УДК 004.8:004.4:004.67 https://doi.org/10.33099/2304-2745/2025-2-85/66-73

Капілевич В. О. (0000-0001-9025-7608)
Звір В. Б. (0000-0002-6823-7552)
Ліпко І. О. (0009-0001-6663-5899)
Ганненко С. О., кандидат технічних наук (0000-0002-8285-1145)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Вимоги до технічних сервісів, які використовують метадані у єдиному інформаційному середовищі сил оборони України

Резюме. У статті розглянуто використання метаданих технічними сервісами для забезпечення обміну, захисту, каталогізації та інтерпретації даних в межах єдиного інформаційного середовища. Надано функціональні та нефункціональні вимоги до технічних сервісів, що дасть змогу формувати гнучкі та адаптивні механізми, які здатні забезпечити взаємосумісність (інтероперабельність) та інформаційну безпеку у складному, динамічному, багатодоменному середовищі.

Ключові слова: єдине інформаційне середовище; технічні сервіси; метадані; інформаційні ресурси; управління інформацією; маркування.

Постановка проблеми. Відповідно до заходів виконання Стратегічного оборонного бюлетеня України (стратегічна ціль 1, завдання 1.5) цифрова трансформація діяльності та впровадження сучасних інформаційних технологій визначені одним із ключових завдань для сил оборони України [1, 2]. Очікуваним результатом реалізації таких заходів є створення та повноцінне функціонування Об'єднаної мережі оборони та мереж операцій, що ґрунтуються на взаємодії в багатодоменному середовищі складових сил оборони, держав – членів НАТО та їх партнерів [2].

Аналіз досвіду асиметричного протистояння Російській Федерації (РФ) свідчить про необхідність постійного покращення інформаційної переваги над ворогом. Це можливо за наявності єдиного інформаційного середовища, в якому довірені особи мають доступ до інформаційних ресурсів, важливих для прийняття рішень з будь-якої підключеної мережі операцій [3, 4]. Завдяки цьому актуальна інформація для прийняття рішень формується на основі даних із широкого спектра доступних джерел, від сенсорних систем і розвідувальних засобів до тактичних каналів зв'язку та логістичних підсистем [5]. Отже, виконання завдань силами оборони по відбиттю збройної агресії відбувається в умовах необхідності взаємодії між різнорідними комунікаційними та інформаційними системами та сервісами. У цьому контексті метадані виступають ключовим інструментом для забезпечення взаємосумісності (інтероперабельності), управління доступом, автоматизації обробки інформації та її семантичного узгодження.

Однак технічні сервіси, які мають використовувати метадані в рамках Об'єднаної мережі оборони та мереж операцій, часто розробляються без урахування узгоджених стандартів метаданих, єдиних вимог до структур, схем, політик доступу та контролю. Це призводить до фрагментації інформаційного середовища, дублювання зусиль, ускладнення обміну інформацією між різними спільнотами інтересів та зниження ефективності спільних дій.

Проблема полягає в тому, що на сьогодні відсутня цілісна система формалізованих вимог до технічних сервісів, які використовують метадані для забезпечення обміну, захисту, каталогізації та інтерпретації даних у рамках єдиного інформаційного середовища (далі – ЄІС). Це створює бар'єри для ефективного управління інформацією між спільнотами інтересів, тому актуальним постає завдання щодо формування відповідних вимог до технічних сервісів, які використовують метадані.

Таким чином, потребує необхідність (доцільність) проведення аналізу ролі метаданих як ключового інструмента у багатодоменному середовищі, окреслення вимог (функціональних та нефункціональних) до технічних сервісів, які працюють з метаданими, а також узагальнення підходів до стандартизації, маркування та управління інформацією.

Аналіз останніх досліджень та публікацій. На сьогодні спостерігається зростаючий інтерес до тематики застосування метаданих, що підтверджується збільшенням кількості наукових публікацій та аналітичних оглядів у цій сфері.

У [6] автори розглядають питання аналізу метаданих для уникнення дублювання інформаційних ресурсів, що дозволяє забезпечити точність в обробці великих обсягів даних. Дослідники розглядають аспекти пошуку дублікатів записів, що є критичним для підтримки якості баз даних, а також висловлюють свої погляди на вирішення проблемних питань, пов'язаних з зайвими витратами часу на здійснення ручного порівняння та видалення дублікатів. Разом з тим, завдяки фокусу на службових метаданих, питанням управління інформації не приділяється достатньої уваги.

Так, у [7] розглянуті питання застосування метаданих у процесах пошуку в частині збільшення результатів пошуку документів, що задовольняють запиту, в рамках деякої статичної колекції документів. Дослідники звернули увагу на аспекти нечіткого пошуку на основі тегів і семантичних мета-сутностей, а також розглянули тегування електронних записів.

У [8] автори звертають увагу на показники якості метаданих та проблемні питання пошуку та виправленню помилок в описі метаданих ресурсів.

Зазначені підходи є недостатніми для формування повноцінної основи, необхідної для розроблення вимог до технічних сервісів, що забезпечують роботу з метаданими.

Метою статті є визначення та обґрунтування вимог до технічних сервісів, що використовують метадані у єдиному інформаційному середовищі.

Викладення основного матеріалу. У контексті сучасних об'єднаних операцій, які здійснюються в умовах багатодоменного середовища (мультідоменні операції), ефективне управління інформацією набуває особливої ваги. Такі умови передбачають одночасну взаємодію у кібер-, повітряному, наземному, морському та космічному доменах із залученням багатьох суб'єктів: військових, цивільних, урядових, міжурядових та комерційних організацій. У цьому контексті метадані виступають критичним інструментом для забезпечення обміну інформацією, її доступності, взаємосумісності (інтероперабельності), достовірності та безпеки.

Метадані являють собою формалізований набір даних, призначений для опису характеристик, призначення, місця розташування або контексту інформаційних ресурсів з метою полегшення їх виявлення, використання та адміністрування [9]. У багатодоменному інформаційному середовищі, де об'єднуються потоки даних із різними рівнями доступу, достовірності, походження та безпеки, метадані виступають ключовим елементом забезпечення семантичної сумісності. Вони створюють інформаційний контекст, необхідний для взаємодії між різними користувачами, цифровими платформами та технічними сервісами в межах однієї або декількох спільнот інтересів [5].

Узгоджені метадані дають змогу:

класифікувати дані за ступенем конфіденційності;

вказувати походження, авторство та час створення ресурсу;

забезпечувати відстежуваність змін;

підтримувати виконання політик доступу;

забезпечувати дотримання національних і міжнародних стандартів з інформаційної безпеки.

У багатодоменному середовищі, особливо під час об'єднаних операцій НАТО, метадані виконують кілька ключових функцій:

ідентифікацію та каталогізацію інформаційних об'єктів для ефективного пошуку та повторного використання;

підтримку обміну між різними спільнотами інтересів, включаючи можливість адаптації до семантичних відмінностей;

реалізацію політик доступу шляхом застосування міток конфіденційності, політик дозволів і механізмів контролю на базі перевірки визначених атрибутів;

забезпечення взаємосумісності (інтероперабельності) на рівні форматів, структур і семантики даних між різними доменами, організаціями та платформами;

підтримку автоматизації процесів прийняття рішень через можливість машинної інтерпретації контексту, значення та правового статусу інформації.

Слід зауважити, що у багатодоменному середовищі забезпечення безпеки та довіри до даних неможливе без використання метаданих. Метадані слугують елементом інформаційного управління та безпеки і є основою для:

реалізації міждоменного захисту інформації, включаючи позначення рівнів доступу, цільових аудиторій, умов обробки тощо;

підтримки відстежуваності у ланцюгу життєвого циклу інформації від її створення до видалення;

інтеграції рішень у хмарних середовищах, де метадані дають змогу підтримувати контроль над ресурсами, навіть коли фізичний контроль над IT-інфраструктурою відсутній;

захисту від втрати інформації та її компрометації, оскільки правильне маркування інформації дозволяє застосовувати відповідні механізми збереження, резервування та аудиту до важливої інформації.

Таким чином, метадані відіграють центральну роль у забезпеченні ефективного та цілеспрямованого управління інформацією як у межах окремих систем і сервісів, так і між ними. Їх широке застосування є характерним як загалом, так і в межах окремих спільнот інтересів, які використовують метадані для підтримки обробки релевантної інформації у своїй предметній галузі. Багато таких спільнот розробили власні специфікації метаданих, які згодом були формалізовані у вигляді угоди зі стандартизації *(en: Standardization Agreement, STANAG)* або іншої нормативної документації. Прикладами застосування чітко визначених метаданих є спільноти інтересів: спільної розвідки, спостереження та рекогносцировки *(en: Joint Intelligence, Surveillance and Reconnaissance, JISR)*, обміну повідомленнями у форматі *(en: Message Text Format, MTF)*, геопросторові та інші.

Незважаючи на відмінності у специфікаціях, спрямованих на окремі сценарії використання, спостерігається значний ступінь перетину метаданих між різними спільнотами інтересів. Загальні елементи, такі як рівень конфіденційності, назва ресурсу, автор або дата створення, часто є присутніми у різних схемах метаданих. Додаткові атрибути, включаючи дату вилучення, юридичний статус, авторські права, список пов'язаних сторін або зв'язки з іншими ресурсами, можуть бути важливими для забезпечення якісного управління інформаційними ресурсами.

Оскільки ці елементи розробляються автономно в межах окремих спільнот інтересів, виникає проблема несумісності термінології, яка ускладнює обмін метаданими між спільнотами та між системами чи сервісами. Для подолання цього бар'єру найбільш ефективним підходом є використання спільного проміжного стандарту, визнаного на рівні корпоративного середовища. Прикладом використання такого підходу серед держав-членів НАТО є Базова специфікація метаданих *(en: Core Metadata Specification)*, яка забезпечує уніфіковану основу, що може адаптуватися до потреб кожної спільноти інтересів в межах спільного інформаційного середовища НАТО [10].

Довідка. *NATO Core Metadata Specification* – це специфікація, яка визначає основні елементи метаданих, необхідні для опису, класифікації, захисту та обміну інформаційними об'єктами в комунікаційних та інформаційних системах держав-членів НАТО та їх партнерів.

Згідно з Класифікатором технічних сервісів комунікаційних та інформаційних систем [11], використання метаданих у межах ЄІС стосується наступних сервісів:

сервісів, що забезпечують взаємодію між спільнотами інтересів: сервісів сховища моделей *(en: Model Repository Services)*, сервісів реєстрації інформації *(en: Information Registry Services)* та інших;

сервісів підтримки службової діяльності: сервісів геопросторових каталогів *(en: Geospatial Catalog Services)*, сервісів геопросторових тайлів веб-карт *(en: Geospatial Web Map Tile Services)* та інших;

сервісів платформ: сервісів маркування інформації *(en: Information Labeling Services)*, сервісів маршрутизації повідомлень *(en: Message Routing Services)*, сервісів надання інформації *(en: Information Discovery Services)*, сервісів сховищ метаданих *(en: Metadata Repository Services)*, сервісів інформаційних анотацій *(en: Information Annotation Services)*, сервісів даних платформ *(en: Data Platform Services)*, сервісів надання інформації про дані *(en: Data Discovery Services)*, сервісів доступу до даних *(en: Data Access Services)* та інших;

сервісів інфраструктури: сервісів розподіленого зберігання об'єктів *(en: Distributed Object Storage Services)* та інших.

Згадані технічні сервіси, що оперують метаданими, відіграють ключову роль у забезпеченні керованого, захищеного та ефективного обміну інформацією. Така роль обумовлює потребу у чіткому визначенні вимог до таких сервісів, які повинні підтримувати високий рівень надійності, сумісності, масштабованості та відповідності політикам безпеки.

У цьому контексті доцільно розрізняти функціональні та нефункціональні вимоги, які формують основу проєктування, розгортання та експлуатації відповідних сервісів у середовищах із різними рівнями довіри, доступу та інфраструктурної підтримки.

Функціональні вимоги визначають, які саме можливості має реалізовувати технічний

сервіс у процесі обробки, обміну та управління метаданими. До ключових функціональних вимог належать вимоги, які наведено у Табл 1.

Таблиця 1

Функціональні вимоги до технічних сервісів

Назва вимоги	Короткий опис вимоги
Створення та редагування метаданих	Сервіси мають дозволяти ручне і автоматизоване формування метаданих відповідно до затверджених профілів, словників та шаблонів (наприклад, *NATO Core Metadata Specification, Dublin Core*). **Довідка.** *Dublin Core* – це загальновизнаний стандарт описових метаданих, який складається з 15 базових елементів, що використовуються для уніфікованого опису інформаційних об'єктів
Зберігання та каталогізація	Забезпечення доступу до репозиторіїв метаданих із підтримкою індексації, пошуку та версіювання; використання моделей даних, які підтримують ієрархічні та зв'язні структури (наприклад, *XML*). **Довідка.** *XML (eXtensible Markup Language)* – це стандарт мови розмітки, розроблений консорціумом W3C, який дає змогу визначати власні структури даних для структурованого подання, зберігання та обміну даними в текстовому форматі
Розпізнавання та інтерпретація маркування	Здатність аналізувати марковану інформацію, зчитувати контекстні атрибути (політика доступу, мітки безпеки, дата створення, джерело тощо) та забезпечувати відповідну обробку в комунікаційних та інформаційних системах та сервісах
Валідація метаданих	Перевірка відповідності формату, структури та змісту метаданих вимогам стандартів і профілів використання
Інтеграція з іншими сервісами	Сервіси повинні мати інтерфейси для взаємодії *(en: Application Programming Interface, API)* з системами зберігання даних, платформами обміну, засобами управління доступом *(ABAC/PBAC)*, а також із сервісами безпеки. **Довідка.** *Attribute-Based Access Control* – це механізм управління доступом, у якому рішення про доступ ґрунтується на оцінці атрибутів суб'єкта, об'єкта, дій та середовища. *Policy-Based Access Control* – це механізм управління доступом, який надає або забороняє доступ до ресурсів на основі заздалегідь визначених політик безпеки.
Аудит і відстежування (трасування)	Реєстрація подій створення, змін, доступу, розповсюдження і знищення метаданих у відповідності до вимог кібербезпеки та принципів забезпечення відповідальності

Нефункціональні вимоги до сервісів роботи з метаданими описують параметри якості, яким мають відповідати сервіси незалежно від їхньої функціональності. До ключових нефункціональних вимог належать вимоги, які наведено у Табл 2.

Таблиця 2

Нефункціональні вимоги до технічних сервісів

Назва вимоги	Короткий опис вимоги
Безпека	Сервіси повинні реалізовувати шифрування даних як під час передавання, так і при зберіганні, автентифікацію користувачів, атрибутивний контроль доступу та підтримку політик конфіденційності (наприклад, згідно з угодами зі стандартизації *STANAG 4774 / 4778*). **Довідка.** *STANAG 4774 (Confidentiality Metadata Label Syntax)* визначає синтаксис метаданих безпеки, зокрема міток конфіденційності, політик доступу, умов публікації та ін., що застосовуються до об'єкта даних [12–14]. *STANAG 4778 (Confidentiality Metadata Binding)* встановлює методи прив'язки цих метаданих до об'єктів даних для забезпечення їхньої цілісності, достовірності та дотримання політик безпеки при обміні інформацією в багатодоменному середовищі [15–17]
Взаємосумісність (інтероперабельність)	Підтримка стандартів обміну метаданими між організаціями, доменами та платформами (наприклад, *NIEM, NATO Core Metadata Specification*). **Довідка.** *NIEM (National Information Exchange Model)* – це загальнонаціональна модель обміну інформацією, розроблена у США для стандартизації, спрощення та пришвидшення міжвідомчого й міжорганізаційного обміну даними. Вона надає узгоджені структурні компоненти (модулі даних, словники, типи об'єктів), які можна повторно використовувати під час проєктування схем *XML* [18].
Масштабованість	Можливість ефективної роботи з великими обсягами метаданих у динамічному середовищі без зниження продуктивності або функціональності
Надійність та відмовостійкість	Забезпечення стабільної роботи сервісу у випадку часткових збоїв IT-інфраструктури або втрати зв'язку, у тому числі завдяки реплікації, резервному копіюванню та автоматичному відновленню
Продуктивність	Обробка запитів повинна відбуватись у прийнятні часові рамки для оперативного прийняття рішень, особливо в контексті розвідки чи управління операцією

Адаптивність	Можливість динамічного оновлення політик, словників, схем метаданих без переривання роботи сервісу

Слід зазначити, що проєктування технічних сервісів має враховувати гібридний характер середовищ, у яких вони працюють – поєднання хмарних, тактичних і локальних компонентів єдиного інформаційного середовища.

Архітектура таких сервісів повинна підтримувати:

модульність (відокремлення ядра сервісу, інтерфейсів, політик, інтерпретаторів);

сумісність з сервісно-орієнтованими архітектурами;

відкриті стандарти обміну повідомленнями *(SOAP, REST, gRPC, MQTT)*;

інтеграцію із системами контролю та управління доступом, що реалізують *ABAC* або *PBAC*.

Довідка. *SOAP (Simple Object Access Protocol)* – це протокол обміну повідомленнями, заснований на *XML*, який використовується для забезпечення суворо структурованої взаємодії між компонентами розподілених систем, зокрема в середовищах, де потрібна висока безпека та надійність.

REST (Representational State Transfer) – архітектурний стиль для побудови вебсервісів, що ґрунтується на стандартних методах протоколу *HTTP (GET, POST, PUT, DELETE). REST* забезпечує простоту реалізації, гнучкість та масштабованість взаємодії між клієнтами та серверами.

gRPC (Google Remote Procedure Calls) – фреймворк відкритого коду, який базується на *HTTP/*2 і протоколі *Protocol Buffers (Protobuf),* оптимізований для високоефективного, двостороннього потокового обміну даними між сервісами у мікросервісній архітектурі.

MQTT (Message Queuing Telemetry Transport) – легкий протокол обміну повідомленнями, спеціально створений для пристроїв із обмеженими ресурсами та нестабільними мережами зв'язку, який використовує модель публікації/підписки (publish/subscribe), особливо поширений в IoT-середовищах *(en: Internet of Things).*

Враховуючи динамічність та чутливість багатодоменних середовищ, технічні сервіси повинні підтримувати:

контекстну оцінку запитів (наприклад, геолокація, час, роль, місія);

динамічне застосування політик безпеки, у тому числі на основі ролей, атрибутів та правил;

використання міток та політик, які реалізують багаторівневий контроль доступу.

Таким чином, технічні сервіси, що працюють з метаданими, повинні реалізовувати комплексні функції підтримки повного життєвого циклу інформації від створення до динамічного управління доступом. Наявність чітко визначених функціональних та нефункціональних вимог забезпечує їхню відповідність викликам багатодоменного інформаційного середовища, підтримує міжвідомчу сумісність та сприяє ефективному застосуванню інформації у процесах прийняття рішень.

У ЄІС, де відбувається взаємодія між численними підрозділами сил оборони, платформами та рівнями оперативного управління, виникає необхідність у впровадженні уніфікованих підходів до стандартизації, маркування (тегування) та управління інформацією (рис. 1). Така уніфікація є необхідною умовою забезпечення взаємосумісності (інтероперабельності), цілісності, захисту та динамічного контролю доступу до даних на всіх етапах їхнього життєвого циклу.

Рис. 1. Уніфікація підходів

Стандартизація інформації будується на основі міжнаціональних практик. Вона полягає в узгодженні форматів, структур та описових моделей інформації, яка здійснюється за допомогою прийнятих стандартів метаданих, форматів обміну та профілів реалізації. У військово-цивільному та міждоменному контексті широко застосовуються такі підходи:

союзна публікація [10], яка забезпечує спільну основу для опису інформаційних об'єктів у системах НАТО, з підтримкою розширення для специфічних потреб певного домену;

угоди зі стандартизації [12–17], які стосуються захисту та прив'язки політик доступу до метаданих і контенту;

національна модель обміну інформацією [18], яка використовується у США для стандартизації обміну інформацією між відомствами, з акцентом на модульність, повторне використання об'єктів та профілювання;

міжнародний стандарт [19], який забезпечує опис, реєстрацію та повторне використання метаданих у межах спільного середовища;

загальновизнаний стандарт *Dublin Core* та профіль застосування *GeoDCAT-AP (en: Geospatial Data Catalog Vocabulary Application Profile)*, які забезпечують базову взаємосумісність (інтероперабельність) для опису інформаційних ресурсів у відкритих екосистемах, зокрема геопросторових.

Довідка. *GeoDCAT-AP (Geospatial Data Catalog Vocabulary Application Profile)* – це профіль застосування стандарту *DCAT*, розроблений для забезпечення взаємосумісності (інтероперабельності) геопросторових метаданих у рамках відкритих державних даних ЄС. GeoDCAT-AP дозволяє публікувати метадані геопросторових наборів даних, сервісів та серій у форматі, сумісному з *DCAT*. Він забезпечує автоматизовану взаємодію між геоінформаційними системами та платформами відкритих даних.

Загальною рисою сучасних підходів є модель відкритої, профільованої стандартизації, коли ядро стандарту може бути адаптоване під конкретні контексти без втрати сумісності з базовим профілем.

Маркування інформації реалізується як засіб управління доступом та контекстної інтерпретації. Маркування (або тегування) інформації метаданими – це основний механізм забезпечення контролю за її обігом, використанням і споживанням у динамічному середовищі.

Такий підхід дає змогу:

прив'язувати політики безпеки безпосередньо до даних;

реалізовувати багаторівневий контроль доступу на основі контексту;

підтримувати функції аудиту, відстеження походження та авторства.

Маркування реалізується за допомогою:

атрибутів безпеки *("classification", "releasability", "caveats"),*

контекстних міток *("timestamp", "geolocation", "source", "mission relevance"),*

профілів доступу (дозволені ролі, цілі використання, умови використання).

Особливого значення маркування набуває у хмарних і гібридних середовищах, де втрачається контроль над фізичним розміщенням даних, а засоби захисту мають супроводжувати сам об'єкт даних незалежно від місця його обробки або зберігання.

Управління інформацією у розподіленому середовищі передбачає підтримку повного життєвого циклу даних, від їх створення і класифікації до архівації або знищення. Цей процес повинен бути керованим, контрольованим і масштабованим.

До ключових складових системи управління інформацією слід віднести:

механізми політик доступу, які забезпечують реалізацію правил на основі атрибутів, ролей або політик контексту операцій; підтримку динамічного оновлення політик відповідно до зміни ситуації;

інструменти оркестрації даних, які будуються на базі сервісів, що автоматизують валідацію, маршрутизацію, фільтрацію та трансформацію інформації згідно з маркуванням та політиками;

взаємосумісні (інтероперабельні) репозиторії метаданих, які будуються у вигляді систем реєстрації, пошуку, та управління описовими даними, і які дозволяють забезпечити видимість інформаційних ресурсів у спільному середовищі;

системи управління даними операції, які створюються у вигляді засобів, що визначають релевантність, актуальність і пріоритетність інформації в контексті конкретної операції.

Попри наявність усталених підходів, впровадження ефективного управління інформацією в умовах багатодоменних операцій стикається з низкою викликів:

розбіжності у політиках, форматах та рівнях класифікації потребують розвитку універсальних профілів;

необхідність оперативного реагування на зміну середовища, операцій, ролей або політичних умов – потребує динамічного застосування та інтерпретації маркування;

все більше систем використовують автоматичне виконання рішень на основі машинно-читаних політик доступу, що потребує їхньої формалізації та уніфікації.

У відповідь на ці виклики активно розвиваються концепції датацентричної безпеки *(en: data-centric security),* інформаційно-центричної мережі *(en: information-centric networking),* архітектури з нульовим рівнем довіри *(en: zero trust architecture)* та інші підходи, що передбачають зміщення фокусу захисту з інфраструктури на самі дані.

Таким чином, узагальнення існуючих підходів до стандартизації, маркування та управління інформацією демонструє тенденцію до формування гнучких та адаптивних механізмів, які здатні забезпечити взаємосумісність (інтероперабельність) та інформаційну безпеку у складному, динамічному, багатоорганізаційному середовищі. Подальше удосконалення цих підходів передбачає інтеграцію сучасних стандартів, розвиток відкритих онтологій, підтримку автоматизованого управління даними, а також урахування досвіду сучасних конфліктів, зокрема російсько-української війни.

Висновки. Метадані є ключовим елементом в управлінні інформацією у багатодоменному середовищі, забезпечуючи семантичну узгодженість, маркування, безпеку, керованість доступом та підтримку взаємосумісності (інтероперабельності) між спільнотами інтересів різних платформ і доменів.

Технічні сервіси, що працюють з метаданими, повинні підтримувати широкі функціональні можливості від генерації, перевірки, збереження та оновлення метаданих до інтеграції із системами управління доступом та політиками безпеки.

Функціональні вимоги до технічних сервісів, що працюють з метаданими, мають охоплювати всі етапи життєвого циклу даних: від маркування, класифікації та опису до забезпечення механізмів пошуку, контролю доступу, та реалізації політик збереження й видалення інформації.

Зі свого боку, нефункціональні вимоги, зокрема у сферах інформаційної безпеки, масштабованості, продуктивності, відповідності прийнятим стандартам обміну інформацією, а також у сфері стійкості до збоїв і здатності до інтеграції в багаторівневі та гібридні середовища, виступають критично важливими умовами для гарантування довіри, стабільності та адаптивності технічних сервісів.

Забезпечення взаємосумісності (інтероперабельності) між різними системами та доменами можливе лише за умови дотримання стандартів метаданих та використання відкритих інтерфейсів, узгоджених словників даних і референтних моделей.

Успішна реалізація міждоменного обміну інформацією передбачає застосування узгоджених підходів до стандартизації, маркування та забезпечення довіри, включно з автоматизованим контролем політик безпеки на основі атрибутів метаданих.

Подальші дослідження слід зосередити на обґрунтуванні вимог до сервісів, які забезпечують датацентричну безпеку у єдиному інформаційному середовищі сил оборони.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегічний оборонний бюлетень України: Указ Президента України від 17.09.2021. № 473. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 13.07.2025).
2. Ліпко І. О., Звір В.Б., Капілевич В.О., Сугак С.О. Запровадження класифікації інформаційних технологій у сфері оборони: досвід НАТО для України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. 2024. № 2 (81). С. 74–85.
3. DOD CLOUD STRATEGY. December 2018. 18 p.
4. Скорик А. Б., Ярош С. П., Меленті Д. О., Вплив руйнівних технологій на розвиток архітектури C4ISR систем. Концептуальні основи побудови архітектури дата-центричної системи-систем // Системи озброєння і військова техніка. 2020. № 4 (64). С. 107–119.
5. AC/322-D(2015)0001-COR1-FINAL, NATO Core Data Framework – a Vision for Data Interoperability. 13 March 2015. CONSULTATION, COMMAND AND CONTROL BOARD (C3B). 6 p.
6. Василенко О. О. Аналіз основних метаданих для пошуку дублікатів бібліографічних записів // Кібербезпека: освіта, наука, техніка. 2025. № 3 (27). С. 87–99.
7. Савицька Л. А., Коробейнікова Т. І., Тягун В. Д. Метод та програмний засіб застосування метаданих в процесах пошуку // Інформаційні технології та комп'ютерна інженерія. 2019. № 3. С. 21–27.
8. Новицький С. В, Новицька Т. Л. Основні типи помилок при внесенні ресурсів до електронної бібліотеки НАПН України як фактор впливу на підтримку інформаційно-дослідної діяльності науковців // Актуальні питання сучасної інформатики : матеріали доп. V Всеукр. наук.-практ. конф. з міжнар. участю "Сучасні

інформаційні технології в освіті та науці". Вип. 8. Житомир, Україна, 2020. С. 84–89.
9. AC/322-D(2005)0053-REV1, NATO Network Enabled Capability (NNEC) Data Strategy, 7 April 2009. NATO C3 Board. 28 p.
10. ADatP-5636 NATO CORE METADATA SPECIFICATION(NCMS), Edition A, Version 1, 18 November 2022. 276 p.
11. Класифікатор технічних сервісів комунікаційних та інформаційних систем, базова версія 0.9 : затв. заступником Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації 25.11.2024 за № 5933/уд.
12. ADatP-4774 CONFIDENTIALITY METADATA LABEL SYNTAX, Edition A, Version 1, 20 December 2017. 108 p.
13. ADatP-4774.1 CONFIDENTIALITY METADATA LABEL SYNTAX (CMLS) – IMPLEMENTATION GUIDANCE, Edition A, Version 1, November 2021. 102 p.
14. ADatP-4774.2 GUIDANCE ON THE DIGITAL LABELLING OF NATO INFORMATION, Edition A, Version 1, June 2021. 36 p.
15. ADatP-4778 METADATA BINDING MECHANISM, Edition A, Version 1, 26 October 2018. 72 p.
16. ADatP-4778.1 METADATA BINDING MECHANISM (MBM) – IMPLEMENTATION GUIDANCE, Edition A, Version 1, November 2021. 28 p.
17. ADatP-4778.2 PROFILES FOR BINDING METADATA TO A DATA OBJECT, Edition A, Version 1, December 2020. 120 p.
18. NIEM Model. URL: https://www.niem.gov/about-niem/niem-model (дата звернення: 14.07.2025).
19. International standard ISO/IEC 11179-3:2013(E), Information technology – Metadata registries (MDR) – Part 3: Registry metamodel and basic attributes. Third edition 2013-02-15. 244 p.

Стаття надійшла до редакційної колегії 24.07.2025

Requirements for technical services that use metadata in the unified information environment of the Defense Forces of Ukraine

Annotation

According to the Strategic Defense Bulletin of Ukraine (strategic goal 1, task 1.5), digital transformation and the implementation of modern information technologies are defined as key priorities for the Defense Forces of Ukraine. The expected outcome of these measures is the creation and full-scale operation of the Federated Defense Network and mission networks, based on multidomain interoperability among components of the Defense Forces, NATO member states, and their partners.

An analysis of Ukraine's experience in asymmetric confrontation with the Russian Federation (RF) highlights the necessity of continuously enhancing information superiority over the adversary.

The purpose of this article is to define and justify the requirements for technical services that utilize metadata within the unified information environment.

Technical services operating with metadata must support extensive functionality, ranging from metadata generation, validation, storage, and updating to integration with access management systems and security policies.

Functional requirements for metadata-based technical services should encompass all stages of the data lifecycle: from labeling, classification, and description to ensuring mechanisms for search, access control, and the enforcement of retention and deletion policies.

At the same time, non-functional requirements – particularly in the areas of information security, scalability, performance, compliance with accepted information exchange standards, fault tolerance, and the ability to integrate into multi-layered and hybrid environments – are critically important conditions for ensuring the trustworthiness, stability, and adaptability of such technical services.

Keywords: unified information environment; technical services; metadata; information resources; information management; labeling.