УДК 004.4'24.056.52:336.764./768(045)
DOI https://doi.org/10.32689/maup.it.2024.1.6

Наталія ГУЛАК
кандидат технічних наук,
доцент кафедри комп'ютеризованих систем захисту інформації,
Національний авіаційний університет, gulak_n@ukr.net
***ORCID:** 0009-0000-9584-7113*

Андрій МАЙСТРЕНКО
магістр, асистент кафедри комп'ютеризованих систем захисту інформації,
Національний авіаційний університет, hondor553@gmail.com
***ORCID:** 0009-0002-1612-9178*

АВТОМАТИЗАЦІЯ МОДУЛЯ ІНФОРМАЦІЙНИХ АКТИВІВ

Анотація. *Стаття докладно розглядає процес автоматизації модуля інформаційних активів як ключовий етап у забезпеченні ефективного управління інформаційною безпекою в сучасних організаціях. Основний акцент робиться на використанні ORM фреймворків, зокрема Hibernate, як засобу спрощення доступу до бази даних та оптимізації управління інформаційними ресурсами.* ***Мета роботи*** *цієї статті полягає у вивченні можливостей підвищення рівня захищеності інформаційних активів через автоматизацію модуля управління ними. Для досягнення цієї мети використано методологію розробки та імплементації програмного модуля на основі Hibernate ORM фреймворку та Java Persistence API. В статті детально описано етапи розробки та впровадження модуля, включаючи інвентаризацію, категоризацію та автоматизацію управління активами. Надано огляд основних переваг використання Hibernate, таких як підвищення продуктивності та надійності системи. Детально проаналізовано критерії ефективності розробленого рішення, включаючи надійність, захищеність, швидкість роботи та доступність.* ***Наукова новизна*** *полягає в застосуванні сучасних технологій для підвищення ефективності та надійності управління інформаційною безпекою. Зроблено висновок про значний внесок автоматизації модуля у підвищення ефективності управління інформаційною безпекою та полегшення користування системою.* ***Висновки*** *статті підтверджують успішність використання ORM фреймворків для автоматизації управління інформаційними активами, що призводить до покращення ефективності та забезпечення високого рівня захисту даних.* ***Ключові слова:*** *інформаційні активи, управління інформаційною безпекою, ORM фреймворки, оцінка ризиків, захист інформаційних активів, система менеджменту інформаційної безпеки.*

Nataliia GULAK, Andrii MAISTRENKO. AUTOMATION OF THE INFORMATION ASSETS MODULE

Abstract. *The article examines in detail the process of automating the information assets module as a key stage in ensuring effective management of information security in modern organizations. The main emphasis is on the use of ORM frameworks, in particular Hibernate, as a means of simplifying access to the database and optimizing the management of information resources.* ***The purpose*** *of this article is to study the possibilities of increasing the level of security of information assets through the automation of their management module. To achieve this goal, the methodology of developing and implementing a software module based on the Hibernate ORM framework and the Java Persistence API was used. The article describes in detail the stages of development and implementation of the module, including inventory, categorization and automation of asset management. An overview of the main benefits of using Hibernate, such as improved system performance and reliability, is provided. The criteria for the effectiveness of the developed solution were analyzed in detail, including reliability, security, speed of operation and availability.* ***Scientific novelty*** *consists in the application of modern technologies to increase the efficiency and reliability of information security management. It was concluded that the automation of the module made a significant contribution to improving the efficiency of information security management and facilitating the use of the system.* ***The conclusions*** *of the article confirm the success of using ORM frameworks for automating the management of information assets, which leads to improved efficiency and ensuring a high level of data protection.* ***Key words:*** *information assets, information security management, ORM (Object Relational Mapping) frameworks, system integration, risk assessment, protection of information assets.*

Вступ. Широке впровадження сучасних інформаційних технологій пов'язане, поряд з раціональним використанням ресурсів розподіленої комп'ютерної мережі, з організацією ефективної протидії загрозам атак на її інфраструктуру. Постійні зміни в конфігурації системи, її параметрах і складі програмного забезпечення вимагають постійного аналізу стану безпеки системи, передбачення та виявлення нових загроз безпеці та застосування превентивних заходів. Автоматизація модуля «Інформаційні активи» є лише першим кроком у напрямку покращення системи управління інформаційною безпекою компанії. Подальші дослідження та розвиток дозволять розширити можливості системи і підвищити її ефективність у забезпеченні безпеки та ефективності використання інформаційних ресурсів.

Головна частина. Модуль обліку інформаційних активів використовується для автоматизації діяльності власників інформаційних активів. Головною метою автоматизації каталогу інформаційних активів є оптимізація та вдосконалення системи управління інформаційної безпеки (ІБ).

До інформаційних активів компанії зазвичай відносять інформацію, апаратне, програмне забезпечення та інші засоби, необхідні для отримання, обробки та зберігання даних, що використовуються у певних бізнес-процесах. Це може бути сховища даних, бази даних, бази клієнтів, виробничі показники (звіти), фінансові звіти, інформаційні системи тощо.

Система повинна забезпечувати єдину інформаційну інфраструктуру у системі менеджменту інформаційної безпеки (СМІБ), що створюється через інтеграцію максимальної кількості інформації в модулі і, тим самим, що дозволяє удосконалювати інформаційну проникність і синергію між структурними підрозділами.

За класифікацією автоматизованих комплексів система, яка розглядається, відноситься до багатофункціональних програмно-технічних комплексів для автоматизації управління організаційними процесами в умовах розподіленого використання інформації різними фахівцями.

Для ефективної роботи таких систем необхідно щоб були виконані наступні вимоги: забезпечення необхідного обсягу інформації; механізм своєчасної актуалізації змісту та базовий набір сервісів роботи з інформацією; створення інтуїтивно зрозумілих інтерфейсів для користувачів; надання послуг, що мають очевидну цінність; можливість вибору типового профілю для користувачів.

Основними принципами створення СМІБ є використання програмного і апаратного забезпечення, здатного працювати з мережею Інтернет; відповідність міжнародним стандартам у сфері ІБ; уніфікація форматів і протоколів інформаційного обміну; використання ефективних методів захисту від несанкціонованого доступу [2].

Особливу увагу потрібно звернути на людський фактор, який відіграє не останню роль як джерело загрозі інформації. Для цього передбачено три основні категорії користувачів: авторизований користувач, адміністратор і супер-адміністратор. Кожен користувач має права і обов'язки відповідно до свого рівня доступу. Коректний розподіл певних прав користувачів надає можливість виконувати конкретні дії з різними типами документів, що знижує ризики незаконного розкриття інформації [1].

Виходячи з політики системи управління інформаційної безпеки (СУІБ) задачі модернізації і розвитку автоматизованих комплексів полягають у наступному: розширенню функціональності для більш ефективного управління інформаційними активами; інтеграції із сучасними технологіями та стандартами безпеки; підтримка масштабованості та гнучкості системи для відповіді на зростаючі потреби користувачів; створення гнучкої архітектури системи, що дозволяє легко додавати нові функції та модулі [3].

«Автоматизація модуля інформаційних активів» має на меті оптимізацію та удосконалення управління інформаційною безпекою. Заснована на застосуванні ORM Фреймворку, вона спрощує роботу з базами даних, забезпечуючи швидкість та масштабованість. Головною метою є забезпечення централізованого зберігання та оцінка ризиків для кожного окремого інформаційного активу відповідно до міжнародних стандартів. Рішення включає функції з розробки плану обробки ризиків, розмежування прав доступу користувачів, відправлення повідомлень власникам активів та побудову звітів. Забезпечується оперативна підтримка інформації, що дозволяє використовувати дані для управління ризиками та інцидентами. Автоматизація модуля сприяє підвищенню продуктивності управління інформаційною безпекою, що є важливим умовою при обмеженому числі персоналу та великій кількості облікових об'єктів [4].

Об'єктом автоматизації є модуль управління інформаційними активами, спрямований на оптимізацію та покращення системи управління інформаційною безпекою в організації. Цей модуль містить інструменти для централізованого зберігання інформації про всі об'єкти оцінки ризиків, а також проведення класифікації та оцінки ризиків для кожного інформаційного активу відповідно до міжнародних стандартів. Об'єкт автоматизації надає можливість розробки планів обробки ризиків, налаштування прав доступу користувачів, сповіщення власників активів та створення звітів. Основною метою автоматизації є забезпечення ефективного управління інформаційною безпекою організації та підвищення його ефективності в умовах обмежених ресурсів та великої кількості облікових об'єктів.[5]

Рішення для автоматизації модуля інформаційних активів реалізоване на основі програмного забезпечення з закритим вихідним кодом і є готовим інструментом для оцінки та обробки ризиків інформаційних активів компанії. Для користування системою не потрібна установка додаткових клієнтських програм, адже достатньо наявності будь-якого сучасного веб-браузера.

Впровадження даного рішення сприяє підвищенню ефективності управління інформаційною безпекою, спрощує процес оцінки та обробки ризиків і забезпечує зручний доступ до необхідної інформації для зацікавлених сторін.

Процес автоматизації спрямований на оптимізацію та покращення системи управління інформаційною безпекою, а також на створення реєстру інформаційних активів і керування записами. Це є центральною точкою, де зберігаються дані про всі активи компанії, визначається їхнє значення, вплив на

бізнес-процеси та подальше використання цих даних у модулі [6].

- Створення довідників активів компанії.
- Оцінка критичності об'єктів захисту.
- Класифікація активів та їх передача в модуль.
- Інтеграція з системами інвентаризації.
- Створення єдиного інформаційного середовища для спільної роботи з суміжними системами.

Проект автоматизації модуля інформаційних активів включає наступні етапи:

1. Інвентаризація інформаційних активів: Визначення всіх інформаційних активів компанії та їх поточний стан.

2. Категоризація інформаційних активів: Визначення ключових активів, які впливають на функціонування бізнес-процесів компанії.

3. Логічне проектування процесу управління каталогом інформаційних активів: Структурування, опис та проектування процесів для подальшої автоматизації.

4. Автоматизація процесу управління каталогом інформаційних активів: Реалізація автоматизації управління каталогом для забезпечення ефективності та точності процесів.

5. Проектування розроблених процесів на систему автоматизації. Імплементація та налагодження розроблених процесів на систему автоматизації з метою їх подальшого використання.[9]

В результаті автоматизації модуля інформаційних активів формується перелік активів, визначається їхня критичність з урахуванням впливу на бізнес-процеси компанії, а також створюються матриці доступу для розподілу прав до інформаційних активів.

Код модуля «Інформаційні активи» використовує ORM (Object Relational Mapping) фреймворк для забезпечення зручного доступу до бази даних. ORM дозволяє розробникам працювати з об'єктами даних, не звертаючись безпосередньо до SQL запитів (рис. 1).

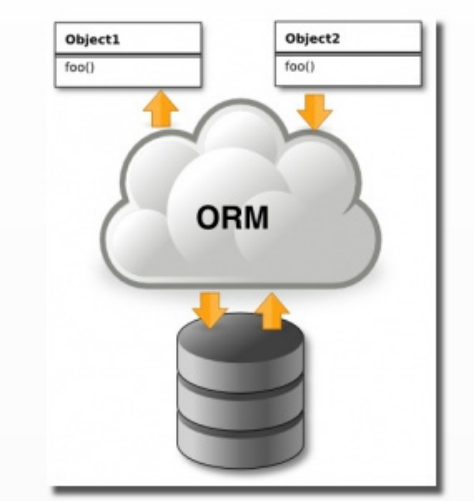

Рис. 1. Структурна схема роботи ORM Фреймворку

В реалізації модуля використовується Hibernate ORM, який є реалізацією специфікації JPA (Java Persistence API). Hibernate спрощує взаємодію з базою даних, адже він автоматично генерує SQL запити на основі об'єктів Java.[10]

Основні переваги використання Hibernate для цього модуля:

- Спрощення роботи з базою даних за рахунок автоматичної генерації SQL запитів.
- Зручний доступ до даних у вигляді об'єктів Java, що полегшує розробку та збереження коду.
- Підтримка високої продуктивності та швидкодії завдяки оптимізації запитів та кешуванню даних.

Крім того, важливою перевагою Hibernate є можливість легкої масштабованості та розширення функціональності за рахунок його гнучкої архітектури.

Для поліпшення роботи СМІБ необхідно проведення робіт з оцінки та обґрунтування різних заходів які можуть забезпечити необхідний рівень захищеності інформаційних активів.[7]

Для оцінки ефективності розробленого програмного продукту необхідно обрати критерії за якими вони будуть порівнюватися.[8]

Перша оцінка була проведена за критеріями (рис. 2): надійність, захищеність, швидкість роботи, доступність.

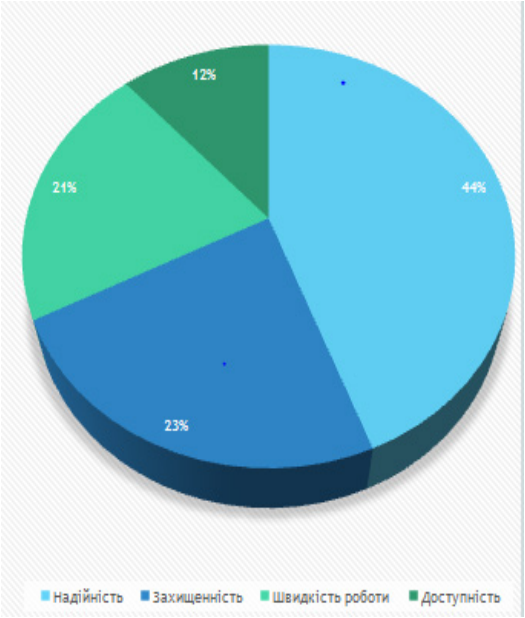

Рис. 2. Кругова діаграма оцінки ефективності за першими критеріями

Друга оцінка ефективності розробленого продукту була проведена за наступними критеріями (рис.3): переносимість, зручність супроводу, ефективність, зручність використання, функціональність.

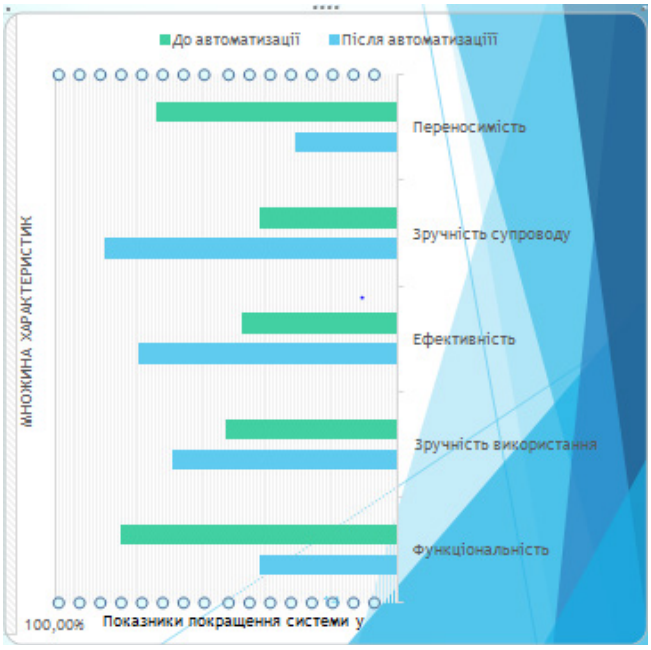

Рис. 3. Показники покращення системи

На основі оцінки ефективності проведеної автоматизації модуля удалося підвисити такі показники: зручність супроводу, ефективність, зручність використання.

Висновки:

1. У процесі розробки модуля "Інформаційні активи" було виявлено, що використання ORM фреймворків, зокрема Hibernate, значно спрощує доступ до бази даних і полегшує управління інформаційними активами компанії. Це дозволяє швидко реалізувати функціонал модуля і забезпечити його високу продуктивність та надійність.

2. Додавання нових можливостей до модуля, таких як інтеграція з іншими системами управління, підтримка розширених звітів та аналітичних інструментів, зробить систему ще більш універсальною та корисною для користувачів, тобто розширить її функціональність.

Список використаних джерел:

1. ДСТУ ISO/IEC 27007:2018: Настанова щодо аудиту систем керування інформаційною безпекою.
2. ДСТУ ISO/IEC 27001: Система менеджменту інформаційної безпеки.
3. Електронний ресурс Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури: http://www.dsszzi.gov.ua/dsszzi/control/ uk/publish/ Режим доступу: вільний.
4. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах. Навчальний посібник. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
5. Інформаційна та кібербезпека: соціотехнічний аспект / В.Бурячок, В. Толубко, В. Хорошко, С. Толюпа. – Київ: ДУТ, 2015. 288 с.
6. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії /Ю. Когут. –Київ: вид-во консалтингова компанія Сидкон, 2021. 364 с.
7. Корченко О.Г. Менеджмент інформаційної безпеки: навчальний посібник/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с.
8. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
9. Остапов С. Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. 476 с.
10. Bauer C. Java Persistence with Hibernate / C. Bauer, G. King, G. Gregory. – New York, USA: Manning Publications, 2016. 960 с. – (2nd edition).