УДК 004.75 DOI: https://doi.org/10.33099/2304-2745/2022-3-76/68-75

Кірпічніков Ю. А., кандидат технічних наук (0000-0001-6893-3569)
Капілевич В. О. (0000-0001-9025-7608)
Андрощук О. В., кандидат психологічних наук (0000-0002-1032-7459)
Петрушен М. В. (0000-0002-7448-2765)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб

Резюме. Обґрунтовано застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для створення єдиного інформаційного простору сил оборони, що дасть змогу ефективно використовувати інформацію, необхідну для прийняття рішень на всіх рівнях (від стратегічного до тактичного) для успішного виконання завдань за призначенням.

Ключові слова: єдиний інформаційний простір; дата-центричний підхід; інформаційна інфраструктура; хмарні технології; хмарні сервіси.

Постановка проблеми. У сучасних умовах розвитку збройних сил передових країн світу та динамічної зміни геополітичної обстановки, швидкість обміну інформацією стає ключовим показником, від якого залежить досягнення стратегічних цілей у сфері оборони. Завдяки розвитку інформаційних технологій та засобів зв'язку, широкому використанню технологій автоматизації управлінської діяльності суттєво збільшується інтенсивність інформаційного обміну, а новим типом службової діяльності посадових осіб оборонних відомств та органів військового управління різних рівнів стає дата-центричний обмін інформацією для прийняття управлінських рішень, комплексної автоматизації процесів управління військами, бойовими засобами (зброєю), а також оборонними ресурсами.

Дата-центричний підхід – це архітектурний підхід, у якому інформаційна інфраструктура створюється навколо загальнодоступного сховища даних. За такого підходу дані відіграють вагомішу роль ніж програмне забезпечення та зміщується фокус на створення системи зберігання та обробки даних з єдиним сховищем даних, з фізичним або логічним доступом до нього. До того ж для уникнення недоліків, які притаманні клієнт-серверній архітектурі, найпоширенішою парадигмою створення єдиного сховища даних на сьогодні стають *хмарні технології*, які дають змогу надати гарантований мережевий доступ за допомогою інформаційно-комунікаційної мережі до віддалених обчислювальних ресурсів серверів і сховищ даних для розподіленої обробки інформації з подальшим наданням цих ресурсів користувачам у якості хмарних сервісів.

Довідка. *Хмарні технології* – це технології розподіленої обробки даних, за допомогою яких обчислювальні ресурси (мережі, сервери, сховища даних, додатки) надаються користувачеві як хмарний сервіс. *Хмарний сервіс* – послуга надання доступу "на вимогу" до колективно використовуваного набору обчислювальних ресурсів, які користувач може оперативно задіяти та отримати результати роботи у вікні web-браузера на підключеному до мережі пристрої [1].

Протягом останніх років для сектору безпеки та оборони України створювались та розвивались різноманітні за призначенням автоматизовані, інформаційні, інформаційно-аналітичні та інші програмні системи, що не зв'язані між собою. Територіально розподілена інформаційна інфраструктура сил оборони на сьогодні характеризується відокремленістю та ізольованістю її складових, які реалізовані у вигляді "вертикальних замкнутих контурів" з відсутністю технічного варіанта обміну між інформаційними системами, які "утримують" інформаційні ресурси з різними ступенями доступу до інформації. Існуючий стан інформаційного середовища є більше статичним, ніж динамічним, що не дає змоги швидко адаптуватись під потреби споживачів інформації та унеможливлює ефективне використання інформації для забезпечення оперативної потреби "потрібна інформація в потрібному місці в потрібний час". Отже,

існуюче інформаційне середовище не дає змоги підтримувати дата-центричний підхід та отримати повною мірою інформаційну перевагу над ворогом.

Аналіз останніх досліджень та публікацій. Світові тенденції щодо застосування для оборонних потреб дата-центричного підходу та використання хмарних технологій спонукають передові країни світу проводити дослідження, направлені на забезпечення створення для власних збройних сил динамічного "безшовного" інформаційного середовища через всю вертикаль управління, де:

інформація є доступною;

засоби створення, обміну та використання інформації є захищеними;

технічні спроможності інформаційно-комунікаційних мереж забезпечують доступ до необхідної інформації, використовуючи наявні інформаційно-комунікаційні технології.

Розуміння необхідності об'єднання інформаційних систем оборонного призначення у цілісну взаємозв'язану інформаційну інфраструктуру ще декілька десятків років назад призвело до появи концепції мережево-центричної війни (*network-centric warfare*) [1]. З еволюційним розвитком цієї концепції, враховуючі перспективні шляхи розвитку озброєння та військової техніки, а також розвиток сучасних інформаційно-комунікаційних технологій, нині активно розглядається створення дата-центричних систем, оптимізованих для ведення бойових дій з використанням єдиного інформаційного простору (ЄІП), відповідно до концепції дата-центричних операцій (*data-centric operation*) [2–7].

Найбільш практичну реалізацію дата-центричний підхід з використанням сучасних інформаційно-комунікаційних технологій отримав у країнах НАТО. Доктринальні вказівки НАТО щодо інтеграції комунікаційних та інформаційних систем у спільних операціях спонукають країни – партнери НАТО розвивати свої спроможності щодо використання ЄІП, створеного згідно еталонної архітектурної моделі – Federal Mission Network (FMN) [8]. Частина країн – партнерів НАТО вже приєдналася до програми FMN, яка на цей час відображає сутність об'єднаних між собою оборонних мереж, в основі яких закладено специфічну для збройних сил кожної країни інформаційну інфраструктуру. Це дає змогу підвищити оперативну сумісність, безпеку роботи мереж, а також економічну ефективність за рахунок повторного використання доступних спроможностей.

Для досягнення технічної сумісності комунікаційних та інформаційних систем країн-партнерів, модель FMN передбачає реалізацію сервісно-орієнтованої архітектури інформаційної інфраструктури з мінімально-необхідним набором базових функціональних сервісів, таких як: електронна пошта, спільна робота з документами, обмін текстовими, аудіо- та відеоповідомленнями тощо, що має дати змогу користувачам у сфері оборони знаходити та обмінюватись потрібною інформацією у потрібний час, у вигляді для ефективного її використання, і водночас забезпечить унеможливлення доступу до інформації особам, які не мають на це право. Поступове нарощування спроможностей до більш складних сервісів, таких як відстеження своїх та дружніх військ (сил), ситуаційної обізнаності, розпізнаванням картини навколишнього середовища, розвитку каналів передачі даних та інших функціональних сервісів кожна країна має застосовувати власні підходи.

Оскільки ініціатива FMN відкрита для країн-партнерів, Україна теж може офіційно приєднатися до неї. Відповідне питання вивчається національними експертами [9]. Проте, враховуючі існуючий стан інформаційної інфраструктури сил оборони та невизначеність підходів щодо подальшого розвитку моделі FMN, актуальним стає завдання моделювання шляхів застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій. Розроблення відповідної моделі дасть змогу системним аналітикам і архітекторам інформаційної інфраструктури проводити дослідження та визначати вимоги до перспективних інформаційних систем, які підтримують роботу у дата-центричному середовищі.

Метою статті є розроблення моделі застосування дата-центричного підходу з використанням хмарних технологій для визначення вимог до інформаційних систем під час побудови інформаційної інфраструктури оборонного призначення.

Викладення основного матеріалу. Створення ЄІП сил оборони передбачає, що інформаційні ресурси розглядаються як стратегічний відомчий набір даних. Традиційна модель "локального володіння інформацією" окремими інформаційними

системами та користувачами має перетворитися на модель "обміну інформацією", у якій вони одночасно є джерелами та приймачами інформації, а інформаційні системи є взаємопов'язаними.

Модель обміну даними між багатьма користувачами ґрунтується на положенні, що джерело інформації має багато способів доставки цієї інформації багатьом користувачам одночасно, а споживачі інформації мають можливість отримувати інформацію від багатьох джерел одночасно. Інформація (набори даних), яка необхідна для прийняття рішень (первинні необроблені дані та відформатовані дані), має бути доступна в реальному часі для визначених та авторизованих користувачів.

Основою створення ЄІП має стати підхід із використанням хмарних технологій та сервісно-орієнтованою архітектурою інформаційної інфраструктури, що забезпечить доступ до інформації, а також до автоматизованих функціональних процесів у вигляді функціональних (хмарних) сервісів. Надання функціональних сервісів має підвищити взаємодію споживачів інформації під час проведення сумісних операцій, забезпечити швидке досягнення нових інформаційних спроможностей та покращити процес обміну інформацією.

ЄІП, що утворюється на основі *хмарного середовища* обміну інформацією, має складатися з багатьох гетерогенних (різнорідних) взаємозалежних інформаційних систем. Функціонування та захист ЄІП покладається на всіх його учасників. Учасники ЄІП мають функціонувати за визначеними правилами (політиками), а доступ до інформації, яка необхідна для прийняття рішень, є динамічним, автоматизованим та гарантованим.

Довідка. *Хмарне середовище* (або хмара) – це набір територіально розподілених центрів обробки даних та інформаційно-комунікаційних мереж, завдяки яким можна отримати доступ до даних з будь-якого пристрою, підключеного до мережі [10].

Основою хмарного середовища обміну інформацією має стати захищена інформаційно-комунікаційна мережа, яка з'єднує інформаційні системи, платформи, спеціалізоване програмне забезпечення, інформаційні бази даних, сенсори, споживачів інформації (від начальників та командирів до солдат на полі бою). Захищена мережа має забезпечити функціонування спеціалізованого програмного забезпечення та надання користувачам функціональних сервісів, використовуючи всі можливості та переваги захищеного середовища передачі даних. Це дасть змогу отримати інформаційну перевагу над ворогом, що зі свого боку має надати оперативну перевагу. Це також критично вплине на процеси обміну інформацією та управління військами завдяки пришвидшенню процесу прийняття рішень та дасть змогу діяти ефективніше в динамічних і складних умовах.

ЄІП має складатися з набору (сукупності) різнотипних спроможностей для збору, зберігання, обробки, передачі та захисту інформації. Це забезпечить створення інформаційного поля для широкого кола користувачів. Ключовим продуктом створення ЄІП є інформація. Великі обсяги даних мають бути доступними користувачам у реальному часі. З боку користувачів, доступ до інформації в ЄІП має бути простим, безперервним, захищеним та надійним, що забезпечується відповідними функціональними сервісами з різними рівнями доступу до інформації. Користувачі повинні бути авторизованими та аутентифікованими, мати можливість швидкого підключення до ЄІП та мати стійке з'єднання.

Користувачам тактичної ланки, які є обмеженими у швидкості передачі даних, також необхідно надати можливість отримати на вимогу необхідні функціональні сервіси. ЄІП має динамічно адаптуватися на рівні сервісів та каналів зв'язку, виходячи з потреб користувачів та їх інформаційних пріоритетів. У разі переривань у з'єднанні, доступ до інформації може тимчасово обмежуватися. Ця спроможність дасть змогу географічно віддаленим користувачам об'єднуватись в спільні групи для виконання спільних завдань.

Надання функціональних сервісів реалізується шляхом створення груп сервісів (Community of Interest Services – COI), у яких формується необхідний обсяг даних, якими обмінюються учасники під час виконання спільних дій [11]. Для кожної COI необхідно домовитися про використання спільного інтерфейсу та структури даних, а також визначити необхідні джерела інформації. Користувачі зможуть знайти та отримати доступ до інформації шляхом розширеного пошуку або шляхом відповідного запиту (інформація на вимогу). Також користувачі попередньо можуть формувати запити на відповідну інформацію з ЄІП (попередній запит на вимогу).

Функціональні сервіси на основі спеціалізованого програмного забезпечення мають забезпечити автоматизовані процеси отримання, обробки та візуалізації інформації у зручному для користувачів вигляді. Таким чином, користувачі отримають можливість використовувати прозорість, доступність, прихованість та живучість інформації та функціональних сервісів, які їм надає захищений ЄІП.

Гетерогенна інфраструктура ЄІП глобально може бути побудована з федеративних об'єднаних мереж, які дають змогу користувачам швидко передавати, зберігати, обробляти та отримувати доступ до секретної інформації з необхідних інформаційних доменів. Засоби зв'язку та автоматизації, базові сервіси та інфраструктура захисту інформації, входять у відповідні інформаційні домени загального портфоліо (набору) функціональних сервісів.

Автоматизований обмін інформаційними потоками між серверами є критично важливим для отримання інформаційної переваги під час використання ЄІП. Процес взаємодії користувачів з ЄІП за допомогою засобів автоматизації забезпечує простий і зрозумілий інтерфейс у процесі обміну інформацією. У якості робочих місць користувачі мають застосовувати "тонкі клієнти", використовуючи хмарні сховища центрів обробки даних (ЦОД) в якості джерел інформації. У тактичній ланці такий підхід знижує ризики, пов'язані з втратою носіїв інформації (тактичних планшетів, комп'ютерів). Користувачі, які не мають стабільного з'єднання з ЦОД, можуть використовувати технологію "товстого клієнту": з попередньо підготовленою мережевою архітектурою та сервісами, які розгорнуті локально під час виконання завдань та із завантаженими даними на своїх серверах. У такому разі відповідні сервери мають періодично з'єднуватись з ЦОД для синхронізації (оновлення) даних, таких як загальна оперативна картина, бойові розпорядження, оновлення дозволів користувачів чи оновлення сервісів.

Інформаційні запити до інформаційних баз даних мають взаємодіяти з усіма базами даних для отримання максимально точного та повного результату. Для забезпечення швидкого отримання інформації відповідно до запиту, має бути забезпечений семантичний, структурований реєстр інформаційних баз даних, що пришвидшує автоматизований пошук інформації за відповідним запитом. Застосування каталогу метаданих дасть змогу забезпечити необхідне індексування даних та створення захищених з'єднань між користувачем та сховищем даних відповідно до політик безпеки.

Згідно з описаним підходом, інформаційні системи (включаючи спеціалізоване програмне забезпечення) виглядатимуть як набір необхідних для виконання завдань функціональних сервісів, які дають змогу автоматизувати необхідні функціональні процеси. Зазначені функціональні сервіси мають бути здатними до динамічної адаптації та нарощування своїх спроможностей, залежно від потреб користувачів. Прикладом є сервіси Command and Control (C2), які використовуються під час спільних операцій (місій) НАТО та забезпечують ситуаційну обізнаність для швидкого та якісного прийняття рішень [12].

Функціональність сервісів C2 нарощується за допомогою розроблення та впровадження нових версій спеціалізованого програмного забезпечення, а не створенням нової інформаційної інфраструктури. Взаємодія між різнорідним за функціональним призначенням спеціалізованим програмним забезпеченням відбувається завдяки обміну між базами даних (у необхідних обсягах для забезпечення взаємодії). Усі сервіси C2 доступні для користувачів незалежно від їх географічного місця розташування. Сервіси C2 є захищеними та функціонують у стабільному, захищеному мережному середовищі, яке побудоване відповідно до прийнятих політик безпеки. Це означає, що користувач може безпечно користуватись сервісами та інформацією відповідно до прийнятих політик безпеки. У разі виникнення ситуації, коли неможливо забезпечити стійкий і надійний доступ до деяких сервісів, за допомогою відповідних технічних рішень доступ до необхідної інформації все одно залишатися надійним та надається в реальному часі.

Таким чином, дата-центричний підхід під час побудови інформаційної інфраструктури з використанням хмарних технологій, дасть змогу користувачам та інформаційним системам обмінюватись необхідною інформацією, а також ділитись новою інформацією, яку вони створюють. Такий підхід дасть змогу пришвидшити ефективність процесів обміну інформацією, а також використовувати стандартизовані (шаблонні) заходи захисту від несанкціонованого доступу до інформації.

Для реалізації запропонованого підходу у вигляді конкретної інформаційної інфраструктури необхідно здійснити трансляцію множини взаємодіючих функціональних процесів, процедур їх реалізації у вигляді функціональних сервісів, додатків та інформаційних систем, відповідних їм даних та користувачів, а також відношень між ними (рис. 1) в модель застосування дата-центричного підходу, яка дасть змогу визначити вимоги до задіяних інформаційних систем.

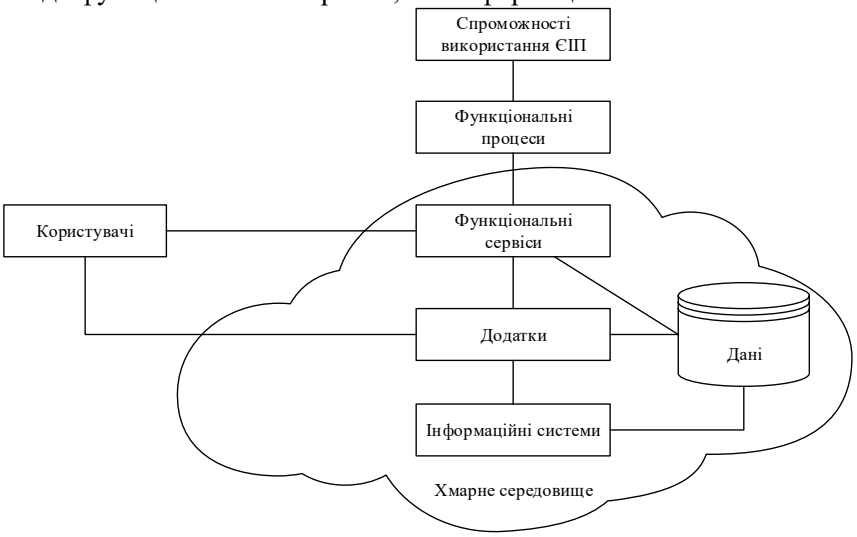


Рис. 1. Схема відношень елементів інформаційної інфраструктури на основі дата-центричного підходу у хмарному середовищі

Вихідними даними для формування моделі, які мають надати системні аналітики та архітектори інформаційної інфраструктури є:

опис необхідних спроможностей, набуття яких потрібно під час створення ЄІП;

опис основних функціональних процесів, зв'язків між спроможностями і функціональними процесами;

опис зв'язків між функціональними сервісами, додатками, що виконують обробку даних, і функціональними процесами;

опис зв'язків між користувачами, функціональними сервісами, додатками та інформаційними системами.

Модель утворюють елементи множин і відношень між ними:

$G = \{g_i \mid i = \overline{1,I}\}$ – множина спроможностей;

$P = \{p_j \mid j = \overline{1,J}\}$ – множина функціональних процесів;

$F = \{f_k \mid k = \overline{1,K}\}$ – множина функцій (функціональних сервісів), що реалізують функціональні процеси;

$U = \{u_l \mid l = \overline{1,L}\}$ – множина користувачів;

$A = \{a_m \mid m = \overline{1,M}\}$ – множина додатків, що реалізують функції;

$S = \{s_n \mid n = \overline{1,N}\}$ – множина інформаційних систем;

$D_{вх} = \{d_t \mid r = \overline{1,T_{вх}}\}$ – множина вхідних даних інформаційних систем;

$D_{вих} = \{d_t \mid r = \overline{1,T_{вих}}\}$ – множина вихідних даних інформаційних систем;

$D = D_{вх} \cup D_{вих}$ – повна множина даних інформаційних систем;

$R_1 = (G, P)$ – відношення "спроможності – функціональні процеси";

$R_2 = (F, P)$ – відношення "функціональні процеси – функції";

$R_3 = (F, A)$ – відношення "функції – додатки";

$R_4 = (S, A)$ – відношення "інформаційні системи – додатки";

$R_5 = (F, U)$ – відношення "функції – користувачі";

$R_6 = (A, U)$ – відношення "додатки – користувачі";

$R_7 = (F, D)$ – відношення "функції – дані";

$R_8 = (A, D)$ – відношення "додатки – дані";

$R_9 = (S, D)$ – відношення "інформаційні системи – дані".

Модель дає змогу описати дата-центричну інформаційну інфраструктуру у вигляді бази даних елементів, наведених множин і зв'язків між ними (рис 2).

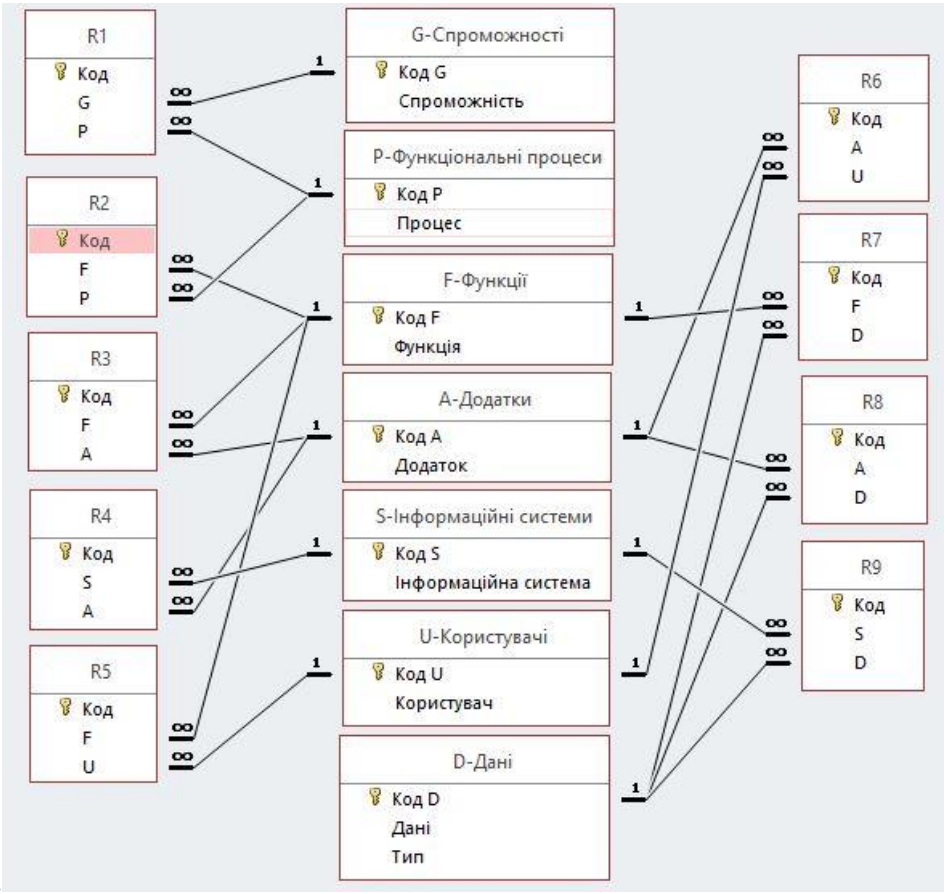


Рис. 2. Концептуальна модель застосування дата-центричного підходу

Формально модель застосування дата-центричного підходу може бути виражена як $M = \langle G, P, F, U, A, S, D, R \rangle$, де $R = \{R_z \mid z = \overline{1, Z}\}$ – множина відношень між елементами множин (G, P, F, U, A, S, D).

Використовуючи запропоновану модель, можна сформулювати порядок визначення вимог до інформаційних систем, створення яких потрібно для набуття необхідних спроможностей в ході побудови інформаційної інфраструктури:

1. Визначення необхідних спроможностей *G* та функціональних процесів *P*, що їх реалізують, формування відношення R_1.

2. Визначення функцій *F* для кожного функціонального процесу на основі аналізу відношень R_1 та R_2.

3. Визначення переліку інформаційних систем *S* на основі отриманої інформації й аналізу відношень R_3 та R_4.

4. Визначення переліку функцій *F* і додатків *A* для кожного користувача на підставі аналізу відношень R_5 і R_6..

5. Формування пар $\langle S\ R_g S \rangle$, де R_g, – відношення між інформаційними системами на підставі отриманої інформації та використання відношень R_7 і R_8.

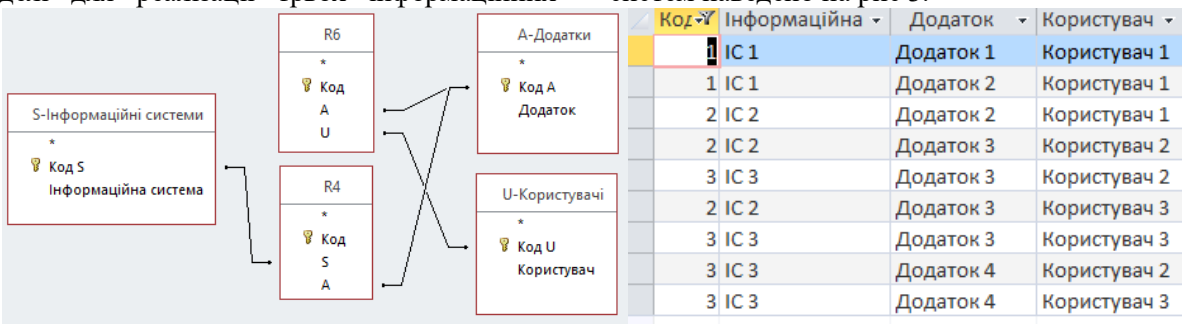
6. Формування пар $\langle S\ R_d S \rangle$, де R_d – відношення приналежності даних інформаційним системам на підставі аналізу відношення R_9.

7. Спільний аналіз сформованих відношень R_g, R_d, а також відношень R_7, R_8 та R_9 для встановлення неоднозначності та суперечливості описів об'єктів даних.

8. Використання отриманої на основі моделі *M* бази даних елементів множин (G, P, F, U, A, S, D) та множини R відношень між елементами для аналізу специфікацій інформаційних систем та визначення вимог до них.

Системні аналітики та архітектори за допомогою побудови реляційних запитів в отриману базу даних можуть розглянути різні варіанти взаємозв'язків між елементами хмарного середовища. Приклад формування запиту у базу даних з тестовими даними

моделі для реалізації трьох інформаційних систем наведено на рис 3.



Код	Інформаційна	Додаток	Користувач
1	ІС 1	Додаток 1	Користувач 1
1	ІС 1	Додаток 2	Користувач 1
2	ІС 2	Додаток 2	Користувач 1
2	ІС 2	Додаток 3	Користувач 2
3	ІС 3	Додаток 3	Користувач 2
2	ІС 2	Додаток 3	Користувач 3
3	ІС 3	Додаток 3	Користувач 3
3	ІС 3	Додаток 4	Користувач 2
3	ІС 3	Додаток 4	Користувач 3

Рис. 3. Приклад запиту у базу даних

Аналіз результатів запитів у базу даних щодо варіантів реалізації взаємозв'язків у хмарному середовищі дасть змогу сформувати раціональну топологію інформаційної інфраструктури та визначити вимоги до інформаційних систем, а саме:

функціональні сервіси, які необхідно надати користувачам;

необхідні додатки для реалізації функціональних сервісів;

вхідні та вихідні дані для обміну між інформаційними системами і користувачами.

Вимоги до реалізації апаратної частини інформаційних систем у розробленій моделі не розглядаються, оскільки обчислювальні ресурси визначають адміністратори хмарного середовища. Для отримання користувачами функціональних (хмарних) сервісів потрібен лише пристрій з web-браузером, який підключено до мережі.

Таким чином, спроможності щодо створення (розвитку) ЄІП набуваються завдяки впровадженню набору інформаційних систем, які реалізуються визначеними додатками та надають певні функціональні сервіси для автоматизації функціональних процесів.

Висновки. Запропонована модель дає змогу описати множину взаємодіючих у ЄІП процесів, процедур їх реалізації і відношень між ними і може бути використана для визначення вимог до інформаційних систем при побудови інформаційної інфраструктури оборонного призначення.

Застосування дата-центричного підходу з використанням хмарних технологій має збільшити швидкість, точність і якість процесу прийняття рішень, які є критичними для прийняття стратегічних рішень та успіху операцій і бойових дій. Це дасть змогу повною мірою використовувати переваги обміну потрібною інформацією через усі домени інформаційного простору – від стратегічної до тактичної ланки (до кожного солдата на полі бою), усунути принцип "ізольованості" інформаційних систем та забезпечити задоволення потреб в інформації, яка необхідна для швидкого прийняття рішень. Традиційна модель "користувач має знати", коли власник інформації вирішує кому надавати до неї доступ, змінюється на модель "користувач має право знати" та модель "користувач має поділитися". У такому інформаційному середовищі підрозділи, сенсори та керівники всіх ланок управління, системи озброєння, системи розвідки поєднані між собою спільною інформаційно-комунікаційною мережею для доставки інформації до окремого солдата на полі бою, для забезпечення інформаційної переваги.

Однією з глобальних змін є те, що дата-центрична архітектура інформаційної інфраструктури з використанням харних технологій не прив'язана до конкретної існуючої мережевої архітектури чи технології, проте забезпечує технічну можливість обміну інформацією між різнорідними за топологією та технологіями інформаційними доменами.

Одночасно зростання спроможностей, які лежать в основі ЄІП сил оборони, потребує розроблення (зміни) концепцій ведення бойових дій, використання нових тактичних дій, нових процесів і процедур забезпечення військ (сил), а також нових підходів до ведення розвідки.

Напрямом подальших досліджень є вивчення безпекових аспектів, пов'язаних із доступом до сховищ даних та безпеки в хмарах, а також визначення особливостей застосування дата-центричного підходу в секторі безпеки і оборони України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основні поняття хмарних технологій. URL: https://dduvs.in.ua (дата звернення: 26.12.2022).
2. Alberts D., Garstka J., Stein F. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, DC : CCRP Publication Series, 1999. 287 p.
3. Understanding Information Age Warfare / D. Alberts, J. Garstka, R. Hayes, D. Signori. Washington, DC : CCRP Publication Series, 2001. 319 p.

4. Alberts D. Information Age Transformation: Getting to a 21st Century Military. Washington, DC : CCRP Publication Series, 2002. 155 p.
5. Alberts D., Hayes R. Power to the Edge: Command, Control, in the Information Age. Washington, DC : CCRP Publication Series, 2005. 303 p.
6. All that glisters: Is network-centric warfare really scientific? / D. Reid, G. Goodman, W. Johnson, R. Giffin // Defense & Security Analysis. 2005. № 21 (4). P. 335–367. URL: https://doi.org/10.1080/14751790520003454 03 (дата звернення: 05.12.2022).
7. Wilson C. CRS Report for Congress. Network Centric Operations: Background and Oversight Issues for Congress. Washington, D.C : Library of Congress, 2007. 121 p.
8. Pullen J. M., Corona F., Zamponi C. NATO Federated Mission Networking Standards for CAX // EasyChair Preprint. 2020. № 4511. P. 2–17.
9. NATO Federated Mission Networking. URL: https://uk.wikipedia.org/wiki/FMN (дата звернення: 06.12.2022).
10. Що таке хмарні технології і навіщо вони потрібні. URL: https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni/ (дата звернення: 06.12.2022).
11. Consultation, Command and Control Board (C3B) - C3 Taxonomy Baseline 5.0 // NATO HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION. 2021. URL: https://www.nato.int/ nato_static_fl2014/assets/pdf/2021/10/pdf/210830-C3-taxonomy-baseline.pdf (дата звернення: 07.12.2022).
12. Data Centric C2-Services Deployment: an Experiment on Fleets of Military Vehicles / G. Pingen, J. van der Geest, M. Beaujon et al. // EasyChair Preprint. 2021. № 6312. C. 2–4.

Стаття надійшла до редакційної колегії 16.01.2023

Application of a data-centric approach when building an information infrastructure using cloud technologies for defense needs

Annotation

In order to ensure the capabilities of the defense forces in terms of building up their information potential, the search for ways to build an information infrastructure is underway. Today, the approach to building the information infrastructure is characterized by the fact that each component of the defense forces builds its own separate information and communication systems, which are similar in terms of construction principles but different in terms of tasks and technical implementation. The absence of a single software and hardware platform makes it impossible to meet the requirements for unification, standardization, scaling, and information security, which leads to unjustified costs at the stages of commissioning and maintenance throughout the life cycle of each system.

Given that the information infrastructure of the defense forces can be represented in the form of a data-center model and in order to avoid the disadvantages inherent in the client-server architecture, an approach is proposed that involves the use of "cloud technologies", which is a technology for providing spatial network access on demand to a common a common data base and functional services.

To ensure the transition from a static model of identification and use of information resources to dynamic mechanisms, a model of functional services of a single information space based on cloud technologies is proposed to provide information advantages in supporting and conducting operations (combat operations). The model provides for the dynamic management of data and functional services in accordance with the needs of users, cyber threats and operational tasks.

Keywords: information space; data-centric approach; information infrastructure; cloud technologies; functional service management model.