И. С. Клезович, Е. В. Рафалова
(*ГГУ имени Ф. Скорины, Гомель*)

ИСПОЛЬЗОВАНИЕ SPRING SECURITY ДЛЯ БАЗОВОЙ ЗАЩИТЫ ПРИЛОЖЕНИЯ

Spring Security – это мощный фреймворк для обеспечения безопасности Spring-приложений. Он предоставляет комплексные решения для аутентификации и авторизации пользователей, включая защиту паролей, управление сессиями и интеграцию с OAuth 2.0.

Процесс установки и базовой настройки Spring Security состоит из нескольких ключевых шагов.

Подключение зависимостей происходит с помощью элементов <groupId>, значение org.springframework.boot и <artifactId>, значение spring-boot-starter-security в родительском элементе </dependency> в конфигурационном файле pom.xml.

Далее необходимо произвести базовую настройку встроенного пользователя в файле конфигурации application.yml с указанием значений свойств name и password.

Конфигурация на основе ролей представлена в листинге 1:

Листинг 1

```
@EnableWebSecurity
public class SecurityConfig extends WebSecurityConfigurerAdapter
{
   @Bean
   public PasswordEncoder passwordEncoder() {
      return new BCryptPasswordEncoder();
   }
   @Override
   protected void configure(AuthenticationManagerBuilder auth)
throws Exception {
      auth.inMemoryAuthentication()
         .withUser("scorina")
           .password("theBest")
           .authorities("STUDENT");
}}
```

Spring Security автоматически предоставляет форму входа по адресу /login и страницу выхода по адресу /logout.

После настройки все URL будут защищены и доступны только авторизованным пользователям.

Система включает в себя несколько ключевых аспектов: пароли шифруются с использованием алгоритма BCrypt, что обеспечивает высокий уровень безопасности. Управление сессиями пользователей осуществляется эффективно, что позволяет гарантировать надежность взаимодействия. Также предусмотрена поддержка OAuth 2.0, что дает возможность аутентификации через социальные сети. Кроме того, реализована встроенная защита от CSRF-атак, что дополнительно укрепляет защиту системы. Приведенная базовая настройка обеспечивает надежную защиту приложения и может быть расширена в зависимости от конкретных требований проекта.

И. А. Красочка, Д. А. Артюх
(*ГрГУ имени Янки Купалы, Гродно*)

ЭФФЕКТИВНОСТЬ РАЗЛИЧНЫХ МЕТОДОВ ВОДЯНОГО ЗНАКА В КОНТЕКСТЕ ИИ-ГЕНЕРИРУЕМОГО АУДИО

В связи с развитием технологий искусственного интеллекта и широким распространением нейросетей, аудиофайлы не только стали важным форматом передачи информации, но и представляют собой объект для потенциальных атак, связанных с клонированием голоса и созданием поддельных аудиозаписей. С учетом этих угроз целью данной работы было исследование эффективности различных методов водяных знаков в контексте защиты аудиоконтента, созданного с использованием нейросетей.

В компьютерной криминалистике выделяют два основных подхода к защите аудиофайлов с помощью водяных знаков. Первый подход основан на встраивании малозаметных сигналов непосредственно в аудиофайл, что позволяет сохранять аутентичность звуковых данных и обнаруживать факт модификации. Второе направление связано с применением методов спектрального анализа и машинного обучения для выявления встроенных меток в измененных или сгенерированных нейросетями аудиофайлах.

Структура аудиофайлов различных форматов, таких как WAV, MP3, FLAC, позволяет применять методы цифровой обработки