УДК 004.9.005.95 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/87-97

Кірпічніков Ю. А., кандидат технічних наук (0000-0001-6893-3569)
Рибидайло А. А., кандидат технічних наук, старший науковий співробітник (0000-0002-6156-469X)
Литовченко Г. Д. (0000-0002-8625-1438)
Бутенко М. П. (0000-0001-7272-5826)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Обґрунтування підходу до удосконалення інформаційної інфраструктури Міністерства оборони України для функціонування в умовах збройної агресії

Резюме. Проведено аналіз підходів до побудови інформаційної інфраструктури Міністерства оборони України, яка має функціонувати в умовах збройної агресії. Обґрунтовано порядок модернізації існуючої інформаційної інфраструктури Міністерства оборони України з урахуванням використання сучасних ІТ-технологій.

Ключові слова: інформаційна інфраструктура; модель життєвого циклу; інформаційна система; каскадна, інкрементна, еволюційна стратегії; верифікація; валідація.

Постановка проблеми. В умовах воєнно-політичної кризи та збройної агресії проти України, її державним інститутам, зокрема Міністерству оборони (МО) України, належить виробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки. Одним із пріоритетних напрямів є цифровізація діяльності та впровадження сучасних інформаційних технологій у сфері оборони для оперативного забезпечення посадових осіб різних рівнів управління Збройними Силами (ЗС) України певними комунікаційними, інформаційними та специфічними за напрямами їх діяльності функціональними сервісами [1]. Ці сервіси має реалізовувати інформаційна інфраструктура, головними вимогами до якої є надійність та безперервність надання якісних сервісів, кібернетична безпека тощо.

Довідка. *Інформаційна інфраструктура* (у загальному розумінні) – сукупність інформаційних (автоматизованих) систем, інформаційних ресурсів, електронних комунікаційних мереж, організаційно-технічних структур, механізмів, що забезпечують їх функціонування [2].

Інформаційна інфраструктура МО України – комплексна структура, яка об'єднує програмно-технічні засоби, організаційні заходи, нормативні документи, персонал та забезпечує функціонування, розвиток інформаційної взаємодії та інформаційного середовища МО та ЗС України [3].

Проблемним питанням є той факт, що інформаційна інфраструктура МО України перебуває на початку свого оновлення, а окремі теоретичні дослідження не охоплюють всього циклу її розвитку. Особливостями розвитку інформаційної інфраструктури на сучасному етапі є високий рівень уніфікації апаратних, зокрема обчислювальних засобів (інфраструктура як сервіс), системного програмного забезпечення (базових сервісів), впровадження різного за призначенням прикладного спеціального програмного забезпечення (функціональних сервісів). У зв'язку з цим необхідно визначити шляхи забезпечення якості як самих сервісів, так і своєчасність та безперервність їх надання. Забезпечення належної якості сервісів є динамічною задачею, складність якої пропорційна завданням та вимогам до інформаційної інфраструктури і, відповідно, до програмно-апаратного обладнання інформаційних систем і мереж, на базі якого побудовані ці системи.

Вирішення цієї задачі полягає в інтеграції програмного забезпечення та обладнання в інформаційні системи, які існують або створюються, та узгодження їх повноцінного використання для досягнення запланованих переваг від провадження цих змін. Нагальною вбачається задача аналізу сучасних підходів щодо удосконалення інформаційної інфраструктури МО України, визначення технологічних підходів та організаційно-технічних заходів із забезпечення її надійного функціонування для забезпечення гарантованого надання якісних сервісів у будь-яких несприятливих умовах. Особливої значимості означене завдання набуває в умовах збройної агресії.

Аналіз останніх досліджень і публікацій. Сучасні підходи щодо розбудови інформаційної інфраструктури розглядаються у багатьох джерелах, зокрема у [4–12], де висвітлюються:

сутність основних підходів до створення інформаційної інфраструктури, їх основні переваги і недоліки;

базові стратегії застосування відомих підходів до розроблення інформаційної інфраструктури;

основні переваги застосування хмарних технологій для надання сервісів;

основні переваги, недоліки і умови застосування блокчейну для забезпечення безпеки, прозорості та надійності даних і транзакцій.

Особливе значення для критично важливих інформаційних систем та сервісів має поняття живучості системи. У роботі [12] розглянуті питання аналізу живучості інформаційних систем і мереж в умовах деструктивних інформаційних впливів, наведена класифікація інформаційних атак в інформаційних мережах та методи їх виявлення.

Довідка. *Живучість* – здатність комп'ютерної (комп'ютеризованої) системи (КС) виконувати задані специфікацією функції при зміненні нормальних зовнішніх умов функціонування на більш жорсткі, навіть за наявності елементів і складових частин, що перебувають у стані відмови, не допускаючи їх переходу у критичні відмови, поки не досягнуто граничного стану [13].

У роботах [14–16] представлено методи забезпечення живучості інформаційно-комунікаційної мережі на основі перерозподілу ресурсів мережі, використання механізмів резервування, реорганізації та реконфігурації для обслуговування потоків вимог у разі виникнення несприятливих впливів. Розглянуті методи дають змогу оцінити інформаційно-комунікаційної мережі та підвищити час її життя. Проте факторів, які враховуються, недостатньо для повноцінного оцінювання якості сервісів і стану інформаційної інфраструктури.

Як показав аналіз, підходи щодо забезпечення функціонування інформаційної інфраструктури, та попередження усіх видів несприятливих впливів ще недостатньо розвинуті. В означених джерелах систематизований аналіз використання відомих підходів та сучасних інформаційних технологій до створення інформаційної інфраструктури в умовах збройної агресії не наведено Це являє собою важливу наукову проблему системного характеру, яка потребує комплексних наукових і прикладних досліджень. Тому актуальною є задача суттєвого підвищення рівня живучості інформаційної інфраструктури, її ефективності та працездатності за рахунок оптимізації її структури, введення надлишкових (апаратних, програмних, часових та ін.) засобів покращання показників відмовостійкості та зниження складності структури таких систем.

Мета статті – обґрунтування рекомендацій щодо шляхів удосконалення інформаційної інфраструктури Міністерства оборони України з урахуванням можливостей новітніх ІТ-технологій для забезпечення її функціонування та надійного застосування в умовах збройної агресії.

Виклад основного матеріалу. Аналіз досвіду забезпечення функціонування інформаційної інфраструктури МО України в контексті збройної агресії, окупації частини території країни та ведення бойових дій виявив низку основних вимог:

можливість швидкого розгортання та надання сервісів, розширення їх функціональності, масштабування, відповідно до значного зростання інформаційних потреб органів військового управління;

створення єдиного інформаційного простору для всіх його учасників, не зважаючи на розосереджене розгортання військ на територіях, розділених силами супротивника, мобільність підрозділів і частин та високу динаміку переміщень угруповань військ у цілому;

забезпечення швидкого надання сервісів безпосереднім учасникам бойових дій (рівнів батальйон – рота – взвод – окремий солдат), у тому числі за допомогою мобільних пристроїв по будь-яким каналам зв'язку;

забезпечення стійкості інформаційної інфраструктури для гарантованого надання сервісів, враховуючі можливість ураження окремих її елементів як кінетичною зброєю, так і шляхом проведення кібератак.

Умови збройної агресії можуть серйозно впливати на функціонування інформаційної інфраструктури МО України. Деякі з основних чинників, які можуть впливати на забезпечення функціонування інформаційної інфраструктури (ІнфІ) в умовах збройної агресії наведені у Табл. 1.

Таблиця 1

Чинники збройної агресії, які впливають на функціонування інформаційної інфраструктури

№	ЧИННИКИ	НАСЛІДКИ ВПЛИВУ
1	***Фізичне пошкодження ІнфІ***	Фізичне пошкодження інформаційних мереж, комп'ютерів, серверів та інших пристроїв, які є складовими частинами ІнфІ
2	***Відключення від мережі***	Відключення від мережі операторів електронних комунікацій, хостинг-провайдерів та інших постачальників послуг, що може призвести до відключення частини ІнфІ
3	***Вразливість мережевої безпеки***	Зростання рівня кіберзагроз: кібератаки, хакерські атаки та віруси, що можуть порушити функціонування ІнфІ та зашкодити їй
4	***Втручання в управління***	Може включати: блокування доступу до деяких вебсайтів та інших дій, що можуть обмежити доступ до інформації та вплинути на функціонування ІнфІ
5	***Недоступність ресурсів***	Відсутність електропостачання та доступу до Інтернету/Інтранету окремих складових ІнфІ може обмежити повноту її функціонування
6	***Нехватка кваліфікованих кадрів***	Відтік кваліфікованих ІТ-спеціалістів може призвести до нестачі кваліфікованих кадрів для підтримки ІнфІ

Одним із перспективних шляхів розвитку інформаційної інфраструктури є використання сучасних потужних програмно-апаратних платформ, сховищ даних з використанням блокчейн-технології, засобів віртуалізації обчислювальних та мережевих ресурсів, а також хмарних технологій.

Побудова інформаційної інфраструктури для оборонних потреб може бути реалізована за допомогою різних підходів, які наведені у Табл. 2.

Таблиця 2

Підходи до реалізації інформаційної інфраструктури

№	ПІДХОДИ	ТЛУМАЧЕННЯ	ВИКОРИСТАННЯ
1	***Централізований***	Уся інформація зберігається в єдиній централізованій базі даних (центр обробки даних), яка забезпечує доступ до інформації всім зацікавленим сторонам у реальному часі	Великі організації та органи управління
2	***Децентралізований***	Кожний підрозділ має власну базу даних (центр обробки даних), яка зберігає інформацію, необхідну для виконання своїх завдань	Організації, де різні підрозділи мають спеціалізовані функції
3	***Гібридний***	Використовуються елементи як централізованого, так і децентралізованого підходів	Територіальна розгалуженість споживачів
4	***Датацентричний***	Усі компоненти інфраструктури мають бути побудовані навколо датацентру та підкорятися його вимогам і потребам, що дає змогу досягти оптимальної ефективності, надійності та безпеки роботи інфраструктури	Дозволяє забезпечити оптимальний рівень обробки і зберігання даних та досягти високої надійності і безпеки роботи інфраструктури
5	***Хмарний***	Інформаційна інфраструктура реалізується на основі сервісів, які надаються приватною хмарою або хмарними провайдерами	Необхідність високої гнучкості та масштабованості
6	***З використанням блокчейну***	Інформація зберігається в розподіленій мережі вузлів, які забезпечують високий рівень безпеки та захисту даних	Необхідність високого рівня безпеки та конфіденційності даних

Аналіз сучасного стану інформаційної інфраструктури МО України показує, що здебільшого їй притаманно використання децентралізованого підходу. Завдання щодо інтеграції окремих інформаційних ресурсів, інформаційних, інформаційно-аналітичних систем та автоматизованих систем управління військами та зброєю не ставилось. *Децентралізований підхід під час побудови інформаційної інфраструктури* базується на використанні розподілених систем, які не залежать від єдиного центру управління та мають можливість забезпечувати працездатність та безпеку інформаційної інфраструктури в умовах обмеженого зв'язку та доступності до ресурсів. Децентралізовані системи можуть забезпечувати високу швидкість та надійність передачі даних й

доступу до цих даних, що є особливо важливим в умовах збройної агресії. Однак слід враховувати, що децентралізовані системи потребують великих витрат на їх розроблення, впровадження та підтримку. Такі системи можуть бути більш складними у використанні для звичайних користувачів, що може потребувати додаткового навчання та підтримки. Крім того, децентралізовані системи можуть бути більш уразливими до атак, оскільки вони не мають єдиного центру управління, який міг би забезпечити захист від зломів та атак хакерів. Для забезпечення безпеки необхідно використовувати спеціальні технології та протоколи. Варто зазначити, що в децентралізованих системах необхідно встановити чіткі правила та процедури для прийняття рішень та вирішення конфліктних ситуацій, оскільки відсутність централізованого управління може призвести до неузгоджених дій та неефективного використання ресурсів.

Отже, для створення сучасної інформаційної інфраструктури доцільно більш детально розглянути підходи, які передбачають *інтеграцію інформаційних ресурсів МО України*, а саме: централізований, гібридний та датацентричний підходи.

Централізований підхід до побудови інформаційної інфраструктури в умовах збройної агресії передбачає, що всі інформаційні (інформаційно-комунікаційні) системи, електронні комунікаційні мережі та інформаційні ресурси керуватимуться централізовано. Це означає, що всі рішення, налаштування та зміни, що приймаються, здійснюватимуться центральним органом управління, який контролює всі аспекти інфраструктури.

Такий підхід має нозку переваг в умовах збройної агресії, коли інформаційна інфраструктура може бути схильна до руйнування або злому. Централізований підхід дає змогу створити більш надійний захист інформації та швидше реагувати на будь-які інциденти, пов’язані з безпекою, краще контролювати доступ до інформації та її використання, а також реагувати на можливі загрози. Перевагою централізованого підходу є можливість оптимізації використання ресурсів та забезпечення рівномірного доступу до інформації. В умовах збройної агресії це особливо важливо, оскільки необхідно забезпечити швидке та ефективне прийняття рішень, що може бути досягнуто лише за наявності доступу до актуальної та достовірної інформації. Ще однією перевагою централізованого підходу є простіше адміністрування складових інформаційної інфраструктури, оскільки всі ресурси знаходяться під контролем центрального вузла. Це дає змогу забезпечити єдиний рівень сервісів та підтримки користувачів, а також швидкого реагування на проблеми та збої в роботі.

Однак такий підхід також має свої недоліки. При централізованому підході необхідно враховувати ризики, пов’язані з єдиною точкою відмови, тобто якщо центральний вузол вийде з ладу, вся інформаційна інфраструктура може стати недоступною. Це може призвести до затримки надання сервісів і, як наслідок, несвоєчасного прийняття управлінських рішень. Крім того, у разі відключення центрального вузла вся інформаційна інфраструктура може стати недоступною.

Під час використання централізованого підходу в умовах збройної агресії необхідно забезпечити ефективне управління та контроль за всіма системами та ресурсами. Це можна досягти через впровадження систем моніторингу та управління, які дають змогу швидко реагувати на можливі проблеми та усувати їх.

Важливим аспектом централізованого підходу є також навчання та підготовка персоналу, який керуватиме всіма системами та ресурсами. Необхідно забезпечити не лише технічну, а й організаційну підготовку персоналу, щоб він міг ефективно працювати в умовах стресу та позаштатних ситуацій.

Ще одним важливим аспектом централізованого підходу в умовах збройної агресії є необхідність постійного оновлення та модернізації систем і ресурсів. Це дасть змогу забезпечити належний рівень функціональності, безпеки та стійкості роботи всієї інфраструктури.

Отже у процесі використання централізованого підходу мають бути враховані його недоліки, такі як: більш висока залежність від центрального вузла; менша гнучкість та можливість повільнішої реакції на зміни зовнішнього середовища. Також використання централізованого підходу може бути більш витратним, оскільки потрібно забезпечити високу надійність та доступність центрального вузла та пов’язаних із ним ресурсів.

Гібридний підхід під час побудови інформаційної інфраструктури за умов збройної агресії передбачає комбінацію централізованого та децентралізованого

підходів. Такий підхід може бути корисним, коли необхідно поєднати переваги обох підходів та зменшити їх недоліки. Наприклад, централізована система може використовуватися для управління спільними ресурсами, тоді як децентралізована система може використовуватися для зберігання та обміну інформацією.

Гібридний підхід доцільно використовувати у ситуаціях, коли уповноважені особи мають різні рівні доступу та контролю. Наприклад, централізована система може використовуватися для управління високорівневими завданнями, такими як розподіл ресурсів, а децентралізована система – для управління процесами нижчестоящими, такими як обмін інформацією між групами і підрозділами. Гібридний підхід за умов збройної агресії може бути ефективним, якщо використовуються найбільш підходящі елементи кожного підходу. Однак перш ніж реалізовувати гібридний підхід, необхідно провести ретельний аналіз ситуації, щоб вибрати оптимальний підхід та оцінити потенційні ризики та переваги.

Недоліком гібридного підходу є складніша архітектура, яка потребує більш високого ступеня інтеграції між різними компонентами інформаційної інфраструктури. Це також може потребувати вищого рівня експертизи та технічних знань для проєктування та управління. Слід зазначити, що гібридний підхід може потребувати додаткових витрат на інфраструктуру та обладнання для інтеграції різних елементів. Це може бути особливо значущим в умовах збройної агресії, коли доступ до ресурсів може бути обмеженим або недоступним. Також гібридний підхід може бути більш складним у реалізації та управлінні, ніж один із підходів окремо. Тому для успішної реалізації гібридного підходу необхідно спланувати та реалізувати кожну його частину, враховуючи конкретні потреби та умови.

Гібридний підхід може включати використання різних технологій і програмних засобів, які дають змогу забезпечувати більш ефективну роботу в умовах збройної агресії:

засоби автоматизованого резервного копіювання даних дають змогу швидко відновлювати дані у разі їх втрати або пошкодження;

використання розподіленого зберігання та обробки даних, спільно з локальними серверами та засобами електронних комунікацій;

різні методи моніторингу та аналізу роботи інфраструктури дають змогу швидко виявляти і усувати можливі проблеми;

методи виявлення вторгнень і захисту від шкідливих програм дають змогу захиститись від зовнішніх загроз;

використання різних стратегій управління інформаційною інфраструктурою, які дають змогу ефективно розподіляти ресурси і вирішувати виникаючі завдання (наприклад, можна використовувати стратегії управління за принципом “розподіленого управління”, коли рішення приймаються лише на рівні локальних об’єктів, а не централізовано).

Для успішної реалізації гібридного підходу необхідно провести аналіз вимог щодо інформаційної інфраструктури в умовах збройної агресії, оцінити всі фактори та ресурси, визначити необхідні технології та програмні засоби для реалізації інфраструктури, а також розглянути потенційні ризики та переваги.

Датацентричний підхід – це архітектурний підхід, у якому інформаційна інфраструктура створюється навколо загальнодоступного сховища даних та полягає в тому, що центральним елементом стає дата центр (центр обробки даних). *Датацентр* – це фізичне місце, де розміщуються сервери, мережеве обладнання та інші компоненти інфраструктури для зберігання, обробки та надання доступу до даних. Сутність датацентричного підходу полягає в тому, що всі інші компоненти інфраструктури повинні бути побудовані навколо датацентру та підкорятися його вимогам і потребам. Це дає змогу досягти оптимальної ефективності, надійності та безпеки роботи інфраструктури.

Для забезпечення високої доступності та надійності інфраструктури, датацентри мають бути забезпечені системами резервного живлення, охолодження, пожежної безпеки та захисту від несанкціонованого доступу. Датацентричний підхід дає змогу забезпечити стійке функціонування інформаційної інфраструктури, що є особливо важливим в умовах зростаючого обсягу даних та недопущення їх втрати в умовах збройної агресії.

Датацентричний підхід має свої недоліки: високі витрати на створення та управління датацентром, складність підтримки та розвитку датацентру, а також ризик виникнення технічних проблем, таких як відмова обладнання. Тому, прийняття рішення про використання датацентричного

підходу має базуватися на аналізі потреб ЗС України та оцінці переваг та недоліків цього підходу в контексті виконання завдань, які покладені на воєнне відомство та стратегії його розвитку. У Табл. 3 наведені переваги і недоліки датацентричного підходу при застосуванні інформаційної інфраструктури в умовах збройної агресії.

Таблиця 3

Переваги і недоліки датацентричного підходу

№	ПЕРЕВАГИ	НЕДОЛІКИ
1	*Централізоване керування*. Дає змогу ефективно керувати і контролювати ІнфІ навіть в умовах збройної агресії, де можуть бути обмежені ресурси та доступ до них	*Залежність від централізованого вузла*. Передбачено наявність централізованого вузла, який забезпечує функціонування всієї ІнфІ. Це означає, що у разі пошкодження або знищення датацентру може виникнути повна втрата доступу до даних і відсутність роботи ІнфІ
2	*Захист інформації*. Дає змогу використовувати передові заходи безпеки, такі як багаторівнева автентифікація, шифрування даних та моніторинг активності, для запобігання несанкціонованому доступу до інформації	*Уразливість до кібератак*. Зосередження великої кількості даних і ресурсів у датацентрах робить їх привабливою мішенню для кібератак. Атака на централізований датацентр може призвести до значних наслідків, таких як втрата конфіденційності, пошкодження або видалення даних
3	*Масштабованість*. Забезпечується можливість легкого масштабування ІнфІ - за необхідності можна швидко додати нові сервери, збільшити ємність зберігання даних та розширити мережеві ресурси, що дає змогу забезпечити стійкість і надійність системи навіть у разі збройної агресії	*Залежність від мережевого зв'язку*. Для ефективного функціонування датацентричної інфраструктури необхідне стійке і надійне мережеве з'єднання. У випадку збройної агресії може бути порушено мережевий зв'язок, що призведе до відсутності доступу до даних і зниження продуктивності

Ураховуючи ці переваги і недоліки, під час застосування датацентричного підходу в умовах збройної агресії необхідно ретельно збалансувати заходи безпеки, резервування даних і стійкість мережевого зв'язку, щоб забезпечити стійку роботу інформаційної інфраструктури навіть у складних умовах.

Датацентричний і централізований підходи являють собою різні моделі організації обчислювальних ресурсів і зберігання даних. Основні відмінності між ними полягають у розташуванні, управлінні та доступі до ресурсів. У Табл. 4 наведені відмінності датацентричного і централізованого підходів під час побудови інформаційної інфраструктури.

Таблиця 4

Відмінності датацентричного і централізованого підходів

№	Відмінність	ПІДХОДИ	
		Централізований	**Датацентричний**
1	***Розташування***	Обчислювальні ресурси та зберігання даних знаходяться в одному фізичному місці або декількох центральних локаціях	Ресурси розподілені у вигляді датацентрів, розташованих в різних географічних областях
2	***Управління***	Управління обчислювальними ресурсами та зберіганням даних здійснюється централізовано. Відомство в цілому або військове формування приймає рішення щодо розподілу ресурсів і забезпечує їх функціонування	Кожний датацентр може мати власну команду управління, що робить його більш автономним
3	***Доступ до ресурсів***	Доступ до ресурсів здійснюється через мережу, зв'язок з центральними серверами або системами зберігання даних	Доступ до ресурсів може бути розподіленим між різними датацентрами, що забезпечує резервування та більшу надійність
4	***Відмовостійкість***	Відмова одного центрального сервера або системи може призвести до зупинки всієї інфраструктури	Ресурси розподілені по різних датацентрах, і в разі відмови одного датацентру інші можуть продовжувати роботу
5	***Масштабованість***	Масштабування може бути обмеженим обсягом ресурсів, що доступні у центральній локації	Дозволяє більш гнучко масштабувати ресурси шляхом додавання або видалення датацентрів у відповідності до потреб

Обидва підходи мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб і вимог воєнного відомства. Можна також використовувати гібридні підходи, комбінуючи централізовану та датацентричну моделі, щоб поєднати переваги обох підходів.

Сутність *хмарного підходу* полягає в тому, що комп'ютерні ресурси та послуги надаються через глобальну мережу Інтернет з

використанням технологій віртуалізації та розподілу ресурсів. Замість того, щоб використовувати окремі фізичні сервери та обладнання, можна розмістити їх у приватній хмарі воєнного відомства або орендувати потрібні ресурси від хмарних провайдерів.

Хмарний підхід в умовах збройної агресії може мати низку переваг, які можуть забезпечити ЗС України ефективне подолання викликів та ризиків (Табл. 5).

Таблиця 5

Переваги хмарного підходу

№	ПЕРЕВАГИ	ТЛУМАЧЕННЯ
1	***Гнучкість***	Дає змогу швидко масштабувати та налаштовувати ресурси відповідно до поточних потреб, що особливо важливо в умовах збройної агресії, коли організація може зіткнутися з несподіваними та екстреними ситуаціями, які потребують швидкого реагування
2	***Розподілене зберігання та обчислення***	Дані можуть зберігатися в різних регіонах і центрах обробки даних, що забезпечує доступність та надійність. Користувачі можуть отримувати доступ до ресурсів та даних з будь-якого місця, де є Інтернет. Високий рівень доступності та надійності дає змогу організації підтримувати працездатність своєї інформаційної інфраструктури навіть в умовах збройної агресії
3	***Захист даних***	Високий рівень захисту даних, використовуючи різні сучасні технології та механізми шифрування, що може допомагає зберегти секретність даних, навіть якщо вона піддається кібератакам чи іншим формам збройної агресії
4	**Самообслуговування**	Користувачі можуть самостійно замовляти та налаштовувати ресурси через панель управління хмарним провайдером без необхідності втручання інженерів
	Автоматизація	Багато операцій, таких як резервне копіювання, моніторинг та автоматичне масштабування, можуть бути автоматизовані, що спрощує управління інфраструктурою
4	***Спільна робота***	Хмарні послуги зазвичай надають можливість спільної роботи над документами та проєктами, що може бути корисним для командної роботи в умовах збройної агресії
5	***Економічна ефективність***	Хмарні послуги можуть бути економічно ефективнішими, ніж локальні системи, оскільки вони дають змогу уникнути витрат на придбання (постійну модернізацію) та обслуговування устаткування

Загалом, хмарний підхід дає змогу зосередитися на основних завданнях, зменшуючи необхідність у великих капіталовкладеннях у фізичне обладнання та забезпечуючи гнучкість та швидкість в розвитку інформаційних рішень.

Використання блокчейну в умовах збройної агресії може бути корисним підходом для забезпечення безпеки, надійності зберігання даних.

Довідка. *Блокчейн* – це децентралізована та неруйнівна база даних, яка зберігає інформацію в ланцюжку блоків, кожен з яких містить інформацію про транзакцію та хеш попереднього блоку. Це дає змогу створювати ланцюжок блоків, який не може бути змінений або підроблений, і забезпечує надійність зберігання даних [8].

Використання блокчейн-технології в умовах збройної агресії може бути використаний для більш надійної реалізації функціональних сервісів воєнного відомства:

зберігання та управління даними у децентралізованій мережі, забезпечуючи високий рівень безпеки та захисту від несанкціонованого доступу;

підвищення ефективності процесів постачання та логістики шляхом використання блокчейн-рішень для управління ланцюгами постачання та відстеження руху вантажів;

використання смарт-контрактів для автоматизації та управління різними видами операцій: закупівля, контроль і облік запасів, управління бюджетами та інші;

створення децентралізованих систем обміну інформацією та координації між різними відділами та підрозділами військових формувань, забезпечуючи швидкий обмін інформацією та прийняття оперативних рішень;

управління інтелектуальною власністю та захисту авторських прав, що може бути корисним у галузі оборони та безпеки, де інтелектуальна власність є ключовим ресурсом;

управління даними та аналітики, що може допомогти швидше та точніше аналізувати дані та приймати рішення на їх основі.

Наприклад, блокчейн може використовуватися для зберігання та обміну медичною інформацією військовослужбовців, для забезпечення прозорості бюджетування та фінансового управління, а також для зберігання та обміну інформацією про логістичні та інші операції. Блокчейн може забезпечити захист від хакерських атак та інших видів кібератак шляхом створення

неруйнівних ланцюжків даних та зменшення ризиків несанкціонованого доступу до ресурсів.

Для реалізації підходу з використанням блокчейну необхідно провести такі етапи (рис. 1):

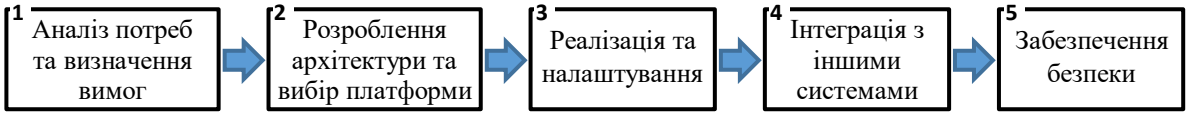

Рис. 1. Порядок реалізації блокчейну

Етап 1. *Аналіз потреб та визначення вимог* – визначаються дані та операції, які зберігатимуться та оброблятимуться в блокчейні, потрібні рівні доступу та контролю інформації, алгоритми та протоколи шифрування.

Етап 2. *Розроблення архітектури та вибір платформи* – на основі аналізу вимог розроблення архітектури блокчейн-рішення, вибір платформи та інструментів для реалізації, визначення параметрів мережі та її конфігурації.

Етап 3. *Реалізація та налаштування* – створення вузлів мережі, налаштування алгоритмів та протоколів, проведення тестування та оптимізації продуктивності.

Етап 4. *Інтеграція з іншими системами* для обміну інформацією та управління даними.

Етап 5. *Забезпечення безпеки* – проведення заходів забезпечення безпеки блокчейн-рішення, які включають захист від хакерських атак, контроль доступу та автентифікацію, моніторинг та аналіз дій користувачів.

Під час використання блокчейну слід враховувати деякі фактори – обмежена масштабованість та висока вартість створення та підтримки блокчейн-систем. Крім того, необхідно забезпечити безпеку доступу до блокчейн-системи та інформації, що зберігається в ній. Важливим аспектом також є вибір відповідної платформи блокчейну для конкретних потреб та завдань, а також забезпечення відповідної підтримки та навчання персоналу.

Проведений аналіз дає змогу дійти висновку – кожному з підходів притаманні власні переваги і недоліки та їх використання доцільне за певних умов і цілей створення інформаційної інфраструктури. Отже, у якості ***рекомендацій*** стосовно шляхів удосконалення інформаційної інфраструктури МО України для забезпечення її функціонування та надійного застосування в умовах збройної агресії. нагальним вважається поєднання розглянутих підходів для послаблення недоліків кожного з підходів та посилення їх переваг при комплексному використанні.

Для реалізації об’єднаного підходу у процесі створення інформаційної інфраструктури в умовах збройної агресії необхідно провести аналіз потреб та можливостей у рамках конкретного контексту конфлікту (або збройної агресії). Такий аналіз має враховувати не лише технічні аспекти, а й культурні, соціальні та політичні аспекти. Крім того, потрібно врахувати потреби посадових (службових) осіб МО і ЗС України. Тобто, необхідно розробити стратегію доступу до інформації та зв’язку у межах повноважень посадових осіб.

Розглянемо більш детально ***аспекти***, які потрібно враховувати під час реалізації об’єднаного підходу у процесі створення інформаційної інфраструктури, яка має зберігати функціональність в умовах збройної агресії.

Управління даними. В умовах збройної агресії управління даними може стати критично важливим для забезпечення їх безпеки та своєчасності прийняття управлінських рішень. Важливо розробити стратегію управління даними. У межах цієї стратегії можна використовувати технології блокчейну для забезпечення цілісності та безпеки даних, а також для створення системи керування доступом до даних. Це дасть змогу запобігти несанкціонованому доступу до даних та забезпечити контроль над їх використанням.

Безпека даних. Можна використовувати різні методи та технології:

шифрування даних;

застосування багатофакторної автентифікації – використання пароля, біометричних даних (наприклад, відбитків пальців або сканування особи), а також апаратних (наприклад, токенів) та програмних (наприклад, програмне забезпечення аутентифікації, що встановлюється на смартфони посадових осіб) засобів аутентифікації.

Довідка. *Токен* (захищений носій) – компактний пристрій у вигляді USB-флешки, призначений для забезпечення інформаційної

безпеки користувача, віддаленого доступу до інформації та використовується для ідентифікації його власника. На токені зберігається кваліфікований електронний підпис, який генерується у акредитованих центрах сертифікації ключів за безпосередньої участі власника ключа.

Важливим фактором є навчання користувачів та посилення культури безпеки. Користувачі повинні знати, як правильно використовувати інформаційну інфраструктуру та як захищати свої дані, а також розуміти наслідки порушення правил безпеки. Потрібно мати плани та процедури реагування на можливі порушення безпеки, включаючи резервне копіювання даних, детектування та запобігання атак, та відновлення після порушень.

Надійність та доступність. Гібридна інфраструктура може використовувати як локальні, так і хмарні ресурси, що дає змогу підвищити доступність систем та забезпечити їхню працездатність у разі відключення будь-якої з частин інфраструктури. Технологія блокчейну може також підвищити надійність системи, оскільки вона дає змогу створення надійних та стійких до змін систем зберігання даних. Крім того, блокчейн-технологія дає змогу захистити дані від несанкціонованого доступу та внесення змін до них.

Масштабованість системи. Хмарні рішення можуть бути використані підрозділами ЗС України за потреби швидкої масштабованості інформаційної інфраструктури в умовах збройної агресії. Залежно від ситуації, обсяг даних і кількість користувачів може значно змінюватися, і застосування хмарних сервісів дає змогу швидко масштабувати інфраструктуру для задоволення нових потреб.

Таким чином, удосконалення інформаційної інфраструктури на основі об'єднаного підходу в умовах збройної агресії є складним проєктом. Виходячи з проведеного у роботі аналізу, у Табл. 6 сформульовані вимоги до удосконаленої інформаційної інфраструктури, які потрібно задовольнити під час реалізації проєкту.

Таблиця 6

Вимоги до нової інформаційної інфраструктури МО України

№	ВИМОГИ
1	Необхідність дотримання міжнародних стандартів безпеки інформації ISO/IEC 27001 і національних стандартів України, якими імплементовані міжнародні стандарти безпеки інформації ISO/IEC 270XX, що забезпечить довіру до інформаційної інфраструктури міжнародних партнерів
2	Урахування можливих ризиків та уразливостей системи – DDOS-атаки, кібершпигунство, виток даних та інші види кіберзагроз. Для чого необхідно включити в проєкт заходи захисту інформації та введення механізмів швидкого реагування на інциденти безпеки
3	Визначення стратегії резервного копіювання та відновлення даних в умовах збройної агресії може відповідно до плану резервного копіювання даних та процедури відновлення
4	Визначення процедур керування доступом до інформації. Для запобігання несанкціонованому доступу до даних відповідно до стратегії управління доступом на основі рольової моделі доступу, двофакторної автентифікації та інших сучасних методів
5	Визначення місця розміщення ІнфІ для забезпечення можливості захисту від можливих ударів та терористичних актів супротивника, а також забезпечити її захист від природних катастроф, таких як землетруси, повені та інші
6	Врахування вимог до енергозабезпечення. В умовах збройної агресії можливі перебої в енергопостачанні, тому необхідно врахувати цей фактор під час вибору місця розміщення компонентів ІнфІ та визначення резервних джерел живлення
7	Розроблення стратегії моніторингу та аналізу інформації про стан ІнфІ у режимі реального часу для оперативного реагування на можливі загрози та вразливості
8	Кадрове забезпечення. Для забезпечення ефективної роботи ІнфІ необхідно готувати професійних фахівців, які мають відповідні знання та досвід роботи з сучасними ІТ-технологіями
9	Визначення плану дій при евакуації у разі виникнення загрози життю та здоров'ю персоналу

Для успішної реалізації такого проєкту потрібне проведення організаційних заходів, які наведені на рис. 2.

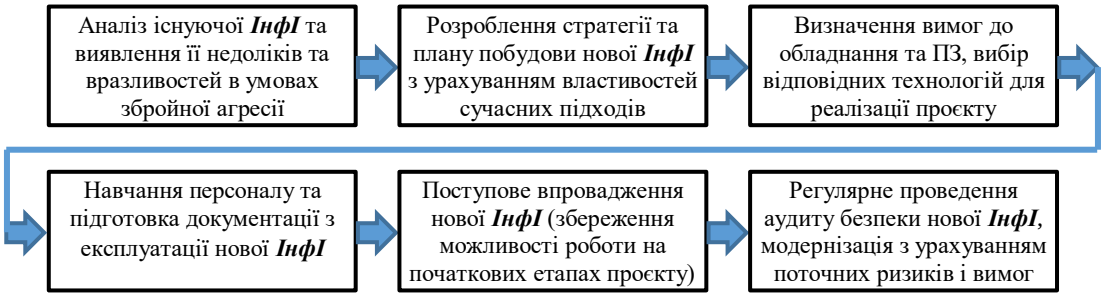

Рис. 2. Порядок удосконалення інформаційної інфраструктури МО України

Необхідно враховувати, що процес реалізації такого проєкту може зайняти тривалий час і вимагати значних інвестицій. У будь-якому випадку проведення ретельного аналізу та розроблення детального плану проєкту допоможе мінімізувати ризики та підвищити шанси на успіх.

Висновок. Розвиток інформаційної інфраструктури МО України має збільшити швидкість, точність і якість процесу прийняття рішень, які є критичними для прийняття стратегічних рішень та успіху операцій і бойових дій. Це дасть змогу повною мірою використовувати переваги обміну потрібною інформацією через всі домени інформаційного простору – від стратегічної до тактичної ланки, усунути принцип "ізольованості" існуючих інформаційних систем та забезпечити задоволення потреб в інформації, яка необхідна для швидкого прийняття рішень.

Подальші дослідженя доцільно зосередити на аналізі можливих ризиків під час функціонування інформаційної інфраструктури та обґрунтуванні заходів щодо їх уникнення або нівелювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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 р. № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/ 2021#Text (дата звернення: 10.07.2023).
2. Інформаційна інфраструктура // Матеріал з Вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Інформаційна_інфраструктура (дата звернення: 10.07.2023).
3. Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України.
4. Інформаційне забезпечення інноваційного розвитку: світовий та вітчизняний досвід: монографія / Т. В. Писаренко, Т. К. Кваша, Н. В. Березняк, О. В. Прудка. Київ : УкрІНТЕІ, 2015. 239 с.
5. Інформаційні системи і технології на підприємствах : конспект лекцій / В. М. Охріменко, Т. Б. Воронкова. Харків : ХНАМГ, 2006. 185 с. URL: http://eprints.kname.edu.ua/17149/1/In.form_systens_et_technologies_Ochrimenko.pdf (дата звернення: 11.07.2023).
6. Попова І. А., Сєрєбряк К. І. Модернізація інформаційної інфраструктури задля активізації міжрегіонального співробітництва // Інвестиції: практика та досвід. 2015. № 24. С. 49–52. URL: http://nbuv.gov.ua/UJRN/ipd_2015_24_12 (дата звернення: 11.07.2023).
7. Лазебник Л. Л., Войтенко В. О. Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства // Науковий вісник Міжнародного гуманітарного університету. 2020. DOI: https://doi.org/10.32841/2413-2675/2020-42-3.
8. Демчишак Н. Б., Радик В. В. Розвиток цифрової інфраструктури та блокчейн-технологій в Україні // Інноваційна економіка. 2020. № 3–4. DOI: https://doi.org/10.37332/2309-1533.2020.3-4.27.
9. Мануілов Я. С. Використання технології "блокчейн" у телекомунікаціях // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71). № 3. DOI: https://doi.org/10.32838/2663-5941/2021.3/20.
10. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління обороннними ресурсами / Ю. А. Кірпічніков та ін. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2019. № 1 (65). С. 86–91. DOI: https://doi.org/10.33099/2304-2745/2019-1-65/86-91.
11. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб / Ю. А. Кірпічніков та ін. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 3 (76). С. 68–75. DOI: https://doi.org/10.33099/2304-2745/2022-3-76/68-75.
12. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. Київ : Наук. думка, 2011. 256 с.
13. ДСТУ ISO/IEC 2382:2017.
14. Грищенко И. В. Метод повышения живучести инфокоммуникационной сети // Холодильна техніка і технологія. 2013. № 6. (146). С. 66–70.
15. Князева Н. О., Грищенко И. В., Шестопалов С. В. Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети // Холодильная техника и технология. 2014. № 4 (150). С. 65–71.
16. Зінченко А. А., Масесов М. О., Пантась І. О. Аналіз методів підвищення живучості телекомунікаційних мереж // Сучасні інформаційні технології у сфері безпеки та оборони. 2021. № 2 (41). DOI: https://doi.org/10.33099/2311-7249/2021-41-2-5-10.

Стаття надійшла до редакційної колегії 11.08.2023

Justification of the approach to improving the information infrastructure of the Ministry of Defense of Ukraine for functioning in conditions of armed aggression

Annotation

In the context of the military-political crisis and armed aggression against Ukraine, its state institutions, in particular the Ministry of Defense (MoD) of Ukraine, have to develop and apply new modern approaches to the development of its own information space, ensuring its stability and security. The peculiarities of information infrastructure development at the current stage are a high level of unification of hardware, including computing (infrastructure as a service), system software (basic services), and the introduction of special purpose application software (functional services). Ensuring the proper quality of services is a dynamic task, the complexity of which is proportional to the tasks and requirements for the information infrastructure.

The purpose of the article is to substantiate recommendations on ways to improve the information infrastructure of the Ministry of Defense of Ukraine, taking into account the capabilities of the latest IT technologies to ensure its functioning and reliable use in the context of armed aggression.

Building an information infrastructure for defense needs can be realized using different approaches. Each of the approaches has its own advantages and disadvantages, and their use is advisable under certain conditions and goals of information infrastructure creation. Implementation of a unified approach to the creation of information infrastructure for its sustainable functioning in the context of armed aggression requires an analysis of needs and capabilities within the specific context of the conflict (or armed aggression). Improving the information infrastructure based on a unified approach is a complex project. The author proposes a procedure for improving the information infrastructure of the Ministry of Defense of Ukraine.

Keywords: information infrastructure; life cycle model; information system; cascade, incremental, evolutionary strategies; verification; validation.