УДК 004.7 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/108-120

Ліпко І. О. (0009-0001-6663-5899)
Звір В. Б. (0000-0002-6823-7552)
Миколенко Ю. М., кандидат військових наук (0000-0001-9740-2521)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави

Резюме. У статті проведено дослідження доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО, діючого нормативного забезпечення впровадження інформаційних технологій у Міністерстві оборони України. За результатами проведених досліджень запропонована модель доктринального та нормативного забезпечення заходів із досягнення взаємосумісності комунікаційних та інформаційних систем сил оборони.

Ключові слова: доктринальне та нормативне забезпечення; FMN; взаємосумісність комунікаційних та інформаційних систем.

Постановка проблеми. Стратегічними документами держави визначені напрями зосередження основних зусиль складових сектору безпеки і оборони щодо європейського та євроатлантичного прагнення України.

Основою Стратегії воєнної безпеки України є всеохоплююча оборона України, одним із основних напрямів її досягнення є упровадження в силах оборони передового досвіду, принципів і стандартів держав – членів НАТО, участь у спільних операціях та навчаннях для досягнення критеріїв членства в НАТО з подальшою інтеграцією в євроатлантичні безпекові структури [1].

Розвиток оперативних, бойових і спеціальних спроможностей сил оборони має бути зосереджено на запровадженні, у тому числі інформаційних технологій та електронних комунікацій. Їх запровадження має здійснюватися у рамках Стратегічної цілі 1. Завдання 1.5: Цифровізація діяльності та впровадження сучасних інформаційних технологій, зокрема електронних комунікацій, у сфері оборони.

Також слід зауважити, що практично у всіх стратегічних цілях відслідковуються вимоги щодо розвитку складових сил безпеки та оборони відповідно до підходів та стандартів НАТО.

Для виконання стратегічних цілей та завдань у листопаді 2022 року Міністром оборони України було затверджено Статут програми проєктів "Впровадження ефективного оборонного менеджменту і системи об'єднаного керівництва силами оборони та військового управління у Збройних Силах України", яким визначено Завдання 1.5. У рамках визначеного завдання мають бути організовані заходи щодо стандартизації, оптимізації та забезпечення взаємосумісності комунікаційних та інформаційних систем сил оборони держави. Очікуваним результатом вказаного мають бути розроблені відомчі документи щодо створення, функціонування та забезпечення Об'єднаної мережі оборони та мереж операцій з урахуванням стандартів та підходів НАТО.

Таким чином, вбачається актуальним розроблення структури відомчих документів для досягнення визначеного запланованого результату.

Аналіз останніх досліджень і публікацій. Розвиток сучасної IT-інфраструктури в силах оборони розглядається як розвиток спеціальних спроможностей цих сил. Такий розвиток здійснюється у рамках оборонного планування розвитку військ (сил) на основі спроможностей за базовими складовими спроможності DOTMLPFI (*en: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability; укр: Доктринальна база, Організація, Підготовка, Ресурсне забезпечення, Управління та освіта, Персонал, Військова інфраструктура, Взаємосумісність*), порядок щодо організації та його здійснення визначені у наказі [2] та доктринальному документі [3].

Протягом останніх років вітчизняними науковцями була проведена значна кількість досліджень як з питання оборонного планування, так і з питання імплементації документів і стандартів НАТО [4–9] (вказаний перелік наукових досліджень не є вичерпним). Внаслідок вказаного у Міністерстві оборони

України (далі – МО України) та Збройних Силах України (далі – ЗС України) побудовано цілісну систему оборонного планування, яка відповідає підходам та стандартам НАТО.

Таким чином, з урахуванням вказаних джерел одним із важливих аспектів розвитку спроможностей є розвиток доктринальної та нормативної бази D *(Doctrine)*. Під розвитком доктринальної та нормативної бази розуміється процес створення необхідних концепцій, настанов, стандартів, процедур, інструкцій тощо, що визначають методи та способи виконання завдань з розвитку конкретної спроможності, у тому числі, створення нових спроможностей, у нашому випадку – з розвитку комунікаційних та інформаційних систем та ІТ-сервісів (далі для позначення ІТ-сервісів використовується термін "сервіс").

Водночас, у [2–9] не враховані особливості доктринального та нормативного забезпечення розвитку такої специфічної сфери, як ІТ-сфера, яка є високотехнологічною, характеризується швидкою та постійною зміною технологій обробки даних й інформації, у тому числі обладнання, на якому здійснюється така обробка (у середньому життєвий цикл інформаційної технології становить близько 3-5 років). Наглядним прикладом вказаного є порівняння можливостей сучасного смартфона та смартфона, який використовувався у 2018 році. При цьому, спроможності сучасного смартфона перевищують спроможності ПЕОМ 2013 року. Хмарні обчислення, які є тенденцією сьогодення, на початку 2010-х років були на початковому рівні розвитку. І таких прикладів в ІТ-сфері можливо навести безліч.

Відповідно до положень [1] у силах оборони України має бути розгорнута об'єднана мережа оборони та мережі операцій, обмін інформацією в яких здійснюється відповідно до технічних та процедурних принципів та рівнів взаємосумісності НАТО.

Під *об'єднаною мережею оборони* розуміється єдина мережа, яка поєднує в собі окремі мережі та/або інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи складових сил оборони, обмін інформацією між якими здійснюється відповідно до технічних, процедурних принципів, принципів захисту інформації та рівнів взаємосумісності.

У свою чергу, *мережа операції* являє собою єдиний комплекс спроможностей, який включає в себе сукупність незалежних електронних комунікаційних та інформаційних систем, управління, процеси і процедури, створені для проведення операції, навчання, тренування або перевірки на взаємосумісність.

На сьогодні, в НАТО досягнення взаємосумісності здійснюється у рамках ініціативи FMN *(en: Federated Mission Networking, укр: Об'єднана мережа для проведення операцій)* [10], яку було започатковано в НАТО з 2015 року.

У МО України в продовж останніх років було напрацьовано ряд відомчих документів, які є підґрунтям запровадження вказаної ініціативи НАТО FMN. Основними такими документами є:

Концепція розвитку ІТ-інфраструктури МО України та ЗС України (затверджена у листопаді 2021 року Міністром оборони України);

ключова доктрина "Зв'язок та інформаційні системи" (затверджена у липні 2020 року Головнокомандувачем ЗС України);

Об'єднана оперативна концепція сил оборони 2030 (затверджена у листопаді 2021 року начальником Генерального штабу ЗС України).

При цьому, положення вказаних доктринальних документів також розповсюджуються на складові сектору безпеки та оборони України.

Слід зазначити, що систематизованих досліджень з питання розвитку доктринальної та нормативної бази в інтересах сил оборони для досягнення технічних та процедурних принципів та рівнів взаємосумісності з НАТО в доступному для аналізу україномовному домені не знайдено. У науковій літературі висвітлена, в основному, тематика, що стосується технічної сторони взаємосумісності комунікаційних та інформаційних систем. Так, публікації [11–13] направлені на досягнення цієї взаємосумісності у тактичному просторі – на рівні, так званих, "солдатських" мереж передачі даних. У дослідженнях [14–15] розглянуто дата-центричний підхід, який, згідно положень ініціативи FMN, є основою побудови інформаційної інфраструктури із використанням хмарних технологій.

Мета статті – на основі аналізу підходів НАТО щодо доктринального забезпечення ініціативи FMN та набутого вітчизняного досвіду розробити модель структури

доктринальних та нормативних документів з питання досягнення взаємосумісності комунікаційних та інформаційних систем.

Виклад основного матеріалу. На засіданні Комісії Україна-НАТО на рівні глав держав та урядів (у рамках Саміту НАТО в Уельсі) було проголошено про створення С4-Трастового фонду Україна – НАТО *(en: NATO Ukraine C4 Trust Fund)* (далі – С4-фонд). Виконавчим органом фонду було визначено Агенцію НАТО зі зв'язку та інформації *(en: NATO Communications and Information Agency, NCIA Agency)*. Керівництво фондом було покладено на такі держави – члени НАТО: Німеччина, Канада, Велика Британія. Також до спонсорства у фонді було залучено Данію, Ісландію, Латвію, Польщу, Туреччину та Сполучені Штати Америки. Починаючи з грудня 2021 року всі трастові фонди та програми, які були направлені на допомогу Україні, у тому числі, й С4-фонд, були об'єднані в єдиний Трастовий фонд НАТО з Комплексного пакету допомоги Україні *(en: NATO-Ukraine Comprehensive Assistance Package (CAP) Trust Fund)*.

Довідка. В НАТО [16] запроваджено концептуальну семантичну модель, яка складається з:

- домену С3-системи *(en: Consultation, Command and Control (C3) systems)*, який у свою чергу включає у себе:

консультації *(en: Consultation)* – політичні консультації, кризисне управління, консультації з питань застосування ядерної зброї, співробітництво у сфері партнерства заради миру, захисту цивільного населення тощо, що є відповідальністю цивільної структури НАТО;

систему управління (командування та управління) *(en: Command and Control, C2)*, яка є відповідальністю військової структури НАТО;

сенсорні системи та командні пункти;

- комунікаційних та інформаційних систем *(en: Communication and information systems, CIS)*, які забезпечують підтримку С3-системи. Наприклад, С2-системи *(en: Command and Control (C2) systems)* забезпечують управління підпорядкованими органами управління та частинами (підрозділами).

Також у збройних силах США широко використовуються такі поняття для С-систем:

С3-системи *(en: Command, Control and Communication (C3) systems)* – є узагальнюючим терміном для позначення сукупності стратегічних та тактичних комунікаційних та інформаційних систем, за допомогою яких здійснюється передача інформації та даних;

С4ISR-системи *(en: Command, Control, Communication and Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є концепцією побудови сучасних комунікаційних та інформаційних систем разом із системами спостереження та розвідки для забезпечення переваги у ситуаційній обізнаності, у т.ч. про противника і навколишнє середовище, та скорочення часу на визначення та ураження цілей;

С5ISR-системи *(en: Command, Control, Communication, Computers and Cyber (C5) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є концепцією побудови майбутніх комунікаційних та інформаційних систем разом із системами спостереження та розвідки для забезпечення переваги над противником у кіберпросторі;

С6ISR-системи *(en: Command, Control, Communication, Computers, Cyber and Combat (C6) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є також концепцією побудови майбутніх комунікаційних та інформаційних систем із застосуванням бойових тактичних систем.

Слід зауважити, що [16] запроваджено військовим стандартом ВСТ 01.112.004 – 2017 (01) "Військовий зв'язок та інформаційні системи. Словник НАТО з систем зв'язку та інформаційних систем (AAP-31 (Edition 3), IDT)".

Основним завданням С4-фонду є трансформація ЗС України завдяки модернізації їх С4-спроможностей, а також підвищення взаємосумісності із С4-системами НАТО. Вказаний фонд виявився ефективним механізмом досягнення вказаного завдання, у рамках якого здійснюється обмін знаннями, постачання обладнання, побудова спільних мереж тощо.

Завдяки вказаному фонду представникам складових сектору безпеки та оборони було надано доступ до інформаційного ресурсу НАТО *Tidepedia* (https://tide.act.nato.int), який є надсучасною базою С4-знань НАТО, та є платформою обміну знаннями з експертами НАТО у відповідних сферах діяльності. Слід зауважити, що Tidepedia це те джерело інформації, завдяки якому представники сил оборони мають можливість доступу до інформації про ініціативу FMN.

Довідка. Вікі Tidepedia є частиною ініціативи НАТО TIDE, яка спирається на Технології *(en: Technologies)* з метою досягнення переваги в Інформації *(en: Information)*, Прийняті рішень *(en: Decision)* та Застосуванні військ *(en: Execution)*. Метою вікі є забезпечити в мережі Інтернет всеохоплююче і стійке середовище співпраці та сховище інформації для спільноти оперативних експертів, менеджерів програм та проєктів, розробників спроможностей та менеджерів вимог, дослідників, експериментаторів та організацій підтримки, які зацікавлені в консультаціях, командуванні та управлінні *(en: consultation, command and control, C3)* НАТО, держав – членів та партнерів НАТО, а також асоційованих наукових та промислових підприємств. Цей веб-сайт розміщений на ресурсах Союзного командування НАТО з трансформації *(en: Allied Command Transformation, ACT)*.

У загальному вигляді концептуальна модель доктринального забезпечення

взаємосумісності комунікаційних та інформаційних систем в НАТО наведена на рис. 1.

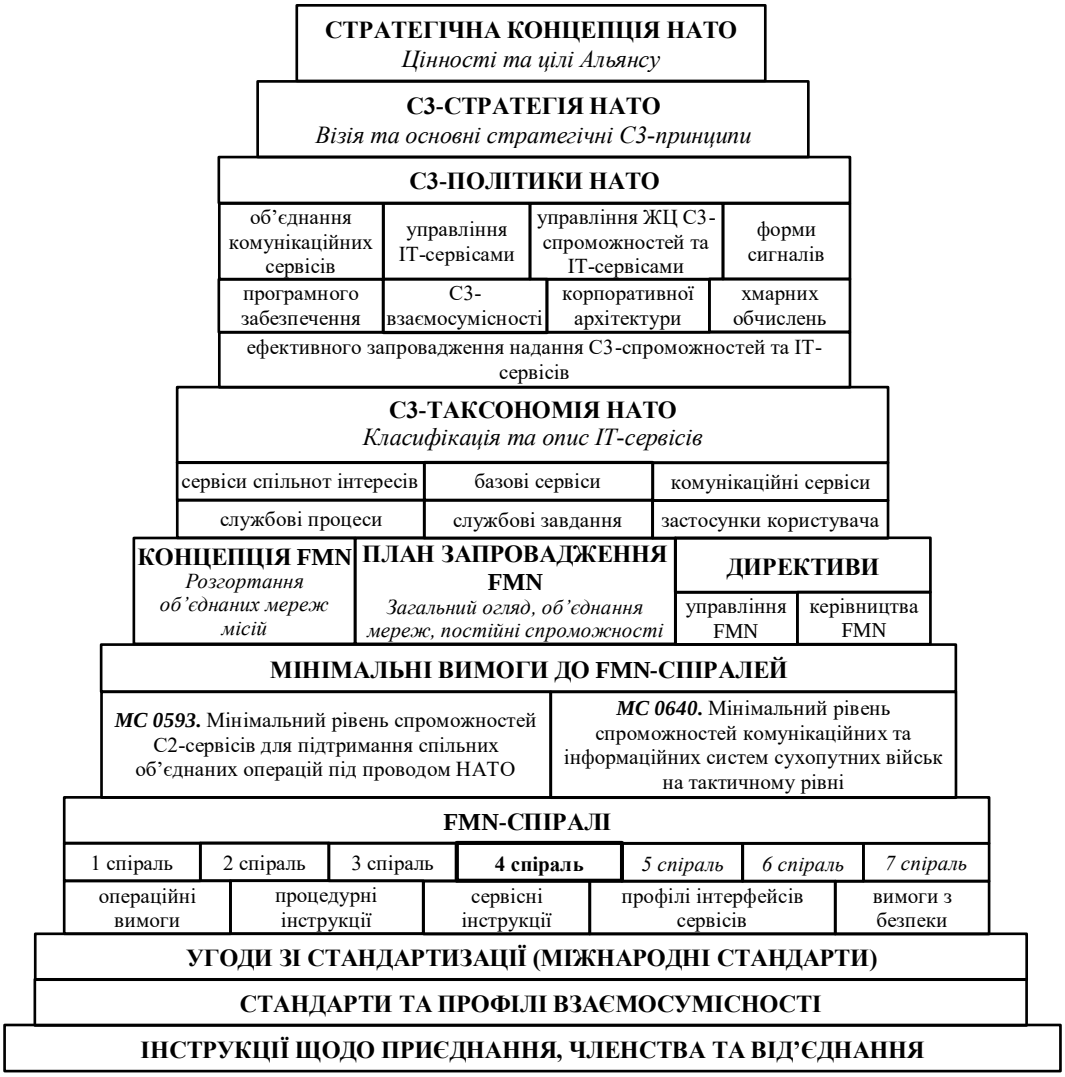


Рис. 1. Концептуальна модель доктринального забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО

Стратегічна концепція НАТО *(en: NATO Strategic Concept)* є ключовим документом, що визначає цінності та цілі Альянсу. У ній міститься колективна оцінка викликів безпеці, що існують для держав – членів НАТО, визначаються політичні і воєнні завдання щодо протидії цим викликам. У останній концепції, яку було прийнято у минулому році на Саміті НАТО у Мадриді, зазначено що одним із основоположних завдань НАТО є цифрова трансформація НАТО, запровадження новітніх технологій, вдосконалення комп'ютерних мереж та інфраструктури тощо [17].

С3-стратегією Альянсу *(en: Alliance C3 Strategy)* визначено візію та основні стратегічні принципи, якими повинні керуватися зацікавлені сторони НАТО під час своєї діяльності. Вказаною візією визначено, що інформаційна перевага та перевага у швидкості прийняття рішень досягається за рахунок ефективного використання ІТ-технологій шляхом надання зацікавленим сторонам розширених С3-спроможностей. Прикладами вказаних принципів є: забезпечення розвитку С3-спроможностей та сервісів відповідно до DOTMLPFI, С3-спроможності визначаються та надаються в якості сервісів тощо. При цьому, стратегічною ціллю для держав – членів НАТО та держав – партнерів НАТО, у разі їх залучення в операціях під проводом НАТО, повинно бути дотримання принципів FMN.

С3-політики Альянсу *(en: Alliance C3 Policy)* є фундаментальним механізмом забезпечення виконання Альянсом своїх основних завдань шляхом узгодженого запровадження та надання взаємосумісних та сучасних С3-спроможностей та сервісів. С3-політики складаються з таких окремих політик, які наведено у Табл. 1.

Таблиця 1

Перелік С3-політик НАТО

№	ПОЛІТИКА	ТЛУМАЧЕННЯ
1	**Управління ІТ-сервісами** *NATO Information and Communications Technology Service Management Policy*	Обов'язкові принципи щодо надання, використання та управління сервісами в НАТО відповідно до положень ITIL *(Information Technology Infrastructure Library)*
2	**Управління життєвим циклом С3-спроможностей та ІТ-сервісів** *C3 Capabilities and ICT Services Lifecycle Management Policy*	визначає основні напрями розвитку, запровадження, використання та еволюції С3-спроможностей та сервісів НАТО, функції та завдання різного роду зацікавлених сторін в цих процесах
3	**З питання форми сигналів** *Waveform Policy*	визначає принципи направлені на досягнення взаємосумісності безпровідних мереж із використанням технологій програмованого радіозв'язку та сучасних сумісних форм сигналів коливань
4	**С3-взаємосумісності** *Alliance Consultation, Command and Control (C3) Interoperability Policy*	визначає принципи та основні завдання з розвитку та ефективного використання С3-спроможностей та сервісів з метою досягнення взаємосумісності та підтримки обміну інформацією через основні виміри: технічні, процедурні та людські
5	**Об'єднання комунікаційних сервісів** *Federation of Communications Services Policy*	визначає принципи об'єднання мереж через сервіс-провайдерів НАТО та національних сервіс-провайдерів з мето підтримки процесів, завдань та місій НАТО
6	**Програмного забезпечення** *NATO Software Policy*	визначає заходи з підвищення якості, економічної ефективності, взаємосумісності як у межах НАТО, так і поза ним, національного використання та безпеки НАТО програмного забезпечення, яке придбане або знаходиться під управлінням структур НАТО
7	**Ефективного запровадження надання С3-спроможностей та ІТ-сервісів** *Policy on the Efficient Implementation of C3 Capabilities and ICT Services Delivery*	визначає принципи зі сприяння, розвитку, оцінки, вибору та запровадження пропозицій щодо визначення вимог до С3-спроможностей та сервісів для їх вчасного придбання у найбільш ефективний спосіб
8	**Корпоративної архітектури** *NATO Enterprise Architecture Policy*	описує вимоги для стандартизації С3-спроможностей та взаємосумісних сервісів з метою досягнення цілей НАТО та супроводження щоденних службових процесів, заходів, тренувань та навчань
9	**Хмарних обчислень** *NATO Cloud Computing Policy*	визначає принципи забезпечення, підтримки та використання спільної сервіс-орієнтованої обчислювальної інфраструктури (хмари) для досягнення більшої доступності, гнучкості, безпеки та мобільності з метою зменшення витрати

Як було раніше зазначено у С3-стратегії Альянсу, С3-спроможності визначаються та надаються в якості сервісів. Ураховуючи вказане, класифікацію та опис сервісів в НАТО визначено у документі С3-таксономія *(en: C3 Taxonomy)*. На це час, С3-таксономія складається з таких окремих таксономій:

сервіси спільнот інтересів *(en: C3 Community of Interest Services Taxonomy)*;

базові сервіси *(en: C3 Core Services Taxonomy)*;

комунікаційні сервіси *(en: C3 Communications Services Taxonomy)*;

службові процеси *(en: C3 Business Processes Taxonomy)*;

службові завдання *(en: C3 Business Roles Taxonomy)*;

застосунки користувача *(en: C3 User Applications Taxonomy)*.

Слід зауважити, що протягом наступних років до вказаної таксономії заплановано включити додаткові таксономії, у яких класифікують та нададуть опис С3-спроможностей, обладнання та інформаційних продуктів.

Запровадження ініціативи FMN здійснюється відповідно до:

Концепції FMN *(en: FMN Concept)*: описує підходи із забезпечення комплексного керівництва з розгортання об'єднаних мереж місій, які будуть спроможними до ефективного обміну інформацією між НАТО, державами – членами НАТО, державами – партнерами НАТО та не-НАТО організаціями, які приймають участь в операціях;

Плану запровадження (реалізації) ініціативи FMN в НАТО *(en: NATO FMN Implementation Plan),* який є комплексним документом, що складається з трьох основних розділів та більше 20 додатків до них, у яких викладено:

загальний опис запровадження ініціативи FMN;

принципи об'єднання мереж;

постійні спроможності НАТО.

У цих документах закладено основна парадигма FMN: об'єднані мережі місій

повинні будуватись на довірі й узгодженості та бути спроможними забезпечити командування та управління в операціях під проводом НАТО.

На підставі вказаних документів розроблено відповідні директиви НАТО, якими визначені:

завдання та повноваження, відповідальність та обов'язки, функції та процеси структур, які задіяні в керівництві FMN – у Директиві з керівництва FMN *(en: FMN Governance Directive)*;

завдання, структуру та основні обов'язки структур з управління FMN, зокрема визначені процеси, ключові продукти та взаємозв'язок між цими продуктами та структурами – у Директиві з управління FMN *(en: FMN Management Directive)*.

Основою для розроблення вимог до сервісів, що визначаються у "спіралях FMN", є Мінімальні вимоги до FMN-спіралей. Вказані вимоги розробляються відповідно до таких документів Військового комітету НАТО:

мінімальний рівень спроможностей С2-сервісів для підтримання спільних об'єднаних операцій під проводом НАТО *(en: MC 0593. Minimum Level of C2 Service Capabilities in Support of Combined Joint NATO Led Operations)*;

мінімальний рівень спроможностей комунікаційних та інформаційних систем сухопутних військ на тактичному рівні *(en: MC 0640. Minimum Level of CIS Capabilities at Land Tactical Level)*.

Розвиток FMN спирається на так звані "спіралі FMN", якими визначаються переліки сервісів, які повинні функціонувати протягом проведення операцій під проводом НАТО, та вимог щодо їх побудови для забезпечення їх взаємосумісності. Реалізація спіралей здійснюється в рамках 4-х річного циклу від затвердження вимог до їх реалізації у діючих комунікаційних та інформаційних системах. На сьогодні вже розроблено 4 спіралі та здійснюється робота над 5 спіраллю.

Зазвичай спіралі складаються з операційних вимог *(en: Operational Requirements)*, процедурних *(en: Procedural Instructions)* та сервісних *(en: Service Instructions)* інструкцій, профілів інтерфейсів сервісів *(en: Service Interface Profile)* та вимог з безпеки *(en: Security Requirements)*.

Операційними вимогами визначені загальні вимоги до системи в цілому, які реалізовані у цій спіралі та можуть у подальшому удосконалюватися.

У процедурних інструкціях описуються процеси, інформаційні продукти та завдання.

Вимоги з технічної побудови сервісів та завдання з їх запровадження визначені у сервісних інструкціях.

А у профілях інтерфейсів сервісів визначені інтерфейси для сервісів, які використовують різні протоколи, для їх взаємодії в рамках однієї коаліційної мережі операцій.

Діюча 4 спіраль FMN складається з:

специфікації спіралі, у якій описані загальні положення про взаємосумісність, архітектуру взаємосумісності, коротка характеристика процедурних та сервісних інструкцій разом із описом внесених до них змін, терміни та їх визначення, надано перелік стандартів та їх короткий опис, наведено посилання на використані джерела інформації тощо;

загального опису операційних вимог, які були використані для розроблення цієї спіралі та попередніх спіралей;

загального опису вимог до безпеки, які були використані для розроблення цієї спіралі та попередніх спіралей;

процедурних інструкцій, якими описано 13 процесів (наприклад, Процедурною інструкцією з комунікації визначені правила розподілу фізичних IP-адрес та номерів автономних систем для різних типів мереж й інтерфейсів; залежності цієї інструкції від інших та з іншими процедурними та сервісними інструкціями тощо);

сервісних інструкцій, якими визначені технічні вимоги до 22 сервісів (наприклад, Сервісною інструкцією з комунікації визначені профілі стандартів (тобто, наборів стандартів) доступу до комунікацій та транспорту комунікацій; опис концепції системи; залежності цієї інструкції від інших та з іншими процедурними та сервісними інструкціями тощо);

11 профілів інтерфейсів сервісів (наприклад, Профілем інтерфейсу сервісу для зв'язування метаданих із загальними форматами даних визначено використання відкритого XML-формату, який описано у міжнародному стандарті ISO/IEC 29500, та офісних застосунків корпорації Microsoft (Word, Excel, PowerPoint) тощо).

Довідка. Розроблення процедурних інструкцій здійснюється з урахуванням положень директив, політик, союзних публікацій НАТО у відповідній сфері. Наприклад, Процедурну інструкцію для командування та управління сухопутними операціями розроблено на виконання

таких документів: директиви Військового комітету НАТО MC 0640, об'єднаної публікації США JP 3.2 "Сухопутні операції", союзних об'єднаних публікацій AJP-3.2 "Союзна об'єднана доктрина для сухопутних операцій", AJP-3 "Союзна об'єднана доктрина для ведення операцій", AJP-5 "Союзна об'єднана доктрина планування операцій" тощо.

Технічні вимоги до сервісів визначаються відповідно до положень угод зі стандартизації НАТО (STANAGs), міжнародних стандартів, розроблених різного роду міжнародними організаціями, як от, Міжнародною організацією зі стандартизації (стандарти ISO), Міжнародною електротехнічною комісією (стандарти IEC), Міжнародною спілкою електрозв'язку (стандарти ITU), W3-консорціумом (стандарти HTML, XML, CSS тощо) тощо, та достатньо широко використовуються стандарти мережі Інтернет – запити коментарів RFC.

Відповідно до принципів С3-взаємосумісності НАТО, викладених у Політиці НАТО із С3-взаємосумісності:

стандарти та профілі повинні бути включені до Стандартів та профілів взаємосумісності НАТО *(en: NATO Interoperability Standards and Profiles, NISP)*;

структури НАТО повинні розробляти та публікувати в *NISP* профілі інтерфейсів сервісів, що стосуються С3-спроможностей та сервісів, та ці профілі повинні бути доступними для верифікації та валідації протягом тестування структурами НАТО та державами – членами НАТО.

На цей час, діючий *NISP* викладено у союзній публікації з даних *ADatP-34(N)* 14 версії від 26.05.2021 [18] та затверджено угодою зі стандартизації *STANAG 5524*. Оновлення вказаної публікації здійснюється фактично один раз на 1-2 роки.

Особливістю *NISP* є те що, у ньому наведено перелік стандартів та профілів та посилання на них в мережі Інтернет які є:

обов'язковими до запровадження;

інформативними, необов'язковими до запровадження, але вони можуть через деякий час набути статус – обов'язкові до запровадження.

Приклад побудови одного із сервісів наведено у Табл. 2.

Таблиця 2

Приклад вимог до сервісу згідно *NISP*

СЕРВІС	**ВИМОГИ ДО СЕРВІСУ**
Сервіс відео-конференційного зв'язку	*STANAG 4705* (Міжнародна мережева нумерація для систем зв'язку, що використовуються в НАТО); *STANAG 5046* (Система каталогів військових комунікацій НАТО). *Вказані угоди запроваджені в Україні у якості військових стандартів ВСТ 01.112.008 – 2020 (01) та ВСТ 01.112.012 – 2020 (01) відповідно*
	використовувати протоколи *SIP (Session Initiation Protocol), SDP (Session Description Protocol)* та *BFCP (Binary Floor Control Protocol)*, які визначені стандартами мережі Інтернет – запитами коментарів *RFC 3621, 3622, 3264, 4566, 4582* тощо
	використовувати кодеки G.722.1, G.711 та H.264, вимоги до яких визначено Міжнародною спілкою електрозв'язку, а саме: ITU-T G.722.1:2005, ITU-T G.711:1988, ITU-T H.264:2017 тощо

Для кожної мережі операції розробляються Інструкції щодо приєднання, членства та від'єднання *(en: FMN Joining, Membership and Exit Instructions, FMN JMEI)*, які складаються з розділів, у яких визначається:

процес приєднання до мережі;

членство (функціонування) у складі мережі;

процес від'єднання від мережі;

технічні інструкції розгортання сервісів.

Питання взаємосумісності досліджуються та вивчаються у двох площинах: теоретичній та практичній:

TIDE-спринти (en: TIDE Sprints) являють собою, так звані, "мозкові центри" сприяння розвитку та запровадження інновацій, обміну концептуальними та практичними ідеями що стосується взаємосумісності С2-систем та сервісів між НАТО та її партнерами;

TIDE-хакатони (en: TIDE Hackathons) є середовищем обміну знаннями між експертами та новачками, яке спрямоване на вирішення ряду проблем, що складно вирішуються традиційними методами;

навчання із взаємосумісності CWIX *(en: Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise)* протягом яких здійснюється тестування спроможностей та сервісів на взаємосумісність згідно розроблених протоколів та профілів із залученням оперативного складу, технічного персоналу та представників розробника.

Таким чином, в НАТО реалізовано комплексний підхід (так званий *comprehensive approach*) із запровадження бачення НАТО щодо побудови сучасних збройних сил, які будуть спроможні протистояти викликам з безпеки, що існують для держав – членів

НАТО, та відповідатимуть стратегічній концепції НАТО:

на стратегічному рівні розроблені відповідні стратегії та політики, якими визначено основні напрями розвитку комунікаційних та інформаційних систем;

здійснено класифікацію сервісів та відповідних процесів для запровадження сервіс-орієнтованої архітектури;

розроблено концепцію та директивні документи з питань досягнення взаємосумісності, якими визначені підходи, процеси запровадження та організаційна структура, завдання та функції особового складу;

на підставі оперативних вимог визначені мінімальні вимоги до комунікаційних та інформаційних систем та сервісів, які повинні надаватися оперативному складу через ці системи;

визначено перелік сервісів та процедурні, технічні й безпекові вимоги до них на підставі угод зі стандартизації НАТО та міжнародних стандартів;

розроблені (стандартизовані) перелік та шаблони (приклади) документів, на підставі яких розробляється визначений пакет документів для кожної операції під проводом НАТО (мережі операцій) та у яких зазначаються конкретні вимоги до сервісів, які повинні функціонувати протягом цієї операції (місії);

практичне опробування теоретичних вимог впродовж ряду спеціалізованих навчань НАТО та навчань направлених на підготовку сил і засобів НАТО для реагування на кризові ситуації.

У МО України, крім зазначених вище доктринальних документів, відпрацьовано такі відомчі документи:

доктринальні документи зі зв'язку та інформаційних систем видів та родів військ (сил) ЗС України;

накази МО України та Генерального штабу ЗС України, якими визначені вимоги до функціонування декількох комунікаційних та інформаційних систем та модернізації озброєння та військової техніки;

наказ Головнокомандувача ЗС України, яким визначено перелік сервісів, які мають бути розгорнуті на пунктах управління органів військового управління;

Модель життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем в системі МО України (затверджено Міністром оборони України 10.04.2023);

Перелік процесів моделі життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем в системі МО України (затверджено заступником Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації 07.06.2023);

військові стандарти, якими запроваджено декілька угод зі стандартизації НАТО, які включені до Переліку стандартів та профілів взаємосумісності НАТО та застосовуються у 4 спіралі.

Порівняння доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем НАТО та МО України наведено у Табл. 3.

Таблиця 3

ПОРІВНЯННЯ ДОКТРИНАЛЬНОГО ТА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ	
Стратегічні підходи щодо досягнення взаємосумісності	
НАТО	**МО України**
Стратегічна концепція НАТО; С3-стратегія Альянсу; С3-політики Альянсу	Стратегія національної безпеки України; Стратегія воєнної безпеки України; Стратегічний оборонний бюлетень України. В МО України розроблено: Концепція розвитку ІТ-інфраструктури МО України та ЗС України; ключова доктрина "Зв'язок та інформаційні системи"; Об'єднана оперативна концепція сил оборони 2030. ***Не розроблено єдиного бачення щодо порядку запровадження політик НАТО***
Класифікація сервісів	
С3-таксономія, уточнення якої здійснюється раз на 1-2 роки	Положеннями Додатку 1 Доктрини "Зв'язок та інформаційні системи" визначена необхідність розроблення Класифікатора та опису сервісів
Концепція та директивні документи з питань досягнення взаємосумісності	
Концепція FMN; План запровадження (реалізації) ініціативи FMN в НАТО; Директива з керівництва FMN;	Концепція розвитку ІТ-інфраструктури МО України та ЗС України (зміст Концепції потребує доопрацювання)

ПОРІВНЯННЯ ДОКТРИНАЛЬНОГО ТА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ	
Директива з управління FMN	
Мінімальні вимоги до комунікаційних та інформаційних систем та сервісів	
Директиви Військового комітету НАТО МС 0593 та МС 0640	Наказ Головнокомандувача ЗС України від 14.12.2020 № 221 “Про затвердження Матриці надання мінімально необхідних сервісів (базових та функціональних) оперативному складу органів військового управління на пунктах управління ЗС України” (визначено лише перелік сервісів, які повинні бути розгорнуті на пунктах управління органів військового управління)
FMN-спіралі: перелік сервісів та процедурні, технічні й безпекові вимоги до них	
4 спіраль FMN: специфікації спіралі; загальний опис операційних вимог; загальний опис вимог до безпеки; 13 процедурних інструкцій з описами процесів; 22 сервісні інструкції з технічними описами сервісів; 11 профілів інтерфейсів сервісів	Накази МО України та Генерального штабу ЗС України з питань функціонування комунікаційних та інформаційних систем (спеціального програмного забезпечення): електронного документообігу; використання мережі Інтернет (вперше були описані сервіси, як складові системи); використання безпровідних мереж; електронної комунікаційної мережі ЗС України; функціонування автоматизованої системи управління ЗС України “Дніпро” (описані деякі сервіси разом з процедурними та технічними вимогами); інтеграційної платформи “Дельта”; комплексів “Ореанда”, “Дзвін-АС” тощо; спеціального програмного забезпечення “Віраж-Планшет”, “Коровай” тощо
Стандарти та профілі взаємосумісності	
STANAG 5524 / Союзна публікація з даних ADatP-34(N) Стандарти та профілі взаємосумісності НАТО	Положеннями Додатку 1 Доктрини “Зв’язок та інформаційні системи” визначена необхідність розроблення Переліку стандартів та профілів взаємосумісності
Стандартизовані перелік та шаблони (приклади) документів мережі операцій	
Інструкції щодо приєднання, членства та від’єднання (FMN JMEI)	Окремі підходи (форми документів) використовуються в розпорядчих та планувальних документах
Практичне опробування під час навчань	
Спеціалізовані навчання НАТО CWIX; TIDE-хакатони; TIDE-спринти	Участь представників МО України у навчаннях CWIX; Проведення національних хакатонів із залученням представників сил оборони та участь переможців цих хакатонів у TIDE-хакатонах; Участь представників сил оборони у TIDE-спринтах

Ураховуючи викладене, можна дійти висновку, що у МО України відсутній комплексний підхід запровадження доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем за таких причин:

потребують доопрацювання стратегічні концептуальні документи з питань взаємосумісності згідно стратегій та політик НАТО;

відсутні класифікація сервісів та не визначено мінімальний рівень вимог до них;

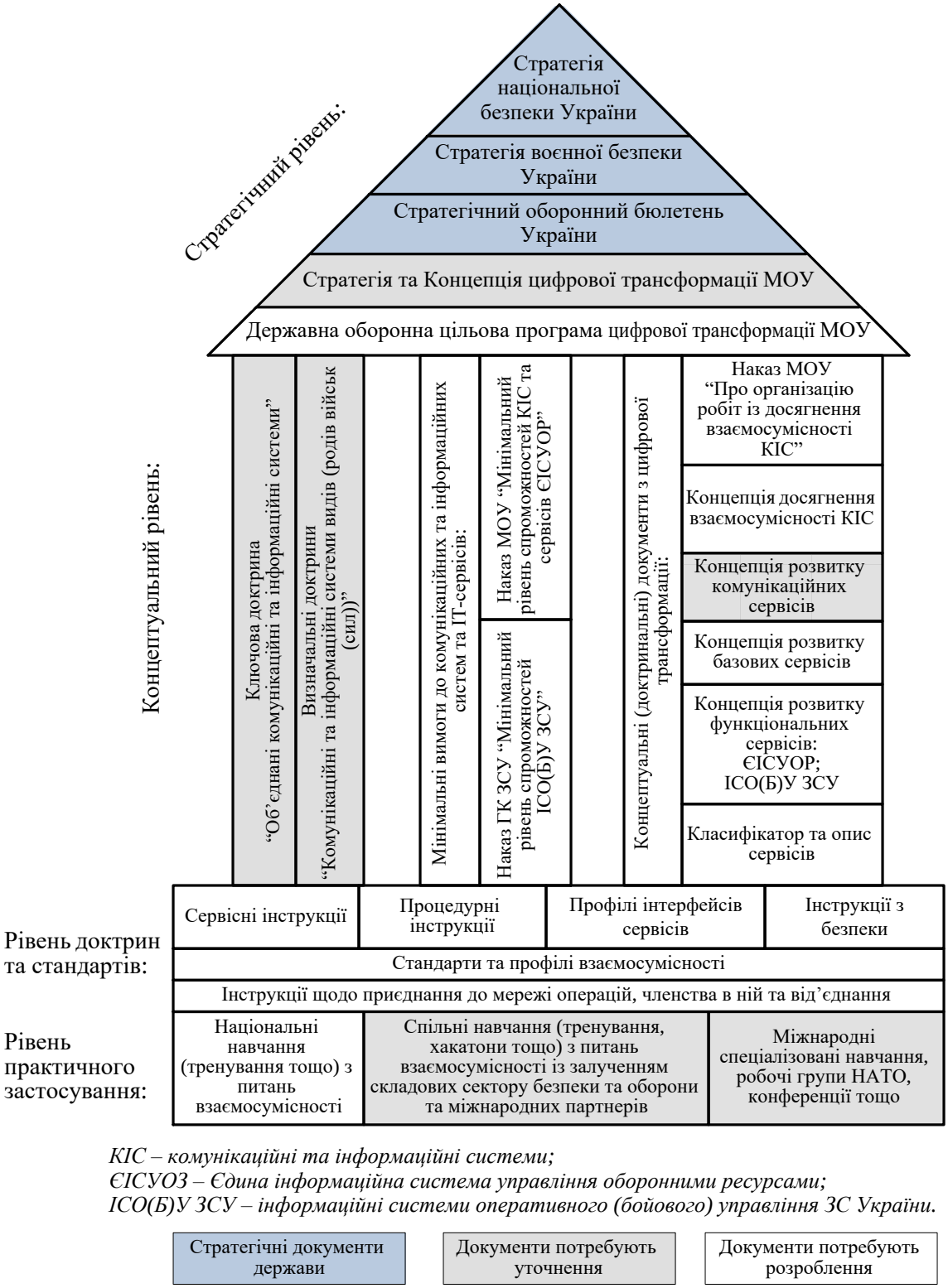
не організовано роботу відповідних робочих груп, їх завдання та обов’язки;

робота щодо запровадження процедурних та технічних інструкцій здійснюється окремими підрозділами, при цьому обмін відповідною інформацією між ними не здійснюється.

Для вирішення вказаного проблемного питання та з урахуванням досвіду НАТО розроблена модель доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем, яку наведено на рис. 2.

Вказана модель являє собою складну систему – “будівлю” – так званий “Будинок КІС – взаємосумісності”, що має чотири рівня.

Стратегічний рівень або “дах будівлі” представлений стратегіями національної і воєнної безпеки та стратегічним оборонним бюлетенем. Цифрову трансформацію МО України пропонується здійснювати за окремою Державною цільовою оборонною програмою цифрової трансформації МО України. Для цього необхідно розробити на довгострокову перспективу відповідні Стратегію та Концепцію цифрової трансформації МО України. Їх розроблення пропонується здійснити з урахуванням С3-стратегії й С3-політик НАТО та розробленої Концепції розвитку ІТ-інфраструктури МО України та ЗС України.



КІС – комунікаційні та інформаційні системи;
ЄІСУОЗ – Єдина інформаційна система управління оборонними ресурсами;
ІСО(Б)У ЗСУ – інформаційні системи оперативного (бойового) управління ЗС України.

Рис. 2. Модель доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем ("Будинок КІС – взаємосумісності")

У рамках вказаної програми доцільно здійснювати удосконалення доктринального та нормативного забезпечення, розроблення, зокрема модернізацію, нових спроможностей комунікаційних та інформаційних систем й сервісів, як інноваційних проєктів. Керівником програми призначити одного із заступників Міністра оборони України. При цьому, в рамках програм розвитку видів і родів військ (сил) планувати заходи із утримання діючих спроможностей комунікаційних та інформаційних систем,

постачання військ (сил) озброєнням та військовою технікою, зокрема спеціальною технікою, прийнятою на озброєння (постачання), або із визначеними технічними характеристиками. Застосування вказаного підходу потребує удосконалення нормативних документів з оборонного планування у МО України, а саме: положень [2–3]. На сьогодні, розвиток спроможностей комунікаційних та інформаційних систем здійснюється в рамках окремих програм розвитку видів і родів військ (сил), які не завжди є взаємоузгодженими.

Концептуальний рівень або "стіни будівлі" містить три складових:

1. Доктринальні документи представлені ключовою доктриною (об'єднані комунікаційні та інформаційні системи) та визначальними доктринами (з управління радіочастотним ресурсом в операціях, операцій в кіберпросторі та радіоелектронної боротьби в операціях), доктриною Військ зв'язку та кібербезпеки ЗС України, бойовими статутами видів та родів військ (сил) щодо організації комунікаційних та інформаційних систем в операціях.

2. Мінімальні вимоги до комунікаційних та інформаційних систем та сервісів відповідно до висунутих до них оперативних вимог. Вказані вимоги доцільно викласти у двох наказах:

Міністерства оборони України, яким визначити мінімальний рівень спроможностей комунікаційних та інформаційних систем та сервісів Єдиної інформаційної системи управління оборонними ресурсами;

Головнокомандувача ЗС України, яким визначити мінімальний рівень спроможностей інформаційних систем оперативного (бойового) управління ЗС України.

3. Концептуальні (доктринальні) документи з цифрової трансформації якими визначити:

структуру, завдання та функції робочих груп, відповідальних за відпрацювання (оновлення) документів з питання взаємосумісності;

концепцію взаємосумісності та концептуальні напрями розвитку функціональних, базових та комунікаційних сервісів тощо.

Рівень доктрин та стандартів або "фундамент будівлі" визначає процедурні та технічні вимоги до сервісів, вимоги до безпеки сервісів, шаблони (приклади) документів для розгортання мереж операцій тощо. Цей рівень є найбільш трудомістким, в частині що стосується документального забезпечення, та наявності підготовленого особового складу. Вирішення вказаного проблемного питання потребуватиме залучення як фахівців з інших складових сил оборони держави, так і цивільних фахівців з державних та комерційних структур.

Рівень практичного застосування або "середовище для побудови будівлі" є практичним випробуванням теоретичних рішень з побудови комунікаційних та інформаційних систем: навчання, тренування, хакатони тощо.

Висновки. Ураховуючи прагнення України до вступу в НАТО запровадження положень концепції НАТО FMN в силах оборони є важливим фактором інтеграції України у євроатлантичні безпекові структури та досягнення спроможностей забезпечення оборони території України й протиборства у кіберпросторі як складовій інформаційного простору держави.

У статті проведено детальний аналіз доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО та МО України, на підставі якого розроблена відповідна модель доктринального та нормативного забезпечення, яку доцільно запровадити у МО України, а в подальшому, після її апробації, і в силах оборони держави. Як показує досвід запровадження доктринальних документів у МО України, складові сектору безпеки і оборони використовують доктринальні документи МО України або на їх основі розробляють власні, із незначними уточненнями, що стосуються завдань та функцій цих складових.

Подальші дослідження доцільно зосередити на детальному аналізі змісту розглянутих документів НАТО, їх адаптації в МО України в рамках оборонного планування. При цьому першочерговим заходом має бути розроблення власного Класифікатора сервісів та визначення мінімальних вимог до сервісів, які повинні надаватися оперативному складу пунктів управління ЗС України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегічний оборонний бюлетень України : Указ Президента України від 17.09.2021 р. № 473. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 10.07.2023).
2. Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони : наказ

Міністерства оборони України від 22.12.2020 р. № 484. URL: https://zakon.rada.gov.ua/laws/show/z0196-21#Text (дата звернення: 10.08.2023).
3. Доктрина з оборонного планування у Збройних Силах України (ВКП 5-00(67)01.01) : затверджена Головнокомандувачем Збройних Сил України 13.11.2020.
4. Руснак І. С., Петренко А. Г., Яковенко А. В., Романюк І. М., Кохно В. Д. Оборонне планування на основі спроможностей: особливості та перспективи впровадження // Наука і оборона. 2017. № 2. С. 3–10.
5. Оборонна реформа: системний підхід до оборонного менеджменту : монографія / А. Павліковський та ін. ; за заг. ред. д-ра військ. наук А. Сиротенка. Київ : НУОУ, 2020. 276 с.
6. Щипанський П. В., Саганюк Ф. В., Мудрак Ю. М. Оборонний менеджмент: підходи до управління процесами оборонного планування // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 1 (71). С. 52–58.
7. Малишев О. В., Малишева Н. Р., Калмиков В. Г., Левчук О. В. Оборонне планування на основі спроможностей в Україні: поточний стан і перспективи // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2020. № 3 (70). С. 54–61.
8. Поляєв А. І. Підходи щодо розроблення методики імплементації концептуальних документів стратегічного та оборонного планування // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 2 (72). С. 78–83.
9. Мудрак Ю. М. Підходи до імплементації стандартів НАТО у Збройних Силах України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2020. № 2 (69). С. 6–10.
10. Ліпко І. О., Капілевич В. О. Актуальні підходи щодо забезпечення взаємосумісності інформаційних систем складових сил оборони України // Комп'ютерні системи та мережні технологій (CSNT-2023) : зб. тез доп. XIV Міжнар. наук.-практ. конф. (м. Київ, 13-14 квіт. 2023 р.) / Нац. авіац. ун-т. Київ, 2023. С. 109–112.
11. Слюсар В. І. Тактичні перспективи FMN // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я : тези доп. XXVIII Міжнар. наук.-практ. конф. MicroCAD-2020 (м. Харків 21-23 жовт. 2020 р.) у 5 ч., Ч. V / Національний технічний університет "Харківський політехнічний інститут. Харків, 2020. С. 229.
12. Слюсар В. І. Федеративна мережа місій як середовище поширення даних доповненої реальності // Перспективи розвитку озброєння та військової техніки Сухопутних військ : зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 16-17 трав. 2019 р.) / Національна академія Сухопутних військ ім. Гетьмана Петра Сагайдачного. Львів, 2019. С. 263–264.
13. Корольов В. М., Заєць Я. Г. Щодо вимог до інформаційних (автоматизованих) систем тактичного рівня з урахуванням стандартів НАТО // Перспективи розвитку озброєння та військової техніки Сухопутних військ : зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 17-18 трав. 2023 р.) / Національна академія Сухопутних військ ім. Гетьмана Петра Сагайдачного. Львів, 2023. С. 200–201.
14. Кірпічніков Ю. А., Капілевич В. О., Андрощук О. В., Петрушен М. В. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 3 (76). С. 68–75.
15. Кірпічніков Ю. А., Головченко О. В., Андрощук О. В., Петрушен М. В., Розумний О. Д. Модель оцінювання альтернативних варіантів впровадження інформаційно-комунікаційних сервісів з використанням хмарних технологій для оборонних потреб // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2023. № 1 (77). С. 79–88.
16. STANAG 5064 (Ed: 1) / AAP-31 (Ed: 3) (2005) (Ver. 1). NATO glossary of communication and information systems terms and definitions. URL: https://nso.nato.int/nso/nsdd/main/list-promulg (дата звернення: 10.07.2023).
17. Стратегічна концепція НАТО – 2022 : ухвал. главами держав і урядів на Мадридському саміті НАТО 29.06.2022 р. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ukr.pdf (дата звернення: 10.07.2023).
18. NATO Interoperability Standards and Profiles. URL: https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/index.html (дата звернення: 10.07.2023).

Стаття надійшла до редакційної колегії 11.08.2023

Model for achieving interoperability of communication and information systems: implementation of NATO experience in the interests of the national defense forces

Annotation

The basis of Ukraine's Military Security Strategy is the comprehensive defense of Ukraine. One of the main directions to achieve this is the integration of advanced practices, principles, and standards of NATO into the national defense forces, participation in joint operations and exercises to meet NATO membership criteria, and subsequent integration into Euro-Atlantic security structures. The defense forces of Ukraine should establish a joint defense network and mission networks, with information exchange aligned with NATO's technical and procedural principles and interoperability levels. Currently, NATO interoperability is pursued through the Federated Mission Networking (FMN) initiative, initiated within NATO since 2015.

The goal of the article is to develop a model for the doctrinal and normative documents' structure based on the analysis of NATO's approaches to doctrinal support for the FMN initiative and the experience gained domestically. This model aims to achieve interoperability of communication and information systems.

The article provides a detailed analysis of doctrinal and normative support for interoperability of communication and information systems within NATO and the Ukrainian Ministry of Defense. Based on this analysis, an appropriate model for doctrinal and normative support has been developed, intended for implementation within the Ukrainian Ministry of Defense, and subsequently, after its approval, within the national defense forces. The experience of implementing doctrinal documents within the Ukrainian Ministry of Defense shows that the security and defense sectors use these documents, sometimes with slight modifications, for their roles and responsibilities.

Keywords: doctrinal and normative support; FMN; interoperability of communication and information systems.