IMPROVEMENT OF THE INFORMATION INFRASTRUCTURE OF A LAW ENFORCEMENT AGENCY: A METHODOLOGICAL APPROACH

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ СИЛОВОГО ВІДОМСТВА: МЕТОДИЧНИЙ ПІДХІД

Anatolii Rybydajlo[1]
Hanna Lytovchenko[2]

DOI: https://doi.org/10.30525/978-9934-26-472-6-3

В умовах воєнно-політичної кризи та збройної агресії Російської Федерації (РФ) 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].

Під *інформаційною інфраструктурою* розуміють сукупність інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

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

Проблемним питанням є той факт, що існуюча інформаційна інфраструктура Міністерства оборони України за даним напрямом тільки починає розвиватися, а окремі теоретичні дослідження не охоплюють всього циклу її розвитку.

[1] National Defence University of Ukraine, Ukraine
[2] National Defence University of Ukraine, Ukraine

Нагальною вбачається задача аналізу сучасних підходів стосовно розбудови (модернізації/удосконалення) інформаційної інфраструктури (ІнфІ) Міністерства оборони (МО) України, яка є основою Єдиного інформаційного середовища воєнного відомства, для надання можливості обґрунтування управлінських рішень, які приймаються керівництвом Збройних Сил (ЗС) України. Особливу значущість означене завдання приймає в умовах збройного конфлікту.

Основні чинники, які можуть впливати на функціонування ІнфІ в умовах збройного конфлікту:

- фізичне пошкодження складових ІнфІ;
- відключення від мережі;
- вразливість мережевої безпеки;
- недоступність ресурсів (електроенергія та доступ до Інтернету);
- нехватка кваліфікованих кадрів (відтік кваліфікованих спеціалістів).

Побудова інформаційної інфраструктури для оборонних потреб може бути реалізована за допомогою апробованих підходів: централізований, децентралізований, гібридний, датацентричний, хмарний, з використанням блокчейну.

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 дозволяє створювати ланцюжок блоків, який не може бути змінений або підроблений, і забезпечує надійність і прозорість зберігання даних. Наприклад, блокчейн може використовуватися для зберігання та обміну медичної інформації військовослужбовців, для забезпечення прозорості бюджетування та фінансового управління, а також для зберігання та обміну інформацією про логістичні та інші операції.

Конкретний підхід до побудови інформаційної інфраструктури буде залежати від вимог конкретної організації та її цілей. Далі розглянуто особливості застосування підходів до побудови ІнфІ.

Використанню *централізованого підходу* для побудови ІнфІ, яка має зберігати стійкість в умовах збройної агресії притаманні певні ризики: втрата доступності (фізичне знищення центрального серверу – ЦС); порушення безпеки (зловмисники отримають доступ до ЦС); втрата даних та/або контролю; ризик витрат (потреба у відновленні інфраструктури).

Децентралізований підхід при побудові інформаційної інфраструктури в умовах збройної агресії 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.

Гібридний підхід при побудові інформаційної інфраструктури за умов збройної агресії передбачає інтеграцію переваг централізованого та децентралізованого підходів у межах однієї системи. Однак йому притаманні свої недоліки, такі як складність проєктування та впровадження, а також можливі проблеми взаємодії різних компонентів системи.

Хмарний підхід при побудові інформаційної інфраструктури в умовах збройної агресії може мати низку переваг, які можуть дозволити організації ефективно впоратися з викликами та ризиками, пов'язаними з цією ситуацією: можливість швидкого масштабування; високий рівень доступності, надійності і захисту даних; можливість спільної роботи користувачів.

Проведений аналіз дозволяє 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 при створенні інформаційної інфраструктури, яка має зберігати необхідний рівень стійкості в умовах збройної агресії проведено аналіз можливостей та потреб у рамках збройної агресії РФ проти України. Для забезпечення функціонування ІнфІ в умовах збройної агресії вона має відповідати наступним вимогам:

- дотримання міжнародних стандартів безпеки інформації ISO/IEC 27001 і національних стандартів України;
- врахування можливих ризиків та уразливостей системи – введення механізмів швидкого реагування на інциденти безпеки;
- розробка і впровадження плану резервного копіювання даних та процедури відновлення;
- розробка стратегії управління доступом на основі рольової моделі;
- забезпечити захисту ІнфІ від можливих ударів та терористичних актів супротивника;
- врахування вимог до безперебійного енергозабезпечення;
- належне кадрове забезпечення;
- розроблення плану дій при евакуації у разі виникнення загрози життю та здоров'ю персоналу.

Для успішної реалізації проєкту щодо удосконалення ІнфІ МО та ЗС України потрібна його грамотна, яка включає певні кроки (рис. 1).

Рис. 1. Порядок удосконалення інформаційної інфраструктури МО України

Розвиток ІнфІ МО України має збільшити швидкість, точність та якість процесу прийняття рішень, які є критичними для прийняття стратегічних рішень та успіху операцій і бойових дій. Це дозволить в повній мірі 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.

Список використаних джерел:

1. Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України.

2. Попова І.А. Модернізація інформаційної інфраструктури задля активізації міжрегіонального співробітництва [Електронний ресурс] / І.А. Попова, К.І. Сєрєбряк // Інвестиції: практика та досвід. – 2015. – № 24. – С. 49-52. – Режим доступу: http://nbuv.gov.ua/UJRN/ipd_2015_24_12

3. Лазебник Л.Л. Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства. / Л.Л. Лазебник, В.О. Войтенко // Науковий вісник Міжнародного гуманітарного університету.– 2020. – № 40. – С. 18-22.

4. Демчишак Н.Б. Розвиток цифрової інфраструктури та блокчейн-технологій в Україні. / Н.Б. Демчишак, В.В. Радик // Науковий журнал “Інноваційна економіка”. – 2020. – № 3–4. – С. 188-194.

5. Кірпічніков Ю.А. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб / Ю.А. Кірпічніков, В.О. Капілевич, О.В. Андрощук [та ін.] // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2022. – № 3(76). – С. 68-75.