АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 005.8:004.056

DOI https://doi.org/10.5281/zenodo.16885042

Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту

Саврацький Олександр Олександрович,
аспірант кафедри кібербезпеки
Національний університет "Одеська юридична академія", Україна,
https://orcid.org/0009-0005-3396-4855

Прийнято: 22.07.2025 | Опубліковано: 31.07.2025

Анотація: В статті проведено дослідження ефективності та перспектив впровадження командного підходу до управління проєктами у сфері кіберзахисту в Україні в умовах гібридної війни, цифровізації та зростання кіберзагроз. Враховуючи специфіку проєктів із кібербезпеки, яка спирається на їхню складність, критичність термінів та міждисциплінарний характер, командна модель управління розглядається як один із ключових інструментів підвищення їх ефективності.

Дослідження є междисциплінарним і передбачає одночасний аналіз чинної нормативно-правової бази, практичного досвіду реалізації проєктів кіберзахисту, аналіз статистичних даних щодо кіберінцидентів, а також огляд міжнародних стандартів, зокрема NIST Cybersecurity Framework 2.0. Використано елементи порівняльного, аналітичного та системного підходів, що дозволило інтегрувати дані з різних джерел для формулювання практичних рекомендацій.

Встановлено, що саме командний підхід забезпечує високу адаптивність до змін, прискорює реагування на загрози, сприяє інтеграції різнопрофільних фахівців та зміцнює співпрацю між державними структурами, приватним сектором і громадськими ініціативами. Водночас визначено низку викликів для вказаного підходу: нестача уніфікованих стандартів комунікації, брак кадрів, обмежене фінансування, відсутність системного моніторингу ефективності командної роботи.

Як відповідь на виклики запропоновано наступні оптимізаційні заходи: розвиток профільних освітніх програм, впровадження сертифікацій, стандартизація метрик оцінки командної ефективності, автоматизація процесів за допомогою сучасних цифрових інструментів, а також посилення міжвідомчої та міжнародної координації. Обґрунтовано потребу в ухваленні закону про захист критичної інфраструктури як законодавчої основи для командної взаємодії у сфері кібербезпеки.

В результаті доведено доцільність системного впровадження командного підходу в проєктах кіберзахисту. Адже в перспективі він здатен підтримувати більш стійку, оперативну й інтегровану модель протидії кіберзагрозам, адаптовану до умов воєнного часу та стрімкого технологічного розвитку.

Ключові слова: менеджмент, інформаційна безпека, командна взаємодія, цифрові ризики, публічно-приватне партнерство, нормативно-правове регулювання, кадровий потенціал, штучний інтелект.

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Prospects for applying a team approach in the process of managing projects in the field of cyber security

Olexander Savratsky,
Postgraduate student of the Department of Cybersecurity
National University "Odesa Law Academy", Ukraine,
https://orcid.org/0009-0005-3396-4855

Abstract: The purpose of the study is to examine the effectiveness and prospects of implementing a team-based approach to project management in the field of cyber security in Ukraine in the context of hybrid warfare, digitalization, and growing cyber threats. Given the specific nature of cybersecurity projects — high complexity, critical deadlines, and interdisciplinary nature — the team management model is considered one of the key tools for improving their effectiveness.

The research methodology involved a comprehensive analysis of the current regulatory framework, practical experience in implementing cybersecurity projects, analysis of statistical data on cyber incidents, and a review of international standards such as NIST Cybersecurity Framework 2.0. Elements of comparative, analytical, and systematic approaches were used, which made it possible to integrate data from various sources to formulate practical recommendations.

As a result, it was found that a team approach ensures high adaptability to change, accelerates response to threats, promotes the integration of multidisciplinary specialists, and strengthens cooperation between government agencies, the private sector, and public initiatives. At the same time, a number of challenges were identified: lack of unified communication standards, shortage of personnel, limited funding, and lack of systematic monitoring of teamwork effectiveness.

The study proposes optimization measures, including the development of educational programs, the introduction of certifications, the standardization of metrics for assessing team effectiveness, the automation of processes using modern digital tools (e.g., Jira, STIX/TAXII), and the strengthening of interagency and international coordination. The need to adopt a law on critical infrastructure protection as a legislative basis for teamwork in the field of cybersecurity is justified.

The conclusions of the study indicate the feasibility of systematically implementing a team approach in Ukrainian cyber defense projects. In the long term, it can provide a more stable, responsive, and integrated model for countering cyber threats, adapted to the conditions of wartime and rapid technological development.

Keywords: interagency coordination, information security, teamwork, digital risks, public-private partnerships, regulatory framework, human resources, artificial intelligence.

Постановка проблеми. В умовах стрімкого зростання кіберзагроз, внаслідок гібридної війни та активної цифровізації всіх сфер суспільного життя, Україна стикається з необхідністю ефективного управління проєктами кіберзахисту. Головною метою при цьому виступає забезпечення безпеки критичної інфраструктури та державних інформаційних систем. Командний підхід, який передбачає інтеграцію зусиль державних органів, приватного сектору та громадських ініціатив, є перспективним інструментом для вирішення складних завдань у цій сфері. Проте сучасна практика реалізації таких проєктів в Україні стикається із низкою проблем, а саме: недостатня координація міжвідомчої взаємодії, брак кваліфікованих кадрів, обмеженість фінансування та відсутність уніфікованих стандартів комунікації й оцінки ефективності командної роботи. Наявні проблеми ускладнюють оперативне реагування на кіберінциденти та знижують результативність проєктів. Таким

чином, виникає потреба в дослідженні особливостей і перспектив застосування командного підходу для управління проєктами кіберзахисту в Україні, а також у розробці рекомендацій для його оптимізації з урахуванням реального контексту та міжнародного досвіду.

Аналіз останніх досліджень і публікацій. Ключові аспекти управління проєктами висвітлювалися в наукових працях низки вітчизняних та іноземних дослідників. Ратушняк О. Г. [1] наголошує на чіткому розподілі ролей у команді для ефективної реалізації складних проєктів кіберзахисту. Данченко О. Б., Бедрій Д. І., Семко І. Б. [2] пропонують модель формування команд, акцентуючи на синергії через інтеграцію управлінських функцій. Косенко Н. В., Доценко Н. В., Чумаченко І. В. [3] підкреслюють важливість інформаційних технологій і компетентнісного підходу для оптимізації командної роботи в умовах кіберзагроз. Немченко Т., В'юник О. [5] досліджують гнучкі методології в IT-менеджменті, зазначаючи, що Agile і інструменти, як Jira, підвищують адаптивність команд у кіберзахисті. Галушка З. І. [6] підкреслює роль Agile у забезпеченні гнучкості та синергії в міждисциплінарних командах. Судук О. Ю., Щербакова А. С. [7] акцентують на ітеративному підході Agile для оперативного реагування на кіберзагрози. Гуцуляк Н., Синиченко А. [8] пропонують методи формування «суперкоманд» для роботи в умовах невизначеності. Соломон Д. [9] аналізує модель Такмена, яка сприяє стабільності команд у кіберзахисті. Пітерсен Р., Сантос Д., Сміт М. К., Ветцель К. А., Вітте Г. [10] у NIST 800-181 наголошують на сертифікаціях і чіткому розподілі ролей. Арсенович Л. [11] пропонує тренінги для підвищення цифрової компетентності фахівців. Горбаченко С., Чепурна О., Слатвінська В. [12] підкреслюють що основними характеристиками управління проєктами є значне поширення найбільш гнучких практик Agile та Scrum. Цюприк І. В. [16] акцентує на публічно-приватному партнерстві для

інноваційних рішень. Паско С. Е. [17] у NIST Framework 2.0 пропонує структурований ризик-менеджмент. Даврі Е. С. та ін. [18] підкреслюють роль сертифікацій у підготовці команд. Опанасенко М. І., Поночовний П. М. [19] досліджують хмарні рішення Cisco Cloudlock для автоматизації захисту. Кочман К. П., Форос Г. В. [20] пропонують STIX/TAXII для пришвидшення інформаційного обміну.

Вказані науковці в цілому підтверджують ефективність командного підходу в управлінні проєктами, хоча й вказують на наявність таких проблем, як брак кадрів, координації та фінансування, які потребують стандартизації та автоматизації. З іншого боку проєкти в сфері кіберзахисту мають власну специфіку на яку все ще не звертають достатньо уваги, а, отже, в цьому напряму все ще є перспективи для наукового пошуку.

Виділення невирішених раніше частин загальної проблеми. Проблема управління проєктами кіберзахисту в Україні за допомогою командного підходу залишається частково нерозв'язаною через низку специфічних аспектів, які раніше не отримували достатньої уваги в наукових дослідженнях та практичній реалізації. По-перше, недостатньо досліджено механізми ефективної міжвідомчої координації в умовах обмежених ресурсів і високої динаміки кіберзагроз, що ускладнює створення цілісних систем захисту критичної інфраструктури. По-друге, бракує комплексного аналізу ролі громадських ініціатив у командній роботі, зокрема їхнього внеску в підвищення кіберобізнаності та підтримку освітніх програм. По-третє, відсутність стандартизованих метрик для оцінки ефективності командної роботи в проєктах кіберзахисту обмежує можливості моніторингу та вдосконалення процесів. Нарешті, питання адаптації міжнародного досвіду, такого як стандарти NIST Cybersecurity Framework, до українських реалій залишається недостатньо опрацьованим, що гальмує інтеграцію передових

практик у національну систему кібербезпеки. Зазначені невирішені аспекти загальної проблеми потребують поглибленого вивчення для розробки дієвих рекомендацій щодо оптимізації командного підходу в управлінні проєктами кіберзахисту.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз перспектив і особливостей застосування командного підходу в управлінні проєктами кіберзахисту в Україні на основі реальних даних, а також розробка практичних рекомендацій для його оптимізації. Для досягнення цієї мети поставлено такі завдання:

- Дослідити теоретичні основи командного підходу, визначивши його ключові характеристики та роль у проєктах кіберзахисту з урахуванням їхньої специфіки, такої як висока складність і критичність термінів.
- Оцінити сучасний стан кіберзахисту в Україні, зокрема проаналізувати основні кіберзагрози, нормативно-правову базу (зокрема Указ Президента №447/2021) та проблеми реалізації проєктів, такі як недостатнє фінансування та дефіцит кадрів.
- Визначити особливості командної роботи в українських проєктах кіберзахисту, включаючи міжвідомчу співпрацю, залучення приватного сектору та громадянського суспільства, а також проаналізувати практичні кейси, такі як впровадження систем моніторингу кіберзагроз і створення реєстру об’єктів критичної інформаційної інфраструктури.
- Окреслити перспективи розвитку командного підходу через інтеграцію міжнародного досвіду (зокрема NIST Cybersecurity Framework 2.0), розвиток кадрового потенціалу, державно-приватне партнерство та технологічні інновації.
- Запропонувати конкретні заходи для оптимізації командного підходу, включаючи спрощення комунікаційних процесів, розробку програм

підготовки фахівців, впровадження стандартизованих метрик оцінки ефективності та підтримку законодавчих ініціатив, таких як закон про захист критичної інфраструктури.

- Сформулювати висновки щодо переваг і викликів командного підходу та визначити напрями подальших досліджень, зокрема в контексті воєнного стану та використання нових технологій.

Виклад основного матеріалу дослідження. Команда — це не просто група людей, а об'єднання фахівців, які працюють злагоджено задля досягнення спільної мети, демонструючи високу взаємодію при мінімальному управлінському втручанні

Ратушняк О. Г. вважає команду проєкту основною складовою його реалізації, підкреслюючи, що це група співробітників, які працюють під керівництвом менеджера проєкту та припиняють своє існування після завершення проєкту [1]. Данченко О. Б., Бедрій Д. І. і Семко І. Б. підкреслюють відповідальність команди за виконання широкого спектра управлінських функцій — від ініціації й планування до контролю та завершення проєкту [2]. Подібне розуміння пропонують Косенко Н. В., Доценко Н. В. і Чумаченко І. В., які розуміють групу учасників проєкту, відповідальних за виконання управлінських операцій, зокрема ініціювання, планування, реалізацію, моніторинг, контроль і завершення [3].

Узагальнюючи підходи дослідників, можна визначити команду проєкту як групу фахівців, об'єднаних задля досягнення конкретних цілей, які взаємодіють між собою, застосовуючи власні знання, навички та ресурси для успішного виконання поставлених завдань у межах встановлених термінів, бюджету та стандартів якості. Управління проєктами є ефективним інструментом для керівництва, що забезпечує чіткість у процесі реалізації проєкту. Воно сприяє прозорості всіх процесів, дозволяє точно оцінювати

ресурси та терміни, а також контролювати навантаження учасників команди [4].

Командний підхід у управлінні проєктами є ключовим елементом успішної реалізації складних завдань, особливо у таких динамічних сферах, як кібербезпека. Він ґрунтується на спільній роботі групи фахівців, які об'єднані не лише спільною метою, але й чітким розподілом ролей та відповідальностей. Така організація роботи дозволяє максимально ефективно використовувати навички та знання кожного учасника, забезпечуючи синергію та взаємодоповнюваність [5].

Однією з основних характеристик командної роботи є співпраця, яка передбачає постійний обмін інформацією, ідеями та ресурсами. Це дозволяє швидше вирішувати складні завдання та адаптуватися до змін. Важливим аспектом є також спільне прийняття рішень, оскільки колективний підхід дозволяє враховувати різні точки зору та знаходити оптимальні рішення. Чітка комунікація, у свою чергу, запобігає недорозумінням та забезпечує узгодженість дій усіх членів команди [6,7].

Формування ефективної команди – це процес, який проходить кілька етапів, описаних у моделі Такмена. Спочатку команда проходить період знайомства та адаптації, потім – етап обговорення та конфліктів, де визначаються лідери та розподіляються ролі. Наступний крок – встановлення норм і правил спільної роботи, що дозволяє команді стабілізуватися. Лише після цього вона переходить до фази продуктивної діяльності, де кожен член команди максимально ефективно виконує свої обов'язки. Завершальний етап – це аналіз результатів та розпуск команди після досягнення мети [8,9].

Ефективна команда характеризується високим рівнем довіри, яка дозволяє членам групи вільно висловлювати думки та пропозиції без страху критики. Чіткий розподіл обов'язків забезпечує відсутність дублювання

функцій та ефективне використання ресурсів. Адаптивність до змін є особливо важливою у кібербезпеці, де нові загрози можуть виникати в будь-який момент. Високий рівень мотивації, у свою чергу, підтримує зацікавленість кожного учасника у досягненні спільного результату [10].

Можна стверджувати, що у сфері кібербезпеки командний підхід набуває ще більшого значення через високий рівень складності та динамічності проєктів. Інтеграція різних технологій, аналіз великих масивів даних та прогнозування потенційних загроз вимагають узгодженої роботи фахівців різних профілів. Крім того, критичність термінів обумовлена швидким розвитком кібератак, тому команда повинна вміти оперативно реагувати та впроваджувати рішення [11].

Міждисциплінарна взаємодія є невід'ємною частиною проєктів з кібербезпеки, оскільки вони часто об'єднують не лише IT-фахівців, але й юристів, аналітиків безпеки, представників державних структур та інших експертів. Наприклад, розробка системи захисту критичної інфраструктури вимагає спільної роботи програмістів, які створюють технічні рішення, аналітиків, які оцінюють ризики, та регуляторних органів, які забезпечують відповідність законодавчим вимогам.

З огляду на вищевказане командний підхід забезпечує низку переваг в управлінні проєктами кіберзахисту, які складено в таблиці 1.

Таблиця 1

Переваги та виклики командного підходу в управлінні проєктами кіберзахисту

Пункти	Склад	Опис
Переваги	Гнучкість	Команди можуть швидко адаптуватися до нових загроз чи змін у проєктних вимогах.
	Швидке реагування	Розподіл ролей дозволяє оперативно вирішувати критичні завдання, наприклад, реагувати на

		кібератаки в реальному часі.
	Синергія	Поєднання різноманітних компетенцій сприяє комплексному підходу до вирішення проблем.
Виклики	Комунікація	Недостатня координація може призвести до затримок чи помилок.
	Координація	Складність управління міждисциплінарними командами, особливо за участі різних організацій.

Джерело: складено автором за даними [11,12]

На основі досліджень науковців у сфері кібербзахисту та інформаційних технологій Арсенович Л., Горбаченко С., Чепурна О. та Слатвінська В., які присвячені аналізу управління проєктами та фахівцями в данній сфері, можливо сформулювати висновок, що ефективне управління викликами у сфері кібербезпеки потребує комплексного підходу, який поєднує чітку комунікацію, стандартизовані процедури та сучасні інструменти координації [11,12]. Горбаченко С. стверджує, що зосередження на більш ефективній особистій комунікації в команді надає більшої швидкості та ефективності реалізації проєкту [12]. Відкриті та надійні комунікаційні канали між членами команди, партнерами та державними органами дозволяють оперативно обмінюватися інформацією про загрози та координувати дії. Стандартизовані процедури, такі як регламенти реагування на інциденти або протоколи обробки даних, забезпечують узгодженість дій і зменшують ризики помилок. Для підтримки цих процесів активно використовуються спеціалізовані системи управління проєктами, такі як Jira чи Trello, які дозволяють відстежувати завдання, контролювати терміни та розподіляти ресурси.

З точки зору впливу зовнішних чинників важливо зазначити, що Україна, починаючи з 2014 року, перебуває під постійним тиском кібератак, які стали невід'ємною частиною гібридної агресії. Ці атаки спрямовані на

критичну інфраструктуру, державні установи та фінансові системи, що становить серйозну загрозу національній безпеці. Одним із найбільш відомих прикладів є атака на енергетичні мережі в 2015 році, яка призвела до масштабних відключень електроенергії. У 2017 році вірус NotPetya паралізував роботу багатьох українських та міжнародних компаній, демонструючи вразливість сучасних інформаційних систем. За даними Держспецзв'язку, у 2024 році кількість кіберінцидентів зросла на 20% порівняно з попереднім роком, що свідчить про посилення гібридної війни [13]. Серед найпоширеніших атак – фішинг, DDoS-атаки та використання шкідливого ПЗ, які вимагають постійного вдосконалення захисту.

Для протидії цим загрозам Україна розробила низку нормативно-правових документів, серед яких ключовим є Стратегія кібербезпеки, затверджена Указом Президента №447/2021. Цей документ визначає основні пріоритети, такі як захист критичної інфраструктури, підготовка кваліфікованих фахівців та розвиток міжнародного співробітництва [14]. Постанова КМУ №1295 встановлює організаційно-технічну модель кіберзахисту, що включає стандарти для державних і приватних організацій [15]. Держспецзв'язок також розробив методичні рекомендації, які деталізують алгоритми реагування на кіберінциденти та впровадження заходів безпеки.

Однак, незважаючи на наявність вказаних документів, їхнє фактичне впровадження ускладнюється через брак чітких механізмів контролю та недостатнє фінансування. Деякі положення залишаються формальними через відсутність конкретних інструкцій або ресурсів для їх виконання. Крім того, динамічний розвиток кіберзагроз вимагає постійного оновлення нормативної бази, що також ускладнює процес її застосування на практиці. Тому для підвищення ефективності кіберзахисту необхідно не лише вдосконалювати

законодавство, але й забезпечувати його реалізацію через чіткі механізми, фінансову підтримку та постійний моніторинг виконання.

Узагальнюючи вищевказане можна стверджувати, що проблема реалізації проєктів кіберзахисту складається з наступних аспектів. По-перше, недостатнє фінансування. Адже за даними звіту РНБО, бюджет на кібербезпеку становить лише 0,8% від загальних витрат на оборону, що обмежує впровадження сучасних технологій. По-друге, брак кваліфікованих кадрів. За оцінками експертів, дефіцит фахівців із кіберзахисту в Україні становить близько 5 000 осіб, що ускладнює формування ефективних команд. По-третє, відсутність незалежного аудиту, тобто регулярного зовнішнього оцінювання систем кіберзахисту, що знижує їхню ефективність та прозорість.

Відтак управління проєктами кіберзахисту в Україні вимагає злагодженої командної роботи, адже сучасні кіберзагрози вирізняються складністю та швидкістю ескалації. Командний підхід дозволяє інтегрувати експертизу фахівців із різних сфер, що є вирішальним для створення ефективних систем захисту в умовах гібридної війни та цифровізації.

Ключовою особливістю при цьому виступає необхідність міжвідомчої співпраці в межах команд. Державні структури, зокрема Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України та Збройні Сили України, координують зусилля для захисту критичної інфраструктури, наприклад, енергетичних чи фінансових систем. Залучення приватного сектору додає доступ до інноваційних рішень: компанії, такі як ISSP, розробляють системи аналізу загроз у реальному часі [16]. Громадські ініціативи, наприклад освітні проєкти, сприяють підвищенню рівня кіберобізнаності. Проєкти також потребують індивідуального підходу до кожного об'єкта захисту, що вимагає гнучкого розподілу ресурсів залежно від пріоритетності.

З іншого боку практичне застосування командного підходу ілюструють успішні ініціативи. Наприклад, створення системи моніторингу кіберзагроз, передбачене Постановою КМУ №1295, дозволило оперативно виявляти вразливості завдяки співпраці державних і приватних команд [15]. Формування реєстру об'єктів критичної інформаційної інфраструктури також демонструє ефективність командної роботи, хоча труднощі з уніфікацією даних залишаються. Оперативний обмін інформацією через захищені канали забезпечує швидке реагування на загрози. Проте відсутність єдиних стандартів обміну даними створює перепони, що потребують нагального вирішення.

Розвиток командного підходу в Україні може значно посилити кіберзахист через адаптацію передового досвіду, підготовку фахівців, співпрацю з бізнесом та інновації. Вивчення практик країн із розвиненою кібербезпекою, зокрема NIST Cybersecurity Framework 2.0, дозволяє оптимізувати організацію командної роботи через чіткий розподіл функцій і ризик-менеджмент [17]. Це може прискорити реагування на загрози в українських умовах.

Однак для ефективного функціонування команд потрібна належна підготовка кадрів не тільки високого професійного рівня, а й з навичками групової взаємодії. Сертифікаційні програми та розширення переліку професій у кібербезпеці допоможуть подолати дефіцит фахівців. Освітні ініціативи за підтримки міжнародних платформ, таких як EC-Council, сприятимуть підготовці спеціалістів для міждисциплінарних команд [18].

Збільшення ефективності підготовки персоналу можливе за рахунок співпраці з приватним сектором, зокрема з компаніями на кшталт Cisco. Вказані компанії здатні забезпечити доступ до сучасних технологій, таких як хмарні рішення для захисту даних [19]. Впровадження автоматизованих систем управління, наприклад Jira, та протоколів обміну інформацією, таких

як STIX/TAXII, оптимізує командну роботу, забезпечуючи швидший аналіз загроз [20].

Перспективи розвитку командного підходу та відповідні виклики узагальнено в таблиці 2.

Таблиця 2

Застосування та перспективи командного підходу в проєктах кіберзахисту

Аспект	Опис	Виклики
Міжвідомча співпраця	Координація державних органів для захисту інфраструктури	Відсутність єдиних стандартів взаємодії.
Приватний сектор	Інтеграція технологій бізнесу	Різні цілі держави та компаній.
Комунікація	Швидкий обмін даними через захищені канали	Брак уніфікованих протоколів.
Міжнародний досвід	Адаптація NIST Framework	Складність адаптації до України.
Кадри	Сертифікація фахівців	Дефіцит спеціалістів.
Інновації	Автоматизація та STIX/TAXII	Висока вартість впровадження.

Джерело: складено автором за даними [15-20]

Для підвищення ефективності командного підходу в управлінні проєктами кіберзахисту в Україні необхідно зосередитися на вдосконаленні управлінських процесів, підготовці фахівців, запровадженні інструментів контролю та розвитку законодавчої бази. Ці напрями дозволять не лише подолати наявні виклики, а й забезпечити стійкість систем кібербезпеки в умовах зростання загроз.

Оптимізація управлінських процесів передбачає впровадження послідовних методів, які спрощують комунікацію між учасниками проєктів. Чітке визначення етапів реалізації, від планування до виконання, дозволяє уникнути плутанини та забезпечує прозорість. Наприклад, використання методологій, таких як Agile, може сприяти гнучкому управлінню, коли команди швидко адаптуються до нових викликів, зберігаючи чіткий розподіл завдань [12]. Це особливо важливо для проєктів, де терміни виконання є критично стислими через швидку еволюцію кіберзагроз.

Розробка програм навчання та сертифікації фахівців із кіберзахисту є ще одним важливим кроком. Створення комплексних освітніх ініціатив, які поєднують теоретичні знання з практичними навичками, допоможе підготувати спеціалістів, здатних працювати в міждисциплінарних командах. Такі програми можуть включати тренінги з аналізу загроз, реагування на інциденти та використання сучасних технологій, наприклад, систем на базі штучного інтелекту. Міжнародні сертифікації, такі як CISSP чи CEH, можуть бути інтегровані в національні програми для підвищення кваліфікації [20]. Це дозволить зменшити дефіцит фахівців і посилити кадровий потенціал.

Впровадження механізмів моніторингу та контролю є необхідним для оцінки ефективності командної роботи. Стандартизовані метрики, такі як час реагування на кіберінциденти чи рівень виконання проєктних завдань, допоможуть оцінювати продуктивність команд і виявляти слабкі місця [21]. Наприклад, використання систем управління проєктами, таких як Jira, із вбудованими інструментами аналітики дозволяє відстежувати прогрес у реальному часі та оптимізувати розподіл ресурсів. Це забезпечує прозорість і підзвітність, що є критично важливим для проєктів із захисту критичної інфраструктури.

Розробка законодавчих ініціатив, зокрема закону про захист критичної інфраструктури, може створити міцну правову основу для командної роботи. Такий закон має чітко визначати обов'язки державних і приватних суб'єктів, стандарти взаємодії та механізми фінансування. Це сприятиме кращій координації між учасниками проєктів і забезпечить правову підтримку для впровадження інноваційних рішень. Ухвалення такого закону може також стимулювати міжнародне співробітництво, залучаючи досвід країн із розвиненою системою кібербезпеки.

Можливо стверджувати, що інтеграція міжвідомчої співпраці, приватного сектору та громадських ініціатив, підкріплена стандартизацією процесів і впровадженням технологій, таких як STIX/TAXII, забезпечує швидке реагування та синергію. Також потрібно наголосити на необхідності створення закону про захист критичної інфраструктури, розвиток освітніх програм і стандартизацію метрик оцінки командної роботи, для забезпечення стійкості та адаптивності системи кібербезпеки.

Висновки. Застосування командного підходу в управлінні проєктами кіберзахисту в Україні є важливим інструментом для протидії сучасним кіберзагрозам, які набувають особливого значення в умовах гібридної війни та швидкої цифровізації. Аналіз показав, що командна робота, заснована на міжвідомчій співпраці, залученні приватного сектору та ефективній комунікації, дозволяє оперативно реагувати на виклики та забезпечувати захист критичної інфраструктури. Успішні приклади, такі як впровадження систем моніторингу кіберзагроз і створення реєстру об'єктів критичної інформаційної інфраструктури, підтверджують ефективність цього підходу, хоча труднощі, пов'язані з недостатньою координацією та браком ресурсів, залишаються актуальними.

Перспективи розвитку командного підходу пов'язані з адаптацією міжнародного досвіду, зокрема стандартів NIST, розширенням кадрового потенціалу через освітні програми, поглибленням державно-приватного партнерства та впровадженням технологічних інновацій, таких як автоматизовані системи управління. Оптимізація командної роботи потребує спрощення комунікаційних процесів, чіткого розмежування етапів проєктів, стандартизації метрик оцінки ефективності та розробки законодавчої бази, зокрема закону про захист критичної інфраструктури.

Для подальшого вдосконалення командного підходу в Україні рекомендується посилити координацію між державними органами та приватним сектором, інвестувати в підготовку фахівців і активно залучати міжнародний досвід. Подальші дослідження можуть бути спрямовані на аналіз ефективності командної роботи в умовах воєнного стану та оцінку впливу нових технологій, таких як штучний інтелект, на управління проєктами кіберзахисту.

Список використаних джерел

1. Ратушняк О. Г. Особливості формування та управління командою в проєкті. *Вісник Хмельницького національного університету*. 2025. № 2. С. 164-169. DOI: https://doi.org/10.31891/2307-5740-2025-340-25

2. Данченко О. Б., Бедрій Д. І., Семко І. Б. Концептуальна модель формування високоефективної наукової проектної команди. *Вісник НТУ «ХПІ».* Серія: Стратегічне управління, управління портфелем, програмами та проектами. 2018. № 1 (1277). С. 51-56. DOI: 10.20998/2413-3000.2018.1277.8

3. Косенко Н. В., Доценко Н. В., Чумаченко І. В. Інформаційна технологія проектного управління формування команд з урахуванням

компетентнісного підходу : монографія. Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 134 с.

4. Андрейченко А., Горбаченко С., Дикий О. Особливості управління проєктами у сфері кіберзахисту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. №2(10). С. 45–53. DOI: https://doi.org/10.28925/2663-4023.2020.10.4553

5. Немченко Т., В'юник О. Новітні підходи до управління командами в проєктному IT-менеджменті. *Економіка та суспільство.* 2024. № 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-61.

6. Галушка З. І. Agile-менеджмент як інноваційний підхід до управління проєктами. *Інфраструктура ринку*. 2020. Вип. 47. С. 76–79. DOI: https://doi.org/10.32843/infrastruct47-14

7. Судук О. Ю., Щербакова А. С. Використання принципів Agile-менеджменту при експертизі проєктів та управлінні ефективними командами. *Вісник Національного університету водного господарства та природокористування. Економічні науки*. 2023. Вип. 2. С. 297–304. DOI: 10.31713/ve2202325.

8. Гуцуляк Н., Синиченко А. Сучасні технології командотворення: формування «суперкоманд» для підвищення ефективності персоналу в період невизначеності. *Економіка та суспільство*. 2021. № 34. URL: https://doi.org/10.32782/2524-0072/2021-34-88.

9. Solomon D. The Worth of Steady Digital Team Formation Strategy: A Case Study of Bruce Tuckman's Model in Software Industry. *Advance*. 2020. DOI: https://doi.org/10.31124/advance.12644939.v1.

10. Пітерсен Р., Сантос Д., Сміт М. К., Ветцель К. А., Вітте Г. Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи

NICE). Спеціальна публікація NIST 800-181, редакція 1. 2020. 27 с. DOI: https://doi.org/10.6028/NIST.SP.800-181r1.

11. Арсенович Л. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 3, № 15. С. 93–109. DOI: https://doi.org/10.28925/2663-4023.2022.15.93109.

12. Горбаченко С., Чепурна О., Слатвінська В. Адаптація проєктного підходу до управління стартапами. *Трансформаційна економіка*. 2023. №4 (04). С. 24-28. DOI: https://doi.org/10.32782/2786-8141/2023-4-5 .

13. CERT-UA statistics. Russian cyber operations. Analytics for the H2 2024. State service of special communications and information protection of Ukraine. 2025. 22 p.

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. *Верхован Рада України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.07.2025).

15. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : Постанова Кабінету Міністрів України від 02.09.2022 р. № 991. Дата оновлення: 07.09.2022. *Верхован Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (дата звернення: 20.05.2025).

16. Цюприк І. В. Публічно-приватне партнерство як стратегічний інструмент забезпечення кібербезпеки в умовах правового режиму воєнного стану в Україні. *Міжнародний науковий журнал «Інтернаука»*. Серія: Юридичні науки. 2025. № 6. DOI: https://doi.org/10.25313/2520-2308-2025-6-11078 (дата звернення: 26.05.2025).

17. Pascoe C. E. Public Draft: The NIST Cybersecurity Framework 2.0. *National Institute of Standards and Technology.* 2023. DOI: https://doi.org/10.6028/NIST.CSWP.29.ipd.

18. Davri E. C., Darra E., Monogioudis I., Grigoriadis A., Iliou C., Mengidis N., Farah M. A. B. Cyber security certification programmes. 2021 IEEE *International Conference on Cyber Security and Resilience (CSR)*. 2021. PP. 428–435. DOI: 10.1109/CSR51186.2021.9527974

19. Опанасенко М. І., Поночовний П. М. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock. *Сучасний захист інформації*. 2022. № 4. С. 36–41. DOI: 10.31673/2409-7292.2023.010010

20. Кочман К. П., Форос Г. В. Перспективи вдосконалення інформаційного забезпечення протидії кіберзагрозам у секторі оборони України. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України*: матеріали Науково-практичної конференції (м. Львів, 20 грудня 2024) / упоряд. Т. В. Магеровська. Львів : ЛьвДУВС, 2025. С. 50–53.

21. Горбаченко С. А., Разінкін Н. С. Конспект лекцій з дисципліни «Менеджмент та маркетинг інновацій» для здобувачів спеціальності 073 «Менеджмент». Кафедра кібербезпеки НУ «Одеська юридична академія». Одеса. 2024. 76 с. DOI: https://doi.org/10.32837/11300.29764