

Омельченко М.Я., магістрант
*Київський національний економічний
університет імені Вадима Гетьмана*
m.omelchenko67@gmail.com

Крошко І.А., аспірант
*Київський національний економічний
університет імені Вадима Гетьмана*

БЕЗПЕКА ДАНИХ У СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ: ЗАГРОЗИ ТА ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ

У сучасних умовах цифрової трансформації системи підтримки прийняття рішень (Decision Support Systems, DSS) відіграють ключову роль у забезпеченні ефективного управління бізнес-процесами, фінансовими потоками та стратегічним розвитком організацій. Зростання обсягів даних, використання інтелектуальних алгоритмів і залучення зовнішніх джерел інформації підвищують залежність якості управлінських рішень від достовірності та цілісності даних. У таких умовах безпека даних у DSS набуває особливого значення, оскільки навіть незначні спотворення або несанкціоновані зміни можуть призводити до суттєвих управлінських помилок. При цьому традиційні підходи до захисту інформаційних систем є недостатніми, оскільки не враховують специфіку аналітичних моделей і семантичну цілісність даних, що використовуються у процесі прийняття рішень [1].

З урахуванням специфіки функціонування систем підтримки прийняття рішень ключові загрози пов'язані не лише з несанкціонованим доступом до даних, а передусім із можливістю їх прихованого спотворення, модифікації логіки обробки та маніпулювання результатами аналітики. Вразливість таких систем зумовлена їх багаторівневою архітектурою, використанням різнорідних джерел інформації та інтеграцією інтелектуальних моделей, що ускладнює своєчасне виявлення атак і підвищує ризик формування некоректних управлінських рішень.

До основних загроз, характерних для систем підтримки прийняття рішень, належать [2-5]:

- спотворення вхідних даних на етапі їх збору та інтеграції, зокрема шляхом внесення формально коректної, але недостовірної інформації;
- несанкціонована зміна алгоритмів обробки даних, моделей або розрахункових показників, що призводить до систематичних помилок у результатах;
- атаки на інтелектуальні компоненти, зокрема отруєння навчальних вибірок або маніпуляція вхідними даними під час експлуатації моделей;
- перехоплення або несанкціонований доступ до результатів аналітики та візуалізацій, що містять конфіденційні показники;
- загрози, пов'язані з людським фактором, зокрема внутрішні порушення, надмірна довіра до результатів системи та застосування методів соціальної інженерії.

Зазначені загрози мають різну природу та проявляються на різних рівнях функціонування систем підтримки прийняття рішень. Вони зумовлені як архітектурними особливостями DSS, так і використанням інтелектуальних моделей, що розширює поверхню атак та ускладнює забезпечення цілісності даних і результатів аналітики.

Сучасні DSS мають багаторівневу структуру, де кожен рівень пов'язаний із специфічними ризиками [1].

Рівень консолідації даних (Data Ingestion & ETL) є вразливим до так званих семантичних атак, коли до системи надходять формально коректні, але змістовно викривлені дані. У результаті використання такої інформації формується некоректна

аналітична база для прийняття рішень. Особливої актуальності ця проблема набуває при використанні зовнішніх джерел даних, зокрема відкритих даних та соціальних медіа, достовірність яких складно перевірити.

На рівні обробки та аналітичного ядра (OLAP, моделі) виникають ризики несанкціонованої зміни алгоритмів і формул розрахунку агрегованих показників. У складних багатовимірних системах такі зміни можуть залишатися непоміченими протягом тривалого часу та призводити до систематичних помилок у звітності.

Рівень візуалізації та представлення результатів (Dashboards) характеризується ризиками перехоплення сесій, атак типу «людина посередині», а також витоку інформації через несанкціонований доступ до інтерфейсів, що містять конфіденційні показники.

Із впровадженням інтелектуальних систем, що базуються на методах машинного навчання, безпека DSS набуває нових характеристик і переходить у площину протидії математичним атакам. Однією з ключових загроз є отруєння даних (data poisoning), коли зловмисник впливає на процес навчання моделі шляхом внесення спеціально сформованих даних, що призводить до появи прихованих вразливостей у її поведінці [3].

Іншою загрозою є атаки ухилення (evasion attacks), які полягають у модифікації вхідних даних на етапі використання моделі з метою отримання бажаного результату без явних ознак втручання.

У цих умовах важливим підходом до забезпечення безпеки є використання пояснюваних моделей (Explainable AI), що дозволяють обґрунтовувати отримані результати та виявляти аномальні або потенційно скомпрометовані рішення.

Ураховуючи складність наведених загроз, забезпечення безпеки систем підтримки прийняття рішень потребує комплексного підходу, що охоплює не лише захист даних і моделей, а й ефективне управління доступом до інформації та результатів аналітики. Особливого значення набуває впровадження гнучких механізмів контролю доступу, які дозволяють обмежити можливість несанкціонованого впливу на дані, моделі та аналітичні результати.

У системах підтримки прийняття рішень доступ до даних і функціональних можливостей має бути максимально гранульованим і диференційованим відповідно до ролей користувачів та умов використання системи. Рольова модель керування доступом (Role-Based Access Control, RBAC) передбачає надання прав доступу відповідно до функціональних обов'язків користувача, що забезпечує базову структуру доступу до ресурсів системи. Водночас у складних DSS доцільним є застосування атрибутивного підходу (Attribute-Based Access Control, ABAC), який дозволяє враховувати контекст доступу, зокрема місце перебування користувача, тип використовуваного пристрою, мережеве середовище або рівень допуску до інформації. Такий підхід забезпечує більш гнучке та адаптивне управління доступом [4].

Додатковим механізмом є обмеження доступу на рівні рядків даних (Row-Level Security, RLS), що дозволяє забезпечити доступ користувачів лише до релевантних фрагментів інформації відповідно до їх зони відповідальності. Це дає змогу використовувати єдину аналітичну модель для всієї організації, одночасно забезпечуючи контрольоване розмежування доступу до даних.

Поряд із механізмами контролю доступу важливим складником забезпечення безпеки DSS є організація моніторингу, аудиту та контролю цілісності даних. Зокрема, необхідним є впровадження механізмів відстеження походження даних (data lineage), що дозволяє простежити процес формування аналітичних показників від первинних джерел до кінцевих результатів. Це забезпечує можливість виявлення джерел спотворення даних і підвищує прозорість процесів прийняття рішень. Додатково доцільним є використання журналювання змін, контролю версій моделей та регулярного аудиту аналітичних алгоритмів [5].

Важливу роль відіграє також застосування сучасних криптографічних підходів, зокрема технологій конфіденційних обчислень, що дозволяють виконувати обробку даних без їх розкриття у відкритому вигляді. Це є особливо актуальним для хмарних середовищ, де виникає потреба у забезпеченні конфіденційності даних під час їх передачі та аналізу.

За результатами дослідження встановлено, що безпека даних у системах підтримки прийняття рішень має розглядатися як комплексна характеристика, що охоплює цілісність даних, надійність моделей, контроль доступу та прозорість аналітичних процесів. Ефективне забезпечення безпеки DSS сприяє підвищенню достовірності управлінських рішень і зниженню ризиків, пов'язаних із використанням недостовірної або скомпрометованої інформації.

У сучасних умовах безпека систем підтримки прийняття рішень трансформується із задачі технічного захисту у задачу забезпечення достовірності та обґрунтованості управлінських рішень. Це вимагає інтеграції механізмів контролю даних, моделей і доступу в єдину систему управління безпекою. Такий підхід дозволяє підвищити стійкість DSS до зовнішніх і внутрішніх загроз та забезпечити надійність прийняття рішень в умовах невизначеності.

Список використаних джерел

1. Power, D. J. Decision Support Systems: Concepts and Resources for Managers [Електронний ресурс]. – 2002. – Режим доступу: <https://scholarworks.uni.edu/facbook/67>.
2. Які ключові чинники визначають ефективність DSS при роботі з великими обсягами даних (Big Data)? [Електронний ресурс] // BIT Impulse. – Режим доступу: <https://bitimpulse.com/yaki-klyuchovi-chynnyky-vyznachayut-efektyvnist-dss-pry-roboti-z-velykymy-obsyagamy-danyh-big-data> (дата звернення: 22.04.2026).
3. Вілігура В., Остряньська Є. Дослідження та класифікація основних типів атак на системи штучного інтелекту в кібербезпеці. Комп'ютерні науки та кібербезпека. 2024; № 2(26): С. 6–18. <https://doi.org/10.26565/2519-2310-2024-2-01>.
4. Tahir. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) [Електронний ресурс] // Medium. – 2024. – 3 Dec. – Режим доступу: <https://medium.com/@tahirbalarabe2/who-are-you-and-what-are-you-allowed-to-do-13762a009ef0> (дата звернення: 22.04.2026).
5. Feng Lu. Data Integrity and Lineage by using DLT, Part 2 [Електронний ресурс] – 2018. – Режим доступу: <https://feng.lu/2018/10/03/Data-Integrity-and-Lineage-by-using-DLT-Part-2/> (дата звернення: 22.04.2026).

Науковий керівник: Помазун О.М., к.е.н., доцент