УДК 004.056

Д.Н. КАЛАШНИКОВ, Е.В. МАТРОСОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

УСОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА УЧЕТА ЗАКАЗОВ И ИССЛЕДОВАНИЙ ПРОБ УРАНА С ПРИМЕНЕНИЕМ МЕТОДОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье рассматривается подход к повышению безопасности и надежности системы учёта заказов и исследований рудных проб урана в химико-физической лаборатории. С учётом высокой степени конфиденциальности и критичности данных ядерного анализа предложена методология разработки безопасного программного обеспечения, основанная на принципах SSDLC (Secure Software Development Lifecycle).

Постановка задачи. Процесс обработки и хранения данных о пробах урана требует строгого соблюдения норм информационной и радиационной безопасности. На практике нередко наблюдаются проблемы, связанные с отсутствием системного контроля доступа, незащищёнными каналами передачи данных и рисками несанкционированного изменения результатов исследований [1]. Целью работы является усовершенствование системы учёта лабораторных заказов и результатов анализа проб урана с использованием принципов безопасной разработки программного обеспечения.

Пути решения. В качестве решения предложен комплексный подход, включающий следующие направления:

1. Анализ угроз и моделирование рисков – выявление уязвимостей на этапах регистрации, хранения и передачи данных между подразделениями лаборатории и смежными организациями.

2. Безопасное проектирование – реализация модульной архитектуры с разграничением прав пользователей (лаборант, аналитик, инженер, руководитель проекта), принципом минимальных привилегий и контролем критических операций.

3. Шифрование и защита данных — использование криптографических алгоритмов AES-256 и RSA-2048 для защиты данных проб и протоколов испытаний, а также внедрение безопасных каналов обмена (TLS 1.3).

4. Аутентификация и контроль доступа – применение многофакторной аутентификации и ролевой модели безопасности с журналированием всех действий пользователей.

5. Тестирование и аудит – использование инструментов статического анализа исходного кода (SonarQube, OWASP Dependency-Check) и регулярное проведение тестов на проникновение.

6. Мониторинг и инцидент-менеджмент – создание защищённого журнала аудита с функцией автоматического оповещения о подозрительных действиях и аномалиях.

Новые идеи и результаты. Разработанный прототип системы обеспечивает разграничение доступа на уровне заказов и данных исследований в среде химико-физической лаборатории, специализирующейся на исследовании проб урана. Система обеспечивает сквозное шифрование данных, автоматический контроль целостности записей и отслеживание цепочки действий пользователя. [2]. Реализованы сценарии для различных категорий пользователей – от операторов пробоподготовки до инженеров-аналитиков и руководителей подразделений. Такой подход позволил оптимизировать маршрутизацию данных и сократить время обработки заказов. Кроме того, интеграция с существующими лабораторными измерительными комплексами позволила автоматизировать передачу результатов анализов, снизив влияние человеческого фактора и минимизировав вероятность искажения данных.

Заключение

Интеграция методов безопасной разработки в систему учёта лабораторных заказов и исследований проб урана позволяет достичь высокого уровня информационной защиты, минимизировать человеческий фактор и обеспечить соответствие требованиям отраслевых стандартов по кибербезопасности. Выводы.

1. Применение SSDLC позволяет встроить контроль безопасности в каждый этап разработки и эксплуатации лабораторных систем.

2. Реализация шифрования, многофакторной аутентификации и разграничения прав доступа повышает доверие к результатам исследований.

3. Внедрение механизмов мониторинга и аудита способствует раннему выявлению инцидентов и минимизации последствий возможных атак.

4. Разработанный подход может быть масштабирован на другие виды лабораторий, работающих с чувствительными материалами.

Список литературы

1. OWASP Foundation. OWASP Secure Software Development Lifecycle Project, 2024.

2. ISO/IEC 27034-1:2023. Information technology – Security techniques – Application security.