УДК 004.774:614.8

# ВЕБ-ПРИЛОЖЕНИЕ ФИКСАЦИИ И АНАЛИЗА НАРУШЕНИЙ ПРОИЗВОДСТВЕННОЙ БЕЗОПАСНОСТИ НА ОПАСНОМ ПРОИЗВОДСТВЕННОМ ОБЪЕКТЕ

*Медведюк А.А.*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Воробей А.В. – магистр технических наук, ассистент кафедры ИПиЭ*

**Аннотация.** Разработано веб-приложение для фиксации и анализа нарушений производственной безопасности на опасных производственных объектах. Система построена по трёхуровневой архитектуре с использованием Spring Boot, PostgreSQL, WebSocket и Thymeleaf. Реализованы модули регистрации нарушений с категоризацией по степени тяжести, система экстренного оповещения (SOS), мониторинг местоположения персонала, контроль задач с таймерами безопасности, чек-листы, расчёт рисков и аналитика с экспортом отчётов в Excel и PDF. Предусмотрена ролевая модель доступа. Контейнеризация Docker обеспечивает воспроизводимость и масштабируемость.

**Ключевые слова:** производственная безопасность, веб-приложение, охрана труда, анализ нарушений, ОПО

***Введение.*** Обеспечение производственной безопасности на опасных производственных объектах (ОПО) является приоритетной задачей охраны труда. Ежегодно в мире фиксируются миллионы несчастных случаев, значительная часть – на предприятиях повышенной опасности [1]. В Республике Беларусь регулирование осуществляется на основании Закона «О промышленной безопасности» [2].

Традиционная фиксация нарушений с использованием бумажных журналов характеризуется низкой оперативностью и сложностью анализа данных [3]. Автоматизация мониторинга позволяет повысить скорость реагирования, прозрачность контроля и качество управленческих решений [4].

Цель работы – разработка веб-приложения для комплексной автоматизации фиксации и анализа нарушений промышленной безопасности на ОПО.

***Основная часть.*** Функциональные требования системы:

– регистрация нарушений с указанием категории, степени тяжести, геолокации и фото;
– управление заявками;
– система SOS;
– контроль задач с таймерами безопасности;
– электронные чек-листы и расчёт рисков;
– аналитика и экспорт отчётов;
– ролевая модель доступа (работник, специалист, администратор).

На рисунке 1 изображена архитектура веб-приложения фиксации и анализа нарушений производственной безопасности, простроенная по трёхуровневой модели: Presentation Layer, Business Logic Layer, Persistence Layer [5].

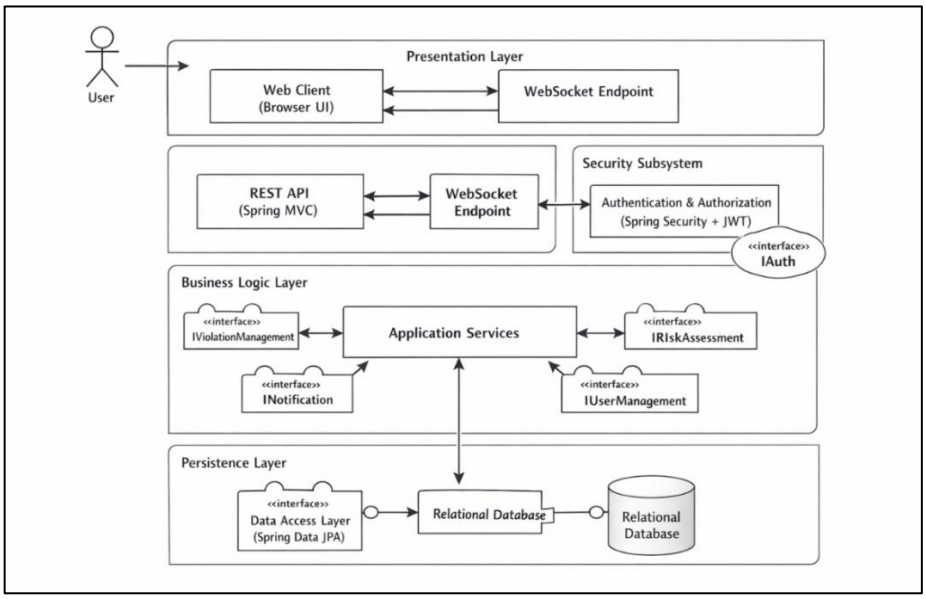


Рисунок 1 – Архитектура веб-приложения фиксации и анализа нарушений производственной безопасности

Уровень представления реализован на Thymeleaf и Bootstrap 5. Для функций реального времени используется WebSocket (STOMP / SockJS) [6].

Бизнес-логика реализована на Spring Boot 3.2. Аутентификация и авторизация выполняются с применением JWT (access – 24 ч, refresh – 7 дней) и 2FA.

Уровень доступа к данным основан на Spring Data JPA и PostgreSQL 15. Миграции выполняются с помощью Flyway. В таблице 1 представлен используемый технологический стек веб-приложения.

Таблица 1 – Технологический стек веб-приложения

| **Компонент** | **Технология** |
|---|---|
| Серверная платформа | Java 17, Spring Boot 3.2 |
| Безопасность | Spring Security, JWT, 2FA |
| Доступ к данным | Spring Data JPA, Hibernate |
| СУБД | PostgreSQL 15 |
| Миграции | Flyway |
| Реальное время | WebSocket (STOMP / SockJS) |
| Представление | Thymeleaf, Bootstrap 5, Leaflet.js |
| Отчётность | Apache POI (Excel), iText (PDF) |

Модель данных включает 22 сущности. Ключевая сущность «Violation» содержит категорию, степень тяжести (низкая, средняя, высокая, критическая), статус, описание, координаты и ссылки на фото.

Система реализует ролевую модель доступа, определяющую три уровня привилегий (таблица 2).

Таблица 2 – Ролевая модель доступа

| **Роль** | **Функциональные возможности** |
|---|---|
| Работник (USER) | Фиксация нарушений, подача заявок, отправка SOS-сигнала, обмен сообщениями, создание таймеров безопасности |
| Специалист (SPECIALIST) | Обработка SOS-сигналов, мониторинг таймеров и SOS-сигналов на карте, обработка заявок и нарушений, мониторинг персонала, оценка рисков, аналитика, работа с чек-листами, обмен сообщениями, экспорт отчётов |
| Администратор (ADMIN) | Полный доступ: управление пользователями, сервисами, новостями, аналитикой, экспорт отчётов, настройки системы |

Модуль обеспечения безопасности включает:

– SOS – отправка тревожного сигнала с геолокацией и мгновенной доставкой

специалистам через WebSocket.

– мониторинг местоположения – отображение персонала на карте (Leaflet.js) и журналирование маршрутов [7].

– таймеры безопасности – автоматическое уведомление при отсутствии подтверждения активности работника.

Аналитический модуль формирует отчёты по динамике нарушений, категориям, степени тяжести и статистике SOS. Поддерживается экспорт в Excel и PDF.

Информационная безопасность обеспечивается HTTPS (TLS), Spring Security, аннотациями @PreAuthorize и журналом аудита audit_log в соответствии с рекомендациями OWASP [8].

Контейнеризация Docker (docker-compose) позволяет развернуть систему и СУБД одной командой, обеспечивая переносимость и масштабируемость.

***Заключение.*** Разработано веб-приложение для автоматизации процессов фиксации и анализа нарушений производственной безопасности на ОПО. Система обеспечивает:

– оперативную регистрацию нарушений;

– экстренное оповещение с геолокацией;

– аналитическую обработку данных;

– ролевое разграничение доступа.

Использование WebSocket обеспечивает работу в реальном времени, а Docker – переносимость решения. Дальнейшее развитие предполагает внедрение методов машинного обучения для предиктивного анализа рисков.

### *Список литературы*

1. *International Labour Organization. World Statistic [Электронный ресурс]. – Режим доступа: https://www.ilo.org/. – Дата доступа: 01.03.2026.*

2. *О промышленной безопасности: Закон Респ. Беларусь, 5 янв. 2016 г., № 354-З // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/. – Дата доступа: 01.03.2026.*

3. *Петров, А.В. Автоматизация процессов управления охраной труда на промышленных предприятиях / А.В. Петров, И.С. Сидоров // Безопасность труда в промышленности. – 2022. – № 4. – С. 45–52.*

4. *Walls, C. Spring Boot in Action / C. Walls. – Shelter Island : Manning Publications, 2024. – 472 с. – ISBN 978-1-61729-254-5.*

5. *Richardson, C. Microservices Patterns: With Examples in Java / C. Richardson. – Shelter Island : Manning Publications, 2019. – 520 с. – ISBN 978-1-61729-454-9.*

6. *WebSocket Protocol / Internet Engineering Task Force (IETF). – RFC 6455 [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc6455. – Дата доступа: 01.03.2026.*

7. *Leaflet – an open-source JavaScript library for interactive maps [Электронный ресурс]. – Режим доступа: https://leafletjs.com/. – Дата доступа: 01.03.2026.*

8. *OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks [Электронный ресурс]. – Режим доступа: https://owasp.org/Top10/. – Дата доступа: 01.03.2026.*

UDC 004.774:614.8

# WEB APPLICATION FOR RECORDING AND ANALYSIS OF INDUSTRIAL SAFETY VIOLATIONS AT HAZARDOUS PRODUCTION FACILITIES

*Medvedyuk A.A.*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vorobey A.V. – Master of Sci., Assistant of the department of EPaE*

**Annotation**. A web application has been developed for recording and analyzing industrial safety violations at hazardous production facilities. The system is built on a three-tier architecture using Spring Boot, PostgreSQL, WebSocket and Thymeleaf. Modules for registration of violations with categorization by severity, an emergency notification system (SOS), staff location monitoring, task control with security timers, checklists, risk calculation and analytics with the export of reports to Excel and PDF have been implemented. A role-based access model is provided. Docker containerization ensures reproducibility and scalability.

**Keywords**: industrial safety, web application, occupational safety, violation analysis, HPF