УДК 004.056.53
DOI: 10.31673/2409-7292.2025.031671

Рзаєва С.Л., Складанний П.М., Машкіна І.В., Костюк Ю.В.

МОДЕЛЬ РЕАЛІЗАЦІЇ КЕРУВАННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ (RBAC) У БАГАТОРІВНЕВІЙ АРХІТЕКТУРІ СХОВИЩА ДАНИХ

У статті представлено концептуальний підхід щодо побудови моделі управління доступом на основі ролей (Role-Based Access Control, RBAC) у багаторівневій архітектурі сховища даних (Data Warehouse, DWH). У сучасних умовах цифровізації, коли сховища даних відіграють ключову роль у зберіганні, обробці та аналітичному використанні корпоративної інформації, виникає нагальна потреба у формалізованих підходах щодо забезпечення інформаційної безпеки. Особливо актуальним є питання розмежування доступу до чутливої інформації, запобігання витокам конфіденційних даних, підмінам і несанкціонованим змінам даних. Застосування RBAC-моделі дозволяє централізовано визначати повноваження користувачів на основі їхніх ролей у межах організаційної структури сховища, реалізуючи принцип найменших привілеїв та розподілу обов'язків. Розроблена модель орієнтована на багаторівневу архітектуру сховища даних, яка охоплює шість функціональних рівнів: джерела даних, збирання та обробка, інтеграція, фізичне зберігання, аналітика, а також рівень доступу користувачів. Для кожного з рівнів запропоновано власну схему реалізації RBAC, у якій враховано характер доступу до об'єктів, типи ролей, нормативні вимоги (ISO/IEC 27001, GDPR, NIST SP 800-162), а також типові сценарії застосування. Визначено ключові ролі, притаманні середовищам DWH, такі як: Data Steward, ETL Developer, BI Analyst, Access Administrator тощо, із чітким описом їхніх функціональних повноважень, зон відповідальності та сфер застосування. Методологічною основою дослідження виступає функціональне моделювання в нотації IDEF0, що дозволило формалізувати процеси управління доступом у вигляді структурованої графічної моделі. Модель демонструє, яким чином реалізується взаємозв'язок між об'єктами даних, технічними засобами контролю доступу та суб'єктами, відповідальними за безпеку в середовищі DWH. Запропоноване рішення має як теоретичне, так і прикладне значення, оскільки може бути використане як методологічна база для створення політик доступу, розробки внутрішньої документації з безпеки, автоматизації контролю доступу та аудиту в багаторівневих сховищах даних.

Ключові слова: RBAC; доступ на основі ролей; функціональне моделювання; IDEF0; сховище даних; інформаційна безпека; хмарні обчислення; багаторівнева архітектура; контроль доступу.

Вступ

Ключовим компонентом сучасних інформаційних систем організацій/установ є сховища даних (англ. Data Warehouses, скорочено DWH), які послуговують для централізованого зберігання великих обсягів інформаційних даних, різнорідних за своєю структурою, та забезпечують їхню аналітичну обробку. В умовах всебічної цифровізації бізнес-процесів і зростанням обсягів інформаційних даних зростає актуальність розробки інструментів і підходів щодо забезпечення надійного функціонування систем у безпечному середовищі. У зв'язку з цим питання безпечного доступу до чутливої та конфіденційної інформації у сховищах даних набуває особливої актуальності, адже неконтрольоване надання прав доступу до такого роду інформації, може призвести до її витоку, підміни або несанкціонованої модифікації критичних даних. Також не слід забувати той факт, що інформаційні дані у сховищі повинні зберігатися та оброблятися з дотриманням принципів доступності, цілісності й конфіденційності.

Одним з поширених сучасних підходів до реалізації контролю доступу в сховище є модель доступу на основі ролей (англ. Role-Based Access Control, скорочено RBAC). Модель забезпечує процес призначення прав доступу не окремим користувачам, а визначеним ролям, які відповідають їхнім функціональним обов'язкам у структурі організації/установи. Такий підхід забезпечує централізоване та масштабоване управління доступом, сприяє зменшенню кількості помилок у процесі адміністрування прав доступу до об'єктів сховища та відповідає принципам мінімальних привілеїв.

В умовах багаторівневої архітектури сховища даних, яка охоплює рівень джерел даних, рівень попередньої обробки, інтеграційний рівень, рівень зберігання, аналітичний рівень і рівень доступу користувачів, впровадження моделі RBAC вимагає чіткого визначення ролей, їхніх прав доступу до об'єктів сховища і процедур їхнього контролю, на кожному з вказаних

рівнів. Тому, створення формалізованої функціональної моделі, яка дозволить описати, структурувати та реалізувати процеси призначення та перевірки прав доступу в межах багаторівневої архітектури сховища даних є актуальним завданням.

Метою статті є розробка функціональної моделі реалізації механізмів рольового контролю доступу у сховищах даних, з урахуванням багаторівневої організації їх архітектури, та вимог інформаційної безпеки.

Аналіз літературних джерел і постановка проблеми

За останні роки спостерігається зростання наукового інтересу до питань управління доступом до сховищах даних. Однак, попри наявність значної кількості досліджень, питання інтеграції RBAC у багаторівневі сховища даних залишається недостатньо вивченим, особливо в аспектах, що стосуються специфіки кожного рівня архітектури та забезпечення безпеки на всіх етапах обробки даних. Наприклад, у статті «From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts» досліджується ефективність систем RBAC у зменшенні внутрішніх загроз безпеці баз даних у різних організаційних середовищах. У досліджені авторка використовує кількісну методологію, збираючи дані через опитування професіоналів, безпосередньо залучених до безпеки управління базами даних, у сферах технологій, фінансів, охорони здоров'я та урядових установ. За допомогою підтверджувального факторного аналізу (CFA) та моделювання структурних рівнянь (SEM) проаналізовані взаємозв'язки між ефективністю реалізації RBAC, труднощами, що виникають під час впровадження даної моделі в середовищах із підвищеними вимогами до захисту інформації, можливостями її вдосконалення, а також їх сукупним впливом на зниження рівня внутрішніх загроз, які становлять значну проблему для безпеки баз даних, що вимагає надійних та адаптивних заходів безпеки [1].

Стаття «Role-Based Access Control (RBAC)» автора Andrew Carruthers досліджує застосування RBAC в управління безпекою хмарних обчислень у середовищах SAP Business Technology Platform, аналізуючи трансформацію RBAC з традиційного механізму контролю доступу в інтелектуальну систему безпеки хмарних обчислень. Також у статті розглядається питання інтеграції RBAC з технологіями штучного інтелекту та машинного навчання, з метою підвищення здатності системи виявляти та запобігати загрозам безпеці, оптимізуючи процес управління ролями [6].

Автор Maria Penelova у статті «Hybrid Role and Attribute Based Access Control Applied in Information Systems» розглядає питання імплементації RBAC у платформу Snowflake, при цьому наголошуючи, що безпека є невід'ємною частиною архітектури Snowflake. В статті описуються механізми визначення доступу ролей до об'єктів Snowflake, їхню приналежність та взаємодію, забезпечуючи гнучке та масштабоване управління доступом до об'єктів та відповідність політикам безпеки і вимогам регуляторів [7].

У статті «An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud» пропонується модель управління доступом до хмарного середовища, заснованою на оцінці ризику безпеки динамічного зберігання чутливих даних.

Автори зазначають, що традиційні методи шифрування не завжди ефективні для захисту динамічних даних, які часто змінюються та вимагають частого доступу до хмарного середовища. Запропонована модель додає оцінку ризику до традиційного управління доступом на основі атрибутів (ABAC), враховуючи атрибути суб'єкта, ресурсу та середовища. Вона використовує метод аналізу ієрархій процесів (AHP) для кількісної оцінки ризику та реалізується за допомогою мови XACML [3].

Автори статті «Zero-Trust Based Dynamic Access Control for Cloud Computing» розробили модель динамічного управління доступом, засновану на концепції нульової довіри (Zero Trust Architecture, ZTA) для хмарних обчислень. Дана модель включає оцінку довіри користувачів у реальному часі, використовуючи методи машинного навчання. Зпроєктована система DR-TBAC відстежує взаємодію користувачів з хмарною платформою, автоматично коригує

© Рзаєва С.Л., Складанний П.М., Машкіна І.В., Костюк Ю.В. (2025) Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних. Сучасний захист інформації, 3(63), 137–149. https://doi.org/10.31673/2409-7292.2025.031671

правила доступу на основі поведінки користувачів та змін у середовищі, забезпечуючи безпеку та відповідність політикам безпеки і вимогам регуляторів [4].

Виклад основного матеріалу

Багаторівнева архітектура сховища даних забезпечує ефективне збирання, обробку, інтеграцію, зберігання та доступ до даних, з метою їхнього подальшого аналізу й підтримки прийняття рішень. У контексті такої архітектури критично важливим є впровадження ролевого управління доступом (RBAC), що гарантує цілісність, конфіденційність та контрольоване використання інформаційних ресурсів, на кожному з рівнів сховища. У моделі RBAC кожен рівень архітектури розглядається як окрема зона контролю доступу, для якої необхідне формальне визначення політик доступу відповідно до встановлених ролей користувачів. Багаторівнева архітектура сховища охоплює такі ключові рівні: рівень джерел даних (Data Sources Layer), рівень збору та обробки даних (Data Staging Layer), інтеграційний рівень (Integration Layer), фізичний рівень сховища даних (Data Warehouse Storage Layer), аналітичний рівень (Analytics and BI Layer), рівень доступу користувачів (Access Layer).

Рівень джерел даних охоплює всі первинні джерела, з яких надходять дані (до джерел даних належать транзакційні бази даних, зовнішні API, файли, лог-файли тощо). Доступ до джерел даних має регламентуватись відповідно до ролей, які мають право ініціювати процес завантаження даних або моніторингу первинних джерел, що дозволяє обмежити вплив на вихідні дані та забезпечити захист від несанкціонованих витоків інформації вже на етапі її походження.

На етапі збору та обробки даних виконується первинна обробка даних, їхнє очищення, нормалізація та тимчасове зберігання. Реалізація RBAC, на даному рівні, дозволяє обмежити доступ до проміжних результатів обробки, які можуть містити чутливу або нефільтровану інформацію. Доступ на даному рівні зазвичай надається лише технічному персоналу, відповідальному за якість даних, і виключає можливість взаємодії кінцевих користувачів з неочищеними наборами даних.

На інтеграційному рівні відбувається об’єднання даних із різних джерел у єдину узгоджену модель. Застосування ролевого управління доступом забезпечує розмежування доступу до логіки трансформацій та бізнес-правил, які регламентують процеси агрегування даних. Користувачі з ролями аналітики, адміністратори та інтегратори, отримують доступ лише до тих сегментів інформації, що відповідають їхнім посадовим обов’язкам та функціональним повноваженням.

Фізичний рівень сховища даних містить централізоване зберігання інтегрованих даних, як у вигляді фактів та вимірів у багатовимірних моделях, так і у вигляді денормалізованих таблиць. Реалізація RBAC на цьому рівні дозволяє забезпечити політики доступу до конкретних наборів даних або їх частин залежно від ролі користувача. Наприклад, фінансовий аналітик може мати доступ до фінансових фактів, але не до персоніфікованих даних клієнтів. Рівень доступу може бути реалізований як на рівні таблиць, так і на рівні стовпців або записів.

На аналітичному рівні реалізуються, відповідно, аналітичні інструменти та бізнес-інтелект (BI) рішення, які що забезпечують генерацію звітів, дашбордів, OLAP-кубів і інших засобів візуалізації даних. Модель управління доступом на основі ролей впроваджується для регламентування прав доступу користувачів до аналітичних ресурсів, забезпечуючи, що лише користувачі з відповідними ролями можуть переглядати, модифікувати або розповсюджувати конкретні звіти та їхні візуалізації. Такий підхід гарантує цілісність, конфіденційність та відповідність інформації бізнес-вимогам, одночасно адаптуючи аналітичне середовище до функціональних обов’язків користувачів.

Рівень доступу користувачів забезпечує організацію інтерфейсної взаємодії кінцевих користувачів із системою сховища даних. Реалізація механізмів ролевого управління доступом, на даному рівні, породжує процеси автентифікації, авторизації та аудиту дій користувачів. Для кожної ролі чітко визначаються права доступу до інформаційних ресурсів, сервісів та

аналітичних інструментів, що забезпечує ефективне запобігання несанкціонованого доступу до них та порушенню внутрішніх політик безпеки. Крім того, на цьому рівні можуть впроваджуватися механізми багаторівневого контролю доступу у поєднанні з принципом найменших привілеїв (least privilege), що додатково підвищує рівень захисту даних відповідно до ролей користувачів.

Систематизація ролей у контексті сховища даних

Рольова модель контролю доступу (RBAC) передбачає розподіл прав доступу до об'єктів багаторівневої архітектури сховища даних (DWH) на основі функціональних обов'язків користувачів, що реалізуються через концепцію ролей. Така модель набуває особливої актуальності, оскільки різні категорії користувачів взаємодіють з інформацією, яка зберігається у сховищі, на різних етапах її обробки, від моменту завантаження з операційних джерел даних до етапу її аналітичної інтерпретації у вигляді зведених таблиць, або BI-звітів.

Для забезпечення керованого доступу до об'єктів сховища та уникнення надмірного делегування прав користувачам (які не мають на це право) необхідно встановити чіткий розподіл ролей, згідно з функціональними обов'язками, на кожному рівні багаторівневої архітектури сховища даних. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу, сприяє дотриманню принципу найменших привілеїв (least privilege) та підтримує розмежування обов'язків (separation of duties).

У типових DWH-системах доцільно виокремлювати такі узагальнені ролі користувачів:

Data Warehouse Administrator (Адміністратор сховища даних) – відповідає за розгортання, налаштування та обслуговування сховища даних; керування структурою баз даних: схеми, індекси, партиції; забезпечення продуктивності запитів, виконання резервного копіювання та аварійного відновлення. Роль має повноваження на рівні фізичної інфраструктури сховища, тому доступ адміністратора має бути ретельно контрольований, а всі його дії повинні повністю журналюватися для підзвітності та убезпечення витоку чутливої і конфіденційної інформації.

Роль застосовується у СУБД, таких як SQL Server, Oracle, Snowflake, BigQuery тощо.

Data Steward (Куратор даних), до функціональних обов'язків входять:

- визначення стандартів якості даних, контроль відповідності;
- описання метаданих, роз'яснення бізнес-семантики атрибутів;
- погодження змін у джерелах і структурах даних.

Таблиця 1

Рольова модель контролю доступу для ролі Data Steward

Контекст застосування	*Платформи / Сервіси*	*Опис ролі Data Steward*
Система Data Governance / Data Quality	Collibra, Informatica, Talend Data Quality	Забезпечує розмежований контроль якості та відповідності даних
Каталоги метаданих	Apache Atlas, Alation	Має право переглядати, затверджувати та оновлювати атрибути метаданих
Політики даних на рівні підрозділів	Внутрішні політики компанії, системи управління правами доступу	Куратор даних, відповідальний за дотримання правил у закріпленому домені

Функціонал ролі передбачає взаємодію з технічними об'єктами даних (наприклад, словники, зв'язки атрибутів, доступ до реєстрів якості) і має обмежений доступ на операції читання/перевірки/затвердження в системах типу DWH, ETL, BI або системах метаданих. Data Steward не має повноважень змінювати вміст даних або конфігурацію систем, проте може мати доступ для перевірки та погодження змін, що потребують відповідної авторизації. Тобто роль забезпечує чітке відокремлення між тими, хто керує якістю та відповідністю даних, і тими, хто ними оперує технічно, забезпечує реалізацію принципу Data Ownership (володіння даними), тобто це означає, що роль несе відповідальність за певні дані, їх якість, цілісність, захист і

© Рзаєва С.Л., Складанний П.М., Машкіна І.В., Костюк Ю.В. (2025) Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних. Сучасний захист інформації, 3(63), 137–149. https://doi.org/10.31673/2409-7292.2025.031671

правильне використання. Роль Data Steward застосовується на інтеграційному рівні, у каталогах метаданих, аналітичних словниках та системах управління даними Data Governance (табл. 1).

ETL Developer (також використовується синонімічна термінологія: ETL Engineer, Data Integration Developer) – це фахівець, який розробляє та підтримує процеси Extract – Transform – Load, налаштовує джерела даних і проміжні зони (staging area), формує логіку трансформацій для завантаження у сховище. Функціональне призначення даної ролі зумовлено необхідністю забезпечення узгодженості, коректності та безперервності переміщення даних із операційних джерел до відповідних структур сховища.

Роль ETL Developer (розробник процесів витягування, трансформації та завантаження даних) використовується в рамках побудови сховищ даних та процесів інтеграції інформації та фігурує під назвами Data Engineer, ETL Engineer або Integration Developer у документації провідних платформ для обробки даних (табл. 2).

Таблиця 2

Основні платформи та ролі ETL Developer у процесах обробки даних

Контекст застосування	*Платформи / Сервіси*	*Опис ролі ETL Developer*
Хмарні сервіси обробки даних	AWS Glue, Azure Data Factory, Google Cloud Dataflow	Створення, конфігурування та супровід процесів переміщення і трансформації даних
Середовища для розробки потоків даних	Apache NiFi, Talend, Informatica	Розробка та виконання потоків даних (data pipelines)
Методологія DataOps	Команди Dev/Data	Представники інтеграційного та інженерного підрівня, відповідальні за узгоджене і безпечне транспортування даних до аналітичної частини

Включення ролі ETL Developer до системи рольового контролю доступу (RBAC) у межах архітектури сховища даних забезпечує:

- принцип найменших привілеїв (Least Privilege), тобто права доступу обмежуються лише тими рівнями інфраструктури, що є необхідними для виконання професійних завдань, згідно посадових функцій;
- розмежування обов’язків (Separation of Duties), ETL-фахівець не має повноважень змінювати результати аналітичної обробки, що знижує ризики несанкціонованих втручань у аналітичні звіти;
- підвищення керованості доступу та безпеки обробки даних, тобто чітко визначені повноваження дозволяють організувати аудит, моніторинг дій користувачів і контроль за дотриманням політик доступу.

Роль BI Analyst (Аналітик бізнес-даних) передбачає роботу з підготовленими даними в межах аналітичного шару сховища, з метою виявлення закономірностей, побудови статистичних моделей, формування запитів та отримання інформаційних звітів. Аналітик бізнес-даних працює з об’єктами зберігання, агрегованими показниками, представленнями (views) та іншими структурованими формами аналітичних даних.

Доступ аналітика зазвичай обмежується фізичним та аналітичним рівнями, з правом дозволу на операції читання, без можливості змінення вихідних даних або редагування схеми. У RBAC-моделі роль сприяє точному розмежуванню повноважень між технічним персоналом і фахівцями з аналізу, що, у свою чергу, дозволяє гарантувати стабільність структури сховища, уникати втрат або перекручень первинних даних, а також забезпечувати прозорість аналітичних дій.

У багаторівневій архітектурі сховищ даних роль BI Analyst застосовується в організаціях, які активно використовують аналітику для підтримки прийняття рішень, де аналітичний шар сховища відіграє ключову роль у генерації бізнес-інсайтів. Для виконання аналітичних завдань

BI Analyst використовує платформи бізнес-аналітики, такі як Microsoft Power BI, Tableau, Qlik Sense, а також хмарні рішення Google BigQuery, Amazon Redshift, Snowflake, що інтегруються з багаторівневою архітектурою сховищ даних.

Business Data Consumer (Кінцевий користувач / Споживач бізнес-даних) являє собою роль кінцевого споживача інформації, який отримує доступ до вже підготовлених звітів, панелей керування та візуалізацій у бізнес-аналітичних платформах (Power BI, Tableau, Qlik тощо). Дана роль не взаємодіє безпосередньо з базами даних, а отримує агреговану та перевірену інформацію для прийняття рішень на рівні бізнесу і виконуваними ним професійних завдань. Доступ користувачів, які мають роль Business Data Consumer, обмежується рівнем Analytics and BI Layer, із правами перегляду даних та їхньої фільтрації, без можливості зміни структури даних, візуалізації, джерел або логіки аналітики.

Дана роль має найнижчий рівень доступу. Включення ролі до системи RBAC забезпечує дотримання принципу мінімальних привілеїв і дозволяє надійно ізолювати аналітичне середовище від кінцевих користувачів, зберігаючи цілісність даних та стабільність логіки звітності, без ризику пошкодження даних. Застосовується у BI платформах, аналітичних кабінетах, звітних порталах.

Роль Access Administrator / Security Administrator (Адміністратор доступу / Адміністратор безпеки) забезпечує управління та контроль за виконанням політик доступу до багаторівневої архітектури сховища даних. До основних обов'язків ролі входять конфігурування механізмів RBAC, створення ролей і їх призначення користувачам, забезпечення відповідності політик нормативним вимогам, а також ведення журналів доступу, проведення аудиту і реагування на інциденти безпеки.

Хоч роль і має доступ до систем керування доступом і журналів подій, але немає доступу до змісту самих даних у сховищі чи результатів аналітичної обробки. Вона виконує виключно адміністративні та контрольні функції. Чітке визначення цієї ролі в RBAC-моделі є необхідним з позиції регламентованого розмежування обов'язків, уникнення конфлікту інтересів, дотримання вимог стандартів ISO/IEC 27001 та NIST SP 800-53, а також забезпечення прозорості процедур керування доступом.

Управління ролями в архітектурі сховища даних забезпечує не лише дотримання політик безпеки, а й підвищує ефективність адміністрування, автоматизує процеси призначення прав доступу та формалізує взаємодію між функціональними рівнями системи і користувачами.

Формалізація моделі контролю доступу в архітектурі сховища даних за допомогою моделі IDEF0

Для системного опису процесу управлянні рольового контролю доступу (RBAC) багаторівневої архітектури сховища даних застосовано функціональне моделювання на основі методології IDEF0. Дана методологія забезпечує можливість проєктування складної інформаційної системи шляхом побудови графічної моделі, де для кожного модулю моделі визначені стрілки, які відображають вхідні дані, керуючі впливи, механізми реалізації та результати виконання відповідного модулю в межах інформаційної системи. У нашому дослідженні замість інформаційної системи моделюємо сховище даних.

Процес моделювання в нотації IDEF0 розпочинається з побудови контекстної діаграми, яка описує узагальнену функцію «Управління рольовим доступом у сховищі даних» (Manage Role-Based Access in Data Warehouse), яка охоплює всі процеси, пов'язані з організацією, реалізацією, контролем та документуванням доступу користувачів до об'єктів даних відповідно до призначених їм ролей (рис. 1).

Застосування нотації IDEF0 для моделювання процесу реалізації RBAC у сховищах даних дозволяє:

- створити прозору, верифіковану схему контролю доступу, придатну для перевірки, аналізу та подальшого вдосконалення, в межах побудови й підтримки багаторівневої архітектури сховища даних;

- забезпечити узгодженість політик доступу з внутрішніми регламентами та зовнішніми нормативними вимогами (зокрема стандартами ISO/IEC 27001, NIST тощо);
- формалізувати призначення ролей у межах багаторівневої архітектури сховища даних відповідно до принципів конфіденційності, цілісності та доступності інформації;
- забезпечити гнучкість моделі у процесах аудиту, оновлення та масштабування у разі трансформації організаційної структури або впровадження нових технологічних платформ.

Опишемо стрілки входу, виходу, контрою та механізмів, які впливають на функціонування контекстної моделі управління рольовим доступом у сховищі даних.

Вхідні стрілки (Inputs) запускають механізм прийняття рішення щодо призначення доступу ролям та/або користувачам до об'єктів DWH: модель не генерує ролі або запити самостійно, вона реалізує політику надання доступу на підставі визначених правил доступу згідно з політиками безпеки. Контекстна модель містить стрілку входу «Запити користувачів на доступ до ресурсів DWH».

Запити користувачів на доступ до ресурсів DWH – формалізовані запити, що надходять від користувачів на отримання доступу до певних ресурсів сховища даних. Кожен запит містить ідентифікаційні дані суб'єкта, мету доступу до об'єкта, очікуваний рівень прав і обґрунтування необхідності доступу відповідно до функціональних обов'язків.

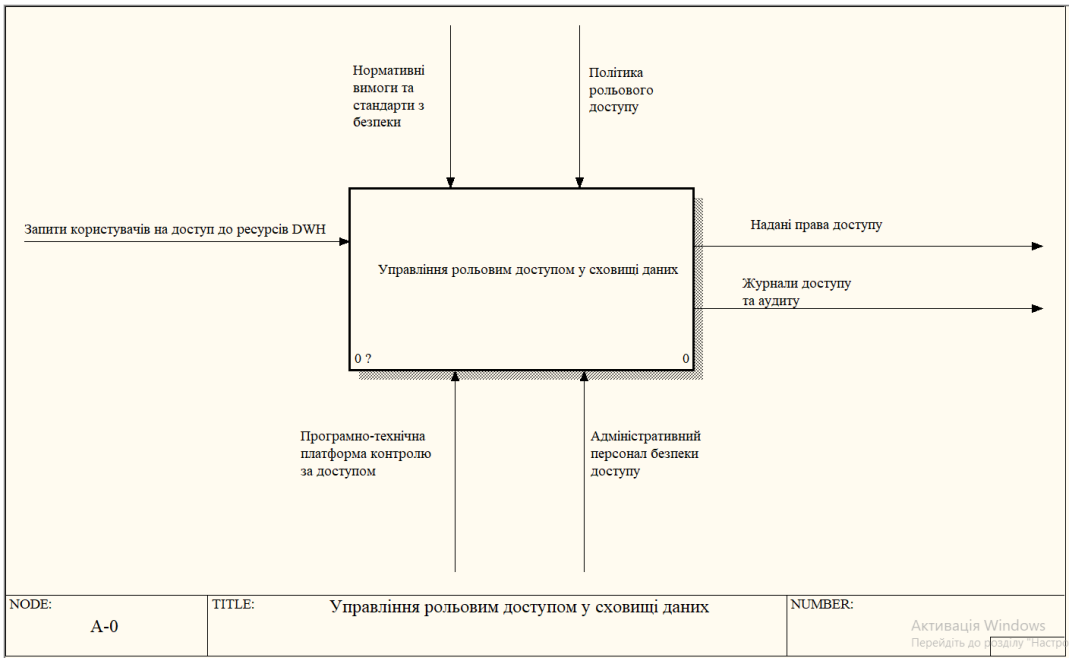

Рис. 1. Контекстна модель «Управління рольовим доступом у сховищі даних»

Керуючі стрілки (Controls) визначають нормативно-регламентне середовище, в межах якого функціонує модель, тобто вона не просто обробляє запити на доступ, а здійснює це у відповідності до заздалегідь встановлених, формалізованих правил і політик безпеки. Контекстна модель має дві стрілки контролю:

Політика рольового доступу (RBAC Policy) – внутрішній регламент, що формалізує принципи реалізації RBAC, а саме створення ролей, їх повноваження, правила призначення ролей, обмеження та дії в разі порушення політик доступу. Забезпечує узгодженість процесів авторизації з організаційною ієрархією.

Нормативні вимоги та стандарти з безпеки – це зовнішні регламенти, що визначають засади забезпечення інформаційної безпеки, зокрема стандарти ISO/IEC 27001, ISO/IEC 29146, GDPR, NIST SP 800-162. Вони встановлюють допустимі межі доступу до даних, вимоги до

автентифікації користувачів, порядок проведення аудитів та інші обов'язкові процедури контролю.

Механізми реалізації (Mechanisms) – це не лише технічне середовище, а й виконавці, без яких не відбувається реалізація політики доступу.

Програмно-технічна платформа контролю доступом являє собою інтегрований набір засобів програмного та апаратного рівня, призначених для реалізації політик рольового доступу в межах архітектури сховища даних. Така платформа є інструментальним середовищем, у якому виконується автентифікація користувачів, авторизація доступу до об'єктів, керування правами, моніторинг і аудит дій користувачів.

До складу програмно-технічної платформи контролю доступом належать:

- системи керування базами даних (DBMS), які реалізують розмежування доступу до структурованих об'єктів на основі ролей (SQL Server, PostgreSQL, Oracle, Snowflake);
- інструменти управління ідентичністю та доступом (IAM), що відповідають за централізоване призначення прав (Azure AD, Okta, AWS IAM);
- платформи обробки та інтеграції даних (ETL/ELT), у яких рольова модель застосовується до об'єктів конвеєрів даних (Talend, Informatica, Apache NiFi);
- аналітичні BI-платформи, які забезпечують контроль доступу до візуалізацій, моделей звітності й аналітичних представлень (Power BI, Tableau, Looker);
- мережеві, серверні та віртуалізаційні засоби, які забезпечують технічну інфраструктуру реалізації контролю доступу, включаючи шлюзи, протоколи захищеної передачі даних (HTTPS, VPN), токенізовану автентифікацію, журнальне сховище та засоби моніторингу.

Адміністративний персонал безпеки доступу – це сукупність посадових осіб, відповідальних за впровадження, супровід і контроль політик рольового доступу в архітектурі сховища даних. До такого складу входять: адміністратори сховища даних, куратори даних, адміністратори BI-платформ, адміністратори ETL/ELT-систем, адміністратори безпеки.

Вихідні стрілки (Outputs) відображають результати функціонування моделі, сприяють підтриманню керованості системи, забезпечують прозорість дій адміністратора та фіксацію користувацьких запитів для подальшого аудиту й підзвітності. До них належать: «Надані права доступу» та «Журнали доступу та аудиту».

Надані права доступу визначають обсяг дозволених дій користувача в межах призначеної ролі та забезпечують доступ до відповідних об'єктів сховища даних, згідно з визначеними повноваженнями. Доступ може бути реалізовано на різних рівнях сховища даних.

Журнали доступу та аудиту становлять вихідний інформаційний потік функції управління рольовим доступом, який фіксує, систематизує та зберігає дані про всі операції, пов'язані з наданням, використанням, зміною або відкликанням прав доступу до об'єктів сховища даних. Вони є обов'язковим елементом системи контролю доступу відповідно до вимог міжнародних стандартів (зокрема ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-53), оскільки забезпечують умови для проведення аудиту, інцидентного реагування та підтвердження відповідності політикам безпеки.

До змісту журналів можуть входити такі категорії інформації:

- ідентифікатори користувачів, які здійснювали операції доступу;
- дати та часові мітки виконання дій (timestamp);
- тип дії (отримання доступу, відмова, призначення ролі, зміна політики, спроба несанкціонованого доступу тощо);
- об'єкти доступу (таблиці, представлення, звіти, конвеєри обробки, атрибути);
- джерело підключення (IP-адреса, домен, автентифікаційний токен, механізм автентифікації);
- результат операції (успішна / невдала).

Формат і структура журналів можуть відрізнятися залежно від платформи реалізації (DBMS, IAM, BI тощо), однак у сучасних системах вони, як правило, відповідають вимогам до машинного зчитування (JSON, XML, CSV) і підтримують інтеграцію з централізованими засобами обробки подій (SIEM-системи, Security Data Lake).

У межах архітектури сховища даних журнали доступу та аудиту використовуються для:

- перевірки дотримання політик доступу (policy enforcement verification);
- виявлення несанкціонованих або аномальних дій (наприклад, звернень до заборонених об’єктів, доступу поза робочим часом тощо);
- проведення внутрішнього або зовнішнього аудиту з боку відповідальних осіб або незалежних регуляторів;
- відновлення подій у випадку інцидентів безпеки;
- оцінки ефективності поточної моделі контролю доступу з метою її вдосконалення.

Збереження журналів має здійснюватися в незмінному, захищеному середовищі, із визначеним строком зберігання та рівнями доступу, що виключають можливість втручання в історичні записи. Журнали мають бути обов’язково включені до сфери контролю під час щорічних перевірок відповідності (compliance audits).

Контекстна діаграма є вихідною точкою для деталізації на наступному рівні (A0), де кожен з підпроцесів (перевірка відповідності ролі, затвердження, технічне призначення прав, логування) може бути описаний окремо. Структура моделі дозволяє не лише описати логіку призначення доступу, але й чітко відмежувати відповідальність між учасниками процесу, мінімізуючи ризики конфлікту повноважень.

Декомпозиція моделі управління рольовим доступом у багаторівневій архітектурі сховища даних

Декомпозиція здійснюється шляхом виокремлення функціональних блоків, що відповідають за специфічні підетапи реалізації RBAC, з урахуванням контексту обробки даних, ролей користувачів і регламентних вимог. Кожен блок деталізації описує окремий рівень архітектури сховища даних, починаючи з рівня джерел даних і закінчуючи рівнем користувацького доступу.

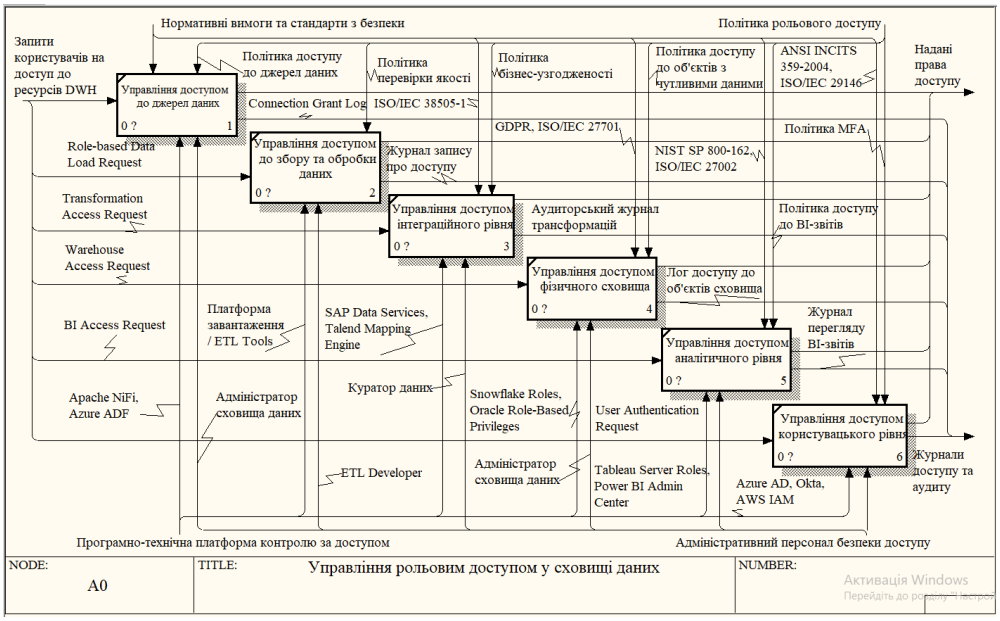

Рис. 2. Декомпозиція моделі «Управління рольовим доступом у сховищі даних»

Для кожного рівня визначено: тип вхідних і вихідних стрілок, контрольні механізми, нормативні бази, які регламентують доступ, та технічні інструменти, що реалізують відповідні

© Рзаєва С.Л., Складанний П.М., Машкіна І.В., Костюк Ю.В. (2025) Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних. Сучасний захист інформації, 3(63), 137–149. https://doi.org/10.31673/2409-7292.2025.031671

процеси. Отже, в результаті декомпозиції отримано шість функціональних підпроцесів відповідно до архітектури сховища даних: управління доступом до джерел даних, управління доступом до збору та обробки даних, управління доступом інтеграційного рівня, управління доступом фізичного сховища, управління доступом аналітичного рівня, управління доступом користувацького рівня. На рисунку 2 подано результат декомпозиції моделі «Управління рольовим доступом у сховищі даних».

Для формалізації процесу управління рольовим доступом у багаторівневій архітектурі сховища даних у межах моделі IDEF0 було реалізовано поетапний розгляд кожного рівня архітектури (від джерел даних до рівня користувацького доступу) через призму застосування контрольованого доступу відповідно до ролей користувачів.

У таблицях 3–8 подано систематизовану інформацію щодо типових стрілок входу, виходу, контролю та механізмів для кожного рівня, а також вказано нормативну базу та опис самої стрілки. Вказана структура дозволяє уніфіковано представити функціонування RBAC-механізмів на кожному рівні, забезпечуючи узгодженість, відтворюваність та відповідність вимогам інформаційної безпеки.

Підпроцес «Управління доступом до джерел даних» описує політики та засоби доступу до первинних джерел інформації, з яких здійснюється завантаження даних у сховище. У таблиці 3 представлено типові запити доступу, нормативні обмеження та контрольні регламенти, які забезпечують отримання лише дозволених обсягів даних згідно з роллю користувача. Засоби оркестрації та механізми аудиту гарантують прозорість доступу на цьому рівні.

Таблиця 3

Управління доступом до джерел даних

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит доступу до систем-джерел / Access Request for Source Systems	ISO/IEC 29146, Azure Data Factory API Access Policy	Формалізоване звернення користувача або служби на доступ до первинних джерел даних
Контроль	Політика доступу до джерел / Source Access Policy	SAP Connector Security Policy, Microsoft Access Control	Визначає, які системи-джерела дозволено для кожної ролі
Контроль	Правила вилучення даних / Data Extraction Rules	Talend Data Integration Governance	Регламентує обсяг, формат, періодичність та тип даних, дозволених до витягування
Механізм	Оркестраційна платформа / Orchestration Platform	Apache NiFi, Azure ADF	Інструменти для реалізації запланованого потоку отримання даних
Вихід	Журнал наданого доступу / Connection Grant Log	ISO/IEC 27002, NIST 800-53 AU-2	Фіксація дозволу на підключення до джерел, реєстрація ролі, об’єкта, часу, дії

Підпроцес «Управління доступом до збору та обробки даних» визначає політики доступу до тимчасового середовища, в якому відбувається первинна обробка даних. Він відображає процедури регламентації доступу до staging-зон, застосування механізмів перевірки якості та реалізацію контролю через ETL-інструменти, при цьому забезпечує фіксацію всіх дій користувачів для цілей аудиту та виявлення відхилень у процесі обробки даних.

Підпроцес «Управління доступом інтеграційного рівня» містить характеристику політик, що регламентують доступ до механізмів інтеграції та трансформації даних. У таблиці 5 описані нормативні обмеження, які визначають дозволені дії відповідно до ролі, вимоги до узгодженості даних та їхньої якості, а також механізми фіксації змін у логіці перетворень.

Таблиця 4

Управління доступом до збору та обробки даних

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит на завантаження staging-даних / Role-based Data Load Request	Talend Data Integration Framework, Informatica MDM	Запит на розміщення тимчасових даних, що обробляються ETL-інструментами
Контроль	Політика контролю доступу / Staging Access Control Policy	ISO/IEC 27001:2022, Snowflake Data Zones	Описує, хто має доступ на читання/запис у зону попередньої обробки
Контроль	Політика перевірки якості / Data Validation Protocol	DAMA-DMBOK, Talend Data Quality	Визначає правила перевірки, очищення, трансформації тимчасових даних перед інтеграцією
Механізм	Платформа завантаження / ETL Tools	SSIS, Talend, Informatica	Виконує автоматизоване наповнення staging-зон
Вихід	Журнал запису про доступу / Staging Access Record	ISO/IEC 27035, SOX ITGC	Протокол дій користувачів у staging-середовищі, з фіксацією часу, джерела та результату

Таблиця 5

Управління доступом інтеграційного рівня

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит на доступ до трансформацій / Transformation Access Request	Talend Studio Roles, SAP BW Transformation Security	Заявка на зміну, перегляд або тестування інтеграційної логіки
Контроль	Матриця ролей трансформації / Integration Role Matrix	NIST SP 800-162, SAP Role-Based Access Matrix	Встановлює, яка роль має які повноваження над об'єктами трансформації
Контроль	Політика бізнес-узгодженості / Data Stewardship Guidelines	DAMA-DMBOK, ISO/IEC 38505-1	Визначає обов’язкові стандарти якості, цілісності, семантики для інтегрованих даних
Механізм	Інтеграційний механізм / Integration Engine	SAP Data Services, Talend Mapping Engine	Інструмент виконання перетворень, об’єднання, логічних перевірок
Вихід	Аудиторський журнал трансформацій / Integration Audit Trail	ISO/IEC 27037, Collibra Governance	Фіксує зміну схем, логіки, параметрів трансформацій з прив’язкою до користувача й часу

Підпроцес «Управління доступом фізичного сховища» описує реалізацію контролю доступу до структурованих об’єктів сховища (схем, таблиць, подань тощо), визначає порядок ініціації запитів, формалізації політики доступу до об’єктів, включаючи врахування критичності даних. Даний підпроцес забезпечує протоколювання кожної операції доступу для гарантування прозорості та відповідності зовнішнім стандартам (табл. 6).

Підпроцес «Управління доступом аналітичного рівня» формалізує підходищо до регламентації доступу до аналітичних звітів, панелей візуалізації та моделей бізнес-аналітики (табл. 7).

Підпроцес «Управління доступом користувацького рівня» охоплює процедури автентифікації, авторизації та керування сесіями користувачів у межах сховища даних. Представлені вимоги до застосування багатофакторної автентифікації, відповідності ролей та повноважень, а також механізми централізованого управління доступом через системи IAM. Реєстрація параметрів доступу гарантує можливість проведення аудиту та розслідування інцидентів безпеки (табл. 8).

Таблиця 6

Управління доступом фізичного сховища

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит на доступ до об'єктів DWH / Warehouse Access Request	SQL Server Security Model, Oracle RBAC	Ініціалізація запиту до таблиць фактів, вимірів, агрегатів
Контроль	Політика доступу до об’єктів / DWH Object Access Policy	ISO/IEC 27001, PostgreSQL ACL	Прив’язка прав (read/write/execute) до конкретних схем, таблиць, подань
Контроль	Політика чутливості даних / Sensitivity Label Rules	GDPR, ISO/IEC 27701, Microsoft Purview	Визначає рівень критичності даних (PII, фінансові) та обмеження доступу за ознакою ролі
Механізм	Рольові механізми СУБД / RDBMS Role-Based Engine	Snowflake Roles, Oracle Role-Based Privileges	Реалізація політик доступу через системи керування базами даних
Вихід	Лог доступу до об'єктів сховища / DWH Object Access Log	NIST 800-53 AU-3, ISO/IEC 27037	Структурований запис кожної операції доступу до об'єкта (запит, зміна, помилка, спроба втручання)

Таблиця 7

Управління доступом аналітичного рівня

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит на доступ до аналітики / BI Access Request	Power BI Security Model, Tableau Access Rules	Запит на доступ до дашбордів, звітів або аналітичних моделей
Контроль	Політика доступу до звітів / BI Role Permissions Matrix	NIST SP 800-162, Looker Roles	Визначає права на перегляд, редагування, створення або обмеження контенту
Контроль	Політика візуалізації / Visualization Access Policy	Microsoft Power BI Row-Level Security	Фільтрація вмісту за атрибутами користувача, рольовими маркерами тощо
Механізм	Платформа BI безпеки / BI Authorization System	Tableau Server Roles, Power BI Admin Center	Механізм реалізації політик доступу до аналітичного контенту
Вихід	Журнал перегляду звітів / BI Access Audit Log	ISO/IEC 27002, SOX	Реєстрація фактів звернення до візуалізацій, фільтрації, перегляду звітів та аналітичної інформації

Таблиця 8

Управління доступом користувацького рівня

Тип стрілки	*Назва стрілки (укр. / англ.)*	*Нормативна база та/або платформа*	*Опис*
Вхід	Запит автентифікації / User Authentication Request	OAuth2, SAML, OpenID, NIST 800-63	Ініціалізація входу до системи (пароль, токен, сертифікат, SSO тощо)
Контроль	Політика RBAC / RBAC Policy Document	ANSI INCITS 359-2004, ISO/IEC 29146	Документ, що формалізує відповідність між користувачем, роллю та правами доступу
Контроль	Політика MFA / Multi-Factor Authentication Policy	NIST 800-63B, ISO/IEC 27001 Annex A.9.4	Вимога автентифікації на основі двох або більше факторів
Механізм	Система керування ідентичністю / IAM System	Azure AD, Okta, AWS IAM	Інструмент для централізованого керування ідентифікацією та призначенням прав
Вихід	Журнали сеансів та авторизації / Session and Auth Logs	ISO/IEC 27037, NIST 800-53 AU-2	Фіксує початок, завершення, параметри та географію автентифікації

Висновки

У межах проведеного дослідження обґрунтовано необхідність і доцільність побудови формалізованої функціональної моделі управління доступом на основі ролей (RBAC) у багаторівневій архітектурі сховищ даних. Запропонований підхід базується на принципах системного аналізу та забезпечує уніфіковану реалізацію механізмів доступу на кожному з архітектурних рівнів: від джерел даних до рівня користувача. Деталізоване подання ролей, політик, механізмів і контрольних процедур сприяє створенню прозорої системи безпеки, що відповідає сучасним викликам у сфері захисту даних. Розроблена модель дозволяє враховувати контекст функціонування DWH, забезпечує дотримання принципу мінімальних привілеїв, розмежування обов'язків і відповідності прав доступу до функціональних обов'язків користувачів. Формалізація моделі в нотації IDEF0 надала можливість структурувати процеси, виділити відповідальних осіб та платформи реалізації, а також встановити зв'язки між вхідними запитами, політиками доступу та журналами контролю. Завдяки цьому досягається не лише технічна реалізація RBAC, а й повноцінна відповідність внутрішнім та зовнішнім нормативним вимогам. У практичному вимірі запропонована модель може слугувати основою для впровадження у корпоративних середовищах, зокрема у випадках, коли система сховища даних є критично важливою для прийняття управлінських рішень, аудиту, відповідності політикам і нормативам. Крім того, модель здатна бути адаптованою до умов хмарних та гібридних середовищ, що розширює сферу її застосування в умовах цифрової трансформації інформаційних інфраструктур. Подальші дослідження доцільно спрямувати на інтеграцію моделі RBAC із атрибутивними підходами (ABAC), динамічними ризиковими моделями та засобами інтелектуального аудиту доступу.

Перелік посилань

1. Marquis, Y. A. (2024). From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts. Journal of Engineering Research and Reports, 26(5), 138–154. https://doi.org/10.9734/jerr/2024/v26i51141
2. Hocine, N. (2021). Agent-based access control framework for enterprise content management. Multiagent and Grid Systems, 17(2), 141–160. https://doi.org/10.3233/MGS-210346
3. Alharbe, N., Aljohani, A., Rakrouki, M. A., & Khayyat, M. (2023). An access control model based on system security risk for dynamic sensitive data storage in the cloud. Applied Sciences, 13(5), 3187. https://doi.org/ 10.3390/ app13053187
4. Wang, R., Li, C., Zhang, K., et al. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity, 8, Article 12, 1–15. https://doi.org/10.1186/s42400-024-00320-x
5. Akuthota, A. K. (2025). Role-based access control (RBAC) in modern cloud security governance: An in-depth analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 45–52. https://doi.org/10.32628/CSEIT25112793
6. Carruthers, A. (2022). Role-based access control (RBAC). In Building the Snowflake Data Cloud (pp. 123–149). Apress. https://doi.org/10.1007/978-1-4842-8593-0_5
7. Penelova, M. (2021). Hybrid role and attribute based access control applied in information systems. Cybernetics and Information Technologies, 21(3), 85–96. https://doi.org/10.2478/cait-2021-0031
8. European Union. (2016). General Data Protection Regulation (GDPR) Regulation (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj
9. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements. https://www.iso.org/standard/82875.html
10. International Organization for Standardization. (2022). ISO/IEC 27002:2022 Code of practice for information security controls. https://www.iso.org/standard/75652.html
11. European Union Agency for Cybersecurity. (n.d.). Guidelines on pseudonymisation techniques and best practices. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
12. European Data Protection Board. (n.d.). Data protection by design and by default Guidelines 4/2019 on Article 25. https:/ / edpb.europa.eu / our-work-tools / our-documents / guidelines / guidelines-42019-article-25-data-protection-design-and_en
13. Костюк, Ю., Довженко, Н., Мазур, Н., Складанний, П., & Рзаєва, С. (2025). Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. Кібербезпека: освіта, наука, техніка, 3(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710

Надійшла 30.07.2025