МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информатики и компьютерных систем

Аннотация к дипломной работе

«Разработка средства диагностики соблюдения политики информационной безопасности с использованием инструментария Jira»

Авдеенко Дарья Олеговна

Научный руководитель — ст. преподаватель Бондаренко Ю. А.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 56 страниц, 15 рисунков, 8 источников.

ДИАГНОСТИКА БЕЗОПАСНОСТИ, JIRA, ПОЛИТИКА БЕЗОПАСНОСТИ, СОТРУДНИК, МОНИТОРИНГ

Объект исследования: процессы соблюдения политики безопасности сотрудника в компании.

Цель работы: разработка средства диагностики соблюдения политики безопасности сотрудника с использованием инструментария Jira для повышения уровня безопасности информации.

Методы исследования: теоретический (анализ, синтез, сравнение) и экспериментальный (моделирование, тестирование, обработка данных).

Результаты работы: разработан и внедрен инструмент для мониторинга и диагностики соблюдения политики безопасности сотрудника. В ходе работы проведен анализ текущих методов и средств обеспечения информационной безопасности в компании, выявлены слабые места и предложены пути их устранения. Инструмент интегрирован с существующей системой управления проектами Jira, что позволило автоматизировать процесс диагностики и снизить человеческий фактор. Экспериментальная проверка показала, что внедрение разработанного средства значительно повысило уровень информационной безопасности компании и снизило количество нарушений.

Степень внедрения: система находится на этапе опытной эксплуатации в компании. Ожидается, что после завершения испытательного периода она будет полностью интегрирована и использована на постоянной основе.

РЭФЕРАТ

Дыпломная работа: 56 старонак, 15 малюнкаў, 8 крыніц.

ДЫЯГНОСТЫКА БЯСПЕКІ, JIRA, ПАЛІТЫКА БЯСПЕКІ, СУПРАЦОЎНІК, МАНІТОРЫНГ

Аб'ект даследавання: працэсы выканання палітыкі бяспекі супрацоўніка ў кампаніі.

Мэта працы: Распрацаваць сродак дыягностыкі выканання палітыкі бяспекі супрацоўніка з выкарыстаннем інструментаў Jira для павышэння ўзроўню інфармацыйнай бяспекі.

Метады даследавання: тэарэтычны (аналіз, сінтэз, параўнанне) і эксперыментальны (мадэляванне, тэставанне, апрацоўка дадзеных).

Вынікі працы: быў распрацаваны і ўкаранёны інструмент для маніторынгу і дыягностыкі выканання палітыкі бяспекі супрацоўніка. Падчас працы быў праведзены аналіз сучасных метадаў і сродкаў забеспячэння інфармацыйнай бяспекі ў кампаніі, выяўлены слабыя месцы і прапанаваны шляхі іх ліквідацыі. Інструмент быў інтэграваны з існуючай сістэмай кіравання праектамі Jira, што дазволіла аўтаматызаваць працэс дыягностыкі і знізіць чалавечы фактар. Эксперыментальная праверка паказала, што ўкараненне распрацаванага сродку значна павысіла ўзровень інфармацыйнай бяспекі кампаніі і знізіла колькасць парушэнняў.

Ступень укаранення: сістэма знаходзіцца на этапе вопытнай эксплуатацыі ў кампаніі. Чакаецца, што пасля заканчэння выпрабавальнага перыяду яна будзе поўнасцю інтэграваная і выкарыстоўваецца на пастаяннай аснове.

ABSTRACT

Diploma thesis: 56 pages, 15 figures, 8 sources.

SECURITY DIAGNOSTICS, JIRA, SECURITY POLICY, EMPLOYEE, MONITORING

Object of research: employee security policy compliance processes in the company.

Purpose of work: To develop a tool for diagnosing employee security policy compliance using Jira tools to enhance information security levels.

Methods of research: theoretical (analysis, synthesis, comparison) and experimental (modelling, testing, data processing).

Results of work: A tool for monitoring and diagnosing employee security policy compliance was developed and implemented. During the research, current methods and tools for ensuring information security in the company were analyzed, weaknesses were identified, and solutions were proposed. The tool was integrated with the existing project management system, Jira, automating the diagnostic process and reducing human error. Experimental verification showed that the implementation of the developed tool significantly increased the company's information security level and reduced the number of violations.

Degree of implementation: The system is in the pilot operation stage in the company. It is expected that after the trial period, it will be fully integrated and used on a permanent basis.