсоемких расчетных задач, требующих для своего эффективного решения высокопроизводительных средств вычислительной техники — суперкомпьютеров (СК). Проблема в том, что далеко не каждый научно-исследовательский институт или университет может позволить себе иметь собственный СК, поэтому важной и актуальной задачей является организация удаленного доступа к СК ресурсам. Вместе с тем, от возможностей средств удаленного доступа, предоставляемых пользователю, во многом зависят востребованность и эффективность использования СК. Следовательно, выбору метода организации удаленного доступа к СК ресурсам следует уделять особое внимание.

При любом методе предоставления удаленного доступа к вычислительным ресурсам необходимо находить баланс между универсальностью предоставляемых решений, информационной безопасностью и удобством проведения вычислений.

Под универсальностью будем понимать возможность удаленного использования СК ресурсов для решения различного круга задач. При определении степени универсальности нужно ответить на следующие вопросы. Какие именно (заранее предустановленные или любые) вычислительные программы можно запускать на СК? Есть ли возможность компиляции и установки собственных программ пользователя на СК? Установлены ли на СК какие-либо специальные программные пакеты, ассоциированные с некоторой предметной областью? Насколько пользователь может влиять на параметры запуска вычислительных заданий для оптимизации времени вычислений?

Безопасность при организации удаленного доступа подразумевает пресечение несанкционированного доступа к СК ресурсу, разграничение прав пользователей; взаимную идентификацию сервера (ресурса) и клиента (пользователя), защиту данных пользователей.

Удобство использования СК ресурса играет немаловажную роль в организации вычислений. Чем более прост и интуитивно понятен интерфейс удаленного взаимодействия с СК, тем более широкий круг специалистов из различных научных и инженерных областей будет заинтересован в использовании данного вычислительного ресурса.

Как правило, СК ресурс использует внутреннюю локальную сеть, и прямой доступ к нему закрыт сетевыми экранами. Это, с одной стороны, обеспечивает защиту от несанкционированного доступа, а, с другой стороны, усложняет использование ресурса удаленными пользователями. В общем случае для организации удаленного доступа к СК ресурсам используется схема, представленная на рисунке 1.

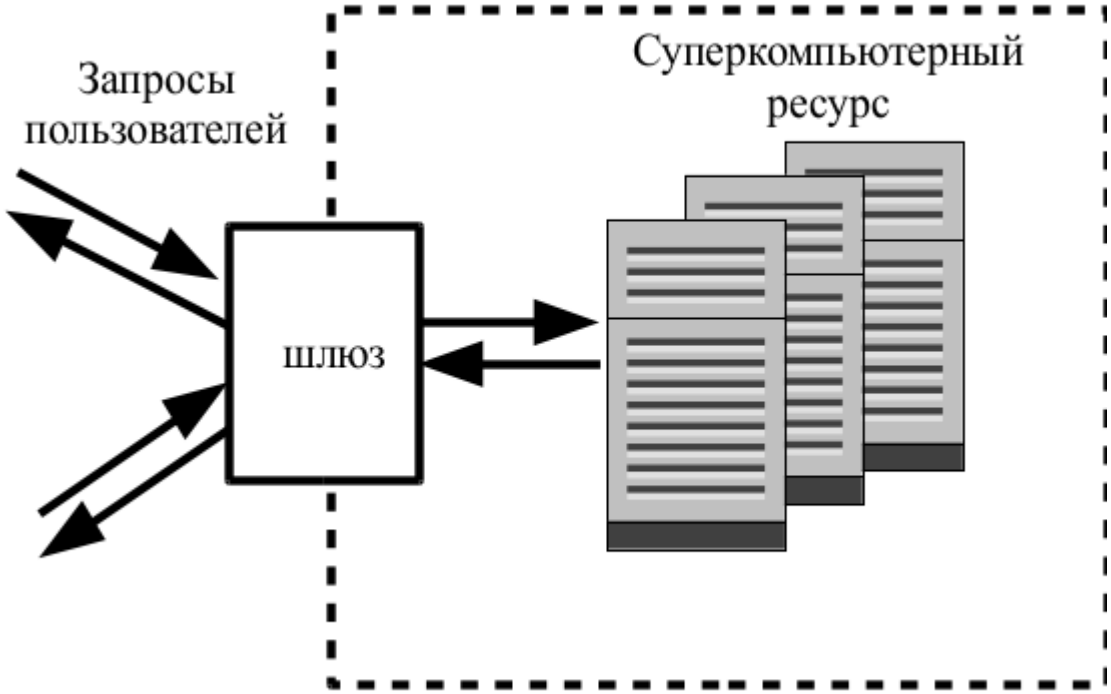

Рис. 1. Общая структура удаленного доступа к СК ресурсам

В качестве шлюза могут быть использованы как стандартные сервисы (например, sshd), так и специализированные веб-сервисы. В зависимости от типа сервиса, играющего роль шлюза, удаленный доступ пользователей к СК ресурсу должен быть организован по-разному. Для организации удаленного доступа используется несколько основных подходов:

- прямой доступ по защищенному протоколу;
- доступ через RESTful веб-сервис;
- доступ с использованием веб-интерфейса;
- доступ через грид.

Эти подходы по-разному расставляют акценты между универсальностью, безопасностью и удобством использования. Рассмотрим эти походы более подробно и остановимся на достоинствах и недостатках каждого.

2. Прямой доступ к СК ресурсам по защищенному протоколу

Одним из наиболее распространенных в настоящее время методов удаленного доступа к СК ресурсам является предоставление прямого доступа по протоколу ssh [1], который позволяет подключаться к консоли удаленного ресурса. Прямой доступ предоставляет пользователю гибкую возможность использовать все средства, имеющиеся на ресурсе, таким образом, обеспечивается максимальная универсальность.

Однако этот метод предъявляет значительные требования к квалификации пользователей. Для получения удаленного доступа к СК необходимо установить на своем локальном компьютере специальную программу-клиент (PuTTY, OpenSSH и т.п.). Перед составлением вычислительных заданий нужно изучить особенности среды исполнения: архитектуру используемого СК, параметры операционной системы, установленной на удаленном ресурсе (как правило, это Unix-подобные операционные системы), а также команды системы пакетной обработки заданий. Затем нужно самостоятельно подготовить вычислительное задание так, чтобы оно могло быть выполнено на выбранном ресурсе, описать это задание на языке, понятном системе обработки заданий, обеспечить доступность входных и получение выходных данных. В качестве примера, можно рассмотреть, СК "Ломоносов" [2], который имеет

неоднородную структуру, включающую вычислительные узлы разных видов и процессоры с различной архитектурой. Он работает под управлением операционной системы Clustrx (Linux) и использует систему обработки заданий SLURM.

С другой стороны, при прямом доступе пользователь может максимально контролировать процесс запуска заданий. Например, при необходимости расчета множества однотипных задач с разными входными параметрами у пользователя есть возможность написать соответствующий скрипт и тем самым автоматизировать запуск.

Безопасность при использовании прямого доступа средствами ssh основана на асимметричной криптографии, но, как правило, без использования инфраструктуры открытых ключей (public key infrastrucute, PKI). При таком подходе пользователь сам некоторым способом передает свой открытый ключ владельцу ресурса. С одной стороны, такой подход проще, так как нет необходимости следить за обновлением сертификатов, с другой стороны, отсутствует стандартная процедура оповещения о компрометации ключа, и практически невозможна делегация полномочий.

Таким образом, метод прямого доступа обладает наибольшей универсальностью, обеспечивает хороший уровень безопасности, и удобен пользователям, обладающим квалификацией системного администратора или хотя бы продвинутого пользователя.

3. Доступ через RESTful веб-сервис

В последние годы архитектура REST (REpresentational State Transfer) [3] стала стандартной архитектурой при дизайне веб-сервисов и веб-API. Доступ к СК ресурсам через веб-сервис в качестве шлюза оправдан в случаях, когда исследователям требуется запускать большое количество вычислительных заданий для решения некоторой проблемы в конкретной прикладной области или данный сервис получает запросы от других сервисов, например при обработке композитных заданий, или веб-интерфейса пользователя. В этом случае на СК осуществляется предварительная установка и настройка часто используемых пакетов прикладных программ (ППП), и веб-сервис разрабатывается для использования этих ППП с учетом их специфики.

Такой подход позволяет владельцам информационно-вычислительных ресурсов поднять эффективность использования ресурсов за счет снижения универсальности.

Другим типичным случаем использования (use case) является случай, когда имеется несколько СК ресурсов, среди которых пользователь выбирает наиболее подходящий. В этом случае использование RESTful веб-сервиса позволяет унифицировать доступ к СК ресурсам и скрыть от пользователя особенности каждого конкретного СК.

Для взаимодействия с сервисом пользователю нужен клиент, умеющий отправлять HTTP-запросы и получать ответы. В качестве клиента может использоваться как интерфейс командной строки (ИКС), так и специализированный веб-интерфейс.

Использование ИКС веб-сервиса требует от пользователя почти такой же высокой квалификации, как и использование прямого доступа по протоколу ssh. В частности, пользователь должен самостоятельно подготавливать файлы с описанием заданий. Вместе с тем, использование ИКС позволяет автоматизировать ряд действий, в том числе запуск однотипных заданий с разными входными параметрами.

Безопасность при использовании RESTful веб-сервиса, как правило, основывается на PKI. Этот подход обеспечивает высокий уровень защиты данных, но требует от пользователя умения выполнять процедуры генерации ключа, а также получения и установки сертификата. Дополнительные сложности обусловлены тем, что у пользователей на компьютерах установлены разные операционные системы, а также разные криптографические библиотеки, поэтому достаточно трудно выработать единые методические рекомендации по работе с сертификатами. При использовании внешних веб-интерфейсов часть сложностей для пользователя маскируется, но при использовании ИКС сложность работы по сравнению с прямым доступом даже выше из-за необходимости непосредственного взаимодействия с PKI-инфраструктурой.

Таким образом, метод доступа через RESTful веб-сервис характеризуется достаточно низкой универсальностью, достаточно высокой гибкостью (хотя и несколько меньшей по сравнению с прямым доступом) и высоким уровнем безопасности. С точки зрения удобства использования, ИКС может быть весьма удобен пользователям, обладающим достаточно высокой квалификацией. С помощью ИКС такие пользователи могут получить гибкий унифицированный интерфейс для взаимодействия с разными СК ресурсами. Остальным пользователям рекомендуется вместо ИКС использовать внешний веб-интерфейс, который рассмотрен в следующем разделе.

4. Доступ с использованием веб-интерфейса

Веб-интерфейс, применяемый для организации доступа к СК ресурсу, может либо сам выступать в роли специализированного шлюза, либо использоваться в качестве внешнего клиента к шлюзу, на котором установлен RESTful веб-сервис. Последний вариант является более общим и, как правило, ориентирован на обслуживание нескольких СК ресурсов, в том числе, в рамках грида. Здесь мы рассмотрим случай использования веб-интерфейса в качестве внешнего клиента. В следующем разделе будет рассмотрено использование веб-интерфейса в гриде.

Наиболее типичным случаем применения веб-интерфейса является его использование для работы с конкретным набором предустановленных ППП. В этом случае можно достичь наиболее эффективного использования СК ресурса.

При совместной работе с сервисом, предоставляющим доступ к конкретным ППП на СК ресурсе, веб-интерфейс должен быть оптимизирован для выполнения заданий этих ППП. Каждый отдельный заранее подготовленный шаблон задания (запуск ППП, обращение к хранилищу данных и т.п.) называется "инструментом". Имея доступ к инструментам, предоставляемым через веб-интерфейс, пользователю достаточно указать конкретные значения входных параметров или файлов с входными данными, а все остальное описание задания для запуска генерируется автоматически. Таким образом, в большинстве случаев на пользовательском компьютере не нужно устанавливать никаких дополнительных программных средств, вся работа (формирование задания, его запуск, контроль выполнения и получение результатов) осуществляется через стандартный веб-браузер.

Аутентификация пользователей при использовании комбинации веб-интерфейса и сервиса-шлюза может основываться на разных технологиях: от простой комбинации логина и пароля до асимметричной криптографии и PKI. При настройке параметров веб-интерфейса администраторы ресурсов имеют возможность выбрать необходимый уровень безопасности, который будет использован при проверке пользователей. Часто при использовании веб-сервисов в качестве шлюза к СК ресурсу поддерживается авторизация с ролевым определением прав доступа пользователей к ресурсам, которая осуществляется с помощью механизма динамического отображения пользователей на локальные учетные записи вычислительного ресурса с соответствующими правами.

Удобство использования систем с веб-интерфейсом во многом зависит от его качества, но для крупных проектов качество веб-интерфейсов, как правило, высокое. При этом требования к знаниям пользователя в области вычислительных технологий минимальны.

Таким образом, доступ через веб-интерфейс максимально маскирует для пользователя устройство конкретных вычислительных ресурсов и актуален для специализированных веб-платформ и порталов, централизованно предоставляющих пользователю ряд сервисов, объединенных единой предметной областью, принципом доступа и интерфейсом. Примерами таких порталов являются Nucleonica [4], который ориентирован на исследователей в области ядерной физики, и Учебно-научный комплекс «Компьютерное моделирование в нанотехнологиях» [5], созданный на основе многофункциональной инструментально-технологической платформы CLAVIRE поддержки облачных вычислений.

5. Доступ через грид

Отдельно рассмотрим случай использования грида как наиболее универсального подхода для построения распределенных вычислительных инфраструктур.

Как и в рассмотренных выше случаях, в гриде удаленный доступ к СК ресурсам организуется посредством промежуточного программного обеспечения (ПО), которое устанавливается на шлюзе. В качестве примера такого программного обеспечения можно рассмотреть Globus Toolkit [6], который используется для построения шлюзов в проекте Worldwide LHC Computing Grid (WLCG) [7]. Шлюз обеспечивает согласование грид-среды и среды исполнения конкретного СК. В этом случае пользователям не требуется изучения особенностей архитектуры и среды исполнения СК. Система управления заданиями грида автоматически учитывает все аппаратные и программные особенности ресурса при запуске задания пользователя. Таким образом, по сравнению с методом прямого доступа, к квалификации пользователей предъявляются значительно меньшие требования. Универсальность при использовании этого подхода несколько ниже, чем при прямом доступе, но выше, чем при использовании веб-сервисов и веб-интерфейсов, и определяется возможностями грид-среды.

Безопасность в гриде, как и при использовании RESTful веб-сервисов, основана на PKI. При этом в гриде для управления правами доступа используется механизм виртуальных организаций (ВО) и так называемые VOMS-сертификаты, содержащие информацию о принадлежности пользователя к некоторой ВО. Для делегации полномочий используются прокси-сертификаты, которые позволяют делегировать полномочия как от пользователей к сервисам, так и между сервисами. Этот подход обеспечивает высокий уровень защиты данных и позволяет гибко и удобно администрировать права доступа, но требует от пользователя глубоких знаний в области PKI для выполнения процедур генерации ключа, получения и установки сертификата, регистрации в ВО, создания и обновления прокси-сертификатов.

Таким образом, метод использования грида для доступа к СК ресурсам снимает с пользователей необходимость изучения особенностей конкретного СК, но одновременно требует изучения особенностей инфраструктуры безопасности, основанной на PKI. Опыт эксплуатации гридов [8,9] показал, что данный подход заметно затрудняет использование СК ресурсов неспециалистами в области компьютерных наук, что, в свою очередь, уменьшает потенциал использования современных технологий для проведения ресурсоемких вычислений.

Дополнительно нужно учитывать, что создание масштабной распределенной вычислительной грид-инфраструктуры требует достаточно высоких накладных расходов для администрирования и поддержки, особенно с финансово-экономической и административной точек зрения. Можно сделать вывод, что применение грида для доступа к СК ресурсам оправдано только при наличии мощной объединяющей организационной структуры (как, например, в случае проекта WLCG, обслуживающего одну научную мегаустановку — Большой адронный коллайдер).

6. Комбинированные решения

Одним из направлений развития технологий обеспечения удаленного доступа к СК ресурсам является организация унифицированного доступа с использованием различных программных надстроек, представляющих собой специальное промежуточное программное обеспечение (ППО). Такое ППО, как правило, объединяет в себе возможности нескольких подходов к организации доступа к СК ресурсам.

Одним из возможных вариантов обеспечения унифицированного интерфейса удаленного доступа является создание ПО, которое обеспечивает единый интерфейс для работы по протоколу ssh, не зависящий от среды исполнения СК. Примером такого ПО является программа piLite [10]. Это консольное клиент-серверное приложение, серверная часть которого устанавливается в качестве шлюза, а клиентская часть – на компьютере пользователя. Программа piLite предлагает удобный унифицированный интерфейс для запуска и управления заданиями, маскируя для пользователя особенности среды выполнения СК, а также

обеспечивая передачу входных и выходных данных. Тем не менее, при стандартном использовании эта программа требует от пользователя установки ssh-клиента и умения работать в командной строке. Интересным вариантом использования программы piLite является использование веб-сервера в качестве клиента. В этом случае пользователь работает только с веб-интерфейсом, а обращения по протоколу ssh с использованием piLite осуществляет веб-сервер. Основным и наиболее целесообразным применением этого ПО является организация доступа к конкретному СК ресурсу.

Более сложной схемой является использование RESTful-сервисов для унификации прямого доступа и доступа через грид. При этом подходе в роли специализированной надстройки используется набор унифицированных RESTful-сервисов для организации шлюза к СК ресурсам [11]. Основные задачи, которые выполняет шлюз удаленного доступа к СК ресурсам, – это регистрация задания пользователя, трансляция его описания в термины среды исполнения конкретного СК ресурса и последующая передача задания на выполнение на этот ресурс. Унификация заключается, во-первых, в выработке единого интерфейса для взаимодействия с сервисами шлюза, а во-вторых, в использовании при разработке сервисов стандартных средств и механизмов: архитектурного стиля REST [3] и протокола обмена данными JSON [12]. Таким образом, шлюз обеспечивает единый интерфейс, не зависящий не только от среды исполнения СК, но и от способа запуска заданий (посредством прямого доступа по протоколу ssh или через грид). В результате от пользователя скрывается специфика запуска заданий, что существенно облегчает работу на нескольких СК ресурсах одновременно.

Подобные решения, в основном, направлены на повышение удобства использования СК ресурсов без ущерба для безопасности. Универсальность использования СК в результате применения таких решений либо не снижается, либо снижается незначительно.

7. Заключение

На основании вышеизложенного можно составить следующую таблицу характеристик различных подходов к организации удаленного доступа.

Характеристика	**Способ организации доступа**			
	Прямой доступ по ssh	**веб-сервис**	**веб-интерфейс**	**грид**
Универсальность	максимально возможная	высокая	средняя	высокая
Удобство использования	низкое	низкое	высокое	среднее
Требуемая квалификация пользователя	высокая	высокая	низкая	средняя
Уровень безопасности	высокий	очень высокий	в зависимости от настроек: от среднего до очень высокого	очень высокий
Работа с несколькими СК ресурсами	- доступ организован по-разному на разные СК; - пользователь сам выбирает ресурс	- доступ унифицирован; - пользователь сам выбирает ресурс	- доступ унифицирован; - ресурс может выбирается автоматически	- доступ унифицирован; - ресурс выбирается автоматически

Формирование вычислительного задания	вручную	- вручную для ИКС; - вручную или автоматически через веб-интерфейс	автоматически	- вручную для ИКС; - вручную или автоматически через веб-интерфейс

Как видно из таблицы, прямой доступ хорошо подходит для высококвалифицированных пользователей, работающих на конкретном СК ресурсе, для которых важно добиться максимальной гибкости в настройках задания за счет учета особенностей среды исполнения конкретного СК.

Для пользователей с аналогичной квалификацией и потребностями, у которых есть доступ сразу к нескольким СК ресурсам, лучше подойдет доступ через веб-сервис.

Также прямой доступ хорошо подходит для решения задачи сравнения возможностей ППП и выбора того ППП, который пользователь собирается использовать в своих исследованиях.

Для пользователей, решающих узконаправленные задачи с использованием конкретных заранее предустановленных ППП, лучше подходит доступ через веб-сервис или через веб-интерфейс, в зависимости от квалификации.

Веб-интерфейс в любом случае оптимален для пользователей, не являющихся специалистами в области компьютерных наук, потому что только веб-интерфейс позволяет таким пользователям сосредоточиться непосредственно на исследованиях и не тратить время на изучение организационных и технических особенностей инфраструктуры для доступа к СК ресурсу возможно за счет снижения эффективности использования СК ресурса.

Организация доступа через грид оправдана только для очень больших коллабораций [7,8]. В этом случае плюсы от использования соответствующей сложной концепции безопасности (управление пользователями, аудит и т.п.), превышают минусы от необходимости поддерживать громоздкую инфраструктуру.

Практика показывает, что наиболее перспективным подходом является организация веб-доступа к СК ресурсам с предустановленными пакетами ППП, предназначенными для решения задач в некоторой конкретной области. Такие проекты в настоящее время наиболее активно развиваются и привлекают наибольшее количество пользователей-участников.

Как можно увидеть из предыдущего обсуждения, важную при работе в распределенных вычислительных инфраструктурах играют роль вопросы безопасности. Для комфортной работы пользователя нужно соблюсти баланс между уровнем безопасности и удобством использования СК ресурсов. Для этого необходимо упростить для пользователей процедуру аутентификации и авторизации при работе с СК ресурсом при сохранении высокой степени безопасности. Использование цифровых сертификатов, хотя и обеспечивает высокий уровень безопасности систем, является достаточно тяжелым решением для конечного пользователя. В настоящее время в веб-технологиях для аналогичных целей используются новые подходы, реализованные в частности, в протоколах OpenID [13], OAuth [14] и BrowserID [15]. Ряд идей, заложенных в указанных подходах, может быть адаптирован для организации доступа к СК ресурсам.

Литература

1. The Secure Shell (SSH) Authentication Protocol, RFC 4252. // Network Working Group of the IETF, 2006.
2. Суперкомпьютер Ломоносов. // URL: http://parallel.ru/cluster/lomonosov.html (дата обращения: 27.05.2015).
3. Fielding R.T. Architectural styles and the design of network-based software architectures. // Dotoral dissertation, University of California, Irvine, 2000.
4. Nucleonica. Web driven nuclear science. // URL: http://www.nucleonica.net (дата обращения: 27.05.2015).

5. Маслов В. Г., Бухановский А. В., Спельников Д. М. Учебно-научный комплекс «Компьютерное моделирование в нанотехнологиях» на основе грид-среды. // Известия высших учебных заведений «Приборостроение», 2011, выпуск 10(54).
6. Foster I., Kesselman C. The Globus Project: A Status Report. // Proc. Heterogeneous Computing Workshop, IEEE Press, 1998, pp. 4–18.
7. WLCG Project. // URL: http://wlcg.web.cern.ch/ (дата обращения: 27.05.2015).
8. Kryukov A.P., Demichev A.P., Ilyin V.A., Shamardin L.V. Architecture of grid for national nanotechnology network (GridNNN). In Distributed Computing and Grid-Technologies in Science and Education: Proceedings of the 4th Intern. Conf, Dubna. 2010, pp.352-356.
9. Dubenskaya Yu Yu, Kryukov A.P., Shamardin L.V. Certreq: a standalone tool for certificate requests generation and certificates retrieving in GridNNN. // The 5th International Conference "Distributed Computing and Grid-technologies in Science and Education", Dubna, 2012
10. Dubenskaya Yu Yu, Kryukov A.P., Demichev A.P., Prikhodko N.V. PiLite: a unified interface to local resource managers on supercomputing resources. // The 6th International Conference "Distributed Computing and Grid-technologies in Science and Education", Dubna, 2014.
11. Крюков А.П., Шамардин Л.В., Приходько Н.В., Демичев А.П. Унифицированный удаленный доступ к суперкомпьютерным ресурсам. // Материалы XII Всероссийской конференции "Высокопроизводительные параллельные вычисления на кластерных системах", Н. Новгород, 2012, с. 228-230.
12. Zyp K.: A JSON Media Type for Describing the Structure and Meaning of JSON Documents. // Techniocal report, IETF Network Workong Group, 2010.
13. Eldon E. Single sign-on service OpenID getting more usage. // URL: http://venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage (дата обращения: 27.05.2015).
14. Eran H.L. Introducing OAuth 2.0. URL: http://hueniverse.com/2010/05/introducing-oauth-2-0 (дата обращения: 27.05.2015).
15. Introducing BrowserID: A better way to sign in. // URL: http://identity.mozilla.com/post/7616727542/introducingbrowserid-a-better-way-to-sign-in (дата обращения: 27.05.2015).