DOI: **10.33099/2311-7249/2024-51-3-96-107**

УДК: 004.02

Дядечко Андрій Олександрович *(доктор філософії)* [1]
Даценко Іван Петрович *(кандидат технічних наук)* [2]
Головченко Олександр Вікторович [3]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Воєнна академія імені Євгенія Березняка, Київ, Україна***
[3] ***Військова частина А3458, Україна***

КОНЦЕПТУАЛЬНІ АСПЕКТИ ТЕХНОЛОГІЧНОЇ ПІДТРИМКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Метою статті є розкрити концептуальні погляди на організацію технологічної підтримки інформаційної інфраструктури Міністерства оборони України, проаналізувати підходи щодо її організації, сформулювати основні і часткові завдання, виробити рекомендації щодо створення перспективної системи технологічної підтримки інформаційної інфраструктури, обґрунтувати її склад, основну функцію та провести її декомпозицію. Під час написання статті застосовано методи системного аналізу, компаративного аналізу та експертного оцінювання. Зазначений методологічний підхід дає змогу розкрити структуру інформаційної інфраструктури, піддати аналізу сучасні технологічні тенденції, провести порівняння з міжнародними стандартами та визначити підходи до організації технологічної підтримки інформаційної інфраструктури Міністерства оборони України, виробити рекомендації щодо організації системи технологічної підтримки інформаційної інфраструктури, визначити її основні функції та завдання. У статті вироблені рекомендації щодо створення перспективної системи технологічної підтримки інформаційної інфраструктури Міністерства оборони України, обґрунтовано її склад, завдання та функції. Практичне значення статті полягає в можливості застосування вироблених рекомендацій для вдосконалення інформаційної інфраструктури Міністерства оборони України. Рекомендації, розроблені у статті, сприятимуть підвищенню ефективності технологічної підтримки, покращенню кібербезпеки та захисту інформації, що є критично важливими для виконання завдань у сфері оборони. Запропоновані концептуальні аспекти удосконалення системи технологічної підтримки дадуть змогу Міністерству оборони України ефективніше використовувати ресурси та забезпечувати стійкість до сучасних загроз.

Ключові слова: *інформаційна інфраструктура, технологічна підтримка, інформаційна система, IT-сервіси, інформаційні технології.*

Вступ

Постановка проблеми. У сучасному світі міждержавних протистоянь і конфліктів інтересів, терористичних дій, гібридних війн і внутрішніх заворушень жодна держава не може існувати без відповідних сил оборони. Не є винятком і Україна. Законом України «Про національну безпеку України» поняття сил оборони визначено, як – Збройні Сили України (далі – ЗС України), а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави [1].

Указом Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» [2] визначено стратегічні цілі та завдання для їх реалізації. Очікуваним результатом є створення за принципами та стандартами, прийнятими в державах-членах НАТО, ефективних, мобільних, оснащених сучасним озброєнням, військовою і спеціальною технікою сил оборони, здатних гарантовано забезпечити оборону держави та адекватно і гнучко реагувати на воєнні загрози національній безпеці України, раціонально використовуючи за таких умов наявний потенціал (спроможності) та оборонні ресурси держави.

Для досягнення якісно нового рівня системи управління силами оборони за напрямом підвищення ефективності керування життєдіяльністю, розвитком, підготовкою і застосуванням сил і формувань в Міністерстві оборони України (далі – МО України) та Генеральному штабі (далі – ГШ) ЗС України плануються та здійснюються заходи щодо впровадження новітніх інформаційних технологій (далі – ІТ), сучасних засобів зв'язку, комплексної автоматизації процесів управління військами,

бойовими засобами (зброєю), а також оборонними ресурсами.

Вирішення зазначених завдань сьогодні можливо лише завдяки комплексному об'єднанню інформаційних систем (далі – ІС) МО України та ГШ ЗС України, що залежно від характеру обробки даних та ступеня автоматизації поділяють на: інформаційно-телекомунікаційні системи (далі – ІТС), автоматизовані системи управління (далі – АСУ), автоматизовані інформаційні системи (далі – АІС), інформаційно-аналітичні системи (далі – ІАС), програмні системи (далі – ПС), бази даних (далі – БД) тощо, у єдину інформаційну інфраструктуру.

Інформаційна інфраструктура (на думку авторів) – сукупність територіально розподілених ІС, інформаційно-телекомунікаційних мереж (далі – ІТМ), систем і засобів захисту інформації, а також організаційних структур, які забезпечують її ефективне функціонування.

Інформаційна інфраструктура має забезпечити автоматизацію інформаційних процесів у різноманітних галузях діяльності сил оборони, що на загальному фоні зростання ролі ІТ у ефективному функціонуванні сил оборони створює передумови для створення Єдиної автоматизованої системи управління ЗС України (далі – ЄАСУ ЗС України) [3].

Підтримка, експлуатація і розвиток інформаційної інфраструктури покладаються на підрозділи зв'язку й інформатизації, які забезпечують процеси автоматизованої обробки інформації та є складовими системи технологічної підтримки (далі – СТП) інформаційної інфраструктури МО України.

Ефективне і надійне функціонування інформаційної інфраструктури вимагає сучасних методів управління. Тому необхідно створити СТП інформаційної інфраструктури, в якій сама інформаційна інфраструктура та її компоненти є об'єктом управління.

Аналіз останніх досліджень і публікацій. Проведений аналіз досліджень у сфері технологічної підтримки інформаційної інфраструктури [5–8] показав, що авторами зазначених публікацій досліджувались підходи до здійснення підтримки окремих інформаційних систем та їх користувачів, тобто напрям досліджень направлений на обґрунтування рекомендацій щодо створення ефективного Service Desk, який буде здійснювати технічну підтримку конкретно визначеної інформаційної системи та її користувачів.

Разом із тим, вузька направленість досліджень не розкриває питань технологічної підтримки інформаційної інфраструктури в цілому, що не дає змогу сформувати бачення її організації на прикладі інформаційної інфраструктури організації.

В [4] було запропоновано застосування методології Control Objectives for Information and related Technology (CobIT) для організації технологічної підтримки інформаційної інфраструктури МО України, проте, на наш погляд, не достатньою мірою обґрунтовано застосування саме цієї методології, не проведено порівняння з іншими підходами щодо управління IT-сервісами. Також в зазначеній науковій праці, як і в [5–8], акцентується увага на створення Service Desk для підтримки користувачів, що певним чином звужує завдання та функції технологічної підтримки інформаційної інфраструктури.

Отже, проаналізовані наукові праці надають можливість сформувати поняття щодо організації підтримки користувачів IT-сервісів, деяких підходів до організації підтримки, проте не розкривають аспекти технологічної підтримки інформаційної інфраструктури в цілому, як більш широкого поняття з набором ширшого спектру функцій та завдань ніж завдання підтримки користувачів.

Мета статті. Розкрити концептуальні погляди на організацію технологічної підтримки інформаційної інфраструктури МО України, проаналізувати підходи щодо її організації, сформулювати основні і часткові завдання, виробити рекомендації щодо створення перспективної системи технологічної підтримки інформаційної інфраструктури, обґрунтувати її склад, основну функцію та провести її декомпозицію.

Виклад основного матеріалу дослідження

На початку дослідження необхідно дати визначення поняттю «технологічної підтримки інформаційної інфраструктури». В проаналізованих нормативно-правових документах України [9–12] немає чіткого та уніфікованого визначення «технологічної підтримки інформаційної інфраструктури». Проте вони частково охоплюють питання, пов'язані з технічною підтримкою та управлінням інформаційною інфраструктурою.

За результатами опрацювання зазначених вище документів було сформульоване визначення, яке на нашу думку повною мірою розкриває сутність поняття «технологічної підтримки інформаційної інфраструктури».

Отже, *технологічна підтримка інформаційної інфраструктури* – це комплекс заходів, процесів та інструментів, спрямованих на забезпечення ефективного функціонування, підтримку, моніторинг та оптимізацію всієї інформаційної інфраструктури організації шляхом здійснення управління апаратним забезпеченням, програмними компонентами, мережевими ресурсами, системами безпеки, резервними копіями та відновленням, а також підтримки користувачів та забезпечення відповідності стандартам безпеки і продуктивності.

Надалі застосування авторами терміну «технологічна підтримка» в тексті статті має на увазі «технологічну підтримку інформаційної інфраструктури» та використовується для

мінімізації повторів.

Поняття інформаційної інфраструктури МО України та ЗС України лише в останні роки набуло практичного значення. Останнім часом практика інформатизації і автоматизації управління оборонними ресурсами, військами (силами) та зброєю обходилася поняттями АІС, АСУ та ІТМ, як досить взаємозалежними, але цілком окремими системами. Однак, поступово визначилася тенденція до створення інтегрованого середовища цих складових. Фахівці в галузі автоматизації управління прийшли до висновку, що роздільне проєктування, планування і управління АІС, АСУ та ІТМ вже не забезпечує достатнього рівня (за показниками оперативності, достовірності, якості та кількості) забезпечення керівного складу та фахівців необхідною для прийняття рішень інформацією. Сьогодні інформаційну інфраструктуру розглядають як розподілену обчислювально-інформаційну систему, що керує потоками даних в інтегрованому, територіально розподіленому інформаційно-телекомунікаційному середовищі [13].

Перехід до управління в межах інформаційної інфраструктури з використанням динамічних, гнучких процесів збору, оброблення, зберігання та представлення відомчої інформації вимагає нових концепцій, технологій, архітектурних рішень при їх побудові, експлуатації і розвитку. Оскільки центральним елементом нового підходу є інтеграція процесів діяльності на розподілених обчислювальних та інформаційних ресурсах в інформаційно-телекомунікаційному середовищі, то особливого значення набуває управління функціонуванням інформаційної інфраструктури.

Головними компонентами інформаційної інфраструктури, що визначають рівень її розвитку, є обчислювальні та телекомунікаційні ресурси. Вони складають технологічний базис інформаційної інфраструктури і є підґрунтям для роботи інших складових, що пов’язані із множиною ІС, електронних інформаційних ресурсів (далі – ЕІР) різних рівнів і масштабів, які впроваджені або створюються та поєднуються системами телекомунікацій.

Результати аналізу існуючої інформаційної інфраструктури МО України показали, що основною проблемою є відсутність певних інтеграційних компонентів [14]:

інтегрованого розподіленого сховища даних, яке має відігравати роль спільного понятєвого й інформаційного середовища рішень з управління ресурсами ЗС України;

інформаційно-аналітичної підтримки прийняття рішень з управління ресурсами ЗС України на підставі інформації інтегрованого розподіленого банку даних;

сервісно-орієнтованого програмного інструментарію обміну інформацією щодо управління ресурсами між ІС різних рівнів ЗС України;

регламентів інформаційного обміну, ідентифікації та автентифікації, адміністрування та моніторингу, які мають забезпечувати оперативне надання інформації з нижніх рівнів управління з виконанням вимог щодо захисту інформації з обмеженим доступом.

Загальна інфраструктура для існуючих систем (служба каталогів, управління ідентифікацією, єдина антивірусна інфраструктура, спільна система захисту і безпеки тощо) відсутня. Технічна інфраструктура є морально застарілою, що ускладнює підтримку її функціонування, потребує утримання великого штату адміністраторів і технічних спеціалістів.

Інженерна інфраструктура є децентралізованою і морально застарілою. У багатьох підрозділах та на рівні оперативних командувань і родів військ, у приміщеннях де розташоване серверне та комунікаційне обладнання, часто відсутнє обладнання для підтримки оптимального температурного режиму та сучасне обладнання для захисту від пожеж. Відсутні системи моніторингу стану обладнання систем інженерного забезпечення та параметрів внутрішніх загроз (дим, вода, вібрації, температура, вологість, відкриття/закриття дверей).

Відсутнє навчання користувачів роботі з системами, нові користувачі отримують знання або з документації (не завжди актуальної та зрозумілої), або від більш досвідчених колег.

Підтримка існуючих систем (як загального користування, так і спеціалізованих) здійснюється не системно, зазвичай інформація про інцидент повідомляється телефоном у підрозділи, відповідальні за технічну підтримку і очікується візит технічного спеціаліста.

Відсутня єдина процедура системи реєстрації та відстеження життєвого циклу повідомлень про інциденти і заявок на обслуговування. Тільки в окремих підрозділах звернення користувачів фіксуються у паперових журналах.

Взаємодія між підрозділами, відповідальними за технічну підтримку знаходиться на низькому рівні. Відсутня чітка процедура управління змінами, в тому числі затвердження змін власниками систем. Проактивний підхід до запобігання настанню інцидентів майже не застосовується. Підтримка нових систем, після впровадження, відсутня або залишається на недостатньому рівні. Цей фактор суттєво знижує позитивний ефект від впровадження ІС.

В цих умовах завдання щодо технологічної підтримки інформаційної інфраструктури є складним у зв’язку з тим, що, з одного боку, у єдиний інформаційний простір необхідно об’єднати інформаційні системи, що створюються різними розробниками, які використовують різні програмні платформи та системи управління базами даних, а з іншого, більшість інформаційних систем продовжують працювати у локальних мережах, внаслідок того, що в них циркулює інформація з обмеженим доступом.

Зростаюча складність управління інформаційною інфраструктурою та брак висококваліфікованого персоналу є проблемою, яка вже існує та буде існувати в найближчому майбутньому.

Аналіз проблем технологічної підтримки інформаційної інфраструктури МО України слід почати з розгляду структури і особливостей основних складових інформаційної інфраструктури. Щоб забезпечити виконання покладених на неї завдань, об'єднати компоненти в цілісну систему, застосовується принцип інтегрованого оброблення інформації.

У загальному вигляді інформаційна інфраструктура складається з таких основних компонентів, які утворюють замкнений контур управління: організаційні структури (органи управління), ІТМ, інформаційні ресурси (рис. 1) [13].

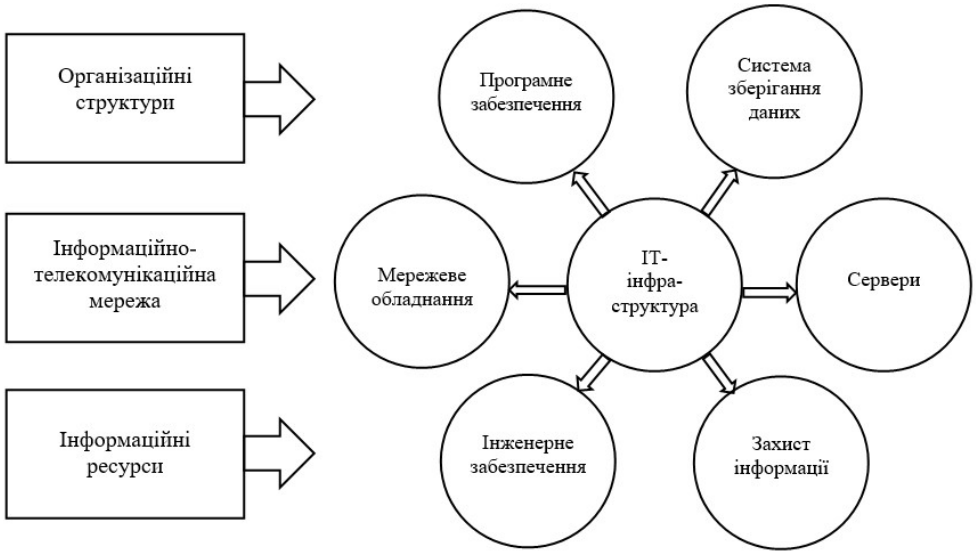

Рисунок 1 – Компоненти інформаційної інфраструктури [13]

Сукупність різнорідних технічних і програмних засобів, протоколів і форматів обміну даними призводить до виникнення гетерогенного середовища, в якості інтеграційної основи якої виступає інформаційна інфраструктура, що забезпечує працездатність складових інформаційних систем, їх взаємодію і функціональне використання.

ІТМ є матеріальною основою обміну інформацією. Вона, з одного боку, має забезпечувати вимоги користувача, з іншого боку, її можливості щодо пропускної спроможності, швидкодії та інших параметрів визначають можливості всієї інформаційної інфраструктури у цілому.

За допомогою комплексу засобів автоматизації (далі – КЗА) ІТ-інфраструктури певний орган управління зберігає, вивчає, перетворює інформацію щодо стану свого об'єкту управління (далі – ОУ), порівнює її з бажаним станом і за необхідності переводить систему в новий стан, який відповідає новим умовам.

Орган управління активно впливає на ОУ, плануючи дії і приймаючи рішення. Орган управління з КЗА є керуючою підсистемою, а ОУ з КЗА – керованою підсистемою (рис. 2) [15].

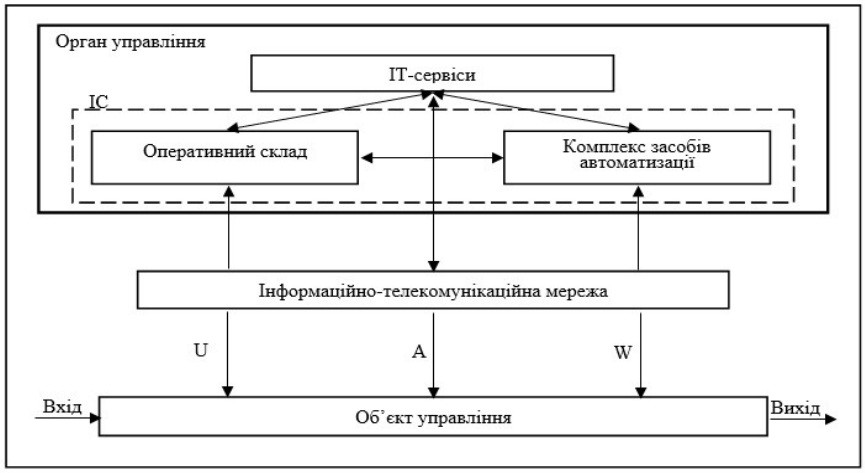

Рисунок 2 – Взаємодія компонентів інформаційної інфраструктури [15]

Входом ОУ є ресурси, необхідні для підтримки діяльності органу управління, виходом є результати діяльності. Орган управління отримує за допомогою КЗА і ІТМ інформацію про стан ОУ, U – вплив середовища функціонування на ОУ, A – керуючі дії, W – інформація щодо стану ОУ.

Проведений вище аналіз продемонстрував наявність суттєвих проблем, які виникли в галузі технологічної підтримки інформаційної інфраструктури, як засобу забезпечення її функціонування. Дійсно, швидкий розвиток ІТ, їх широке впровадження в процеси управління, створили ситуацію, коли сам процес надання інформаційних послуг стає ОУ (див. рис. 2). Великий вибір різноманітних ІС, сервісів, ресурсів перетворює технологічну підтримку інформаційної інфраструктури в режимі реального часу у складну задачу.

Крім того, інформаційна структура, як ОУ, характеризується багатьма додатковими чинниками, здатними впливати на засоби забезпечення її функціонування за показниками оперативності, готовності, стійкості, захисту інформації тощо. Отже, аналіз існуючих розробок у галузі забезпечення функціонування інформаційної інфраструктури необхідно виконати з урахуванням наведених вище проблем.

Задачі підвищення ефективності застосування ІТ виникли з появою в структурі організацій і установ ще перших ЕОМ. Для забезпечення їх функціонування використовувався так званий технологічний підхід, суть якого полягає в підтримці працездатності апаратного і програмного забезпечення окремих ІС.

З розвитком ІТ і широким впровадженням великої кількості різних ІС в діяльність організацій і установ, фокус технологічної підтримки окремих ІС змістився на надання користувачам певного набору функціональності ІС як ІТ-послуги.

Такий підхід отримав назву управління ІТ-послугами – Information Technology Service Management (далі – ITSM), який зосереджений на оптимальному використанні поєднання персоналу, процесів та інформаційних технологій.

Заходи ITSM є невід'ємною частиною технологічної підтримки інформаційної інфраструктури.

ITSM забезпечує структуру та процеси для управління ІТ-сервісами з метою задоволення потреб бізнесу та користувачів. Основні компоненти ITSM, які входять до технологічної підтримки, включають:

1. Управління інцидентами (Incident Management):

Виявлення та реагування на інциденти: швидке виявлення та усунення інцидентів для мінімізації впливу на користувачів та бізнес-процеси.

Реєстрація та відстеження інцидентів: використання системи реєстрації інцидентів для їх документування та моніторингу до повного вирішення.

2. Управління запитами на обслуговування (Service Request Management):

Обробка запитів користувачів: прийом, реєстрація та виконання запитів на обслуговування, таких як встановлення програмного забезпечення (далі – ПЗ), надання доступу тощо.

Автоматизація процесів: використання інструментів автоматизації для прискорення обробки запитів.

3. Управління проблемами (Problem Management):

Виявлення корінних причин: аналіз інцидентів для виявлення повторюваних проблем та їх корінних причин.

Запобігання проблемам: розробка та впровадження рішень для запобігання повторному виникненню проблем.

4. Управління змінами (Change Management):

Контроль змін: планування, оцінка та впровадження змін в ІТ-інфраструктуру для мінімізації ризиків та забезпечення стабільної роботи систем.

Документування змін: ведення детальної документації щодо внесених змін та їхнього впливу.

5. Управління конфігураціями (Configuration Management):

Відстеження активів: управління інформацією про ІТ-активи та їх конфігурації, що дозволяє швидко реагувати на зміни та проблеми.

База даних конфігурацій (CMDB): ведення централізованої бази даних для зберігання інформації про конфігурації ІТ-систем.

6. Управління доступністю (Availability Management):

Забезпечення доступності сервісів: планування та моніторинг доступності ІТ-сервісів відповідно до встановлених рівнів сервісу згідно з угодою Service Level Agreement (далі – SLA).

Відновлення після збоїв: розробка та впровадження заходів для забезпечення безперебійної роботи та швидкого відновлення після збоїв.

7. Управління рівнем сервісу (Service Level Management):

Встановлення та контроль SLA: узгодження рівнів сервісу з організацією та контроль їх дотримання.

Моніторинг та звітність: регулярне вимірювання продуктивності та звітність про відповідність SLA.

8. Управління знаннями (Knowledge Management):

Збір та зберігання знань: створення бази знань для зберігання інформації про вирішення проблем, інструкції та найкращі практики.

Доступ до знань: забезпечення доступу до бази знань для технічного персоналу та користувачів для підвищення ефективності вирішення проблем.

Всі ці компоненти ITSM забезпечують структурований підхід до управління ІТ-сервісами, підвищують ефективність технологічної підтримки, сприяють швидкому вирішенню

інцидентів, покращують задоволеність користувачів та забезпечують стабільну роботу інформаційної інфраструктури.

Найбільш відомою реалізацією ITSM є бібліотека управління IT-процесами Information Technology Infrastructure Library (далі – ITIL) [16-19]. ITIL пропонує структурований опис найбільш часто використовуваних IT-процесів, їх цілей і параметрів, а також зв'язків між окремими IT-процесами. Перевагами ITIL є [16]:

використання передового досвіду і перевірених знань;

спрямованість діяльності IT-підрозділу на вирішення завдань інших підрозділів;

регламентування діяльності угодами про рівень послуг;

стандартизація роботи IT-персоналу;

спрямованість на забезпечення оптимальної якості IT-послуг для споживачів;

використання підходів управління якістю для управління IT-сервісами;

можливість підтвердження вартості IT-сервісу, на підставі угоди про рівень обслуговування.

Іншим відомим ITSM підходом є методологія Control Objectives for Information and related Technology (далі – COBIT) [20–22]. Методологія COBIT – це набір документів, в яких викладено міжнародні стандарти управління, контролю і аудиту інформаційних систем будь-якого масштабу і складності. Принциповою відмінністю COBIT, порівняно з ITIL, є представлення інструментів управління IT-процесами вищого рівня. В ITIL наводиться докладний опис процедур, спрямованих на впровадження IT-процесів на рівні взаємодії керівників підрозділів. COBIT орієнтований на рівень взаємодії кураторів і директорів. Особливістю підходу COBIT є присутність в ньому моделі зрілості інформаційної інфраструктури. Використання моделі зрілості й цілей контролю, робить даний підхід найбільш ефективним для визначення цілей в області IT, побудови системи збалансованих показників для IT-служби і проведення внутрішніх і зовнішніх аудитів в області IT.

Основним стандартом щодо впровадження підходу ITSM є стандарт ISO/IEC 20000 «Information technology - Service management. Specification» [12]. У стандарті надається детальний опис вимог до системи управління IT-сервісами, що визначають відповідальність за їх ініціювання, виконання та підтримку в організаціях. Стратегічною метою стандарту ISO/IEC 20000 є зниження IT-ризиків, виконання вимог договорів, демонстрація якості послуг.

У таблиці 1 наведено порівняльний аналіз розглянутих підходів ITIL, COBIT, ISO/IEC 20000.

Таблиця 1

Порівняльний аналіз підходів ITIL, COBIT, ISO/IEC 20000

Складові аналізу	ITIL	COBIT	ISO/IEC 20000
Призначення	Надає комплекс рекомендацій та найкращих практик для управління IT-послугами, включаючи технологічну підтримку, щоб забезпечити ефективне надання та управління IT-послугами.	Розроблений для надання комплексної моделі управління IT, що забезпечує узгодження IT-цілей з бізнес-цілями та контроль за інформаційними технологіями.	Міжнародний стандарт, який встановлює вимоги до системи управління IT-послугами (IT Service Management System, SMS) для забезпечення стабільного та якісного надання IT-послуг.
Використання	Переважно використовується IT-менеджерами, керівниками IT-служб і фахівцями з управління IT-послугами для впровадження процесів та практик в IT-організаціях.	Використовується керівництвом організацій, IT-менеджерами, аудиторами і консультантами для забезпечення відповідності IT-процесів бізнес-цілям та регуляторним вимогам.	Використовується IT-організаціями, постачальниками IT-послуг і аудиторами для розробки, впровадження та сертифікації системи управління IT-послугами.
Сфера застосування	ITIL охоплює всі аспекти управління IT-послугами, включаючи проєктування, впровадження, експлуатацію та покращення IT-сервісів, зокрема, технологічну підтримку інформаційної інфраструктури.	COBIT охоплює управління IT на стратегічному рівні, включно з управлінням ризиками, відповідністю, IT-ресурсами та процесами, а також технологічну підтримку з погляду забезпечення ефективного контролю.	ISO/IEC 20000 охоплює процеси управління IT-послугами, включно з управління інцидентами, змінами, рівнем послуг, конфігураціями та іншими аспектами, що забезпечують технологічну підтримку інформаційної інфраструктури.
Сфера використання	Використовується для управління щоденною роботою IT-служб, надання послуг кінцевим користувачам, підтримки IT-інфраструктури та забезпечення її безперебійної роботи.	Використовується для розробки і впровадження стратегічного управління IT, забезпечення контролю та відповідності IT-процесів, а також для оцінки ризиків й управління ресурсами.	Використовується для сертифікації IT-організацій щодо відповідності вимогам до управління IT-послугами, зокрема, для забезпечення стабільної та якісної підтримки інформаційної інфраструктури.

Наведене порівняння викладене з метою візуалізації основних характеристик проаналізованих ITSM підходів в контексті технологічної підтримки інформаційної інфраструктури. Глибший аналіз описаних підходів доцільно провести для визначення можливості їх застосування щодо управління інформаційною інфраструктурою Міністерства оборони України, як окреме дослідження.

Враховуючи зазначені підходи до організації технологічної підтримки, на підставі аналізу існуючих проблемних питань щодо організації технологічної підтримки інформаційної інфраструктури МО України та враховуючи вимоги проаналізованих нормативно-правових документів України необхідно створити ефективну СТП інформаційної інфраструктури МО України, що забезпечить виконання основних і часткових завдань технологічної підтримки. Ці завдання запропоновано авторами з врахуванням компонентів ITSM, які входять до технологічної підтримки інформаційної інфраструктури, зокрема компонентів проаналізованих ITSM підходів, з врахуванням існуючих проблемних питань технологічної підтримки виявлених під час аналізу стану інформаційної інфраструктури Міністерства оборони України та з врахуванням вимог існуючих нормативно-правових актів:

1. Моніторинг IT-інфраструктури:

встановлення та налаштування систем моніторингу для відстеження стану серверів, мережевого обладнання, баз даних та інших компонентів IT-інфраструктури;

постійний збір та аналіз даних про продуктивність, доступність та безпеку систем;

оперативне виявлення аномалій та можливих загроз, своєчасне інформування відповідальних підрозділів.

2. Реагування на інциденти:

організація цілодобового чергування груп реагування на інциденти;

проведення першочергових заходів для локалізації та нейтралізації кіберзагроз;

документування інцидентів, проведення аналізу причин їх виникнення та надання рекомендацій щодо запобігання повторення.

3. Забезпечення кібербезпеки:

впровадження та налаштування засобів захисту інформації, таких як міжмережеві екрани, системи виявлення та запобігання вторгненням;

проведення регулярних перевірок безпеки та аудитів IT-систем на наявність вразливостей;

розробка та впровадження політик безпеки інформаційної інфраструктури, зокрема для управління доступом та аутентифікацією.

4. Управління змінами та конфігураціями:

розробка планів змін в IT-інфраструктурі з метою модернізації, оптимізації або усунення недоліків;

ведення документації та контроль за конфігурацією всіх компонентів IT-інфраструктури;

координація впровадження змін із мінімальним впливом на роботу критичних систем та забезпечення зворотної сумісності.

5. Резервне копіювання та відновлення даних:

організація та виконання регулярного резервного копіювання критичних даних та систем;

розробка і тестування планів відновлення після аварій або кібератак;

забезпечення швидкого і повного відновлення функціонування інформаційних систем після інцидентів.

6. Технічна підтримка користувачів:

надання консультацій та допомоги персоналу МО України та ЗС України щодо використання IT-ресурсів;

вирішення технічних проблем користувачів, включаючи усунення неполадок та налаштування обладнання;

організація навчань та розробка інструкцій для користувачів щодо безпечного та ефективного використання IT-систем.

7. Контроль доступу та управління обліковими записами:

управління створенням, зміною та видаленням облікових записів користувачів у інформаційних системах;

налаштування рівнів доступу відповідно до посадових обов'язків та політики безпеки;

регулярний аудит прав доступу та корекція відповідно до змін у структурі та завданнях МО України та ЗС України.

8. Аналіз продуктивності та оптимізація:

збір та аналіз даних про ефективність роботи IT-систем та технологічної підтримки;

виявлення вузьких та проблемних місць в інфраструктурі та розробка планів їх усунення;

впровадження оптимізаційних заходів для підвищення продуктивності та надійності систем.

9. Розробка та підтримка документованих політик і процедур:

розробка та впровадження стандартних операційних процедур для всіх аспектів технологічної підтримки;

регулярне оновлення документів відповідно до змін у законодавстві, нормативних актах та вимогах безпеки;

проведення регулярних тренінгів для персоналу на основі актуальних процедур та політик.

10. Інформаційне забезпечення керівництва:

підготовка регулярних звітів про стан IT-інфраструктури, безпеку та ефективність технологічної підтримки;

надання аналітичних даних для прийняття управлінських рішень щодо розвитку та модернізації IT-систем;

оперативне інформування керівництва про критичні інциденти та заходи, що вживаються для їх усунення.

Ці завдання спрямовані на забезпечення надійного, безперебійного та безпечного функціонування інформаційної інфраструктури МО України, що є критично важливим для підтримки бойової готовності та оперативної діяльності ЗС України.

Частина завдань технологічної підтримки інформаційної інфраструктури Міністерства оборони України відображено в Концепції розвитку ІТ-інфраструктури МО України та ЗС України, затвердженої Міністром оборони України 03.11.2021 року [23]. Відповідно до матриці цілей і завдань Концепція відображає завдання, що направлені на створення та розвиток ІТ-інфраструктури, яка є частиною інформаційної інфраструктури МО України та направлена на розвиток лише однієї складової інформаційної інфраструктури. Заходи для реалізації її завдань здійснюються на етапі створення (модернізації) компонентів ІТ-інфраструктури, на відміну від заходів технологічної підтримки інформаційної інфраструктури, які здійснюються на етапах впровадження та експлуатації і забезпечують функціонування всієї інформаційної інфраструктури МО України, зокрема й її важливої складової – ІТ-інфраструктури.

Зважаючи на завдання технологічної підтримки інформаційної інфраструктури МО України можна обґрунтувати склад перспективної СТП інформаційної інфраструктури МО України та визначити основні завдання її складових частин. Отже, для реалізації зазначених вище ITSM процесів технологічної підтримки інформаційної інфраструктури МО України доцільно створити СТП у наступному складі:

1. Підсистема моніторингу ІТ-інфраструктури.

Основними завданнями цієї підсистеми є:

відстеження стану всіх компонентів ІТ-інфраструктури в режимі реального часу;

аналіз продуктивності та ефективності роботи систем;

інформування про інциденти та можливі загрози;

реагування на виявлені інциденти;

оперативне вирішення технічних проблем;

ведення документації та звітність про інциденти;

планування та координація впровадження змін;

ведення бази даних конфігураційних одиниць.

2. Підсистема кібербезпеки.

Основними завданнями підсистеми є:

впровадження та підтримка заходів кібербезпеки;

управління політиками безпеки інформаційних систем;

проведення аудитів та тестування на вразливості;

управління обліковими записами користувачів;

контроль доступу до конфіденційної інформації;

налаштування та моніторинг систем аутентифікації.

3. Підсистема технічної підтримки.

Основними завданнями підсистеми є:

надання допомоги та консультацій користувачам;

вирішення технічних проблем, з якими стикаються користувачі;

проведення навчань та розробка інструкцій;

діагностика та усунення несправностей;

забезпечення своєчасного обслуговування ІТ-обладнання;

контроль за станом і справністю технічних засобів.

4. Підсистема управління резервним копіюванням та відновленням.

Основними завданнями цієї підсистеми є:

організація регулярного резервного копіювання даних;

зберігання та контроль доступності резервних копій;

забезпечення відповідності процесу резервного копіювання політикам безпеки;

розробка та впровадження планів відновлення;

проведення регулярних тестувань на відновлення систем;

забезпечення швидкого відновлення роботи інформаційної інфраструктури.

5. Підсистема аналітики та звітності.

Основними завданнями підсистеми є:

аналіз даних про ефективність роботи ІТ-інфраструктури;

виявлення проблемних зон та пропозиції щодо оптимізації;

розробка рекомендацій для підвищення продуктивності;

підготовка регулярних звітів для керівництва Міністерства оборони;

інформування про критичні інциденти та прийняті заходи;

надання аналітичних даних для прийняття стратегічних рішень.

6. Підсистема розвитку та модернізації ІТ-інфраструктури.

Основними функціями підсистеми є:

оцінка нових технологій для можливого впровадження;

планування та управління проектами модернізації;

забезпечення сумісності нових технологій з існуючою інфраструктурою;

розробка та оновлення стандартів і політик управління ІТ;

документування процедур та кращих практик;

проведення тренінгів для персоналу щодо нових стандартів і технологій.

Зазначені складові частин утворюють структуру перспективної СТП інформаційної інфраструктури МО України (рис. 3). Запропонована структура перспективної СТП інформаційної інфраструктури МО України та визначені завдання технологічної підтримки дозволили провести декомпозицію основної функції СТП, яка полягає в забезпеченні безперебійного, надійного та ефективного функціонування всієї інформаційної інфраструктури МО України, для більш детального її опису:

1. Моніторинг та управління ІТ-інфраструктурою:

постійний моніторинг стану всіх елементів інформаційної інфраструктури, включаючи сервери, мережеві пристрої, бази даних та прикладні системи;

виявлення та реагування на інциденти, аномалії та потенційні загрози;

Рисунок 3 – Структура перспективної системи технологічної підтримки інформаційної інфраструктури МО України.

забезпечення своєчасного реагування на критичні ситуації для підтримки безперебійної роботи систем.

2. Захист і безпека інформаційних ресурсів:

впровадження і підтримка заходів кібербезпеки для захисту інформаційних систем від несанкціонованого доступу, кібератак та інших загроз;

управління доступом до конфіденційної інформації та забезпечення її захисту відповідно до вимог законодавства;

проведення регулярних перевірок і аудитів безпеки, а також тестування систем на вразливості.

3. Управління інцидентами та проблемами:

оперативне реагування на інциденти, що виникають у процесі експлуатації ІТ-систем, та їх ефективне вирішення;

аналіз кореневих причин інцидентів та впровадження заходів для запобігання їх повторенню;

забезпечення доступності ресурсів і підтримки для вирішення проблем, що виникають у користувачів.

4. Управління змінами та конфігураціями:

управління життєвим циклом змін у ІТ-інфраструктурі для мінімізації ризиків і забезпечення стабільності систем;

ведення та оновлення бази даних конфігураційних одиниць для забезпечення їх контролю та відстеження;

забезпечення координації змін та їх впровадження з мінімальним впливом на поточну роботу систем.

5. Резервне копіювання та відновлення:

організація регулярного резервного копіювання критичних даних та систем;

розробка та впровадження планів відновлення після аварій та забезпечення їх тестування;

забезпечення швидкого відновлення функціонування систем після інцидентів або аварій.

6. Технічна підтримка користувачів:

надання технічної допомоги персоналу Міністерства оборони у використанні ІТ-ресурсів та рішенні технічних проблем;

проведення навчань та консультування користувачів щодо безпечного та ефективного використання ІТ-систем;

забезпечення доступності технічної підтримки через різні канали (телефон, електронна пошта, система заявок).

7. Управління доступом та аутентифікацією:

контроль та управління доступом до інформаційних систем та ресурсів Міністерства оборони;

впровадження політик аутентифікації та авторизації для забезпечення безпеки даних;

управління обліковими записами користувачів та контроль за відповідністю їх прав доступу.

8. Аналітика та звітність:

збір, аналіз та звітність щодо показників ефективності роботи ІТ-інфраструктури;

визначення та аналіз ключових показників

безпеки, ефективності та доступності ІТ-систем;

надання звітів керівництву Міністерства оборони для прийняття обґрунтованих рішень щодо управління інформаційною інфраструктурою.

9. Підтримка розвитку та модернізації ІТ-інфраструктури:

оцінка та впровадження нових технологій та рішень для підвищення ефективності та безпеки ІТ-інфраструктури;

розробка та підтримка проектів з модернізації існуючих систем та впровадження нових технологій;

забезпечення безперервного поліпшення технологічної підтримки відповідно до змін у вимогах та загрозах.

Ці функції, як декомпозиція основної функції СТП, забезпечують комплексний підхід до технологічної підтримки інформаційної інфраструктури МО України, що є критично важливим для забезпечення національної безпеки та ефективності операцій.

Висновки й перспективи подальших досліджень

Отже, в статті розкриті концептуальні погляди на організацію технологічної підтримки інформаційної інфраструктури МО України, сформульовано її завдання, проаналізовані підходи щодо організації технологічної підтримки, що дало змогу виробити рекомендації щодо створення перспективної системи технологічної підтримки інформаційної інфраструктури МО України, обґрунтувати її склад та провести декомпозицію основної функції СТП, для більш детального опису призначення та завдань СТП інформаційної інфраструктури МО України.

Напрямами подальших досліджень можна визначити детальний аналіз описаних вище ITSM підходів до організації технологічної підтримки та обґрунтування можливості їх застосування для управління інформаційною інфраструктурою МО України, пошук та обґрунтування науково-методичного апарату оцінювання ефективності функціонування СТП, розробка функціональної моделі СТП. Зазначені дослідження можуть бути направлені на підвищення ефективності СТП інформаційної інфраструктури МО України, що в цілому дозволить забезпечити надійне та ефективне функціонування інформаційно-комунікаційних систем, розгорнутих на базі інформаційної інфраструктури МО України.

Список бібліографічних посилань

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII (зі змінами). URL: https://zakon.rada.gov.ua/rada/show/2469-19 (дата звернення: 05.07.2024). **2. Про рішення** Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 17.09.2021 № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 05.07.2023). **3. Морозов А. О., Косс В. А.** Управління розробкою Єдиної АСУ Збройних Сил. *Наука і оборона.* 2006. № 2. С. 30–34. **4. Кірпічніков Ю. А., Литовченко Г. Д., Розумний О. Д., Самойленко Н. М.** Підходи до технологічної підтримки інформаційної інфраструктури Міністерства оборони України. *Збірник наукових праць Центру воєнно-стратегічних досліджень*. 2019. № 3 (67). С. 78–82. **5. Огнєва А. М.** Аудит інформаційних систем і технологій. *Вісник Хмельницького Національного університету.* 2009. № 6. Т. 1. С. 229–232. **6. Мороз О. О., Кисса І. І.** Функції міжнаціональних команд віддаленої підтримки кінцевих користувачів інформаційних систем в глобальному ІТ-підприємстві. *Innovation and sustainability*. 2023. № 4. С. 6–18. DOI: https//doi.org/10.31649/ins.2023.4.6.18. **7. Панченко С. М., Антонюк А. Г. Новицький Д. В., Усок С. О., Заморський С. М.** Загальні підходи до створення системи управління і контролю функціонування сервісів інформаційних систем у Збройних Силах України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 3(48). С. 98–106. DOI: https//doi.org/10.33099/2311-7249/2022-48-3-98-106. **8. Заховалко Т. В., Максишко Н. К., Олешко О. В.** Аналіз та удосконалення процесу технічної підтримки користувачів інформаційних систем банку. *Вісник Запорізького Національного університету*. 2014. № 3(14). С. 64–76. **9. Про захист інформації** в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 81/94-ВР (зі змінами), URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення 21.07.2024). **10. Про основні засади** забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 21.07.2024). **11. ДСТУ ISO/IEC 27001:2022.** Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. (ISO/IEC 27001:2022) [Чинний від 31.12.2023]. Вид. офіц. Київ : Держспоживстандарт України, 2023. **12. ДСТУ ISO/IEC 20000-1:2022.** Інформаційні технології. Керування послугами. Частина 1. Вимоги до системи керування послугами. (ISO/IEC 20000-1:2022) [Чинний від 01.08.2019] Вид. офіц. Київ : Держспоживстандарт України, 2023. **13. Обґрунтування архітектурних** рішень щодо побудови інформаційної інфраструктури Міністерства оборони України: звіт про НДР / ЦВСД НУОУ; кер. Ю. А. Кірпічніков; викон.: О. В. Головченко [та ін.]. Київ, 2018. 159 с. № ДР0118U000378. **14. Обґрунтування технологічних рішень** щодо створення захищеної інформаційної інфраструктури Міністерства оборони України: звіт про НДР / ЦВСД НУОУ; кер. Ю. А. Кірпічніков; викон.: О. В. Головченко [та ін.]. Київ, 2016. 205 с. № ДР 0116U000068. **15. Визначення доцільних підходів** до організації технологічних сервісів управління та підтримки інформаційної інфраструктури Міністерства оборони України: звіт про НДР / ЦВСД НУОУ; кер. Ю. А. Кірпічніков; викон.: О. В. Головченко [та ін.]. Київ, 2019. 176 с. № ДР 0119U000312. **16. What is ITIL** Best Practice. ITIL. AXELOS URL: https://www.axelos.com/best-practice-solutions/itil/what-is-itil (дата звернення 21.07.2024). **17. ITIL V3** Service Life Cycle – IT Service Management – ITILIT Service Management – ITIL, ITIL Application Support. URL: http://www.itservicemanagement-itil.com/itil-v3-service-

life-cycle (дата звернення 21.07.2024). **18. ITIL event management**. URL: https://www.bmc.com/guides/itil-event-management.html (дата звернення 21.07.2024). **19. IT Service Management** – ITIL®. URL: http://www.best-management-practice.com/IT-Service-Management-ITIL/ (дата звернення 21.07.2024) **20. Bahrain Government Embraces** COBIT 5 Governance and IT Management By Harikrishnan Sugumaran, ITIL, ToGAF, Khalid Al-Mutawah, Ph.D., Zakareya Ahmed Al-Khaja, Ph.D. URL: http://www.isaca.org/COBIT/focus/Pages/bahrain-government-embraces-cobit-5-governance-and-it-management.aspx (дата звернення 21.07.2024). **21. COBIT 5:** Creating Buy-in and Empowering Teams to Change By Paul Wilkinson and Gary Hardy. URL: http://www.isaca.org/COBIT/focus/Pages/cobit-5-creating-buy-in-and-empowering-teams-to-change.aspx (дата звернення 21.07.2024). **22. Dubai Customs COBIT 5** Implementation By Vishal Vyas, GEIT, Juma Al Ghaith, Ahmad Al Yaqoobi, PMP, and Syed Junaid Hasan, PMP URL: http://www.isaca.org/COBIT/focus/ Pages/dubai-customs-cobit-5-implementation.aspx (дата звернення 21.07.2024). **23. Концепція розвитку** ІТ-інфраструктури Міністерства оборони України та Збройних Сил України. Затв. МО України 03.11.2021 р. ДПЦТтаІБСО МО України, ЦУЗтаІС ГШ ЗС України, 2021, 15 с.

CONCEPTUAL ASPECTS OF TECHNOLOGICAL SUPPORT FOR THE INFORMATION INFRASTRUCTURE IN UKRAINE'S MINISTRY OF DEFENCE

***Diadechko Andrii** (PhD)* [1]
***Datsenko Ivan** (Candidate of Technical Sciences)* [2]
Golovchenko Olexandr [3]

[1] ***National Defence University of Ukraine, Kyiv, Ukraine***
[2] ***Military Academy named after Yevheniy Bereznyak, Kyiv, Ukraine***
[3] ***Military unit A3458, Ukraine***

Formulation of the problem in general. *Effective and reliable functioning of the information infrastructure requires modern management methods. Therefore, it is necessary to create a technological support system for the information infrastructure of Ukraine's Ministry of Defence, where the information infrastructure itself and its components are the objects of management. The purpose of the article is to present conceptual views on the organization of technological support for the information infrastructure of Ukraine's Ministry of Defence, analyze approaches to its organization, formulate the main and specific tasks, develop recommendations for creating a prospective technological support system for the information infrastructure, justify its structure, define its main function, and conduct its decomposition.*

Research methods. *In writing the article, methods of systems analysis, comparative analysis, and expert evaluation were applied. This methodological approach allows for revealing the structure of the information infrastructure, analyzing current technological trends, comparing them with international standards, and determining approaches to organizing technological support for the information infrastructure of Ukraine's Ministry of Defence.*

Analysis of recent researches and publications. *The analyzed scientific works provide an opportunity to form an understanding of the organization of IT service user support and certain approaches to support organization. However, they do not address the aspects of technological support for the information infrastructure as a whole, which is a broader concept with a wider range of functions and tasks than user support.*

Presenting the main material. *The article presents conceptual views on the organization of technological support for the information infrastructure of Ukraine's Ministry of Defence, analyzes approaches to its organization, and formulates the main and specific tasks. Recommendations have been developed for creating a prospective technological support system for the information infrastructure, with its structure, main function, and decomposition substantiated.*

Elements of scientific novelty. *The article provides recommendations for the creation of a prospective technological support system for the information infrastructure of Ukraine's Ministry of Defence, justifying its composition, tasks, and functions.*

Theoretical and practical significance of the article. *The practical significance of the article lies in the potential application of the developed recommendations for improving the information infrastructure of Ukraine's Ministry of Defence. The article presents conceptual views on the organization of technological support for the information infrastructure of Ukraine's Ministry of Defence, formulates its tasks, and analyzes approaches to organizing technological support. This has enabled the development of recommendations for creating a prospective technological support system for the information infrastructure.*

Conclusion and the perspectives of future researches. *Further research directions may include a detailed analysis of the ITSM approaches to organizing technological support described above and justifying their applicability for managing the information infrastructure of Ukraine's Ministry of Defence, as well as the search for and justification of a scientific and methodological framework for evaluating the effectiveness of the technological support system's functioning and the development of its functional model.*

Key words: *Information infrastructure, technological support, information system, IT services, information technology.*

References

1. On the national security of Ukraine [online], (2018). Law of Ukraine No. 2469-VIII, June 21 (as amended). Available at: https://zakon.rada.gov.ua/rada/show/2469-19 [Accessed 07 May 2024]. **2. On the decision** of the National Security and Defence Council of Ukraine dated August 20, 2021 «On the Strategic Defence Bulletin of Ukraine» [online], (2021). Decree of the President of Ukraine No. 473/2021, September 17. Available at: https://www.president.gov.ua/documents/4732021-40121 [Accessed 07 May 2023]. **3. Morozov, A. O., Koss, V. A.,** (2006). Management of the development of the Unified ACS of the Armed Forces. *Science and Defence/* 2, 30-34. **4. Kirpichnikov, Yu. A., Lytovchenko, G. D., Rozumny, O. D., Samoilenko, N. M.,** (2019). Approaches to technological support of the information infrastructure of the Ministry of Defence of Ukraine. *Collection of scientific works of the Center for Military and Strategic Studies*, 3(67), 78-82. **5. Ogneva, A. M.,** (2009). Audit of information systems and technologies. *Bulletin of the Khmelnytskyi National University*. 6, 1, 229-232. **6. Moroz, O. O., Kissa, I. I.,** (2023). Functions of international teams of remote support of end users of information systems in a global IT enterprise. *Innovation and sustainability*. 4, 6-18. DOI: https://doi.org/10.31649/ins.2023.4.6.18. **7. Panchenko, S. M., Antonyuk, A. H. Novytskyi, D. V., Usok, S. O., Zamorskyi, S. M.,** (2022). General approaches to the creation of a system of management and control of the functioning of services of information systems in the Armed Forces of Ukraine. *Modern information technologies in the field of security and defence*. 3(48), 98-106. DOI: https//doi.org/10.33099/2311-7249/2022-48-3-98-106. **8. Zakhovalko, T. V., Maksyshko, N. K., Oleshko, O. V.,** (2014). Analysis and improvement of the process of technical support for users of the bank's information systems. *Bulletin of the Zaporizhia National University*. 3(14), 64-76. **9. On the protection of information** in information and telecommunication systems [online], (1994). Law of Ukraine No. 81/94-BP, 07 May (as amended). Available at: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text [Accessed 21 June 2024). **10. On the main** principles of ensuring cyber security of Ukraine [online], (2017). Law of Ukraine (as amended) No. 2163-VIII, 05 October. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Accessed 21 June 2024]. **11. Derzhspozhyvstandart Ukrainy**, (2022). *Information security, cyber security and privacy protection. Information security management systems. Requirements*. DSTU ISO/IEC 27001:2022. Kyiv: Vyd. ofits. Kyiv. **12. Derzhspozhyvstandart Ukrainy,** (2022). *Information technologies. Management of services. Part 1. Requirements for the service management system*. DSTU ISO/IEC 20000-1:2022. Kyiv: Vyd. ofits. Kyiv. **13. Justification of architectural decisions** regarding the construction of the information infrastructure of the Ministry of Defence of Ukraine: a report on the National People's Republic of Ukraine (2018) / TsVSD NUOU; chief Yu.A. Kirpichnikov; performed by: O.V. Golovchenko [and others]. Kyiv, 159. No. DR 0118U000378. **14. Justification of technological** decisions regarding the creation of a protected information infrastructure of the Ministry of Defence of Ukraine: a report on the NDR (2016) / TsVSD NUOU; driver Yu.A. Kirpichnikov; performed by: O. V. Golovchenko [and others]. Kyiv 205 p. No. DR 0116U000068. **15. Determination of expedient** approaches to the organization of technological services for the management and support of the information infrastructure of the Ministry of Defence of Ukraine: a report on the NDR, (2019). TsVSD NUOU; driver Yu.A. Kirpichnikov; performed by: O.V. Golovchenko [and others]. Kyiv. No. DR 0119U000312. **16. What is ITIL** Best Practice. ITIL. AXELOS [online]. Available at: https://www.axelos.com/best-practice-solutions/itil/what-is-itil [Accessed: 21 July 2024]. **17. ITIL V3** Service Life Cycle – IT Service Management - ITILIT Service Management – ITIL, ITIL Application Support [online]. Available at: http://www.itservicemanagement-itil.com/itil-v3-service-life-cycle [Accessed: 21 July 2024]. **18. ITIL event** management [online]. Available at: https://www.bmc.com/guides/itil-event-management.html [Accessed: 21 July 2024]. **19. IT Service Management -** ITIL® [online]. Available at: http://www.best-management-practice.com/IT-Service-Management-ITIL [Accessed: 21 July 2024]. **20. Bahrain Government Embraces** COBIT 5 Governance and IT Management By Harikrishnan Sugumaran, ITIL, ToGAF, Khalid Al-Mutawah, Ph.D., Zakareya Ahmed Al-Khaja, Ph.D [online]. Available at: http://www.isaca.org/COBIT/focus/Pages/bahrain-government-embraces-cobit-5-governance-and-it-management.aspx [Accessed: 21 July 2024]. **21. COBIT 5:** Creating Buy-in and Empowering Teams to Change By Paul Wilkinson and Gary Hardy [online]. Available at: http://www.isaca.org/COBIT/focus/Pages/cobit-5-creating-buy-in-and-empowering-teams-to-change.aspx [Accessed: 21 July 2024]. **22. Dubai Customs COBIT** 5 Implementation By Vishal Vyas, GEIT, Juma Al Ghaith, Ahmad Al Yaqoobi, PMP, and Syed Junaid Hasan, PMP [online]. Available at: http://www.isaca.org/COBIT/focus/Pages/dubai-customs-cobit-5-implementation.aspx [Accessed: 21 July 2024]. **23. Concept for the development** of IT infrastructure of the Ukraine Ministry of Defense and the Ukraine Armed Forces. Approved by the Ministry of Defense of Ukraine on November 3, 2021. Directorate for Digital Transformation Policy and Information Security in the Field of Defense of the Ukraine Ministry of Defense, Communications and Information Systems Central Directorate of the General Staff of the Ukraine Armed Forces.