

по сравнению с типичными для интернета магазинами. Пользователи считают, что такие блог-магазины хорошо подходят для начинающих компаний, зарождающегося бренда, узко специализирующимся специалистам. Примерами таких блог-магазинов могут стать изготовление hand-made изделий, услуги массажного или косметологического кабинета, продажа собственной выпечки и кондитерских изделий.

Дизайнер не только может оформить внешний вид правильно и эстетично, но также прогрессировать рост продаж, рост репутации и укрепление на конкурентном рынке.

УДК 004.5; 766

Студ. К.С. Марченко
Науч. рук. ассист. С.А. Осоко
(кафедра информатики и веб-дизайна, БГТУ)

АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ НА САЙТАХ СРЕДСТВАМИ PHP

Аутентификация необходима для подтверждения личности зарегистрированного пользователя. Авторизация – для проверки его прав на доступ к определенным ресурсам. Аутентификация осуществляется по: паролю; одноразовому паролю; токену.

При *аутентификация по паролю* пользователь вводит username и password для идентификации и аутентификации в системе, по одному из стандартных протоколов например, HyperText Transfer Protocol, который использует механизмы: Basicaccessauthentication, FormsAuthentication и др.).

Аутентификация по одноразовым паролям обычно применяется как дополнительный уровень защиты. При этом пользователь должен предоставить данные двух типов: что-то, что он знает, и что-то, чем он владеет.

Аудентификация по токену использует один из распространенных форматов токенов для веб-приложений: SAML, JWT, SWT и др.

JSON Web Token (JWT) – содержит три блока, разделенных точками: заголовок, набор полей и подпись. Первые два блока представлены в JSON-формате и дополнительно закодированы в формат base64.

Основная идея JWT в использовании access token – маложивущего токена, выдаваемого сервером и хранящему информацию о пользователе и о самом токене. Refresh token – долгоживущий, выдается вместе с accesstoken в момент аутентификации и используется для его обновления после истечения срока его жизни.

Токены генерируются на сервере. Access token – основывается на секретном ключе, хранящемся на сервере, что позволяет защитить его от подмены. Refresh token хранится на сервере для учета доступа и валидации краденых токенов.