discovery; they can therefore underestimate service availability and the interval during which a user may receive stale state. The study aims to formalize user-visible latency T_visible as a separate measurement object and to establish a reproducible system of companion indicators. The method combines a causal decomposition of the pipeline into admission, batching, consensus, execution, commit, indexing, publication, and discovery stages; a formal visibility predicate for certified state; separation of right-censored observations from competing terminal events; quantile estimation; and separation of polling discretization from systemic latency. In a numerical experiment calibrated against published measurements of pipelined blockchains, the median observed gap between finality and the first read was 168–241 ms, or up to 27% of total latency, while a conservative stale-response indicator at a 200 ms delay reached 0.69. A parallel pipeline with early state publication reduced median T_visible from 889 to 686 ms and the 1-second threshold violation rate from 17.7% to 0.2%. The scientific contribution is an integrated measurement protocol that combines a state-visibility predicate with visibility-gap, stale-response, and service-level violation metrics. The practical value is the ability to compare scenarios consistently, justify SLOs, and assess the availability and integrity of data exposed to end users.

Keywords: end-to-end latency, state visibility, layer-1 blockchain, RPC interface, cyber resilience, stale response, quality of service.

Надійшла до редакції (Received): 30.07.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

УДК 004.056.5:004.65 DOI: 10.31673/2409-7292.2026.035620

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7589-2045
E-mail: s.rzaieva@kubg.edu.ua

Бондарчук Андрій Петрович
доктор технічних наук, професор, завідувач кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5124-5102
E-mail: a.bondarchuk@kubg.edu.ua

Костюк Юлія Володимирівна
доктор філософії, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua

Рзаєв Дмитро Олександрович
старший викладач кафедри інформатики та системології
Київський національний економічний університет імені Вадима Гетьмана, Київ, Україна
ORCID ID: 0000-0002-7149-4971
E-mail: rzaiev@kneu.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7775-6039
E-mail: p.skladannyi@kubg.edu.ua

© Прокопович-Ткаченко Д.І., Пономарьов І.В., Бабенко К.Є. Операційне визначення та метрики наскрізної затримки безпечного доступу до стану блокчейн-систем першого рівня. Сучасний захист інформації, 3(67), 91–103. https://doi.org/10.31673/2409-7292.2026.033419

ФУНКЦІОНАЛЬНА МОДЕЛЬ УПРАВЛІННЯ БЕЗПЕКОЮ В ІНФРАСТРУКТУРІ СХОВИЩ ДАНИХ

У статті розглянуто проблему забезпечення інформаційної безпеки інфраструктури сховищ даних в умовах зростання обсягів інформації, ускладнення архітектури систем зберігання та підвищення вимог до забезпечення конфіденційності, цілісності й доступності даних. Показано, що сучасні сховища даних функціонують у складному інформаційному середовищі, де поєднуються великі обсяги структурованої та неструктурованої інформації, розподілені обчислювальні ресурси, хмарні технології та багаторівневі механізми доступу, що зумовлює необхідність побудови комплексної системи управління інформаційною безпекою. Встановлено обмеженість традиційних підходів до управління безпекою, які не забезпечують достатнього рівня формалізації процесів, ускладнюють координацію інформаційних потоків і не дозволяють повною мірою інтегрувати вимоги міжнародних стандартів у внутрішню архітектуру сховищ даних. Запропоновано системний підхід до побудови функціональної моделі управління інформаційною безпекою інфраструктури сховищ даних на основі методології IDEF0. Для формалізації функціональних процесів використано структуроване моделювання, що дозволяє описати взаємозв'язки між інформаційними потоками, механізмами керування безпекою та інфраструктурними компонентами системи. Побудовано контекстну модель верхнього рівня та виконано її декомпозицію за функціональними рівнями архітектури сховища даних. Для кожного функціонального рівня визначено відповідні механізми забезпечення безпеки, політики доступу, інфраструктурні засоби захисту та зв'язки з нормативно-правовими вимогами. Особливу увагу приділено інтеграції положень міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 та загального регламенту захисту даних GDPR у процеси управління безпекою інфраструктури сховищ даних. Показано, що використання методології IDEF0 дозволяє підвищити рівень структурованості процесів управління інформаційною безпекою, забезпечити формалізацію безпекових процедур та покращити керованість інформаційних потоків. Отримані результати підтверджують доцільність використання структурованого функціонального моделювання для підвищення ефективності управління інформаційною безпекою та забезпечення стійкості інфраструктури сховищ даних до сучасних кіберзагроз і порушень безпеки інформації.

Ключові слова: функціональне моделювання, IDEF0, управління інформаційною безпекою, сховища даних, політика безпеки, декомпозиція, ISO/IEC 27001, GDPR, архітектура даних.

Вступ

Все більш зростаючою умовою у забезпеченні захисту інформаційних даних, в умовах стрімкого зростання цифровізації усіх сфер діяльності, постають питання безпеки інфраструктури сховищ даних, в яких міститься чутлива та конфіденційна інформація. Зберігання, обробка та доступ до комерційних та персональних даних, таких важливих для бізнесу та чутливих до витоків даних, потребує впровадження ефективних методів та моделей захисту інформації. Наразі існуючі підходи до забезпечення механізмів захисту інформаційних даних зосереджуються на технічних аспектах, таких як шифрування даних, автентифікація та авторизація доступу до даних, або аудит доступу. Проте, для забезпечення цілісного та ефективного захисту інфраструктури сховища даних необхідно спроєктувати функціональну модель безпеки, яка формалізує всі процеси та механізми, які забезпечують цілісний та керований процес організації та управління безпекою сховища. Ефективним інструментом побудови моделі комплексного захисту сховища виступає функціональне моделювання, зокрема методологія IDEF0, яка дозволяє описати логіку, взаємозв'язки та модулі системи безпеки.

Постановка проблеми

Незважаючи на наявність значної кількості підходів до забезпечення безпеки сховищ даних, зокрема методів динамічного виявлення загроз, контролю доступу, шифрування та використання блокчейн-технологій, у сучасних дослідженнях відсутній цілісний функціональний підхід до управління інформаційною безпекою інфраструктури сховищ даних. Існуючі рішення переважно орієнтовані на окремі аспекти захисту та не забезпечують формалізацію функцій безпеки як складової інформаційної системи з можливістю структурованого моделювання та подальшої візуалізації засобами CASE-технологій. Це ускладнює побудову інтегрованих систем управління безпекою, здатних враховувати контекст функціонування сховища даних, рівень ризиків та особливості обробки великих обсягів інформації.

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

Аналіз останніх досліджень і публікацій

В умовах стрімкого зростання обсягів інформації, що зберігаються в сховищах даних, питання забезпечення їхньої безпеки набуває особливої актуальності. Аналіз наукових публікацій за останні п’ять років свідчить про зростаючий інтерес до розробки моделей безпеки, які враховують специфіку організації інформаційної інфраструктури сховищ даних.

Стаття «The MESA Security Model 2.0: A Dynamic Framework for Mitigating Stealth Data Exfiltration», авторів Sanjeev Pratap Singh, Naveed Afzal, пропонує динамічну модель безпеки MESA 2.0, спрямовану на виявлення та запобігання прихованому витоку даних. Модель фокусується на швидкому виявленні аномалій та оперативному реагуванню на загрози, що особливо актуально для захисту сховищ даних від складних атак [1]. У науковій роботі "Data Guard: A Fine-Grained Purpose-Based Access Control System for Large Data Warehouses» представлено систему Data Guard, яка реалізує детальний контроль доступу на основі цілей використання даних у великих сховищах. Data Guard дозволяє створювати політики на основі семантичних описів даних та мети доступу до даних. Потім Data Guard перетворює ці політики на SQL-представлення, які маскують дані з базових таблиць сховища. Під час доступу Data Guard забезпечує відповідність вимогам, направляючи доступ до кожної таблиці з відповідним маскування даних, мінімізуючи зусилля, пов'язані з впровадженням Data Guard в існуючих додатках. Система дозволяє створювати політики доступу, що враховують контекст запиту, забезпечуючи гнучке та безпечне управління інформацією [2].

У статті «SSF-CDW: Achieving Scalable, Secure, and Fast OLAP Query for Encrypted Cloud Data Warehouse» автори описали розроблену ними модель SSF-CDW, яка дозволяє виконувати масштабовані, безпечні та швидкі OLAP-запити до зашифрованих хмарних сховищ даних [3]. Модель SSF-CDW покращує запити OLAP, поєднує методи шифрування та оптимізації запитів, забезпечуючи ефективну роботу з великими обсягами даних без компромісів у безпеці. З метою ефективного виконання OLAP-запитів науковці запропонували новий механізм пошуку куба даних з використанням схеми Redis, яка являє собою базу даних в оперативній пам'яті. Даний метод динамічно компілює запити, розбиваючи їх на кілька рівнів та консолідуючи результати, що відображаються у відповідному зашифрованому кубі даних.

Наукове дослідження авторів Huang J., Yi J. «The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins» описує схему управління безпекою хмарного сховища, що поєднує технології блокчейн та цифрових двійників [4]. Дана схема використовує псевдовипадкову функцію (OPRF) для генерації рандомізованих конвергентних ключів, з метою покращення конфіденційності даних, підвищує надійність одночасного управління ключами за допомогою механізму обміну секретами, де конвергентні ключі розділяються на фрагменти ключів та розподіляються в блокчейні для зберігання та ефективно підтримує дедуплікацію безпеки даних на рівні файлів та блоків. Запропонований підхід забезпечує високий рівень захисту даних, прозорість операцій та можливість відстеження змін у реальному часі.

У статті «An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud» автори розробили модель контролю доступу, що базується на оцінці ризиків безпеки системи для динамічного зберігання чутливих даних у хмарному середовищі [5]. Запропоновано метод розрахунку оцінки ризику шляхом поєднання методу аналізу нечіткої узгодженості AHP. Модель враховує змінні фактори ризику та адаптується до поточних умов, забезпечуючи гнучкий та ефективний захист даних.

Проаналізувавши наявні наукові публікації за темою безпеки сховищ даних, слід зазначити, що, незважаючи на різноманіття підходів, таких як динамічне виявлення загроз, контроль доступу, шифрування, використання блокчейн-технологій тощо, у більшості досліджень відсутній цілісний функціональний підхід до управління безпекою, який би враховував структуроване моделювання інфраструктури сховищ даних.. Залишилися відкритими питання формалізації функцій безпеки як складової частини інформаційної

системи, що підтримує сховище даних, із можливістю подальшої візуалізацією інструментальними засобами CASE-технологій. Це ускладнює впровадження інтегрованих рішень управління безпекою інфраструктури сховищ даних, які б враховували контекст роботи системи, рівень ризиків та обсяг оброблюваної інформації.

Основна частина

Сховища даних, як ключовий компонент сучасної інформаційної інфраструктури, зберігають великі обсяги структурованої та неструктурованої інформації, що часто має високий рівень конфіденційності, чутливості або стратегічної цінності. Сховища використовують у бізнесі, державному управлінні, охороні здоров'я, ритейлі, фінансових технологіях, з метою забезпечення ефективності управління інформаційними потоками, високої продуктивності та безпекової надійність захисту даних.

Інфраструктура сучасних сховищ даних включає комплекс апаратних та програмних компонентів, які забезпечують збирання, обробку, зберігання, аналіз великого масиву інформації. Узагальнена архітектура такої інфраструктури зазвичай має такі рівні, з точки зору забезпечення механізмів захисту даних: 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) (рис. 1.).

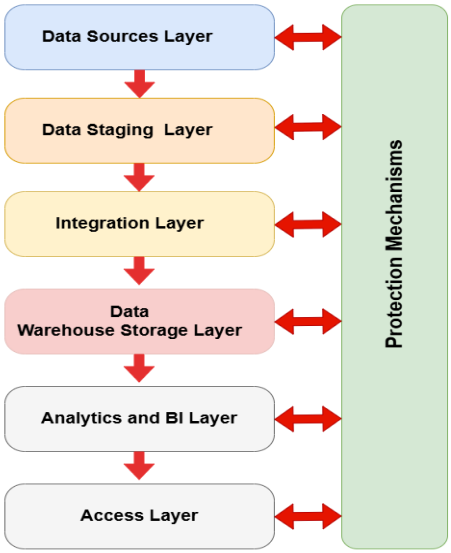

Рис. 1. Security architecture of data storage infrastructure

Рівень джерел даних (Data Sources Layer) є початковим етапом у функціонуванні сховища даних, оскільки саме тут відбувається збирання інформації з усіх доступних систем. До типових джерел належать структуровані дані з реляційних баз даних, інформаційних систем (ERP, CRM) та бухгалтерських платформ, а також напівструктуровані (JSON, XML) та неструктуровані джерела (текстові документи, зображення, відео, аудіо). Дані можуть надходити як з внутрішніх джерел організації, так і з зовнішніх (вебресурсів, відкритих державних баз, API постачальників або соціальних медіа). Різноманітність джерел призводить до відмінностей у форматах даних, способах доступу та частоті оновлення інформації. Деякі джерела забезпечують дані в режимі реального часу (стрімінгові потоки), тоді як інші надсилають оновлення періодично (пакетна обробка). Для нормалізації, консолідації та попереднього очищення даних та їх обробки необхідно використовувати відповідне програмне забезпечення. Для мінімізації навантаження на продуктивні системи використовуються технології типу CDC (Change Data Capture), а також реплікація або інтеграційні сервіси, що забезпечують передачу змін без прямого втручання в роботу джерел.

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

З безпекової точки зору, даний рівень є критично важливим, оскільки його компрометація може призвести до подальшого поширення шкідливої або недостовірної інформації по всій аналітичній інфраструктурі. Основними загрозами є несанкціонований доступ до джерел, модифікація даних, використання незахищених каналів передачі, а також вразливості на рівні API або драйверів підключення. З метою запобігання зазначених ризиків застосовуються такі заходи: шифрування каналів зв'язку (наприклад, TLS), автентифікація та авторизація джерел, політики контролю доступу до даних, аудит транзакцій, а також моніторинг аномальної активності.

Після вилучення з різнорідних джерел дані тимчасово зберігаються у рівні збору та обробки даних, яка є проміжною зоною. Основний функціонал даного рівня полягає в акумуляції необроблених або частково оброблених даних, створюючи масив даних для подальших трансформацій, тобто подальшої обробки даних без втрат або спотворень.. Data Staging зазвичай реалізується за допомогою спеціалізованих сховищ або тимчасових таблиць, що зберігаються в окремому середовищі бази даних або файловій системі. Формат даних може бути як структурованим (CSV, SQL-таблиці), так і напівструктурованим (JSON, XML).

Базові механізми безпеки на рівні збору даних реалізуються за допомогою контролю доступу до тимчасового середовища, шифрування даних при їхньої передачі, валідація форматів тощо. Оскільки тут працюють з «сирими» даними, особливу увагу приділяють захисту від атак SQL-ін'єкцій та виявленню помилок у початкових структурах даних. Усі дії з даними логуються, забезпечуючи контроль та аудит операцій.

Інтеграційний рівень виконує повноцінну трансформацію даних у єдину логічну структуру, тобто перетворює неузгоджені, фрагментовані дані у цілісні, структуровані набори, придатні для подальшого аналізу. На цьому рівні здійснюються процеси очищення, стандартизації, трансформації та консолідації даних, що дозволяє усунути дублікати, виправити помилки форматування, вирівняти структури даних і забезпечити їхню узгодженість на всіх подальших етапах їхньої обробки. З цією метою застосовуються спеціалізовані інструменти ETL (Extract, Transform, Load) або ELT (Extract, Load, Transform), залежно від архітектури системи. Дані інструменти автоматизують процеси витягування даних, їхньої обробки відповідно до заданих бізнес-правил та подальшого завантаження до сховища. Також можуть використовуватися потокові платформи, такі як Apache Kafka або Apache NiFi, що дозволяють обробляти дані в реальному часі. Обов'язковим компонентом інтеграції є контроль походження даних (data lineage), який забезпечує прозорість і відстежуваність усіх трансформацій.

Потенційні загрози інтеграційного рівня можуть проводити спотворення даних під час трансформації, виконувати несанкціоновані зміни ETL-скриптів або ін'єкцію шкідливих даних. Для мінімізації ризиків на даному рівні впроваджуються механізми валідації даних, журналювання ETL-процесів, контроль цілісності інформації та обмеження прав доступу до середовища обробки. У випадках роботи з конфіденційними даними застосовуються методи псевдонімізації, шифрування або маскування під час інтеграції.

Data Warehouse Storage Layer відповідає за зберігання інтегрованих, очищених та структурованих даних, які надійшли з попередніх рівнів. Дані зберігаються у централізованих або розподілених систем управління базами даних, які можуть бути як традиційними реляційними (SQL Server, PostgreSQL, Oracle), так і спеціалізованими сховищами для аналітики (Snowflake, Amazon Redshift, Google BigQuery). Також часто застосовуються хмарні платформи, які забезпечують масштабованість, доступність і керованість. Функціонал даного рівня полягає у забезпеченні фізичної організації даних за допомогою таблиць фактів і розмірностей, індексів, партиціонування, кластерації тощо. Дані на фізичному рівні оптимізуються для швидкого виконання аналітичних запитів (OLAP), що передбачає високопродуктивне читання великих масивів інформації. З точки зору безпеки, фізичний рівень потребує реалізації таких механізмів, як шифрування даних на диску (at-rest encryption), контроль доступу на рівні таблиць, політик керування правами доступу, а також

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

журналювання операцій (Audit Trail). У разі використання хмарних рішень особливо важливим є дотримання політик розмежування клієнтських середовищ (multi-tenancy isolation), управління ключами шифрування та гарантування збереження даних у межах обумовленої юрисдикції.

Analytics and BI Layer здійснює підготовку, обробку та представлення даних, у зрозумілому для користувача вигляді, використовує інструменти бізнес-аналітики (BI), такі як Power BI, Tableau, Qlik Sense тощо та забезпечує доступ до аналітичних панелей, графіків, звітів та візуалізацій, що дає змогу керівникам і аналітикам оперативно оцінювати показники діяльності, з метою підтримки прийняття управлінських рішень. До основних функцій аналітичного рівня належать виконання багатовимірного аналізу даних (OLAP), побудова аналітичних моделей, створення агрегованих представлень та зберігання аналітичних кубів. Також, на даному рівні, можуть використовуватись алгоритми інтелектуального аналізу даних (data mining) і машинного навчання для виявлення прихованих аномалій або закономірностей.

Аналітичний рівень має підвищений ризик витоку чутливої інформації, оскільки користувачі мають доступ до зведених даних, аналітичної інформації з різних джерел. Тому необхідність впровадження багаторівневого контролю доступу, засобів авторизації, маскування конфіденційних атрибутів, журналювання дій користувачів та виявлення аномальної активності є необхідним механізмом забезпечення інформаційної безпеки даного рівня.

Access Layer відповідає за взаємодію кінцевих користувачів із системою зберігання та аналізу даних, з метою забезпечення зручного, безпечного та контрольованого доступу до інформації, у відповідно політики авторизації користувачів. На даному рівні, користувачі, які пройшли перевірко ідентифікації та авторизації, отримують доступ до результатів обробки даних, звітів, дашбордів або інших аналітичних ресурсів через різні інтерфейси, зокрема вебпортали, мобільні додатки, REST API, десктопних застосунків тощо. Окрема увага на рівні доступу приділяється управлінню правами доступу та забезпеченню конфіденційності інформації, тобто кожен користувач бачить тільки ті дані, які дозволено відповідно до його прав доступу до тієї чи іншої інформації, що досягається за допомогою політики доступу, динамічного маскування даних, фільтрації за атрибутами та інші механізми контролю.

Також на цьому рівні впроваджуються механізми автентифікації (наприклад, за допомогою SSO або багатофакторної автентифікації), авторизації на основі ролей (RBAC), шифрування каналів передачі даних (наприклад, HTTPS, TLS), а також моніторинг і логування дій користувачів.

Концептуальна модель безпеки інфраструктури сховищ даних

Формалізація функціональної моделі безпеки інфраструктури сховищ даних виконується за допомогою методології IDEF0 у середовищі ERwin. Методологія IDEF0 (Integration DEfinition for Function Modeling) є стандартом функціонального моделювання систем, що базується на моделі SADT (Structured Analysis and Design Technique) та широко використовується для опису, аналізу та проєктування складних процесів і систем, зокрема у сфері інформаційних технологій та безпеки. IDEF0 дозволяє створювати графічні моделі функцій системи та потоків інформації між ними. У центрі кожної моделі IDEF0 знаходиться компонент (робота), який виконує певну дію над вхідними даними, під впливом керуючих факторів, використовуючи механізми (ресурси), і генерує вихідний результат. Компоненти візуально представлені у вигляді прямокутника (функція) та стрілок чотирьох типів: Input (зображується зліва) вказує на інформацію, що підлягає обробці; Control (зображується зверху) зазначає нормативні документи та правила, які регламентують виконання певних функцій у системі; Mechanism (зображується знизу) перераховує як людські ресурси, так апаратно-програмне забезпечення, хмарні сервіси та Інтернет платформи, що забезпечують виконання функцій у системі; Output (зображується справа) та відображає результат функціонування системи в цілому.

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

Усі моделі IDEF0 створюються контекстна модель (найвищий рівень), яка описує вплив зовнішньої системи на діяльність описуваної системи, в нашому випадку це Security Management in Data Warehouse Infrastructure. Далі відбувається процес декомпозиції моделі, тобто її розбиття на компоненти, які деталізують діяльність моделі, розбиваючи її на підфункції.

На вхід моделі впливають дві стрілки: Data Assets та Security Threats.

Data Flows – це ті дані, що потребують захисту, тобто можуть бути персональні, фінансові, конфіденційні, стратегічні або виробничі дані. Потрапляння такої чутливої інформації у неналежні руки призведе до порушення законодавства, фінансових збитків або репутаційних втрат.

Security Threats – це потенційні або фактичні інформаційні ризики (такі як атаки зловмисників, віруси, витоки даних, SQL-ін'єкції, технічні збої), які є критичними тригерами, що зумовлюють необхідність вживати заходи комплексної безпеки для інфраструктури сховищ даних.

Control Arrows, в даній моделі, описують три стрілки: Security Policy, Compliance Requirements, Concept of the security strategy.

Security Policy (Політика безпеки) являє собою внутрішній нормативний документ організації / установи, що описує стратегію та тактику захисту інформації, в якому визначаються ролей користувачів, правила та привілеї доступу, методи автентифікації та авторизації, методика шифрування даних, аудит системи тощо.

Compliance Requirements (Регуляторні вимоги) представляє зовнішні стандарти та законодавчі акти (GDPR, ISO/IEC 27001, HIPAA тощо), яких повинна дотримуватись організація/ установи.

Security Strategy Concept (Концепція стратегії безпеки) – формує стратегічні, цілі та принципи побудови системи захисту інформаційних даних у сховищі, з метою забезпечення безперервного, комплексного та адаптивного захисту даних в інфраструктурі сховища даних, забезпечує відповідність законодавчим і галузевим вимогам. Концепція описує стратегію реагування на зовнішні (регуляторні зміни, кіберзагрози) та внутрішні (цифрова трансформація, захист інформації, контрактні зобов'язання) чинники, встановлює рамкові умови для реалізації політики інформаційної безпеки, інвестування у захист, підготовки кадрів і модернізації технологій.

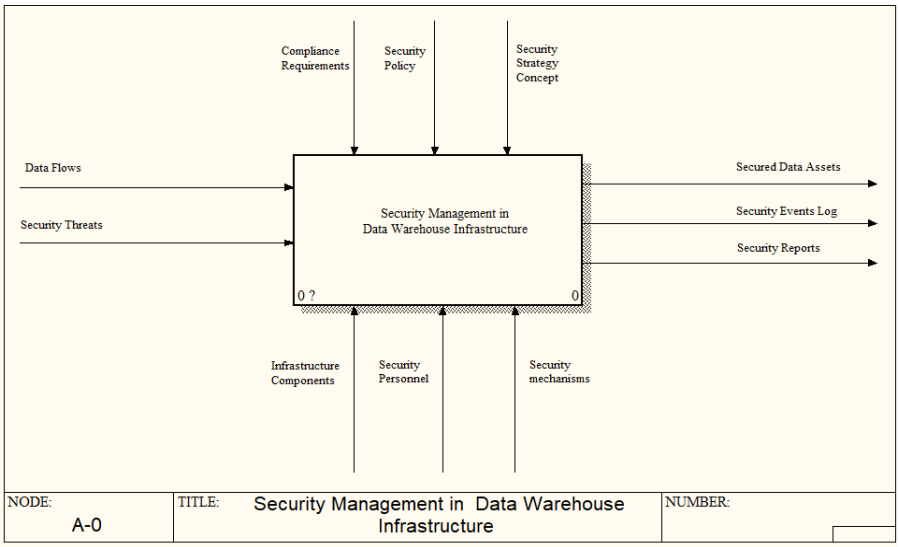

Рис. 2. Контекстна модель Security Management in Data Warehouse Infrastructure

На рис. 2 зображено контекстну модель Manage Security of Data Storage Infrastructure, яка моделює загальний процес забезпечення захисту даних, які зберігаються в інформаційній

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

інфраструктурі, під впливом зовнішніх та внутрішніх факторів, використовуючи відповідні ресурси і чітко описує систему управління безпекою в інфраструктурі сховищ даних.

Механізми є інструментами реалізації процесу, без яких інфраструктура сховища даних не може функціонувати.

На вихід моделі впливають три Output Arrows: Secured Data Assets *(Захищені інформаційні активи),* Security Events Log *(Журнал подій безпеки),* Security Reports *(Звіти безпеки).*

Secured Data Assets – структуровані або агреговані дані, що зберігаються у фізичному або хмарному сховищі, що були зібрані, трансформовані, збережені та захищені в межах інфраструктури сховища даних у відповідності до встановлених політик безпеки установи / організації. Доступ до таких активів надається виключно авторизованим користувачам, контролюється через рівневу модель доступу, захищений за допомогою шифрування at-rest і in-transit, маскування, псевдонімізації тощо.

Security Events Log *(Журнал подій безпеки)* – журнал, в якому виконується хронологічний запис усіх дій, пов'язаних із безпекою в інфраструктурі сховищ даних. Записи проводяться по такій структурі:

- спроби доступу (успішні/невдалі);
- зміни в політиках доступу;
- трансформації даних;
- активація тригерів безпеки (наприклад, підозрілої активності).

Журнал подій дозволяє відновити послідовність подій у разі інциденту або перевірки відповідності дій користувачів згідно їхніх прав доступу до об'єктів сховища даних.

Security Reports *(Звіти безпеки)* – аналітичні, узагальнюючі або регламентні документи, що формуються на основі даних з журналу подій, стану політик, інцидентів та виконання контролів. Призначення звітів у контексті моделі:

- підтвердження відповідності політикам та нормативам (ISO/IEC 27001, GDPR);
- інформування керівництва про стан безпеки в DWH (сховища даних);
- забезпечення прозорості для зовнішніх аудитів або інспекцій (наприклад, регуляторами або партнерами);
- рекомендації щодо покращення безпекових практик у межах усієї інфраструктури.

Отже, структурний аналіз складних функціональних систем методології IDEF0 (Integration Definition for Function Modeling) є потужним засобом побудови ієрархічної моделі, яка дозволяє формалізувати взаємозв'язки між основними компонентами системи: вхідними даними, керуючими впливами, механізмами реалізації та вихідними результатами. У межах побудови моделі Manage Security of Data Storage Infrastructure наступним кроком буде процес декомпозиції даної моделя, з метою деталізації вищерівневих процесів.

Декомпозиція – це процес ієрархічного розбиття моделі верхнього рівня на підмоделі нижчого рівня з метою забезпечення деталізації логіки управління, обробки та взаємодії даних. Модель деталізується у вигляді окремої діаграми, що складається з кількох взаємопов'язаних функціональних блоків (робіт). Критерій доцільності декомпозиції полягає у прагненні досягти зрозумілості та керованості кожного елемента моделі, а також відповідності логіці предметної області. У процесі декомпозиції моделі дотримуються наступні академічно визнані принципи:

- функціональної відповідності, в якому кожен підпроцес повинен відповідати частині логіки моделі вищого рівня;
- безперервності інформаційного потоку, при цьому стрілки моделі декомпозиції мають зберігати семантичну спадкоємність із відповідними стрілками контекстної моделі;
- узгодженості термінології, тобто назви стрілок на нижчому рівні повинні бути адаптовані до термінології предметної області.

У даному випадку контекстна модель Manage Security of Data Storage Infrastructure була декомпозована на шість функціональних підпроцесів відповідно до архітектури сховища

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

даних (рис. 1), тобто утворилось шість робіт: 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). На рисунку три подано результат декомпозиції моделі Manage Security of Data Storage Infrastructure. Сам розподіл базується на концепції багаторівневої архітектури систем збереження та обробки даних, заснований на стандартах ISO/IEC 2382.

Кожний компонент моделі декомпозиції також містить стрілки входу, виходу, контролю та механізмів. В нашому випадку, під час декомпозиції моделі відбулась і декомпозиція стрілок контролю та механізмів, стрілки входу та виходу залишились без декомпозиції, тому що Data Assets, Security Threats (вхід) та Secured Data Assets, Security Events Log, Security Reports (вихід) мають стабільну інформаційну сутність**,** яка не змінюється в залежності від підрівня, передаються до кожної роботи без зміни змісту і не потребують додаткового структурування.

У методології IDEF0 control arrow відображає нормативні, регуляторні або правові акти, які обмежують або регламентують виконання робіт моделі. При переході від верхньорівневої моделі до моделі нижчого рівня стрілки контролю підлягають семантичній декомпозиції, тобто отримують уточнене значення у відповідності до цілей кожної роботи нижчого рівня.

У представленій моделі декомпозиції Manage Security of Data Storage Infrastructure стрілка контролю Security Strategy Concept виконує роль глобального обмежувального чинника, що встановлює на основі нормативно-правових стандартів, таких як GDPR, ISO/IEC 27001, HIPAA, вимоги до інформаційної безпеки всієї інфраструктури сховища даних.

Після декомпозиції моделі і появі шість робіт, відповідно відбулась декомпозиція стрілки на шість підфункцій:

1. Компонент моделі декомпозиції Data Sources Layer має стрілку контролю Політика збору персональних і технічних даних (Personal and Technical Data Collection Policy), яка визначає, які саме дані дозволено збирати, з яких джерел, в який спосіб, хто за це відповідає та як виконується інформування користувачів про збір. Також на даному етапі забезпечується аудит відповідності принципам законності, справедливості й прозорості. Дана політика відповідає ст. 5(1)(c) регламенту GDPR – дані повинні бути зібрані відповідно до принципу мінімізації; також ст. 13–14 зобов'язують інформувати суб'єкта даних про збір; пункт A.5.33 стандарту ISO/IEC 27001, A.5.33 визначає обов'язковість дотримання юридичних, законодавчих та контрактних вимог при зборі даних;

2. Компонент моделі декомпозиції Data Staging Layer має стрілку контролю Політика попередньої обробки та знеособлення даних (Preprocessing and Data Anonymization Policy), яка визначає методи очищення, валідації, нормалізації та знеособлення даних перед їхньої передачі до сховища, з метою обмеження впливу компрометації чутливої інформації та підвищення рівню захисту конфіденційних даних, відповідно до вимог регуляторів. Дана політика відповідає ст. 25 (Data Protection by Design and by Default) регламенту GDPR, яка зазначає, що дані мають бути знеособленими або псевдонімізованими де це можливо; а ст. A.8.11 стандарту ISO/IEC 27001 рекомендує використовувати засоби маскування або знеособлення персональних даних для мінімізації ризиків;

3. Компонент моделі декомпозиції Integration Layer має стрілку контролю Політика цілісності та контролю потоків даних (Data Integrity and Flow Control Policy), яка описує механізми перевірки цілісності даних, контролю дублювання, виявлення помилок під час інтеграції, регламентує порядок оновлення даних, моніторинг аномалій, аудит ETL-процесів. Дана політика відповідає ст. A.8.9 стандарту ISO/IEC 27001 – встановлення та підтримка цілісності інформації під час обробки та передачі та ст. 5(1)(d) регламенту GDPR – персональні дані мають бути точними та, за потреби, оновлюваними;

4. Компонент моделі декомпозиції Data Warehouse Storage Layer має стрілку контролю Політика безпечного зберігання даних (Secure Data Storage Policy), що регламентує процес та

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

методику шифрування на рівні файлової системи та БД, захисту фізичного доступу до серверів, резервного копіювання, відмовостійкості тощо. Дана політика відповідає ст. 32 регламенту GDPR, яка вимагає вжиття заходів для забезпечення конфіденційності, цілісності, доступності, включаючи шифрування та ст. A.8.1 – A.8.4 стандарту ISO/IEC 27001, яка вимагає забезпечувати захист даних при обробці конфіденційної інформації;

5. Компонент моделі декомпозиції Analytics and BI Layer має стрілку контролю Політика контролю доступу до аналітичних даних (Analytical Data Access Control Policy), яка регламентує права доступу до створення аналітичних звітів, умови застосування фільтрації даних, а також допустимі рівні деталізації інформації для різних категорій користувачів. Дана політика враховує бізнес-ролі, рівень критичності інформації та вимоги до журналювання дій у BI-середовищі та відповідає ст. A.5.15 – A.5.18 стандарту ISO/IEC 27001 – обмеження доступу за ролями, принцип найменших привілеїв, ст. 25 та 32 регламенту GDPR – контроль доступу як основний захід безпеки;

6. Компонент моделі декомпозиції Access Layer має стрілку контролю Політика управління доступом користувачів (User Access Management Policy), яка визначає правила створення облікових записів, обов'язкову автентифікацію (зокрема MFA), облік сесій, тайм-аути, механізми відкликання доступу, забезпечуючи регулярний аудит прав користувачів і моніторинг порушень. Дана політика відповідає ст. A.5.15, A.5.16, A.5.17 стандарту ISO/IEC 27001 – доступ дозволяється лише авторизованим користувачам, на основі ролей та потреб, ст. 32 регламенту GDPR – захист доступу через автентифікацію, аудит, обмеження привілеїв.

Таким чином, абстрактне поняття стратегії безпеки трансформується в набір конкретизованих політик, що охоплюють, зокрема, політику захисту первинних даних, політику очищення та нормалізації, політику контролю доступу, політику забезпечення цілісності даних тощо. Вищенаведені елементи є не лише декомпозованими стрілками в термінах IDEF0, а й такими, що мають практичну цінність, оскільки їх реалізація є обов'язковою в межах дотримання сучасних міжнародних стандартів інформаційної безпеки.

Наступним кроком опишімо декомпозицію стрілки контролю Security Policy (Політика безпеки) для моделі декомпозиції Manage Security of Data Storage Infrastructure, яка теж утворила шість стрілок, у відповідності шести компонентам моделі.

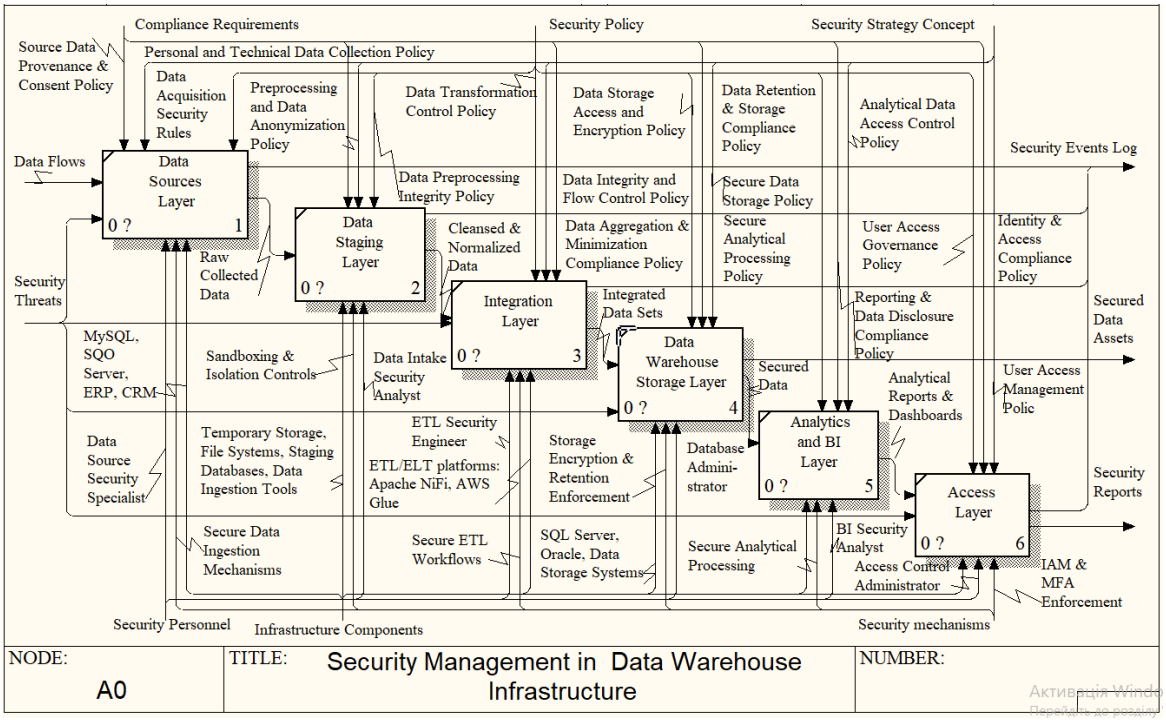

Рис. 3. Декомпозиція моделі Security Management in Data Warehouse Infrastructure

1. Компонент моделі декомпозиції Data Sources Layer має стрілку контролю Data Acquisition Security Rules (Правила безпеки отримання даних), яка описує правила та процедури забезпечення безпечного з'єднання з джерелами, які включають перевірку достовірності даних (використання сертифікатів, TLS/SSL), обмеження доступу до зовнішніх систем (IP allow-lists, API-ключі), контроль входу та авторизації служб. Назва відповідає стандартам NIST SP 800-53 (AC-17, IA-2).

2. Компонент моделі декомпозиції Data Staging Layer містить стрілку контролю Data Preprocessing Integrity Policy (Політика цілісності попередньої обробки даних) і визначає перевірку на відсутність шкідливого вмісту (антивірусні сканування), контроль повноти даних при ETL, журналювання змін, застосованих до даних (data lineage tracking). Назва базується на практиках ISO/IEC 27002 щодо цілісності даних.

3. Компонент моделі декомпозиції Integration Layer (Інтеграційний рівень) має стрілку контролю Data Transformation Control Policy (Політика контролю перетворення даних), яка містить правила перевірки сценаріїв трансформації (ETL/ELT скриптів), логування та валідації перетворених даних, захисту від SQL-ін'єкцій та маніпуляцій [17]. Назва корелює з OWASP Data Protection Guidelines.

4. Компонент моделі декомпозиції Data Warehouse Storage Layer містить стрілку контролю Data Storage Access and Encryption Policy (Політика доступу та шифрування для зберігання даних), яка фіксує методи шифрування даних, контролю доступу до баз даних, аудиту всіх дій з даними [19]. Назва визначається стандартами NIST SP 800-111, ISO/IEC 27040.

5. Компонент моделі декомпозиції Analytics and BI Layer має стрілку контролю Secure Analytical Processing Policy (Політика безпечної аналітичної обробки), яка затверджує методи маскування/анонімізації чутливих полів, запобігання побічним витокам (наприклад, через зворотну інженерію звітів), правила обмеження доступу до детальних даних. [16, 18] Назва базується на рекомендаціях CIS Controls v8 (Control 3: Data Protection).

6. Компонент моделі декомпозиції Access Layer містить стрілку контролю User Access Governance Policy (Політика управління користувацьким доступом), яка встановлює правила багатофакторної автентифікації (MFA), модель рольову доступу (RBAC), моніторингу і аналізу активності користувачів [20, 23]. Назва спирається на ISO/IEC 27001 (контроль A.9 – контроль доступу).

Стрілка контролю Compliance Requirements у моделі декомпозиції Manage Security of Data Storage Infrastructure визначає нормативні та галузеві стандарти, яким має відповідати система управління безпекою даних на всіх рівнях інфраструктури сховища даних, і вона також має бути декомпозованою для кожного компонента моделі, бо різні рівні обробки даних мають різні типи регуляторних зобов'язань. У табл.1 наведено відповідність декомпозиції стрілки коєному модулю моделі.

Концептуальна модель містить стрілку механізмів Security Personnel, який формується з IT-фахівців, що забезпечують функціонування всієї системи в цілому [18, 21]. При декомпозиції иоделі дана стрілка теж пройшла процес розбиття на шість стрілок, відповідно до кількості компонент даного рівня. Розглянемо більш детально персонал IT-фахівців, який на кожному рівні забезпечує безперебійне виконання механізмів безпеки кожного модулю інфраструктури сховища даних.

1. Компонент моделі декомпозиції Data Sources Layer має стрілку механізму Data Source Security Specialist (Фахівець із безпеки джерел даних), який забезпечує захищений доступ до джерел даних, налаштовує автентифікацію API, шифрування каналів (TLS, HTTPS), політики доступу на рівні драйверів, конфігурує CDC (Change Data Capture) та проводить аудит підключень. Роль зустрічається у практиках ETL-проєктів, NIST SP 800-53 (AC-20), а також у документації до Snowflake, AWS Glue, Apache NiFi [17, 20].

2. Компонент моделі декомпозиції Data Staging Layer містить стрілку механізму Data Intake Security Analyst (Аналітик з безпеки даних при прийомі), який контролює шифрування

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

даних у транзиті, реалізує валідацію структур (JSON/XML schemas), проводить антивірусну перевірку, налаштовує тимчасові політики доступу в staging-таблицях, відстежує логування інцидентів на цьому етапі, забезпечує контроль маскування «сирих» даних. IT-фахівець реалізує політику перевірки, валідації та захисту при завантаженні даних (відомо з практик DevSecOps + DataOps), узагальнення ролей в Azure Defender for Data і ETL Data Validation [20].

Таблиця 1

Декомпозиція стрілки контролю "Compliance Requirements"

Модуль моделі	**Назва декомпозованої стрілки контролю**	**Нормативна база**	**Опис політики**
Data Sources Layer	Source Data Provenance & Consent Policy	GDPR, CCPA	Забезпечує легальний збір, обробку та зберігання даних при наявної згоди користувача. Передбачає фіксацію джерела даних і документацію надання дозволу на обробку даних.
Data Staging Layer	Data Quality & Preprocessing Compliance Rules	ISO/IEC 25012, SOX	Регламентує очищення, трансформацію і нормалізацію даних, забезпечує прозорість і відповідність змін даних вимогам якості.
Integration Layer	Data Aggregation & Minimization Compliance Policy	GDPR (ст. 5), HIPAA	Забезпечує обробку лише необхідних даних, контролює унеможливлення надлишкового поєднання даних, запобігає доступу до нерелевантної або надмірної інформації, сприяє дотриманню принципу мінімізації даних відповідно до вимог та регламентів, забезпечує прозорість критеріїв вибору даних для обробки.
Data Warehouse Storage Layer	Data Retention & Storage Compliance Policy	GDPR, ISO 27001, PCI DSS	Визначає правила зберігання, архівації та видалення даних, забезпечує політику шифрування даних, терміну зберігання, автоматичного очищення.
Analytics and BI Layer	Reporting & Data Disclosure Compliance Policy	SOX, GDPR (ст. 15)	Регламентує створення звітів, їхню безпеку та зміст, при цьому забороняє включення чутливих полів без маскування.
Access Layer	Identity & Access Compliance Policy	ISO/IEC 27001, NIST 800-63, GDPR (ст. 32)	Забезпечує автентифікацію користувачів, політику найменших привілеїв, логування та аудиту доступу до даних.

3. Компонент моделі декомпозиції Integration Layer має стрілку механізму ETL Security Engineer (Інженер безпеки інтеграційних процесів), у його обов’язки входить контроль цілісності трансформацій, аудити ETL-процесів, контроль доступу до скриптів, захист скриптів від модифікацій, впровадження політики маскування/псевдонімізації та відповідає за захист логіки ETL/ELT від SQL-ін’єкцій [11], [17, 22]. Визнана роль у команді інтеграції, особливо у хмарних платформах (AWS Glue, Azure Synapse). ISO/IEC 27002:2022.

4. Компонент моделі декомпозиції Data Warehouse Storage Layer містить стрілку механізму Database Administrator (Адміністратор бази даних). Даний IT-фахівець забезпечує ізоляцію доступу (multi-tenancy), керування ключами шифрування та аудит запитів до даних, контролює права на таблиці, індекси. Роль фігурує в Oracle, SQL Server, PostgreSQL, ISO 27001 Annex A.

5. Компонент моделі декомпозиції Analytics and BI Layer має стрілку механізму BI Security Analyst (Аналітик безпеки бізнес-аналітики), який забезпечує багаторівневу авторизацію у BI-середовищі, налаштовує маскування результатів запитів, визначає атрибутивний контроль доступу (ABAC), виявляє аномальну поведінку користувачів через SIEM. Роль зустрічається у практиках Power BI, Tableau, Qlik, Looker, ISO 27017 (cloud security).

6. Компонент моделі декомпозиції Access Layer містить стрілку механізму Access Control Administrator (Адміністратор контролю доступу), в обов’язки якого входить налаштування

політики авторизації (RBAC, ABAC), керування ідентифікацією користувачів, впровадження багатофакторної автентифікації (MFA), управління життєвим циклом акаунтів (provisioning/deprovisioning) [20, 22-23]. Класична роль наявна у будь-якій системі з ідентифікацією користувачів. Згадується в ISO/IEC 27001, NIST 800-63, практиках IAM (Identity & Access Management) [20, 23].

Декомпозиція стрілка контролю Security mechanisms моделі Manage Security of Data Storage Infrastructure на шість функціональних робіт, реалізованої у нотації IDEF0, дозволяє деталізувати специфіку застосування механізмів безпеки на кожного модулю інфраструктури сховища даних [17], [19, 23]. Нижче подано табл. 2, яка містить назви цих механізмів для кожного модулю сховища, їхнє призначення та відповідність нормативним базам [22].

Таблиця 2

Декомпозиція стрілки контролю "Security mechanisms"

Модуль моделі	**Назва декомпозованої стрілки контролю**	**Нормативна база**	**Опис політики**
Data Sources Layer	Secure Data Ingestion Mechanisms	ISO/IEC 27001, NIST SP 800-53 (AC-17, SC-12)	Реалізація захищених протоколів передачі даних (HTTPS, SFTP, VPN), фільтрація та валідація вхідних даних, інтеграція з системами кіберрозвідки (Threat Intelligence Feeds) для запобігання проникненню шкідливого контенту на початковому етапі.
Data Staging Layer	Sandboxing & Isolation Controls	NIST SP 800-207 (Zero Trust), CIS Controls (Control 13)	Дані обробляються в ізольованому середовищі (sandbox), що унеможливлює їх взаємодію з продуктивними системами до моменту перевірки і включають механізми обмеження привілеїв, моніторинг дій
Integration Layer	Secure ETL Workflows	ETL Security Guidelines (IBM, Microsoft), ISO/IEC 27001 A.14.2.5	Забезпечує збереження конфіденційності і цілісності при об'єднанні даних із різних джерел. Включає контроль доступу до скриптів ETL, їх підписування та перевірку цілісності, шифрування проміжних даних, аудит ETL-запитів та обмеження джерел інтеграції.
Data Warehouse Storage Layer	Storage Encryption & Retention Enforcement	SO/IEC 27040, GDPR Art. 32, NIST SP 800-88	Упровадження шифрування даних на рівні диску та на рівні поля (field-level encryption), контрольоване видалення даних (data erasure), політики обмеження термінів зберігання згідно з вимогами нормативів (Data Retention Policies).
Analytics and BI Layer	Secure Analytical Processing	ENISA Big Data Threat Landscape, CIS Controls v8 (Control 5)	Реалізація обмежень на обробку чутливих даних у BI-звітах, маскування конфіденційної інформації, аудит запитів аналітиків, впровадження механізмів запобігання inference attacks.
Access Layer	IAM & MFA Enforcement	NIST SP 800-63B, ISO/IEC 27001 A.9 (Access Control), OWASP ASVS	Управління ролями (RBAC), застосування багатофакторної автентифікації, сесійне логування, політики зміни паролів, SSO-рішення.

Стрілка механізму Infrastructure Components у моделі декомпозиції Security Management in Data Warehouse Infrastructure функціонує як ресурс, який забезпечує апаратну та програмну основу для реалізації всіх процесів управління безпекою в інфраструктурі сховищ даних. Тобто являє собою апаратно-програмний комплекс, який охоплює широкий спектр елементів: від мережевого обладнання (маршрутизаторів, комутаторів, міжмережевих екранів), що забезпечує захищену передачу даних, до серверного обладнання – фізичного або віртуалізованого, яке є основою для розміщення баз даних, платформ ETL/ELT, сховищ даних і обчислювальних середовищ. Інфраструктура також включає хмарні середовища, які сьогодні

дедалі частіше використовуються для масштабованого зберігання даних та аналітики, а також бізнес-інтелект інструменти, що дозволяють візуалізувати інформацію, формувати звіти й приймати обґрунтовані управлінські рішення.

Висновки

У межах даного дослідження здійснено формалізацію процесів управління інформаційною безпекою інфраструктури сховищ даних на основі методології функціонального моделювання IDEF0. Побудована контекстна модель верхнього рівня дозволила визначити ключові структурні компоненти системи, зокрема: об’єкти захисту, нормативно-регламентуючі впливи, технічні та організаційні механізми реалізації безпеки, а також результати функціонування системи у вигляді захищених інформаційних активів та контрольних подій. Проведена декомпозиція функції управління безпекою на шість архітектурних рівнів дозволила ідентифікувати специфіку реалізації політик безпеки, типових загроз і відповідних заходів захисту на кожному з рівнів – від етапу джерел даних до рівня користувацького доступу. Особливу увагу приділено визначенню ролей персоналу з безпеки, а також застосовуваних інфраструктурних платформ, що забезпечують реалізацію захисних функцій. Модель орієнтована на відповідність міжнародним стандартам (ISO/IEC 27001, GDPR) та спрямована на підвищення керованості й прозорості систем захисту інформації.

Отримані результати мають як теоретичне, так і практичне значення. Запропонована модель створює основу для формалізованого опису функцій безпеки на різних рівнях архітектури сховища даних, що є важливим для розробки чітких процедур доступу, контролю та моніторингу обробки, зберігання та використання інформаційних ресурсів з метою запобігання несанкціонованому доступу, забезпечення цілісності даних та дотримання нормативно-правових вимог. Вона може бути інтегрована в процеси стратегічного планування інформаційної безпеки, слугувати базою для уніфікації внутрішніх політик та підтримувати подальше вдосконалення безпекової архітектури шляхом її деталізації за допомогою інструментів моделювання типу CASE.

Перелік посилань

1. Singh, S. P., & Afzal, N. (2024). The MESA security model 2.0: A dynamic framework for mitigating stealth data exfiltration. International Journal of Network Security & Its Applications, 16(3), 23–40. https://doi.org/10.48550/arXiv.2405.10880.

2. Tran, K., Vasudevan, S., Desai, P., Gorelik, A., Ahuja, M., Venkateshababu, A. Y., Verma, M., Hu, D., Moustafa, W. E., Rajamani, V., Gupta, A., Buenrostro, I., & Raina, K. (2025). Data Guard: A fine-grained purpose-based access control system for large data warehouses. Computer Science: Cryptography and Security, 2–13. https://doi.org/10.48550/arXiv.2502.01998.

3. Fugkeaw, S., Suksai, P., & Hak, L. (2024). SSF-CDW: Achieving scalable, secure, and fast OLAP query for encrypted cloud data warehouse. Journal of Cloud Computing, 13, Article 129. https://doi.org/10.1186/s13677-024-00692-y.

4. Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. Journal of Cloud Computing, 13, Article 15. https://doi.org/10.1186/s13677-023-00587-4.

5. 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), Article 3187. https://doi.org/10.3390/app13053187.

6. Лєнков, С., Джулій, В., Муляр, І., & Димбовський, М. (2024). Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі. Pidvodni Tehnologii, 13, 45–59. https://doi.org/10.32347/uwt.2023.13.1205.

7. Головацький, Н. Т. (2024). Питання захисту персональних даних при використанні хмарних технологій. Аналітично-порівняльне правознавство, 5, 72–78. https://doi.org/10.24144/2788-6018.2024.05.72.

8. Фасій, Б. (2024). Національна безпека та захист персональних даних в епоху цифрових технологій. Society and Security, 6(6), 76–82. https://doi.org/10.26642/sas-2024-6(6)-76-82.

9. Пристай, Р. А. (2023). Приватність за замовчуванням: Користувацька модель даних як основа захисту приватності та персональних даних в соціальних мережах. Науковий вісник Ужгородського національного університету. Серія: Право, 80(1), 84–89. https://doi.org/10.24144/2307-3322.2023.80.1.84.

10. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

11. 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.

12. International Organization for Standardization. (2022). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection—Information security controls. https://www.iso.org/standard/75652.html.

13. European Union Agency for Cybersecurity. (2021). Pseudonymisation techniques and best practices. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

14. European Data Protection Board. (2020). Guidelines 4/2019 on Article 25: Data protection by design and by default. https: // edpb.europa.eu /our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

15. 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.

16. Sarker, I. H. (2021). Data science and analytics: An overview from data-driven smart computing, decision-making and applications perspective. SN Computer Science, 2, Article 377. https://doi.org/10.1007/s42979-021-00765-8.

17. Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка, 4(28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857.

18. Shah, J., & Baghela, V. (2025). Developing data governance frameworks for cloud-based platforms: Ensuring data quality and security. International Journal of Research and Analytical Reviews, 12, 252–261.

19. Складанний, П. М., Машкіна, І. В., Рзаєва, С. Л., & Костюк, Ю. В. (2025). Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології, 2, 59–76. https://doi.org/10.31673/2412-4338.2025.027860.

20. Rafi, S., Yogesh, R., & Sriram, M. (2024). Optimized dual access control for cloud-based data storage and distribution using global-context residual recurrent neural network. Computers & Security, 151, Article 104183. https://doi.org/10.1016/j.cose.2024.104183.

21. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956.

22. Amaresam, R. K. (2025). Security and compliance in cloud-native data warehousing: A technical deep dive. International Research Journal of Modernization in Engineering Technology & Science. https://doi.org/10.56726/IRJMETS69854

23. Складанний, П., Костюк, Ю., & Рзаєва, С. (2026). Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Математичні машини і системи, 1, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46.

Rzaeva Svitlana
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7589-2045
E-mail: s.rzaieva@kubg.edu.ua

Andrii Bondarchuk
Doctor of Technical Sciences, Professor, Head of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5124-5102
E-mail: a.bondarchuk@kubg.edu.ua

Yuliia Kostiuk
PhD, Associate Professor
Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua

Dmytro Rzaiev
Senior Lecturer of the Department of Informatics and Systemology,
Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine
ORCID ID: 0000-0002-7149-4971
E-mail: rzaiev@kneu.edu.ua

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118. https://doi.org/10.31673/2409-7292.2026.035620

Pavlo Skladannyi
PhD, Associate Professor
Head of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
E-mail: p.skladannyi@kubg.edu.ua

FUNCTIONAL MODEL OF SECURITY MANAGEMENT IN DATA WAREHOUSE INFRASTRUCTURE

The article considers the problem of ensuring information security of data warehouse infrastructure under conditions of increasing information volumes, growing complexity of storage system architectures, and rising requirements for ensuring data confidentiality, integrity, and availability. It is shown that modern data warehouses operate in a complex information environment characterized by large volumes of structured and unstructured information, distributed computing resources, cloud technologies, and multi-level access mechanisms, which necessitates the development of a comprehensive information security management system. The limitations of traditional security management approaches have been identified, as they do not provide a sufficient level of process formalization, complicate the coordination of information flows, and do not allow full integration of international standard requirements into the internal architecture of data warehouses. A systematic approach to the construction of a functional model for information security management of data warehouse infrastructure based on the IDEF0 methodology is proposed. Structured modeling was used to formalize functional processes, enabling the description of relationships between information flows, security management mechanisms, and infrastructure components of the system. A top-level context model was developed and decomposed according to the functional levels of the data warehouse architecture. For each functional level, appropriate security mechanisms, access policies, infrastructure protection tools, and relationships with regulatory requirements were identified. Particular attention was paid to the integration of the provisions of international standards ISO/IEC 27001, ISO/IEC 27002, and the General Data Protection Regulation (GDPR) into the security management processes of data warehouse infrastructure. It is shown that the use of the IDEF0 methodology makes it possible to increase the level of process structuring in information security management, ensure formalization of security procedures, and improve the controllability of information flows. The obtained results confirm the feasibility of using structured functional modeling to improve the efficiency of information security management and ensure the resilience of data warehouse infrastructure against modern cyber threats and information security violations.

Keywords: functional modeling, IDEF0, information security management, data warehouses, security policy, decomposition, ISO/IEC 27001, GDPR, data architecture.

Надійшла до редакції (Received): 01.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

© Рзаєва С.Л, Бондарчук А.П., Костюк Ю.В., Рзаєв Д.О., Складанний П.М. Функціональна модель управління безпекою в інфраструктурі сховищ даних. Сучасний захист інформації, 3(67), 103–118.
https://doi.org/10.31673/2409-7292.2026.035620