МУРЗИС – модуль усиленного режима защиты информационных систем

Задача разграничения прав доступа к приложениям и сервисам внутрикорпоративной сети и обеспечения защиты информации является важной и одновременно проблемной задачей для большинства средних и крупных организаций. Наиболее часто применяетсяее традиционное решение – внедрение одного из продуктов класса AMS (Access management System). В данной статье рассматривается web-приложение МУРЗИС, с помощью которого задача автоматизации разграничения прав доступа на основе ролевой модели решается достаточно просто и эффективно. Приложение разработано с учетом требований Постановления Правительства от 25 января 2013 года № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг», в котором предусмотрено создание Единой системы идентификации и аутентификации (ЕСИА), а также Методических рекомендаций по использованию ЕСИА. Приложение может применяться в качестве инструмента для реализации концепции «Единого входа» (Single Sign-One), позволяющей пользователю при однократном прохождении процедуры аутентификации получить доступ к множеству информационных ресурсов системы.

С. В. Кирюшкин, *эксперт*
stasvkir@gmail.com

А. Ф. Графов, *эксперт*
graftilly@mail.ru

Хорошо известно, что необходимым условием для внедрения AMS-систем на предприятии является четкая формализация бизнес-процессов управления доступом. Автоматизация процесса управления доступом в соответствии с логикой бизнес-процессов считается одной из основных функций AMS-систем. Ролевая модель управления доступом регламентирует процесс назначения типовых прав доступа.

Обобщенная архитектура системы управления доступом представлена на рис. 1 и представляет собой совокупность следующих взаимосвязанных модулей:

- web-сервера;
- сервера авторизации;
- хранилища данных о пользователях;
- хранилища правил доступа.

О продукте

Производителем данного продукта является компания ООО «Инновационные технологии в бизнесе» (www.itb.spb.ru), основным видом деятельности которой является разработка и реализация проектов информационной безопасности.

Приложение МУРЗИС разработано как web-приложение, работающее под управлением сервера приложений (Apache Tomcat или совместимого с ним). Оно позволяет обрабатывать запросы аналогично proxy-серверу, поддерживая при этом взаимодействие по протоколам HTTP и HTTPS. Приложение МУРЗИС устанавливается как корневой проект сервера приложений, так как это необходимо для устранения процесса внутреннего изменения запрашиваемого адреса.

Сервер Apache Tomcat является программным контейнером сервлетов (серверных приложений) и обеспечивает межсетевое взаимодействие. МУРЗИС и сервер Apache Tomcat взаимодействуют друг с другом в среде приложений Java JDK.

Приложение МУРЗИС предназначено для разграничения прав доступа пользователей к объектам (файлам, программам) и выполняет следующие функции:

- контроль доступа пользователей к защищаемым объектам;
- установление и изменение прав доступа пользователям к защищаемым объектам;

- идентификация и аутентификация пользователей;
- контроль целостности файлов МУРЗИС;
- регистрация и учет следующих событий:
- авторизация пользователя;
- доступ к защищаемому объекту;
- изменение или удаление файлов МУРЗИС.

Учетные записи системных пользователей («admin» и «system») регистрируются автоматически при установке приложения МУРЗИС. Все пользователи, кроме администратора «admin», имеют единственное право доступа к защищаемым объектам – «чтение». Администратор «admin» имеет право редактировать список пользователей и назначать им право доступа к защищаемым объектам. Системный пользователь «system» имеет право доступа к log-файлам.

МУРЗИС поддерживает единственный тип доступа – доступ на чтение информации по группе адресов из заданного проекта.

Объектом доступа является группа адресов, которая состоит из одного или более адресов. Адрес может представлять собой шаблон пути к ресурсу, синтаксис шаблона соответствует синтаксису, поддерживаемому пакетом java.util.regex, который содержится в Java SE 6.

В приложении МУРЗИС сущность (проект) является представлением защищаемой системы и определяется именем сервера, на котором расположена защищаемая система, портом, по которому происходит доступ, и общей частью пути кресурсам, предоставляемым защищаемой системой. Вышеперечисленные параметры могут быть определены отдельно для доступа по протоколу http и https.

Пользователь МУРЗИС характеризуется следующими параметрами: уникальным логином, паролем, списком https-сертификатов и списком ролей. Кроме того, каждому пользователю может быть присвоено условное наименование, которое не используется для авторизации, а служит только для упрощения администрирования системы.

Роль пользователя характеризуется уникальным наименованием роли и списком групп адресов, доступ на чтение информации по которым разрешен соответствующим пользователям.

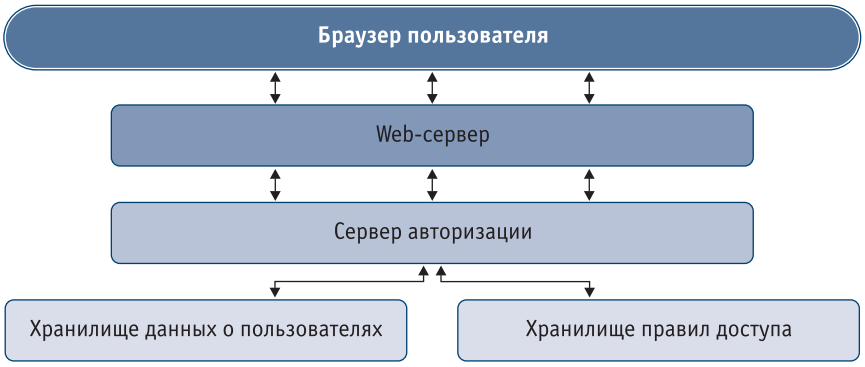

Рис. 1. ***Обобщенная архитектура системы управления доступом***

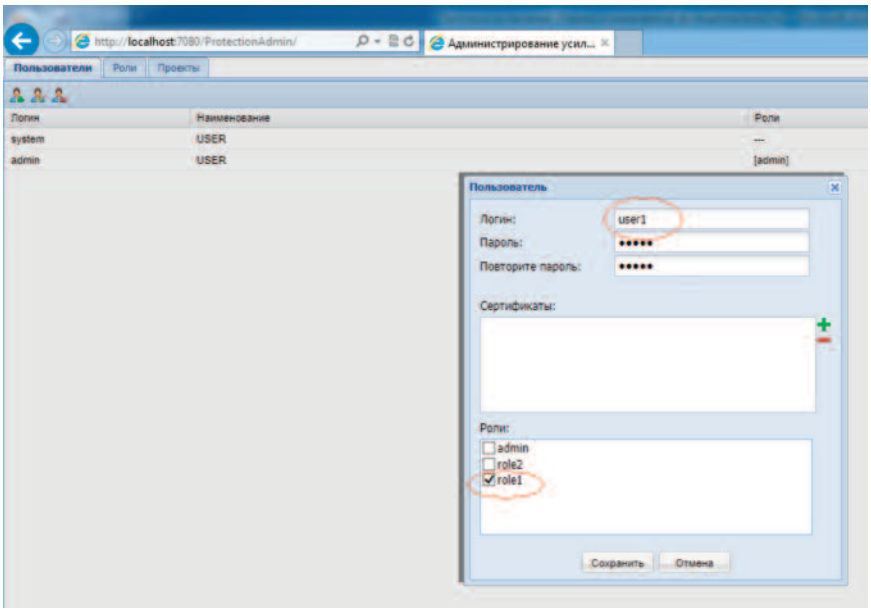

Рис. 2. ***Консоль администратора МУРЗИС***

Основными достоинствами программного средства МУРЗИС являются простота реализации, интуитивно понятный интерфейс и удобная настройка.

Схема работы пользователя МУРЗИС

Для того чтобы подключить программный продукт МУРЗИС к корпоративной сети предприятия, необходимо установить приложения на отдельно выделенную рабочую станцию и провести необходимые операции по его настройке.

Затем пользователю, зарегистрированному в базе данных МУРЗИС, предлагается возможность получить доступ к требуемым информационным ресурсам с помощью web-браузера. В случае если пользователь не авторизован, приложение МУРЗИС выдает ошибку протокола http 401, с необходимостью использования DIGEST-авторизации. В случае успешной авторизации на основании входящего URL определяется объект доступа, производится проверка доступа пользователя к данному объекту и, в случае успеха, осуществляется вызов запрашиваемого ресурса. При этом в заголовок запроса добавляется «SecurityUserId» равный имени пользователя МУРЗИС. В случае отсутствия прав доступа возвращается ошибка http 499. Если по заданному адресу URL запрашиваемый ресурс не может быть найден, пользователю возвращается ошибка http 404.

На рис. 2 представлен фрагмент работы администратора МУРЗИС по назначению прав доступа поль-

зователей к информационным ресурсам.

Аудит операций доступа к информационным ресурсам

Любая операция доступа к информационным ресурсам с помощью МУРЗИС влечет за собой запись в специальный файл протокола приложения следующей информации:

- даты и времени обращения;
- URL, по которому была произведена попытка доступа;
- логина и наименования пользователя, который совершил попытку доступа;
- наименования группы адресов, к которой принадлежит URL, если такая группа была определена (в том числе группы адресов, ответственная за действия, связанные с любыми изменениями в правилах доступа);
- http-код, который был возвращен в ответ на попытку доступа.

Текущий файл протокола создается ежедневно в 0:00:00, одновременно файл протокола предыдущего дня переименовывается и подписывается электронной подписью для контроля его целостности. Текущий файл протокола остается открытым для записи в течение всего дня, что предотвращает запись в него информации другими программами. Запись в текущий файл протокола и в файлы протокола за все предыдущие дни ограничивается средствами операционной системы, права на запись в текущий файл протокола имеет только пользователь, от имени которого запущен МУРЗИС.

Сертификат ФСТЭК России и эксплуатация

Приложение МУРЗИС отвечает требованиям по следующим показателям защищенности:

- идентификация и аутентификация;
- регистрация событий информационной безопасности (использование идентификационного и аутентификационного механизмов, регистрация попыток несанкционированного доступа к информации, доступ к информационным ресурсам, изменение или удаление файлов МУРЗИС);
- разграничение прав доступа к информационным ресурсам и целостность файлов приложения МУРЗИС.

Программное средство МУРЗИС в 2013 году успешно прошло сертификационные испытания в системе сертификации средств защиты информации по требованиям безопасности информации и имеет сертификат ФСТЭК России № 2953 от 09.09.2013.

Приложение МУРЗИС успешно применяется в одной из энергосбытовых компаний Санкт-Петербурга в качестве средства защиты от несанкционированного доступа к биллинговой системе компании. ■

НОВОСТИ