

## МЕТОДИ БАГАТОРІВНЕВОГО АНАЛІЗУ ПРИВАТНОСТІ БІЗНЕС-ПРОЦЕСІВ

Єрохін М. А.

Науковий керівник – д.т.н., проф. Філатов В. О.

Харківський національний університет радіоелектроніки, каф. ШІ,  
м. Харків, Україна

e-mail: [maksym.ierokhin@nure.ua](mailto:maksym.ierokhin@nure.ua)

Proper business process management is a pivotal area for improving the organizational efficacy. Rare research concerns the comprehensive analysis of both BPMN model and the model execution. Moreover, the modern privacy challenges and data flows are scarcely investigated within existing works. This report provides an outlook of the privacy analysis methods in PE-BPMN models, including SQL workflows in collaborative processes. The privacy policies are integrated into the PE-BPMN models and the unwanted data disclosures are identified using novel Pleak tools, advancing the awareness of privacy issues.

Згідно з новітніми нормативними актами з питань контролю та захисту даних, такими як GDPR та LGPD, використання конфіденційних даних має бути обмежене ціллю, для якої вони були зібрані. В контексті бізнес-процесів цей принцип передбачає, що актори та їх пули, залучені до виконання бізнес-процесу, повинні мати доступ до приватних даних лише в мінімально необхідній мірі. Кількісний та якісний аналіз приватності відбувається на рівні моделі та не передбачає імітацію виконання моделі в динаміці [1]. Якщо модель побудована на журналах подій, то до них можливо застосувати евристики для покращення відповідності BPMN моделі реальному виконанню процесу [2].

Для перевірки дотримання політик конфіденційності бізнес-процесу необхідно визначити, хто має доступ до приватних даних, за яких умов і в якій мірі. В інформаційних системах одним із основних способів збереження та обміну даними є СУБД та відповідні SQL запити. У контексті бізнес-процесів до моделей з посиленою приватністю PE-BPMN було додано стереотипи для задання політик приватності для кожного пула акторів, а також SQL запити, які необхідні для кожної задачі актора.

Мінімізація витоків даних передбачає не лише визначення того, хто має пряий доступ до певного набору даних, але також хто має доступ до похідних до цього набору даних через ланцюги операцій, обчислень та обмін повідомленнями. Деякі з вузлів обробки приватних даних можуть бути захищені технологіями підвищення конфіденційності (PET), такими як шифрування, обчислення з багатьма учасниками та диференційна приватність [3]. Технології приватності та SQL запити для обміну даними та задання політик додаються за допомогою нестандартних стереотипів

ВРМН. Для обробки складних багатоагентних циклічних ВРМН моделей було застосовано метод розгортання мереж Петрі.

Аналіз SQL потоків відбувається на рівні побудованої мережі Петрі.

Вихідними даними аналізаторів є звіти щодо об'єктів витоків, розподілу шуму, чуттєвості припущень потенційного зловмисника при використанні технологій диференційної приватності, а також звіт щодо покрокових умов появи прямих та непрямих витоків (рис. 1).

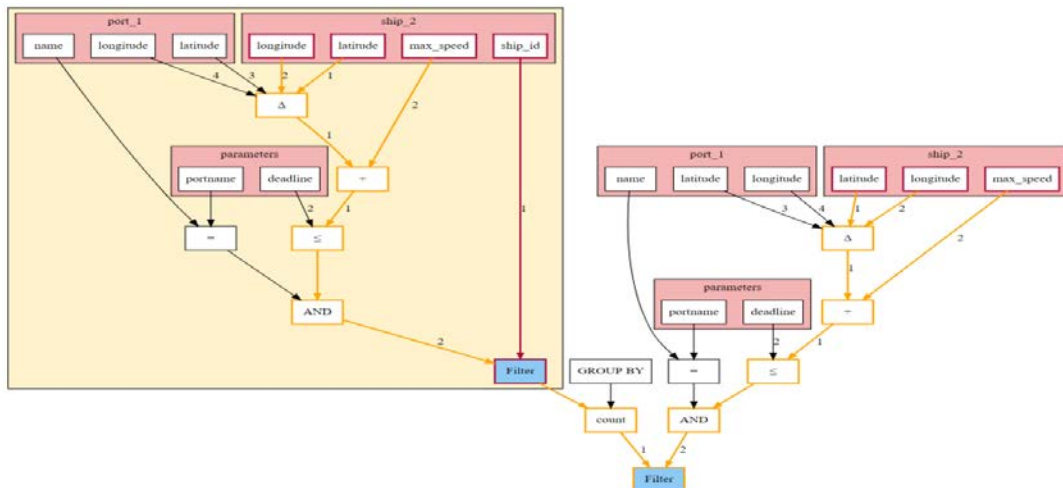


Рисунок 1 – Приклад звіту про умови витоків в ВРМН моделі

Під час кількісного та якісного аналізу програмний комплекс дозволяє отримати відповіді на запитання: «Які дані витікають під час обміну між пулами? За яких обставин? Наскільки багато даних витікає при несанкціонованому доступі?».

З посиленням державних вимог дотримання конфіденційності даних та їх похідних методи та інструменти аналізу різноманітних витоків стають об'єктом досліджень, зокрема в контексті моделей ВРМН.

Інформаційна технологія Pleak призначена для кількісного та якісного аналізу PE-BPMN моделей та поступово розширює інструментарій для аналізу моделей різного ступеню складності та з урахуванням різноманітних технологій збереження конфіденційності.

Список використаних джерел:

1. Filatov V., Yerokhin M. Improved multiobjective optimization in business process management using R-NSGA-II. Radio Electronics, Computer Science, Control. 2023. No 3. P. 187–193.
2. Discovering business process simulation models in the presence of multitasking and availability constraints / B. Estrada-Torres et al. Data and Knowledge Engineering. 2021. Vol. 134, No. 1. P. 1–20.
3. Multi-level privacy analysis of business processes: the PLEAK toolset / M. Dumas et al. International Journal on Software Tools for Technology Transfer. 2022. Vol. 24. P. 183–203.