УДК 004.9.005.95 DOI: https://doi.org/10.33099/2304-2745/2024-1-80/66-76

Рибидайло А. А., кандидат технічних наук, старший науковий співробітник (0000-0002-6156-469X)
Кірпічніков Ю. А., кандидат технічних наук (0000-0001-6893-3569)
Васюхно С. І. (0000-0002-0884-0405)
Петрушен М. В. (0000-0002-7448-2765)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Порядок вибору та впровадження технологічних рішень для забезпечення функціонування інформаційної інфраструктури Міністерства оборони України: методичний підхід

Резюме. Проведено аналіз складових забезпечення функціонування інформаційної інфраструктури воєнного відомства. З'ясовано, що ефективне застосування ІнфІ ґрунтується на використанні раціональних технологічних рішень. Обґрунтовано порядок вибору та впровадження технологічних рішень з урахуванням використання сучасних ІТ-технологій.

Ключові слова: інформаційної інфраструктура; технологічні підходи і рішення; зрілість інформаційної інфраструктури; критерії оцінювання зрілості інформаційної інфраструктури.

Постановка проблеми. Забезпечення функціонування інформаційної інфраструктури (ІнфІ) Міністерства оборони (МО) України включає комплекс заходів та технічних рішень, спрямованих на забезпечення ефективного та безперебійного функціонування систем, мереж, програм та інших компонентів інформаційної інфраструктури в сфері оборони.

Функціями ІнфІ є:

забезпечення доступу до даних і ресурсів – цифрових даних, файлів, додатків та інших ресурсів, необхідних для роботи користувачів;

забезпечення комунікацій – зв'язок між користувачами, включаючи локальні мережі, бездротовий доступ, відеоконференції та інші засоби комунікації;

зберігання і обробка даних – надаються системи для зберігання, обробки, аналізу та управління даними, включаючи сервери, бази даних та інші програмні рішення;

забезпечення безпеки – ІнфІ включає заходи безпеки, такі як антивірусні програми, файрволи, системи контролю доступу та інші технології, що захищають інформацію від несанкціонованого доступу та загроз;

підтримка роботи систем – ІнфІ може надавати різноманітні інструменти для підтримки і управління комп'ютерними системами, включаючи моніторинг, управління конфігурацією та інші інструменти для забезпечення ефективної роботи систем.

При цьому означені функції сприяють ефективній роботі та комунікації у військовому відомстві. У цьому контексті є потреба постійного моніторингу поточного стану ІнфІ МО України з метою застосування певних заходів для забезпечення її ефективного функціонування. Забезпечення функціонування інформаційної інфраструктури Міністерства оборони України є стратегічно важливою проблемою, оскільки вона впливає на здатність країни ефективно реагувати на загрози та забезпечувати національну безпеку. Нагальним вбачається завдання обґрунтування підходу щодо вибору потрібних (раціональних) технічних рішень та застосування певних організаційних заходів для забезпечення функціонування ІнфІ МО України.

Аналіз останніх досліджень і публікацій. Складові забезпечення функціонування ІІ МО України наведені у Табл. 1.

Таблиця 1

Складові забезпечення функціонування ІнфІ МО України

№	Аспект	Сутність забезпечення функціонування ІнфІ
1	**Безпека інформації**	Розробка та впровадження заходів забезпечення кібербезпеки для захисту інформації від несанкціонованого доступу, кібератак, витоків інформації та інших загроз
2	**Інфраструктура електронних комунікацій**	Забезпечення належного функціонування електронних комунікацій, включаючи надійні мережі для обміну інформацією між різними підрозділами та

№	Аспект	Сутність забезпечення функціонування ІнфІ
		командуванням
3	**Обробка та зберігання даних**	Розробка систем для ефективної обробки, зберігання та управління великими обсягами даних, що включають в себе відомості про оборонні операції, ресурси, кадри, логістику тощо
4	**Електронна безпека**	Використання електронних систем та технологій для захисту приміщень, територій та об'єктів від неприязних дій
5	**Моніторинг і аналітика**	Впровадження систем моніторингу для відстеження стану інформаційної інфраструктури та аналітичних інструментів для швидкого аналізу та прийняття рішень
6	**Інтеграція з іншими системами**	Забезпечення сумісності та інтеграції інформаційної інфраструктури Міністерства оборони України з іншими галузевими та міжнародними інформаційними системами
7	**Безперебійність роботи**	Розробка планів та впровадження резервних та відновлювальних систем для забезпечення неперервності роботи інформаційної інфраструктури навіть під час екстрених ситуацій чи атак
8	**Навчання та підтримка персоналу**	Організація навчальних програм для персоналу щодо ефективного використання та підтримки інформаційних технологій

З Табл. 1 видно, що забезпечення функціонування інформаційної інфраструктури можна розбити на складові. По кожному аспекту забезпечення у відкритому доступі наведено чимало джерел з певними напрацюваннями фахівців з відповідної галузі. У джерелах [1-6] висвітлюються результати досліджень, які можуть бути використані для обґрунтування шляхів розвитку ІнфІ.

У посібнику [1] викладено загальні поняття безпеки інформаційних ресурсів. Розглянуті способи побудови інформаційно-комунікаційних систем і мереж на основі сучасних способів передачі й обробки інформації та способи захисту інформації в інформаційних системах і мережах. В роботі [2] розглядається метод моніторингу стану безпеки заданих сегментів інфраструктури. Показано, що пропоновані удосконалення дозволяють забезпечити підвищення ймовірності оцінювання їх стану по відношенню до захищеності. Враховано, що характеристики сегментів містять велику кількість контрольованих параметрів, які з метою підвищення ефективності роботи систем моніторингу можуть бути об'єднані у відповідності до їх вагових внесків в окремих елементах, що підтримують функціонування різноманітних складових та процесів у системах забезпечення інформаційної безпеки.

У джерелах [3-4] висвітлюються сучасні наукові підходи стосовно обробки та зберігання даних, забезпечення безперебійності роботи ІнфІ та електронного захисту об'єктів критичної інфраструктури.

В роботах [5-6] визначено, що основні принципи та цілі системного моніторингу спрямовані на забезпечення доступності, надійності та ефективності інфраструктури. Розглянуті метрики, які вимірюються при системному моніторингу: використання процесора, пам'яті, дискового простору та інші. При цьому можна отримати певний обсяг інформації про стан ІнфІ та продуктивність.

Аналіз результатів досліджень, які наведені в [1-6] дозволяє дійти висновку, що зусилля фахівців було зосереджено на конкретних складових забезпечення функціонування інформаційної інфраструктури. Проте обґрунтування загального підходу щодо вибору потрібних (раціональних) технічних рішень для розв'язання означеного завдання не наведено.

Мета статті – обґрунтування методичного підходу щодо вибору технологічних рішень для забезпечення функціонування інформаційної інфраструктури воєнного відомства.

Виклад основного матеріалу

Забезпечення функціонування інформаційної інфраструктури може бути досягнуто за допомогою різних технологічних підходів і рішень, які відрізняються за своєю природою і рівнем конкретності.

Технологічні підходи – це загальні стратегічні концепції та методи, які описують, як досягнути певної мети або результату. Вони не визначають конкретних інструментів або технологій, але надають загальний напрямок дій. Технологічні підходи можуть включати такі концепції, як віртуалізація, хмарні обчислення, мікросервісна архітектура, безпека, моніторинг. Вони визначають загальну стратегію для переходу на певні технології і можуть бути адаптовані під конкретні потреби.

Технологічні рішення – це конкретні інструменти, програмне забезпечення, обладнання та послуги, які використовуються для реалізації технологічних підходів. Вони представляють собою конкретні виробничі продукти або рішення, які можуть бути імплементовані в інфраструктурі.

Технологічні рішення можуть включати хмарні платформи, контейнеризацію, бази даних, системи моніторингу, інструменти автоматизації, служби резервного копіювання, системи безпеки та інше. Вони надають конкретні засоби для впровадження технологічних підходів і можуть бути вибрані відповідно до потреб МО України.

Отже, технологічні підходи визначають загальну стратегію та напрямок дій, тоді як технологічні рішення конкретизують інструменти та технології, які будуть використовуватися для досягнення цієї стратегії. Технологічні підходи дозволяють організаціям визначити, куди вони спрямовуються відповідно до свого функціонального призначення, а технологічні рішення – як саме досягти цієї мети.

На сьогодні ІТ-фахівцями для оцінювання ІнфІ використовується комплексна характеристика "зрілість інформаційної інфраструктури". *Зрілість інформаційної інфраструктури* – це ступінь готовності та ефективності інформаційних технологій та інфраструктури в організації або відомстві. Це поняття визначає, наскільки добре розвинуті, інтегровані і оптимізовані інформаційні системи, мережі, обладнання та процеси в контексті конкретного суб'єкта.

Зрілість інформаційної інфраструктури може бути виміряна на різних рівнях, існують різні методики та моделі для оцінки цього показника [7]. Зазвичай оцінка зрілості інформаційної інфраструктури включає в себе такі аспекти.

1. *Технологічні ресурси* – оцінка доступності, якості і сучасності апаратного та програмного забезпечення, серверів, мережевої інфраструктури тощо.

2. *Процеси та практики* – аналіз та оцінка інформаційних процесів, стандартів, методів управління даними, забезпечення безпеки.

3. *Людські ресурси* – оцінка наявності та кваліфікації персоналу, який відповідає за інформаційну інфраструктуру.

4. *Готовність до інтеграції* – спроможність інформаційної інфраструктури взаємодіяти з іншими системами та інтерфейсами.

5. *Якість функціонування та стратегія* – визначення того, наскільки інформаційна інфраструктура підтримує виконання завдань та стратегію розвитку воєнного відомства.

Високий рівень зрілості інформаційної інфраструктури сприяє підвищенню продуктивності, зменшенню ризиків, покращенню якості функціонування воєнного відомства і підвищенню обороноздатності держави в цілому.

Моделі для оцінки зрілості інформаційної інфраструктури включають різноманітні підходи та методики [8-14], які дозволяють визначити рівень зрілості інфраструктури організації (Табл. 2).

Таблиця 2

Моделі для оцінки зрілості інформаційної інфраструктури

№	НАЗВА МОДЕЛІ	ХАРАКТЕРИСТИКА ТА ПРИЗНАЧЕННЯ
1	**Модель зрілості інформаційних технологій (ITIL)**	ITIL – визначає стандарти та методики, а також набір рекомендацій та найкращих практик у сфері управління інформаційними технологіями. ITIL включає в себе ряд процесів та функцій для управління ІТ-сервісами, і може бути використано для оцінки та покращення зрілості інформаційної інфраструктури
2	**Модель зрілості керування даними (Data Management Maturity Model - DMMM)**	Створена для оцінки та покращення зрілості управління даними в організаціях. DMMM визначає різні рівні зрілості в галузі зберігання, обробки, аналізу та захисту даних
3	**Модель зрілості управління конфіденційністю даних (Privacy Maturity Model)**	Призначена для оцінювання рівня зрілості заходів щодо захисту приватності даних в організації. Враховує різні аспекти, включаючи політики, процедури та технології
4	**Модель зрілості інформаційної безпеки (Information Security Maturity Model)**	Визначає, наскільки добре захищені інформаційні ресурси та процеси
5	**Модель зрілості ІТ-господарювання (IT Governance Maturity Model)**	Спрямована на оцінку зрілості систем управління ІТ-процесами та ресурсами, включаючи стратегічне планування, фінансове управління, управління ризиками та інше
6	**COBIT (Control Objectives for Information and Related Technologies)**	COBIT – це модель управління ІТ-процесами та засобами, яка надає структурований підхід до оцінки зрілості ІТ-господарювання в організації. COBIT визначає ключові процеси та практики управління, і дозволяє оцінювати їх виконання на різних рівнях зрілості

№	НАЗВА МОДЕЛІ	ХАРАКТЕРИСТИКА ТА ПРИЗНАЧЕННЯ
7	**ISO/IEC 27001**	Міжнародна стандартна система управління інформаційною безпекою допомагає оцінити та забезпечити безпеку інформаційних активів в організації. ISO/IEC 27001 вимагає визначення ризиків та впровадження заходів для їх мінімізації
8	**CMMI (Capability Maturity Model Integration)**	Модель визначає зрілість процесів розробки програмного забезпечення та процесів управління проєктами. Вона може бути використана для оцінки і покращення процесів IT-розробки та управління проектами
9	**TOGAF (The Open Group Architecture Framework)**	TOGAF – це *фреймворк* для управління корпоративною архітектурою. Надає методологію та структуру для розробки та оцінки архітектури інформаційної інфраструктури в організації

Довідка. *Framework*, каркас, платформа, структура, інфраструктура) – інфраструктура програмних рішень, що полегшує розробку складних систем. Основне завдання фреймворків – прискорення та спрощення розробки. Вони надають розробникам готові структури, які вже не потрібно писати з нуля і можна використовувати для створення програм, сайтів.

Ці моделі призначені для аналізу та покращення зрілості ІнфІ, зокрема шляхом впровадження новітніх (більш ефективних) технологічних рішень, що сприяє підвищенню її продуктивності, безпеки та конкурентоспроможності. Кожна з цих моделей має свої власні переваги і підходи до оцінки зрілості інформаційної інфраструктури. Вибір конкретної моделі залежить від конкретних потреб воєнного відомства на сьогодні й у перспективі.

Вибір альтернативних технологічних рішень для забезпечення функціонування інформаційної інфраструктури пов’язаний із зрілістю інформаційної інфраструктури. Зрілість інформаційної інфраструктури визначається рівнем розвиненості та стабільності інфраструктури, її спроможністю задовольняти вимоги та потреби організації. У Табл. 3 наведені аспекти, що пов’язують вибір альтернативних технологічних рішень та рівень зрілості інформаційної інфраструктури.

Таблиця 3

Зв’язок технологій і зрілості інформаційної інфраструктури

№	АСПЕКТ	ЗВ’ЯЗОК
1	**Зрілість інфраструктури впливає на вибір технологій**	Чим зріліше ІнфІ, тим більше можливостей та ресурсів вона може виділити на вибір та впровадження альтернативних технологій. Нові технології можуть бути коштовними або складними у впровадженні, тому організації із зрілою інфраструктурою можуть вибирати рішення, які найкраще відповідають їхнім потребам
2	**Новітні технології можуть покращити зрілість інфраструктури**	Вибір сучасних технологій може сприяти покращенню зрілості інфраструктури. Нові рішення можуть дозволити впроваджувати кращі практики, підвищувати безпеку, масштабованість та доступність системи
3	**Потреби і вимоги інформаційної інфраструктури визначають вибір рішень**	Рішення повинні відповідати потребам і вимогам інфраструктури. Якщо інфраструктура вимагає високої доступності, то вибирати технології, що дозволяють забезпечити високу доступність, стає пріоритетом. Якщо інфраструктура потребує швидкого масштабування, то технології для гнучкого масштабування обираються в першу чергу
4	**Постійна оцінка та адаптація до нових вимог**	Організації зі зрілою інфраструктурою повинні постійно оцінювати свої потреби та технологічні зміни, а також оновлювати свою інфраструктуру відповідно до нових вимог та можливостей. Змінні вимоги організації можуть вимагати нових технологій. Зрілість інфраструктури може вплинути на здатність до швидкої адаптації та впровадження нових рішень. Висока зрілість може сприяти більшій системності та керованості у процесі розвитку
5	**Збільшення ефективності та зниження витрат**	Вибір альтернативних технологій може сприяти підвищенню ефективності та зниженню витрат на утримання інфраструктури, що позитивно впливає на її зрілість
6	**Аналіз ризиків і вигід**	При виборі альтернативних технологій слід аналізувати ризики та потенційні вигоди для інфраструктури. Зрілість інфраструктури може впливати на рівень прийняття ризику. Організації з більш зрілою інфраструктурою зазвичай мають більш потужну експертизу в оцінці та зменшенні ризиків
7	**Функціональні-процеси та інтеграція**	Зрілість інфраструктури також враховується при виборі альтернативних технологій для забезпечення легкої інтеграції з існуючими функціональними процесами та складовими системами
8	**Службовий персонал**	Зрілість інфраструктури впливає на навички та навченість персоналу. Вибір альтернативних технологій повинен враховувати готовність та можливість персоналу адаптуватися до нових рішень

Зв'язок технологічних підходів та рішень зі зрілістю полягає в тому, що вони можуть бути впроваджені в різний спосіб, залежно від рівня готовності та потреб організації.

Застосування технологічних підходів і рішень для забезпечення функціонування ІнфІ може дозволити МО України підвищити рівень зрілості своєї інфраструктури, забезпечити більшу гнучкість та реагування на зміни в предметному середовищі, підвищити доступність та зменшити витрати на обслуговування.

Вище наведений матеріал дозволяє дійти висновку про доцільність обґрунтування вибору технологічних рішень для забезпечення функціонування ІнфІ МО України шляхом застосування апробованих методик оцінки її зрілості, яка здійснюється:

за відповідним планом для покращення функціональних спроможностей ІнфІ;

при виникненні проблем по конкретному напрямку функціонування ІнфІ.

Для оцінки зрілості інформаційної інфраструктури можна використовувати різні критерії. Нижче наведені загальні критерії, які можна враховувати при оцінці.

1. ***Наявність інформаційних систем.*** Оцінюється кількість та якість інформаційних систем, які використовуються у воєнному відомстві та задовольняють його потреби.

2. ***Стійкість та доступність.*** Оцінюється стійкість інформаційної інфраструктури до відмов та забезпечення надійного доступу до даних і ресурсів.

Для оцінювання стійкості інформаційної інфраструктури до відмов та забезпечення надійного доступу до даних і ресурсів можна використовувати різні показники і метрики, які наведені у Табл. 4.

Таблиця 4

Стійкість та доступність ІнфІ МО України

№	Показник	Метрики
1	**Доступність** (*Availability*)	Час роботи (*Uptime*) – термін, який ІнфІ була доступною без відмов (метрика може бути виражена у відсотках річного часу). Середній час відновлення після відмови (*Mean Time to Recovery*, MTTR) – термін, у який швидко система може бути відновлена до нормального режиму роботи. Середній інтервал часу між відмовами (*Mean Time Between Failures*, MTBF) – ця метрика вказує на стійкість системи до відмов
2	**Пропускна спроможність** (*Throughput*)	Кількість даних, яку система може обробити або передати протягом певного часу – це метрика для оцінки продуктивності системи
3	**Затримка** (*Latency*)	Час, необхідний для передачі даних від вхідного пункту до виходу – актуальна для систем, де низька затримка важлива (наприклад, в бойових системах)
4	**Втрата даних** (*Data Loss Metrics*)	Кількість втрачених даних внаслідок відмов або інцидентів – визначається, наскільки система стійка стосовно уникнення втрат даних
5	**Показники обсягу та виділеного резервного обладнання** (*Failover Metrics*)	Виділений резервний час обслуговування (*Downtime*). Кількість обладнання, яке може використовуватися для автоматичного переключення у разі відмови (*Failover*)
6	**Показники віддаленого адміністрування** (*Remote Administration Metrics*)	Час інциденту виправлення (*Incident Resolution Time*). Час адміністрування з віддаленої точки (*Remote Administration Time*)
7	**Показники безпеки** (*Security Metrics*)	Кількість виявлених інцидентів безпеки. Час виявлення та час відновлення після інциденту
8	**Показники використання ресурсів** (*Resource Utilization Metrics*)	Використання ресурсів, таких як CPU, пам'ять, мережевий трафік тощо – ці показники можуть дозволити визначити, чи не наближається інфраструктура до свого максимального обсягу та чи не обтяжена вона

Це лише деякі з можливих метрик та показників для оцінювання стійкості ІнфІ. Вибір конкретних метрик буде залежати від конкретних потреб МО України. Доцільне регулярно збирати та аналізувати ці дані для постійного вдосконалення стійкості ІнфІ.

Вибір альтернативних технологічних рішень може значно впливати на показники стійкості ІнфІ до відмов та забезпечення надійного доступу до даних і ресурсів. При цьому слід брати до уваги різні аспекти, які можуть вплинути на стійкість системи (Табл. 5).

Таблиця 5

Вплив технологічних рішень на показники стійкості ІнфІ

№	АСПЕКТИ	ТЛУМАЧЕННЯ ВПЛИВУ
1	**Архітектура і дизайн системи**	Вибір архітектурних рішень, таких як розподілені системи або системи з резервним обладнанням, може впливати на здатність системи опирати відмови. Наприклад, системи з резервним обладнанням можуть автоматично переключатися на резервні ресурси у випадку відмови.
2	**Вибір технологій та**	Використання технологій і платформ з високою стійкістю і надійністю може

№	АСПЕКТИ	ТЛУМАЧЕННЯ ВПЛИВУ
	платформ	позитивно впливати на стійкість системи. Наприклад, використання дискових масивів з резервними дисками або віртуалізація для швидкої міграції ресурсів
3	**Резервне копіювання та відновлення даних**	Вибір систем резервного копіювання та відновлення даних може вплинути на швидкість відновлення системи після відмови. Ефективні рішення забезпечують швидке відновлення даних і системи
4	**Засоби моніторингу та управління**	Використання потужних інструментів моніторингу та управління допомагає вчасно виявляти відмови та реагувати на них. Вибір відповідних інструментів може покращити стійкість інфраструктури
5	**Безпека**	Вибір технологій і рішень для забезпечення безпеки даних та інфраструктури важливий для стійкості системи. Якщо система не належним чином захищена, вона може бути уразливою перед атаками та втратою даних
6	**Інфраструктура та мережева топологія**	Вибір інфраструктури та мережевої топології може впливати на стійкість системи до збоїв мережі та втрати зв'язку. Наприклад, розгалужена мережева топологія може зменшити ризики відмови мережі
7	**Функціональні процеси та плани аварійного відновлення**	Вибір технологічних рішень повинен бути сумісним з функціональними процесами та планами аварійного відновлення організації. Наявність готових планів може допомогти в разі відмови
8	**Економічні обмеження**	Вибір альтернативних технологічних рішень також залежить від економічних обмежень. Деякі рішення можуть бути дорожчими, і важливо збалансувати вартість і стійкість.

Вибір альтернативних технологій повинен відповідати конкретним потребам МО України. Перед прийняттям рішення важливо провести аналіз та оцінку ризиків, які можуть виникнути внаслідок змін в інфраструктурі.

3. ***Інтеграція***. Оцінюється рівень інтеграції інформаційних систем та даних в МО України, що дозволяє оптимізувати функціональні процеси та підвищувати ефективність. Оцінювання інтеграції інформаційних систем та даних в ІнфІ, вибір альтернативних технологічних рішень для поліпшення цього критерію зрілості ІнфІ можна проводити з вираховуванням показників та метрик, які наведені у Табл. 6.

Таблиця 6

Вплив технологічних рішень на показники інтеграції ІнфІ

№	ПОКАЗНИКИ	МЕТРИКИ
1	**Час інтеграції**	Середня кількість часу, який потрібно для інтеграції нових систем та даних у хмарній інфраструктурі
2	**Вартість інтеграції**	Витрати на інтеграцію, включаючи витрати на програмне забезпечення, послуги та ресурси
3	**Рівень автоматизації**	Визначення того, наскільки процеси інтеграції автоматизовані та уніфіковані
4	**Відмови**	Кількість відмов або помилок, пов’язаних з інтеграцією систем та даних
5	**Рівень доступності та надійності**	Час доступності інтегрованих систем та даних та їх надійність
6	**Продуктивність**	Вимірювання продуктивності систем та даних, що інтегруються
7	**Забезпечення відповідності**	Визначення того, наскільки інтегровані системи дотримуються вимог до безпеки, відповідності та регуляторних стандартів

Для поліпшення інтеграції можуть бути застосовані наступні технологічні рішення:

Інтегровані платформи (*Integration Platforms*). Використання платформ для інтеграції даних та додатків, які надають інструменти для автоматизації процесів інтеграції.

API-орієнтована архітектура (API-First). Розробка додатків та систем з обов’язковим використанням API, що дозволяє легко інтегрувати їх з іншими системами.

Централізована система керування даними (Master Data Management, MDM). Впровадження MDM для забезпечення єдиної версії даних та їх гармонізації.

Платформи для інтеграції великих обсягів даних (Big Data Integration Platforms). Використання інструментів для інтеграції та аналізу великих обсягів даних у хмарній інфраструктурі.

Розумний аналіз даних та штучний інтелект (AI). Використання розумних аналітичних інструментів та AI для автоматизації процесів інтеграції та виявлення *патернів* (повторюваних елементів) у даних.

Інструменти для моніторингу та управління інтеграцією (Integration Monitoring and Management Tools). Використання інструментів для моніторингу та управління процесами інтеграції для забезпечення їх ефективності та доступності.

Інтеграція через хмарні послуги (Cloud Integration Services). Використання хмарних послуг для інтеграції систем та даних з інших джерел.

Концепція "Event-Driven" інтеграції: Розробка систем, які реагують на події та взаємодіють з іншими системами на основі подій.

Використання мікросервісної архітектури (Microservices). Розробка додатків у вигляді мікросервісів, які можна легко інтегрувати в інші системи.

Забезпечення безпеки та відповідності: Використання рішень для забезпечення безпеки та відповідності при інтеграції даних та систем.

Вибір конкретних альтернативних технологічних рішень повинен базуватися на потребах та цілях МО України, а також на аналізі показників та метрик для оцінювання інтеграції.

4. *Захист інформації*. Оцінюється рівень захисту даних та інформаційних ресурсів від несанкціонованого доступу та загроз безпеці.

5. *Відповідність стандартам та регуляторним вимогам*. Оцінюється відповідність інформаційної інфраструктури вимогам законодавства, стандартам безпеки, нормативам тощо.

6. *Ефективність та продуктивність*. Оцінюється продуктивність систем та технологій, які використовуються в організації, та їх вплив на робочий процес.

Для оцінювання ефективності та продуктивності інформаційних систем в ІнфІ, вибору технологічних рішень для покращення цих критеріїв зрілості ІнфІ можна використовувати показники та метрики, які наведені у Табл. 7.

Таблиця 7

Вплив технологічних рішень на показники ефективності та продуктивності ІнфІ

№	ПОКАЗНИКИ	МЕТРИКИ
1	**Час відгуку системи** (*Response Time*)	Середній час відгуку системи на запити користувачів, що вимірює продуктивність та відчуття швидкості
2	**Продуктивність серверів та ресурсів**	Використання CPU, пам’яті та інших ресурсів серверів, що вказує на їхню продуктивність
3	**Пропускна здатність** (*Throughput*)	Кількість операцій, які система може обробити протягом певного часу
4	**Кількість оброблених запитів** (*Request Volume*)	Кількість запитів, які система може обробити в одиницю часу
5	**Час завантаження сторінок** (*Page Load Time*)	Середній час завантаження веб-сторінок для веб-додатків
6	**Кількість відмов** (*Failure Rate*)	Відсоток запитів, що призвели до відмов або помилок
7	**Використання мережевих ресурсів** (*Network Utilization*)	Використання мережевої пропускної здатності системою та її вплив на продуктивність
8	**Використання сховища даних** (*Storage Utilization*)	Використання сховища даних і його вплив на продуктивність
9	**Метрики вартості** (*Cost Metrics*)	Витрати на інфраструктуру та послуги обчислення відносно продуктивності

Для підвищення ефективності та продуктивності ІнфІ можуть бути використані такі технологічні рішення:

- *скейлінг ресурсів* (Resource Scaling) - використання можливості хмарних платформ для автоматичного масштабування ресурсів в залежності від навантаження, щоб покращити продуктивність;

- *кешування* (Caching) - використання технології кешування для збереження часто використовуваних даних та зменшення часу відгуку;

- *використання CDN* (Content Delivery Network) для розподілення контенту та зменшення часу завантаження веб-сторінок;

- *оптимізація запитів* (Query Optimization) - покращення ефективності запитів до баз даних та інших ресурсів;

- *контейнеризація та оркестрація* - використання контейнерів та платформ оркестрації для поліпшення масштабованості та продуктивності;

- *розподілена архітектура* (Distributed Architecture) - використання розподілених систем та мікросервісів для розділення

функціональності та поліпшення продуктивності;

- *штучний інтелект* (ШІ) *та аналітика даних* для оптимізації роботи систем та покращення продуктивності;

- *оптимізація баз даних*;

- *моніторинг та аналіз продуктивності* (Performance Monitoring and Analysis).

Довідка. Контейнерне оркестрування належить до інструментів та платформ, які використовують для автоматизації, управління та планування додатків, визначених окремими контейнерами. Інструменти оркестрування контейнерів дозволяють запускати та керувати всіма контейнерами в інформаційному середовищі та розв'язувати проблеми, яких могло не бути на стадії розробки на одній машині

7. *Можливість масштабування*. Оцінюється можливість розширення ІнфІ для відповіді на зростання обсягів даних та користувачів.

показники та метрики, які можна використати для оцінювання можливості масштабування ІнфІ наведені у Табл.8.

Таблиця 8

Показники і метрики для оцінювання можливості масштабування

№	ПОКАЗНИКИ	ТЛУМАЧЕННЯ
1	**Горизонтальне та вертикальне масштабування** (*Horizontal and Vertical Scaling*)	Визначення, наскільки легко можна додавати або збільшувати ресурси системи
2	**Час масштабування (***Scaling Time***)**	Середній час, який потрібен для масштабування інфраструктури
3	**Масштабованість додатків** (*Application Scalability*)	Здатність додатків адаптуватися до змін обсягів роботи та ресурсів
4	**Автоматичне масштабування** (*Auto-Scaling*)	Визначення, наскільки система може автоматично реагувати на зміни навантаження
5	**Кількість серверів** (*Number of Servers*)	Середній час завантаження веб-сторінок для веб-додатків
6	**Використання ресурсів** (*Resource Utilization*)	Відсоток запитів, що призвели до відмов або помилок
7	**Підтримка географічно розподіленої інфраструктури** (*Geo-Distribution Support*)	Використання мережевої пропускної здатності системою та її вплив на продуктивність
8	**Масштабування даних** (*Data Scaling*)	Здатність масштабувати обсяг та обробку даних
9	**Збільшення потужності мережі** (*Network Capacity Expansion*)	Можливість розширення мережевої пропускної здатності для підтримки масштабування

З метою поліпшення масштабованості, окрім технологічних рішень щодо підвищення ефективності та продуктивності ІнфІ (наведені після Табл. 8) можна застосувати технології:

мультирегіональної інфраструктури (Multi-Region Implementation) - розгортання інфраструктури в кількох регіонах для забезпечення вищої доступності та масштабованості;

автоматичного масштабування (Auto-Scaling Systems) – автоматичне реагування на зміни навантаження;

кешування і CDN (Caching and Content Delivery Networks) - для збільшення продуктивності та масштабованості вмісту.

8. ***Планування та управління***. Оцінюється наявність стратегічного планування і управління інформаційною інфраструктурою для досягнення цілей воєнного відомства.

9. *Підтримка та обслуговування*. Оцінюється доступність служби підтримки, процеси обслуговування та реагування на інциденти.

10. *Вартість та бюджет*. Оцінюється вартість утримання інформаційної інфраструктури та відповідність бюджетним обмеженням.

Для оцінювання вартості утримання ІнфІ використовуються показники та метрики, які наведені у Табл. 9.

Таблиця 9

Показники і метрики для оцінювання вартості утримання

№	ПОКАЗНИКИ	ТЛУМАЧЕННЯ
1	**Витрати на хмарні послуги** (*Cloud Service Costs*)	Витрати на обчислення, сховище даних, мережеві послуги та інше
2	**Витрати на обслуговування та підтримку (***Maintenance and Support Costs***)**	Включають витрати на підтримку, оновлення та адміністрування хмарної інфраструктури
3	**Витрати на ліцензії та програмне забезпечення**	Витрати на програмне забезпечення, ліцензії та вартість використання сторонніх продуктів

№	ПОКАЗНИКИ	ТЛУМАЧЕННЯ
	(*Software Licensing Costs*)	
4	**Витрати на безпеку та відповідність** (*Security and Compliance Costs*)	Включають витрати на заходи забезпечення безпеки та дотримання регуляторних вимог
5	**Затрати на персонал** (*Personnel Costs*)	Оцінювання витрат на кваліфікований персонал для управління та підтримки інфраструктури. Навчання персоналу для роботи з новітніми технологіями
6	**Амортизація обладнання** (*Equipment Depreciation*)	Включає витрати на амортизацію обладнання та ресурсів
7	**Резервні копії і відновлення** (*Backup and Recovery Costs*)	Вартість резервних копій даних та процедур відновлення
8	**Витрати на моніторинг та управління** (*Monitoring and Management Costs*)	Визначення витрат на інструменти та послуги для моніторингу та управління ІнфІ

Для зменшення витрат можна запропонувати наступні технологічні рішення:

- *оптимізація ресурсів* (Resource Optimization) - використання інструментів для автоматичного скасування не використаних ресурсів;
- *автоматизація процес*ів (Process Automation) - автоматизовані процеси для зменшення ручної роботи та підвищення продуктивності;
- *моніторинг та аналіз витрат* (Cost Control and Analysis) - інструменти моніторингу та аналізу витрат для ідентифікації зайвих витрат та оптимізації;
- *міграція на більш ефективні платформи* (Migration to More Cost-Effective Platforms);
- *оцінка ресурсів для масштабування* (Scaling Resource Assessment) - періодичне оцінювання необхідності та ресурсів для масштабування та вимкнення ресурсів за потребою;
- *користування хмарними резервними копіями* (Cloud Backups) замість коштовної локальної інфраструктури.
- *раціоналізація програмного забезпечення* (Software Rationalization).

Зазначені критерії можуть бути адаптовані для конкретної ситуації, а оцінка зрілості інформаційної інфраструктури може використовувати комбінацію різних методик, таких як аудит, анкети, оцінки експертів тощо. Важливо також регулярно проводити оцінку зрілості для забезпечення постійного вдосконалення інформаційної інфраструктури організації.

Для обґрунтування порядку вибору раціональних технологічних рішень для забезпечення функціонування інформаційної інфраструктури воєнного відомства можна застосувати комплексний і системний підходи, які є тісно пов’язаними, але мають свої відмінності. У Табл. 10 наведені їх особливості та можливість інтеграції.

Таблиця 10

Характеристики комплексного та системного підходів

№	Характеристики	Комплексний підхід (КП)	Системний підхід (СП)
1	**Призначення**	КП спрямований на врахування всіх аспектів інформаційної інфраструктури, включаючи технічні, організаційні, людські та стратегічні компоненти	СП спрямований на розгляд інформаційної інфраструктури як інтегрованої системи, де всі елементи взаємодіють та взаємозалежні
2	**Мета**	Підвищення ефективності та оптимізація роботи системи в цілому, реагуючи на внутрішні та зовнішні виклики	Розуміння взаємозв’язків та взаємодії між частинами системи для досягнення гармонії та оптимального функціонування
	Відмінності		
3	**Орієнтація**	КП орієнтований на вивчення всіх аспектів, але акцентується на повному підході до проблеми або завдання	СП фокусується на розумінні внутрішніх взаємозв’язків та взаємодії між компонентами системи
4	**Практична реалізація**	КП може включати різні методології та підходи для оптимізації різних аспектів системи	СП реалізується через визначення структури та взаємозв’язків між компонентами системи
5	**Можливість інтеграції**	КП і СП орієнтовані на комплексне розгляд системи, їх можна успішно інтегрувати. Використання СП дозволить враховувати взаємозв’язки між компонентами системи в рамках КП	

В цілому, обидва підходи важливі для вибору технологічних рішень як стосовно забезпечення функціонування ІнфІ воєнного відомства, так і успішного її вдосконалення, і їх взаємодія може забезпечити більш глибоке та комплексне розуміння системи.

Застосування інтегрованого підходу при виборі технологічних рішень для забезпечення стійкого функціонування ІнфІ Міністерства

оборони України та їх впровадження включає кілька етапів, які дозволяють забезпечити раціональний вибір технологічних рішень. На рис. 1 наведено загальний опис можливих кроків на кожному етапі.

Рис. 1. Порядок вибору технологічних рішень для забезпечення функціонування ІнфІ воєнного відомства

Висновки.

1. Обґрунтування порядку вибору раціональних технологічних рішень для забезпечення функціонування ІнфІ воєнного відомства базується на застосуванні інтегрованого (комплексного і системного підходів) та використанні апробованих методик оцінювання складових зрілості ІнфІ.

2. Впровадження інтегрованого підходу потребує детального аналізу методик оцінювання зрілості ІнфІ та їх певної адаптації стосовно обґрунтування вибору тих чи інших технологічних рішень.

3. Впровадження технологічних рішень має спиратись на конкретні методики оцінювання зрілості ІнфІ відповідно до критеріїв: стійкість; інтегрованість; ефективність та продуктивність; масштабованість; вартість.

Впровадження запропонованого підходу дозволить створити комплексне рішення, яке враховує критерії оцінювання ІнфІ та забезпечить вибір раціональних технологічних рішень для досягнення стратегічних цілей Міністерства оборони України. 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.

Подальші дослідження доцільно зосередити на аналізі етапів вибору і впровадження можливих технологічні рішень

для забезпечення функціонуванні ІнфІ та обґрунтуванні заходів щодо уникнення ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Інформаційна безпека держави : навч. посіб. для студ. спец. 6.170103 “Управління інформаційною безпекою”, 125 “Кібербезпека”/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК “Орхідея”, 2018. – 166 с.
2. Н.Ф. Казакова1, Т.І. Соклакова. Удосконалення методу моніторингу рівня інформаційної безпеки у спеціальних сегментах національної інформаційної інфраструктури // Бионика интеллекта. 2015. № 1 (84). С. 56–64.
3. Удосконалення методів обробки та зберігання даних за допомогою інструментів “Big Data” та Map Reduce / І.М. Онищенко // Економіко-математичне моделювання соціально-економічних систем: Зб. наук. пр. - К.: МННЦІТС НАН та МОН України, 2017. Вип. 22. С. 159-178.
4. Мартинюк В,В., Паламарчук Н.А., Паламарчук С.А., Сівоха О.М. Задачі вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури / В.В. Мартинюк та ін. // Збірник наукових праць ВІТІ № 2 – 2020. С. 54-63. URL: http://www.viti.edu.ua/files/zbk/2020/6_2_2020.pdf (дата звернення: 01.08.2023).
5. Визначення системного моніторингу та його роль у сучасних інформаційних технологіях. URL: https://learn.ztu.edu.ua/pluginfile.php/319789/mod_resource/content/7/SNM%20 Theme%20%2301-08.pdf (дата звернення 30.03.2024).
6. Ефективний моніторинг IT-інфраструктури – що і як моніторити? URL: https://onbiz.biz/monitoring-of-it-infrastructure (дата звернення 30.03.2024).
7. Модель технологической зрелости CMMI. URL: https://tenstep.com.ua/open/A1.1CMMI.htm (дата звернення 22.01.2024).
8. Методології у сфері IT: ITIL, COBIT, PRINCE2 та інші. URL: https://kr-labs.com.ua/blog/metodologiyi-u-sferi-it-itil-cobit-ta-inshi (дата звернення 15.04.2024).
9. Моделі зрілості (Maturity models). URL: https://www.maxzosim.com/modieli-zrilosti (дата звернення 15.04.2024).
10. Інтеграція моделі зрілості можливостей. Вичерпний посібник. URL: https://visuresolutions.com/uk/%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA-cmmi/cmmi (дата звернення 15.04.2024).
11. А.И. Пушкарь В.В. Гаркин Использование модели зрелости IT-инфраструктуры в оценке качества информационных систем предприятия, Вісник СумДУ. Серія “Економіка”, №3'2013 с.130-145.
12. Лазебник Л.Л., Войтенко В.ОР. Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства // Науковий вісник Міжнародного гуманітарного університету, 2020. DOI: https://doi.org/10.32841/2413-2675/2020-42-3 (дата звернення: 15.04.2024).
13. І.А. Попова, К.І. Серебряк. Модернізація інформаційної інфраструктури задля активізації міжрегіонального співробітництва // Економічна наука. Східноукраїнський національний університет імені В. Даля, м. Сєвєродонецьк, С. 48-53.
14. Кірпічніков Ю.А. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами / Ю.А. Кірпічніков, О.В. Андрощук, М.В. Петрушен [та ін.] // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2019, № 1(65). С. 86-91.

Стаття надійшла до редакційної колегії 16.04.2024

The procedure for selecting and implementing technological solutions to ensure the information infrastructure functioning of the Ministry of Defence of Ukraine: a methodological approach

Annotation

Ensuring the functioning of the Ministry of Defence’s information infrastructure is a strategically important issue, as it affects the country's ability to effectively respond to threats and ensure national security. The task of substantiating the approach to selecting the necessary (rational) technical solutions and applying certain organizational measures to ensure the functioning of the Ministry of Defence Information Infrastructure of Ukraine is considered important.

Today, IT specialists use a comprehensive characteristic of “information infrastructure maturity” to assess the information infrastructure. Information infrastructure maturity is the degree of readiness and efficiency of information technology and infrastructure in an organization or agency. This concept determines how well developed, integrated and optimized information systems, networks, equipment and processes are in the context of a particular entity. The choice of alternative technological solutions to ensure the functioning of the Information Infrastructure is related to the maturity of the information infrastructure.

The article analyzes the indicators and metrics of the criteria for evaluating the information infrastructure: sustainability and availability; level of integration of information systems; efficiency and productivity; scalability; and cost of maintenance. Alternative technological solutions that can influence the indicators of the maturity of the information infrastructure are presented.

The justification of the procedure for selecting rational technological solutions to ensure the functioning of the military department's information system is based on the use of an integrated (comprehensive and systematic) approach. The implementation of the proposed approach will allow creating a comprehensive solution, taking into account the criteria for evaluating the information infrastructure and ensuring the selection of rational technological solutions to achieve the strategic goals of the Ministry of Defence of Ukraine.

Keywords: information infrastructure; technological approaches and solutions; maturity of information infrastructure; criteria for assessing the maturity of information infrastructure.