Практическая работа «JavaEE Security» в курсе «Разработчик JavaEE»

В рамках данного задания необходимо приобрести навыки разработки приложения, обеспечивающего механизмы разграничения доступа к ресурсам, а также научиться производить аутентификацию и авторизацию пользователей с использованием возможностей платформы JavaEE. В качестве задания слушателю предлагается реализовать механизм входа в информационную систему, используя возможности спецификации JAAS, а также научиться контролировать доступ к основным ресурсам, требующих подтверждение авторизации и проверки наличия необходимых ролей для работы с ними.

Работа будет включать следующие этапы:

1. Разработка/изменение страница входа пользователя с поддержкой спецификации JAAS.
2. Разработка RESTful-сервисов, предоставляющих возможность программного входа/выхода из приложения.
3. Декларативное объявление ролевого доступа к сервлетам, EJB, CDI-бинам и прочему бизнес-функционалу приложения.
4. Поддержка двухфакторной аутентификации (ДФА) *

Выполнение данного задания предполагает расширение возможностей существующего web-приложения из предыдущих домашних работ.

Итак, в рамках работы следует:

- Разработать стилизованную страницы входа в приложение с поддержкой *FORM*-метода аутентификации, используя стандартные механизмы, предлагаемые JavaEE Security. Важным является созданием класса, имплементирующего интерфейс LoginModule, производящего авторизацию на основе данных, хранящихся на уровне БД (таблица пользователей – логин и хэш-пароля). После успешной авторизации пользователю должны быть выданы права на основании связанной таблицы ролей.
- Предусмотреть RESTful веб-сервисы, предоставляющие возможность программной авторизации пользователя в приложении, а также возможного выхода из него.
- Добавить кнопку «Выход» на всех авторизованных страницах приложения (например, в разделе навигации).
- Предусмотреть на выбор слушателя разграничение ролевого доступа к бизнес-логике сервлетов, EJB и т.д. Необходимо иметь, как минимум две основных роли: рядовой пользователь и администратор, разграничивающих доступ к функционалу системы.
- Разработать интерфейсную часть для управлением справочником ролей с возможностью присвоения их пользователям системы. Данный функционал доступен только администраторам системы.
- Разработать сервисы и интерфейсную часть с поддержкой ДФА в системе. В данном задании не требуется реальной отправки смс-сообщения пользователя, это значение достаточно генерировать случайно на сервере (опциональное задание)*.