Современные проблемы дистанционного зондирования Земли из космоса.
2011. Т.8. № 3. С. 155-160

Управление доступом к WEB-ресурсам в распределенных системах дистанционного мониторинга

М.А. Бурцев, А.С. Мамаев, А.А. Прошин, Е.В. Флитман

Институт космических исследований РАН,
117997, Москва, Профсоюзная, 84/32
E-mail: info@smis.iki.rssi.ru

В рамках разрабатываемых в ИКИ РАН распределенных информационных систем дистанционного мониторинга Земли реализуется доступ к большому набору различных спутниковых данных и продуктов их тематической обработки, а также к различной сопутствующей информации, для которых существенно различается политика предоставления доступа к данным. Доступ к данным в системе преимущественно реализуется на базе специализированных картографических WEB интерфейсов, расположенных на территориально разнесенных серверах. Для того, чтобы воспользоваться ими, пользователю необходимо пройти аутентификацию на любом из серверов, после чего он получает доступ к тем или иным интерфейсам в зависимости от того, какие права прописаны для соответствующей учетной записи. При этом даже в рамках одного интерфейса различным пользователям могут быть доступны разные наборы данных, в частности, данные разного пространственного разрешения, данные за различные периоды времени и т.п. Настоящая статья посвящена описанию системы управления доступом к WEB-ресурсам, позволяющей обеспечить авторизованный доступ большого числа пользователей, обладающих различными правами доступа.

Ключевые слова: распределенные информационные системы, авторизация, управление доступом.

Введение

В рамках разрабатываемых в ИКИ РАН распределенных информационных систем дистанционного мониторинга Земли реализуется доступ к большому числу различных типов спутниковых данных и результатов их обработки, а также к различной сопутствующей информации. Доступ к данным преимущественно реализуется на базе специализированных картографических WEB интерфейсов, расположенных на территориально разнесенных серверах. Так как большая часть как интерфейсов, так и данных является закрытой, то доступ к ним реализуется только для зарегистрированных пользователей. При этом возникает задача реализации однократной (единой) авторизации пользователя в системе, после которой он смог бы обращаться к WEB интерфейсам, расположенным на любом из серверов системы.

Характерной особенностью рассматриваемого класса информационных систем является относительно большое число реализованных вариантов доступа и фильтров на получение данных для различных пользователей. В зависимости от принадлежности к той или иной группе пользователь может иметь доступ как к различным WEB интерфейсам, так и к различным типам данных в рамках этих интерфейсов. При этом для каждого типа данных может быть дополнительно реализован фильтр, ограничивающий доступ к соответствующим данным по различным критериям: по диапазону дат, диапазону координат, по максимальному разрешению и др. Отметим также, что число зарегистрированных пользователей в некоторых из разрабатываемых нами систем превышает тысячу. Есте-

ственно, что для того, чтобы управлять правами такого большого числа пользователей, необходим удобный инструментарий, позволяющий легко оперировать правами различных групп пользователей.

Для решения вышеперечисленных задач в ИКИ РАН была реализована система управления доступом к WEB ресурсам, отвечающая как за единую авторизацию пользователей, так и за управление правами пользователей по доступу к различным WEB интерфейсам и типам данных. Ниже сначала приводятся сведения об используемых при построении этой системы технологиях, а затем кратко описывается реализация рассматриваемой системы.

Используемые технологии

Разрабатываемые нами WEB-интерфейсы для доступа к данным, как правило, реализуются под управлением WEB сервера Apache. Встроенный в Apache механизм авторизации предполагает хранение учетной записи пользователя отдельно на каждом сервере, поэтому при его непосредственном использовании пользователю пришлось бы проходить авторизацию при каждом обращении к другому серверу распределенной системы дистанционного мониторинга. В связи с этим было решено использовать специальный инструментарий Apache, который позволяет внедряться в запрос клиента (браузера) на стадии установления соединения с сервером и реализовывать свой обработчик процедуры авторизации. Хранение учетных записей пользователей было решено реализовать в специализированной базе данных на центральном узле информационной системы и реплицировать ее на остальные сервера стандартными средствами СУБД. При авторизации пользователя на другом сервере, находящемся в этом же домене, было решено использовать механизм «Cookie», а при переходе между доменами используется зашифрованная информация из строки запроса.

После аутентификации пользователю присваивается уникальный шифрованный ключ, внутри которого хранится информация о времени последнего посещения, ip адрес, идентификатор пользователя в системе, и другая служебная информация. Ключ записывается в Cookie после авторизации пользователя на странице аутентификации по имени учетной записи и паролю. Ключ можно передавать в строке запроса для перехода между серверами с разными доменными именами. При обращении браузера к любому WEB-интерфейсу ключ будет взят из Cookie или строки запроса и расшифрован на стадии запроса к серверу Apache, и, если все необходимые проверки пройдут успешно, пользователь получит доступ к WEB-интерфейсу. Наличие доступа проверяется дополнительно самим Apache с использованием модуля для проверки имени учетной записи и пароля из базы данных. Фильтрация данных по различным критериям производится в сервисах предоставления данных на основе параметров учетной записи. Для удобной работы с учетными записями пользователей реализован специализированный WEB интерфейс, позволяющий назначать права доступа как группам пользователей, так и отдельным пользователям. Такая схема позволяет контролировать множество дополнительных параметров, введенных разработчиком, модернизировать доступ под конкретную задачу и динамически генерировать данные в интерфейсе на основе учетной записи пользователя.

Реализация

За основу был взят стандартный модуль для авторизации Apache в связке с СУБД Mysql (рис. 1). На основе использования модуля сервера Apache mod_perl, позволяющего встраивать программный код в HTML документ, в ИКИ РАН был разработан модуль единой аутентификации пользователей (рис. 2) и различные схемы управления доступа к данным.

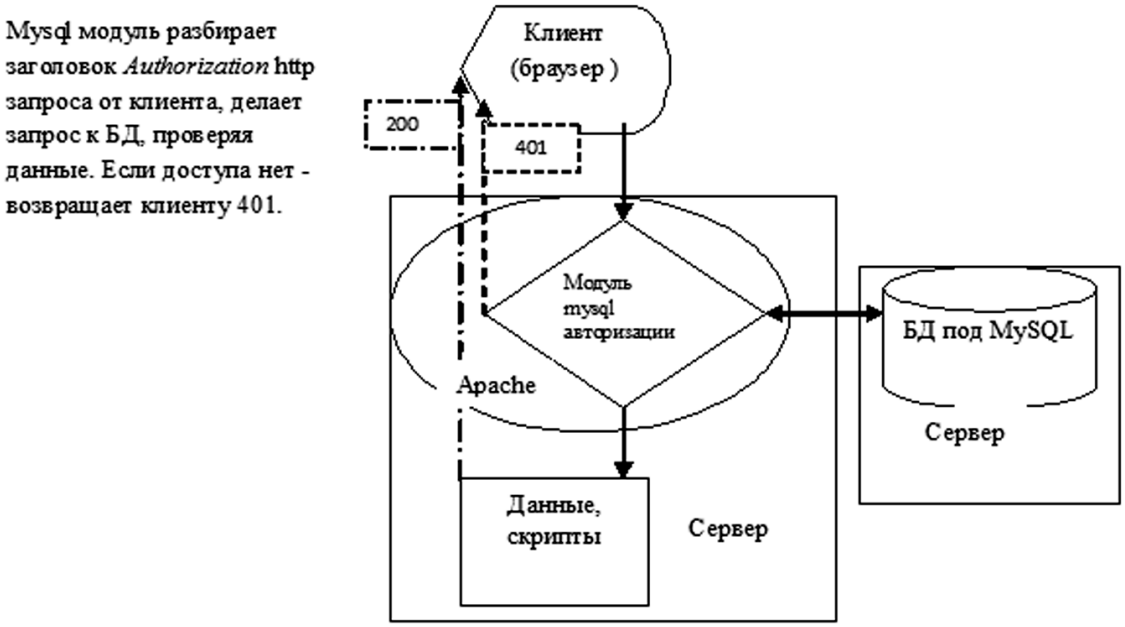

Рис. 1. Модуль mysql авторизации Apache

Приведенные решения осуществляют контроль доступа на стороне сервера, не вмешиваясь в работу интерфейсов. При этом модуль единой авторизации для контроля может использовать любые параметры, передаваемые в строке запроса или cookie, также он может использовать параметры из настроек сервера. Фильтрация наборов данных по различным критериям для каждого конкретного типа данных производится в соответствующем сервисе доступа к данным. При формировании HTML страниц может также использоваться директива «include», позволяющая включить или скрыть отдельные фрагменты документа в зависимости от прав пользователя.

Перечислим основные особенности рассматриваемого подхода:

• Единая аутентификация пользователя для предоставления доступа к WEB-интерфейсам информационной системы на основе авторизации;

• Аутентификация на каждом сервере происходит независимо от работоспособности других серверов;

• Управление учетными записями пользователей через WEB-интерфейс;

• Авторизация осуществляется на уровне WEB-сервера, не затрагивая работу WEB-интерфейсов;

• Для авторизации может дополнительно использоваться информация, находящаяся в запросе клиента;

• Поддерживается единая аутентификация на серверах, входящих в разные домены.

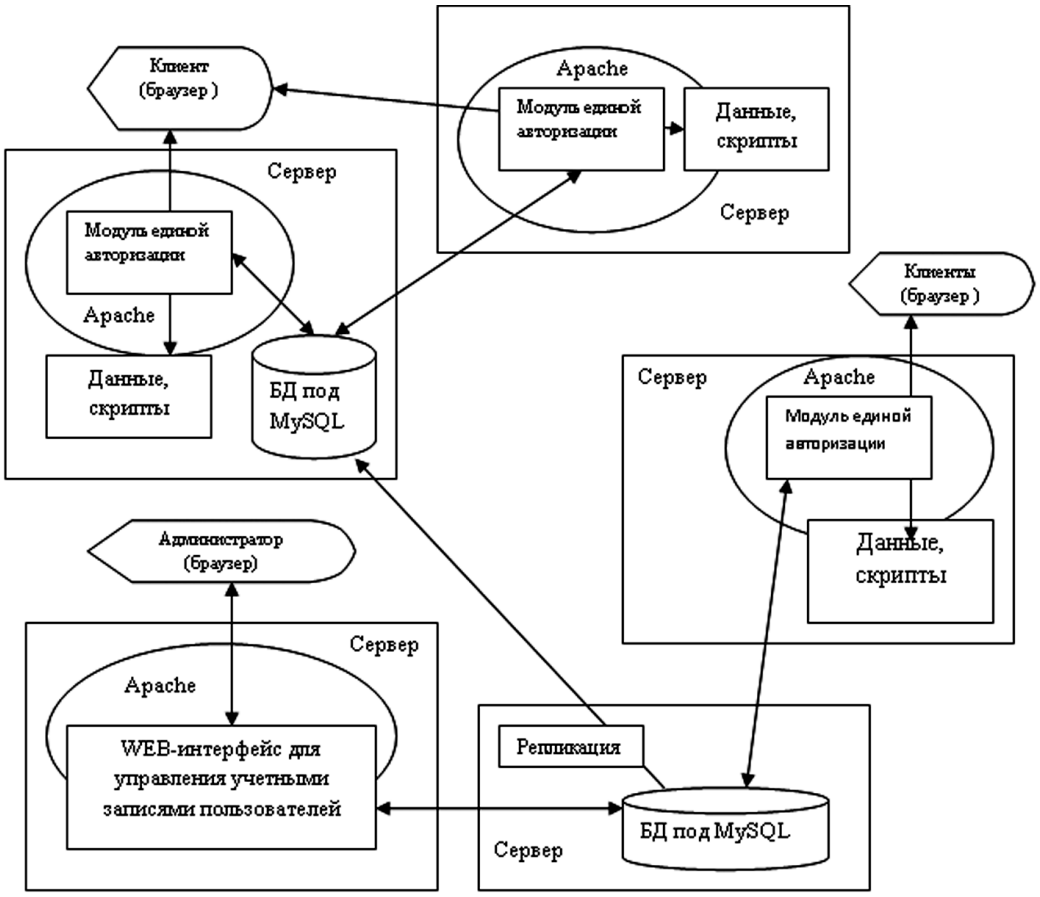

Рис. 2. Модуль единой авторизации и интерфейс управления пользователями

В конечном итоге, используя стандартный инструментарий Web-сервера Apache и разработанный модуль единой авторизации, можно выделить следующие схемы для организации удаленного доступа:

• Авторизация в рамках одного доменного имени. Используется идентификатор сессии передаваемый в cookie.

• Авторизация в рамках нескольких доменных имен. Используется идентификатор сессии, передаваемый в строке запроса.

• Доступ между серверами без авторизации для служебных интерфейсов. Используется жесткая привязка доступа к ip адресам.

• Доступ с авторизацией через центральный прокси-сервер. Авторизация происходит только на одном сервере, а дальше запросы проксируются по путям без авторизации через этот же сервер.

Назначение прав доступа пользователю осуществляется администратором через удаленный WEB-интерфейс (Рис. 3). Администратор регистрирует пользователя, создавая ему учетную запись в системе с уникальным логином и паролем. Каждая учетная запись входит в определенное число групп. Группа обладает правами доступа только к заданным электронным ресурсам. Таким образом, пользователю разрешен доступ только к четко фиксированному количеству электронных ресурсов. При этом каждой учетной записи могут быть заданы дополнительные ограничения доступа, например по Субъекту РФ. После заведения учетной записи можно осуществлять назначение, прав работая с группами.

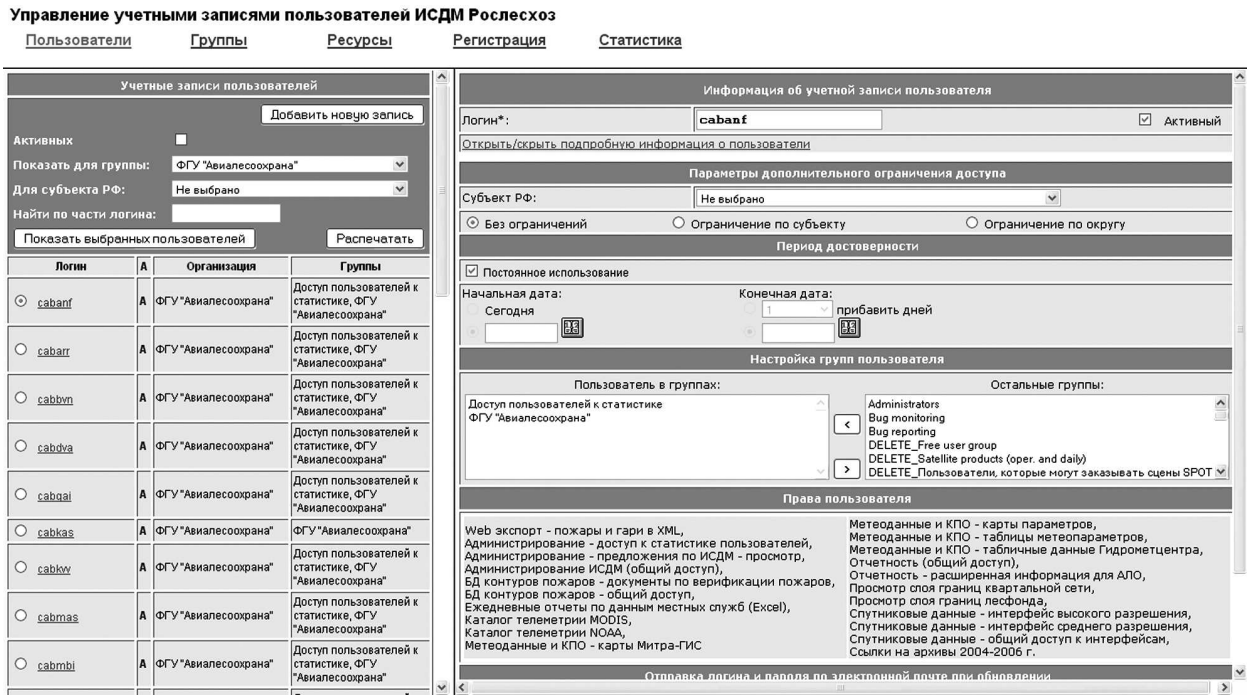

Рис. 3. Интерфейс управления учетными записями пользователей

Заключение

Представленная в данной статье система управления доступа к WEB-ресурсам в настоящее время успешно используется нами в реально эксплуатируемых системах дистанционного мониторинга Земли, в частности, в системе дистанционного мониторинга лесных пожаров Рослесхоза (ИСДМ Рослесхоз) [1], в системе дистанционного мониторинга земель агропромышленного комплекса (СДМЗ АПК) [2] и в работе сервиса спутникового мониторинга состояния растительности «Вега» [4]. Выработанные нами подходы, на наш взгляд, могут представлять интерес для других информационных систем такого класса.

Литература

1. *Барталев С.А., Ершов Д.В., Коровин Г.Н., Котельников Р.В., Лупян Е.А., Щетинский В.Е*. Основные возможности и структура информационной системы дистанционного мониторинга лесных пожаров Федерального агентства лесного хозяйства (ИСДМ Рослесхоз) // Современные проблемы дистанционного зондирования Земли из космоса, 2010. Т.7. № 2. С.97-105.
2. *Лупян Е.А., Барталев С.А., Бурцев М.А., Крашенинникова Ю.С., Мазуров А.А., Матвеев А.М., Толпин В.А., Флитман Е.В.* Организация работы с данными в системе дистанционного мониторинга сельскохозяйственных земель агропромышленного комплекса (СДМЗ АПК) // Материалы Всероссийской научной конференции «Методическое обеспечение мониторинга земель сельскохозяйственного назначения». 29-30 сентября 2009 года. Сборник научных статей. Москва. – М.:РАСХН, 2009.
3. *Ефремов В.Ю., Балашов И.В., Бурцев М.А., Лупян Е.А., Прошин А.А., Толпин В.А*. Построение комплексных картографических Web-интерфейсов для работы со спутниковыми данными и результатами их обработки в различных системах дистанционного мониторинга // Восьмая

всероссийская открытая ежегодная конференция «Современные проблемы дистанционного зондирования Земли из космоса». Москва. ИКИ РАН. 15-19 ноября 2010. Сборник тезисов конференции. С. 87.
4. *Лупян Е.А., Савин И.Ю., Барталев С.А., Толпин В.А., Балашов И.В., Плотников Д.Е*. Спутниковый сервис мониторинга состояния растительности («Вега») // Современные проблемы дистанционного зондирования Земли из космоса, 2011. Т.8. № 1. С.190-198.

WEB resources access control for remote monitoring distributed systems

M.A. Bourtsev, A.S. Mamaev, A.A. Proshin, E.V. Flitman

Space Research Institute of RAS
117997, 84/32, Profsoyuznaya Str., Moscow, Russia
E-mail: info@smis.iki.rssi.ru

Earth remote monitoring distributed systems developed by IKI provide the end-user with a large spectrum of satellite data and its processing results with various related information. The access policy for various types of data also varies. The basic means of accessing the data are the designated cartographic web-interfaces installed on geographically distributed servers. The user has to pass the authentication procedure on any of the servers to get access to the interfaces depending on the rights for his account. Even more, a single interface can provide different sets of data for different accounts and account groups. This paper describes a web resources access control system providing authorized access for large amount of users with different access rights.

Keywords: information distributed systems, authentication, access control.