УПРАВЛІННЯ ПРОЕКТАМИ, КОМУНІКАТИВНЕ ЗАБЕЗПЕЧЕННЯ ТА ЛІДЕРСТВО У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ІНСТИТУЦІОНАЛЬНІ ЗАСАДИ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

PROJECT MANAGEMENT, COMMUNICATION SUPPORT AND LEADERSHIP IN THE SPHERE OF NATIONAL SECURITY: INSTITUTIONAL PRINCIPLES OF ANALYTICAL ACTIVITY IN THE INFORMATION SOCIETY

УДК 005.8:351.86:007
DOI https://doi.org/10.32782/pma2663-5240-2024.39.56

Шестаковська Т.Л.
д. наук з держ. упр., доцент,
ректор
Чернігівський інститут інформації, бізнесу і права ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая»
ORCID ID: 0000-0002-8098-8439

Яровой Т.С.
д. наук з держ. упр., доцент,
професор кафедри публічного управління та адміністрування
Чернігівський інститут інформації, бізнесу і права ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая»
ORCID ID: 0000-0002-7266-3829

Кириченко Г.В.
к. наук з держ. упр.,
доцент кафедри публічного управління та адміністрування
Чернігівський інститут інформації, бізнесу і права ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая»
ORCID ID: 0000-0003-1067-8758

У статті здійснено комплексний аналіз управління проєктами, комунікативного забезпечення та лідерства у сфері національної безпеки в умовах сучасного інформаційного суспільства. Розглянуто ключові теоретико-методологічні засади управління безпековими проєктами, зокрема їх планування, реалізацію, моніторинг та оцінку ефективності. Особливу увагу приділено питанням комунікативного забезпечення, що включає оперативний обмін інформацією між державними інституціями, використання цифрових технологій у стратегічних комунікаціях та механізми інформаційно-аналітичної діяльності. Метою даної роботи є аналіз ключових аспектів управління безпековими проєктами, визначення стратегічних підходів до комунікативного забезпечення та дослідження ролі лідерства у формуванні ефективної системи безпеки держави. Розглянуто основні принципи інформаційно-аналітичної діяльності, проаналізовано сучасні виклики у сфері національної безпеки та запропоновано шляхи підвищення ефективності управлінських процесів у даній галузі. Аналізується роль лідерства в управлінні безпековими проєктами, зокрема трансформаційний, ситуаційний та діджитал-лідерський підходи, що забезпечують адаптацію до динамічних змін у сфері національної безпеки. Запропоновано концептуальну модель аналітичної діяльності в умовах інформаційного суспільства, яка включає державні аналітичні центри, незалежні експертні організації та міжнародну співпрацю. Розглянуто сучасні виклики національній безпеці, зокрема загрози у кіберпросторі, інформаційні маніпуляції та гібридні війни, що потребують удосконалення механізмів аналізу ризиків та оперативного реагування. Запропоновано практичні рекомендації щодо розвитку управлінських компетенцій керівників у сфері безпеки, впровадження цифрових технологій для аналітичного забезпечення та створення ефективної комунікаційної інфраструктури міждержавного рівня. Результати дослідження можуть бути використані державними органами, аналітичними центрами та освітніми установами для підвищення ефективності управління проєктами у сфері національної безпеки.

Ключові слова: *аналітична діяльність, національна безпека, інституціональні засади, інформаційне суспільство, лідерство, комунікативне забезпечення, управління проектами.*

The article provides a comprehensive analysis of project management, communication support, and leadership in the field of national security in the context of a modern information society. The key theoretical and methodological principles of security project management are considered, in particular their planning, implementation, monitoring, and effectiveness assessment. Particular attention is paid to issues of communication support, which includes the operational exchange of information between state institutions, the use of digital technologies in strategic communications, and mechanisms of information and analytical activities. The purpose of this work is to analyze key aspects of security project management, determine strategic approaches to communication support, and study the role of leadership in the formation of an effective state security system. The basic principles of information and analytical activities are considered, modern challenges in the field of national security are analyzed, and ways to increase the efficiency of management processes in this area are proposed. The role of leadership in security project management is analyzed, in particular, transformational, situational and digital leadership approaches that ensure adaptation to dynamic changes in the field of national security. A conceptual model of analytical activity in the information society is proposed, which includes state analytical centers, independent expert organizations and international cooperation. Modern challenges to national security are considered, in particular, threats in cyberspace, information manipulation and hybrid wars, which require improving risk analysis mechanisms and operational response. Practical recommendations are proposed for the development of managerial competencies of security managers, the implementation of digital technologies for analytical support and the creation of an effective communication infrastructure at the interstate level. The results of the study can be used by state bodies, analytical centers and educational institutions to improve the efficiency of project management in the field of national security.

Key words: *analytical activities, national security, institutional frameworks, information society, leadership, communication support, project management.*

Постановка проблеми. Сучасний світ характеризується стрімким розвитком інформаційних технологій, що суттєво впливає на всі сфери суспільного життя, включаючи національну безпеку. В умовах цифрової трансформації державні інститути стикаються з новими викликами, такими як інформаційні війни, кібератаки, гібридні загрози та глобальні геополітичні зміни. Успішне протистояння цим викликам потребує ефективного управління безпековими проєктами, налагодження стратегічних комунікацій та формування лідерських компетенцій у сфері національної безпеки. Управління проєктами у сфері національної безпеки відрізняється високим рівнем складності та необхідністю врахування численних ризиків. Сучасні методології управління, такі як PMBOK, PRINCE2 та Agile, дозволяють ефективніше реалізовувати державні ініціативи, спрямовані на зміцнення безпеки країни [5]. При цьому ключовими аспектами успішної реалізації безпекових програм є не лише проєктне планування та контроль за виконанням, а й ефективна комунікація між державними органами, військовими структурами, громадянським суспільством та міжнародними партнерами. Одним із головних факторів, що визначає ефективність національної безпеки, є якість інформаційно-аналітичної діяльності. Оперативний збір, аналіз та обробка даних дозволяють не лише виявляти потенційні загрози, але й своєчасно реагувати на них, знижуючи рівень ризиків для держави та суспільства [1]. У зв'язку з цим постає необхідність удосконалення методологічних підходів до оцінювання ефективності державного механізму аналітичного забезпечення безпекової політики [4]. Не менш важливим аспектом є питання лідерства у сфері національної безпеки. В сучасних умовах управлінці повинні не лише ефективно керувати проєктами, а й мати високий рівень стратегічного мислення, здатність швидко ухвалювати рішення та адаптуватися до динамічного середовища. Лідерство у цій сфері має різні форми, зокрема трансформаційне, ситуаційне та діджитал-лідерство, кожне з яких відіграє важливу роль у забезпеченні ефективності безпекової політики [2]. Таким чином, дослідження інституціональних засад управління проєктами, комунікаційних механізмів та лідерських підходів у сфері національної безпеки є надзвичайно актуальним.

Аналіз останніх досліджень і публікацій. Питання управління проєктами, комунікативного забезпечення та лідерства у сфері національної безпеки широко досліджуються в науковій літературі, особливо в контексті сучасних викликів, пов'язаних із цифровізацією, гібридними загрозами та необхідністю ефективного інформаційно-аналітичного забезпечення державної політики безпеки. Значну увагу інформаційно-аналітичним аспектам управління національною безпекою приділяє Варенко В.М., який у своєму навчальному посібнику розглядає основи інформаційно-аналітичної діяльності, її роль у стратегічному плануванні та ухваленні рішень у сфері безпеки. Він підкреслює, що якісне інформаційне забезпечення є ключовим елементом ефективного державного управління, особливо в умовах динамічного інформаційного середовища [1]. Ситник Г.П. та Орел М.Г. у своїй праці досліджують питання національної безпеки в контексті європейської інтеграції України. Автори наголошують на необхідності адаптації українських підходів до управління безпековими проєктами відповідно до міжнародних стандартів, а також на важливості стратегічних комунікацій у процесі європейської інтеграції. Вони підкреслюють, що інтеграція України у міжнародні безпекові структури потребує ефективної взаємодії між державними та міжнародними інституціями, а також формування компетентного лідерства у сфері безпеки [2].

Монографія Криштановича М.Ф. та його колег присвячена аналізу державної політики забезпечення національної безпеки України. У роботі акцентується увага на основних напрямах безпекової політики, підходах до аналізу ризиків та загроз, а також на необхідності впровадження сучасних технологій у систему державного управління. Зокрема, автори відзначають важливість розвитку аналітичних центрів та інформаційно-аналітичних платформ, що дозволяють забезпечити ефективний моніторинг загроз і прогнозування потенційних кризових ситуацій [3].

Соколов В.А. та Шевченко М.М. досліджують методологічні підходи до оцінювання ефективності державного механізму інформаційно-аналітичного забезпечення політики національної безпеки. Автори підкреслюють, що одним із ключових критеріїв ефективності є здатність державних органів оперативно реагувати на загрози, використовуючи сучасні цифрові аналітичні інструменти. Вони також наголошують на важливості інтеграції Big Data-аналітики та штучного інтелекту у процес ухвалення управлінських рішень у сфері національної безпеки [4].

Керівництво з управління проєктами розвитку, підготовлене Цепендою І.Є. та Кропельницькою С.О., висвітлює питання ефективного проєктного менеджменту та

впровадження міжнародних стандартів у цій сфері. Особливу увагу приділено адаптації сучасних методологій управління проєктами до державного сектору, що є актуальним для сфери національної безпеки. Авторами розглянуто принципи Agile, PRINCE2 та PMBOK як основні підходи до управління проєктами, які можуть бути ефективно застосовані для реалізації державних безпекових ініціатив [5].

У колективній монографії під редакцією Омельяненка В.А. розглядаються інновації та механізми управління технологічним трансфером, що також має значний вплив на сферу національної безпеки. Автори підкреслюють, що в умовах глобальної цифровізації ефективність системи національної безпеки значною мірою залежить від здатності держави інтегрувати новітні технології у процеси управління ризиками, кібербезпеку та інформаційно-аналітичне забезпечення [6].

Таким чином, аналіз наукових публікацій дозволяє зробити висновок, що питання управління проєктами, комунікаційного забезпечення та лідерства у сфері національної безпеки є актуальними та потребують подальших досліджень. Важливим напрямом наукових розвідок є інтеграція сучасних цифрових технологій в управлінські процеси, розробка ефективних комунікативних стратегій та формування лідерських компетенцій, що дозволить підвищити ефективність державної політики у сфері безпеки.

Метою статті є дослідження інституціональних засад управління проєктами, комунікативного забезпечення та лідерства у сфері національної безпеки в умовах інформаційного суспільства.

Виклад основного матеріалу. Управління проєктами у сфері національної безпеки є складним та багатокомпонентним процесом, який охоплює стратегічне планування, реалізацію, моніторинг та оцінку заходів, спрямованих на забезпечення безпеки держави. Враховуючи сучасні виклики, такі як зростання гібридних загроз, кібернетичні атаки, інформаційні маніпуляції та тероризм, ефективне управління безпековими проєктами вимагає застосування сучасних методологій, міжнародних стандартів та цифрових технологій [2].

Управління проєктами у сфері безпеки має низку особливостей, які відрізняють його від класичних підходів у бізнесі чи соціальних програмах. Це передусім висока ступінь ризику, потреба в оперативному прийнятті рішень, багаторівнева координація між державними структурами та міжнародними партнерами, а також необхідність врахування політичних, соціальних і економічних чинників. З огляду на це, у сфері національної безпеки активно застосовуються адаптовані підходи до управління проєктами, включаючи PMBOK (Project Management Body of Knowledge), PRINCE2 (Projects in Controlled Environments) та Agile, які дозволяють підвищити ефективність реалізації безпекових ініціатив [5].

Процес управління безпековими проєктами складається з кількох ключових етапів:

1. Ініціація проєкту. Визначення проблеми або загрози, що потребує вирішення. Формування команди проєкту, розподіл ролей та відповідальності. Аналіз загроз і оцінка ризиків, що можуть впливати на проєкт. Визначення зацікавлених сторін та ключових учасників, зокрема державних органів, міжнародних партнерів, громадянського суспільства.

2. Планування. Встановлення стратегічних цілей та завдань проєкту. Розробка плану заходів, включаючи часові рамки, розподіл ресурсів та фінансування. Визначення критеріїв оцінки ефективності реалізації проєкту. Впровадження ризик-менеджменту для прогнозування та запобігання можливим загрозам.

3. Реалізація. Виконання заходів відповідно до плану проєкту. Залучення державних установ, військових, правоохоронних органів, міжнародних партнерів та громадських організацій. Використання сучасних цифрових інструментів та аналітичних платформ для моніторингу ситуації в реальному часі.

4. Моніторинг та контроль. Аналіз ефективності реалізації проєкту за допомогою ключових показників продуктивності (KPI). Виявлення проблемних аспектів та впровадження коригувальних заходів. Оцінка ефективності інформаційного забезпечення та комунікаційних стратегій.

5. Завершення проєкту та аналіз отриманих результатів. Підбиття підсумків виконаних заходів та оцінка їхнього впливу на національну безпеку. Визначення подальших кроків та перспектив розвитку безпекових ініціатив. Формування звітності та розробка рекомендацій для майбутніх проєктів.

Одним із ключових факторів ефективного управління проєктами у сфері національної безпеки є впровадження цифрових технологій. Використання Big Data, штучного інтелекту (AI), систем прогнозного аналізу дозволяє значно покращити процеси оцінки ризиків, виявлення загроз та ухвалення стратегічних рішень [6].

Зокрема, сучасні системи управління проєктами включають: Автоматизовані платформи управління ризиками, які аналізують

потенційні загрози та пропонують сценарії реагування. Аналітичні інформаційні системи, що дозволяють інтегрувати дані з різних джерел та прогнозувати динаміку загроз. Системи кібербезпеки, які забезпечують захист критично важливих інфраструктурних об'єктів від кібератак. Штучний інтелект та машинне навчання, що допомагають виявляти небезпечні патерни в інформаційних потоках.

Незважаючи на розвиток методологічних підходів, управління проєктами у сфері національної безпеки стикається з низкою викликів: Висока динамічність загроз, що ускладнює довгострокове прогнозування та планування. Недостатня координація між державними та міжнародними структурами, що може призводити до дублювання заходів або неефективного використання ресурсів. Брак професійних кадрів, здатних працювати за сучасними стандартами управління безпековими проєктами. Фінансові та ресурсні обмеження, що знижують можливість реалізації масштабних програм. Гібридні загрози та інформаційні війни, які потребують нового підходу до управління інформацією та стратегічними комунікаціями [3].

Для підвищення ефективності управління проєктами у сфері національної безпеки необхідно: Інтегрувати міжнародні стандарти та методології проєктного менеджменту у систему державного управління безпекою. Розвивати систему стратегічних комунікацій, що дозволить швидше реагувати на кризові ситуації та покращить координацію між державними органами. Впроваджувати цифрові технології та автоматизовані аналітичні системи, які допоможуть ефективніше аналізувати дані та прогнозувати потенційні загрози. Зміцнювати міжнародну співпрацю, обмінюючись досвідом і впроваджуючи найкращі практики управління безпековими проєктами. Підвищувати рівень підготовки кадрів, зокрема шляхом впровадження спеціалізованих освітніх програм із проєктного менеджменту в секторі безпеки [5].

Таким чином, управління проєктами у сфері національної безпеки є важливим елементом державної політики, що потребує комплексного підходу, включаючи стратегічне планування, ефективну комунікацію, застосування цифрових технологій та розвиток компетентного лідерства. Вдосконалення цих аспектів сприятиме підвищенню стійкості держави перед сучасними загрозами та забезпеченню національної безпеки в умовах глобальної нестабільності.

Комунікативне забезпечення є одним із ключових елементів ефективної аналітичної діяльності у сфері національної безпеки. В умовах інформаційного суспільства, коли обсяг та швидкість поширення інформації зростають експоненціально, якість комунікації між державними органами, аналітичними центрами, правоохоронними структурами та громадянським суспільством визначає оперативність та обґрунтованість прийняття стратегічних рішень.

Аналітична діяльність у сфері національної безпеки спрямована на збір, обробку, аналіз та інтерпретацію інформації для прогнозування загроз та розробки відповідних механізмів реагування [1]. У цьому процесі комунікація відіграє критичну роль, оскільки саме через ефективний обмін інформацією забезпечується своєчасне ухвалення рішень та координація дій між зацікавленими сторонами.

Комунікативне забезпечення аналітичної діяльності включає кілька ключових аспектів:

1. Оперативний обмін інформацією між державними структурами: Співпраця між Міністерством оборони, Службою безпеки України, правоохоронними органами, аналітичними центрами та міжнародними партнерами. Використання сучасних цифрових платформ для безпечного обміну інформацією в режимі реального часу. Інтеграція баз даних, що дозволяє оперативно отримувати актуальні відомості щодо потенційних загроз [3].

2. Інформаційна взаємодія з громадянським суспільством: Побудова ефективної системи стратегічних комунікацій для протидії дезінформації та маніпуляціям у медіапросторі. Залучення експертної спільноти та аналітичних центрів до розробки інформаційної політики. Формування прозорої та достовірної системи комунікації між державою та суспільством, що сприяє підвищенню довіри до урядових структур [2].

3. Використання цифрових технологій у комунікації та аналізі даних: Запровадження автоматизованих аналітичних систем на основі штучного інтелекту (AI) та Big Data для обробки великих масивів інформації. Використання алгоритмів машинного навчання для прогнозування тенденцій у сфері безпеки та аналізу потенційних загроз. Впровадження кібербезпекових систем для захисту каналів комунікації від несанкціонованого доступу та кібератак [6].

4. Кризова комунікація та управління інформаційними потоками в умовах надзвичайних ситуацій: Формування чіткої системи інформування населення та медіа в умовах кризових ситуацій. Розробка стандартів комунікації в умовах гібридних загроз, зокрема інформаційних атак та кібершпигунства. Взаємодія з

міжнародними партнерами для обміну досвідом та координації дій у разі масштабних безпекових криз [4].

Окремої уваги заслуговує стратегічна комунікація як невід'ємна складова інформаційної політики держави у сфері безпеки. Вона включає: Протидію дезінформації та фейковим новинам через моніторинг інформаційного простору та спростування неправдивої інформації. Розробку інформаційних кампаній для підвищення рівня обізнаності населення щодо питань національної безпеки. Міжнародне співробітництво у сфері інформаційної безпеки, що включає координацію з НАТО, ЄС та іншими міжнародними організаціями.

Згідно з дослідженнями, представленими Соколовим В.А. та Шевченком М.М., для підвищення ефективності інформаційно-аналітичного забезпечення політики національної безпеки необхідно впроваджувати інструменти глибокого аналізу даних та сучасні методи обробки інформації. Це дозволяє не лише забезпечити високий рівень ситуаційної обізнаності, але й мінімізувати вплив інформаційних маніпуляцій на громадську думку та політичні процеси в країні [4].

Незважаючи на важливість якісного комунікативного забезпечення у сфері національної безпеки, існує низка викликів, що перешкоджають його ефективній реалізації: Фрагментованість інформаційного простору та відсутність єдиної централізованої системи обміну аналітичними даними. Інформаційні загрози та кібератаки, що можуть спотворювати інформацію та ускладнювати її аналіз. Низький рівень координації між державними установами, що призводить до дублювання аналітичної діяльності та втрати часу на обробку важливої інформації. Недостатній рівень інформаційної грамотності серед населення, що робить суспільство вразливим до інформаційних маніпуляцій та дезінформаційних кампаній [3].

З метою підвищення ефективності комунікативного забезпечення у сфері національної безпеки необхідно: Запровадити єдину державну платформу для обміну аналітичними даними між силовими структурами, урядом та аналітичними центрами. Розвивати технології штучного інтелекту та Big Data-аналітики для автоматизованого моніторингу інформаційного простору та прогнозування загроз. Посилити міжнародне співробітництво у сфері інформаційної безпеки, зокрема шляхом обміну досвідом із країнами-членами НАТО та ЄС. Впровадити освітні програми з інформаційної грамотності, спрямовані на підвищення стійкості суспільства до інформаційних маніпуляцій. Розширити можливості кризових комунікацій, що дозволить оперативно реагувати на загрози та мінімізувати панічні настрої у разі кризових ситуацій.

Таким чином, комунікативне забезпечення аналітичної діяльності у сфері національної безпеки є багаторівневим процесом, який включає ефективну взаємодію між державними структурами, громадянським суспільством, міжнародними партнерами та засобами масової інформації. Використання сучасних цифрових технологій, стратегічних комунікацій та інструментів прогнозного аналізу дозволяє забезпечити якісний рівень інформаційно-аналітичного супроводу безпекових рішень та підвищити стійкість держави до сучасних загроз.

Лідерство відіграє ключову роль у забезпеченні ефективного управління проєктами у сфері національної безпеки. В умовах глобальної нестабільності, зростання гібридних загроз, інформаційних воєн і кібернетичних атак ефективні лідери стають визначальним чинником успішної реалізації державних безпекових стратегій. Лідерство в цій сфері поєднує стратегічне бачення, здатність ухвалювати рішення в умовах невизначеності, навички кризового менеджменту та ефективну комунікацію як із підлеглими, так і з партнерами [2].

Лідер, який здійснює управління безпековими проєктами, повинен володіти рядом критичних якостей: Стратегічне мислення – здатність аналізувати ситуацію в довгостроковій перспективі, передбачати загрози та розробляти ефективні відповіді на них. Рішучість і відповідальність – швидке ухвалення рішень на основі обмежених даних та готовність нести відповідальність за їх наслідки. Адаптивність – вміння працювати в умовах швидкоплинних змін, що є особливо важливим у контексті гібридних загроз і динамічної міжнародної обстановки. Ефективна комунікація – здатність чітко доносити інформацію до команди, державних інституцій, міжнародних партнерів і громадськості. Кризове управління – навички швидкого реагування та координації дій у випадку надзвичайних ситуацій або воєнних конфліктів.

У сучасній практиці управління безпековими проєктами можна виділити кілька основних моделей лідерства:

1. Трансформаційне лідерство. Лідери цього типу надихають свої команди на досягнення високих результатів, орієнтуючись на загальні цінності та довгострокові цілі. Вони сприяють впровадженню інноваційних рішень, мотивують підлеглих до розвитку і професійного вдосконалення. Трансформаційні лідери

відіграють важливу роль у реформах сектору національної безпеки, зокрема в процесах модернізації збройних сил, кібербезпеки та інформаційної політики [3].

2. Ситуаційне лідерство. Гнучкий підхід, що передбачає зміну стилю керівництва залежно від поточної ситуації та особливостей команди. У кризових умовах ситуаційний лідер може діяти більш директивно, тоді як у стабільний період він може делегувати повноваження та сприяти колективному прийняттю рішень. Такий стиль є особливо ефективним у правоохоронних органах, військових структурах та антикризових управлінських групах [4].

3. Діджитал-лідерство. Враховуючи значний вплив цифрових технологій на безпекову сферу, сучасні керівники повинні володіти цифровими компетенціями. Лідери цього типу активно використовують аналітичні платформи, штучний інтелект, кібербезпекові рішення та Big Data для ухвалення управлінських рішень. Діджитал-лідерство є критично важливим у сфері інформаційної безпеки, боротьби з дезінформацією та кіберзахисту державних ресурсів [6].

Лідер у сфері національної безпеки несе відповідальність за ефективність реалізації стратегічних ініціатив та координацію між різними рівнями управління. Основні функції лідера включають: Формування бачення проєкту – розробка стратегічного плану та визначення пріоритетних завдань. Організація роботи команди – створення ефективної системи управління кадрами, делегування обов'язків та забезпечення мотивації. Моніторинг і контроль – оцінка поточного стану виконання проєкту, коригування дій відповідно до зміненої ситуації. Координація взаємодії з партнерами – встановлення зв'язків з міжнародними організаціями, приватним сектором та громадянським суспільством для ефективного виконання безпекових ініціатив. Реагування на кризи – швидке прийняття рішень та впровадження антикризових заходів у разі виникнення загроз державній безпеці [5].

Попри важливість ефективного лідерства, існує низка викликів, що ускладнюють діяльність керівників у безпековій сфері: Високий рівень відповідальності та стресу, що може впливати на якість ухвалених рішень. Брак професійно підготовлених кадрів, які володіють сучасними методами управління безпековими проєктами. Швидкість змін у сфері безпеки, що вимагає високого рівня адаптивності від керівників. Політичний та бюрократичний тиск, що може ускладнювати реалізацію ефективних реформ. Зростання інформаційних загроз, включаючи дезінформацію та кібератаки, що потребують спеціальних навичок цифрового лідерства [4].

Для підвищення ефективності лідерства в управлінні безпековими проєктами необхідно: Розвивати освітні програми з лідерства у сфері безпеки, що включають навчання стратегічного мислення, кризового менеджменту та цифрових компетенцій. Запроваджувати програми підготовки діджитал-лідерів, які володіють знаннями у сфері кібербезпеки, штучного інтелекту та стратегічних комунікацій. Посилювати міжнародну співпрацю через обмін досвідом з провідними експертами з управління національною безпекою. Впроваджувати системи психологічної підтримки для керівників, що працюють у високостресових умовах. Забезпечувати відкритість і підзвітність лідерів, що сприятиме підвищенню рівня довіри суспільства до безпекових структур [3].

Таким чином, лідерство є одним із вирішальних чинників успішного управління проєктами у сфері національної безпеки. Високий рівень компетентності, стратегічне бачення, здатність адаптуватися до змін і використання сучасних цифрових технологій дозволять ефективно протидіяти загрозам та забезпечити стабільність держави в умовах глобальних викликів.

Аналітична діяльність у сфері національної безпеки є важливим інструментом державного управління, який забезпечує ефективне прогнозування загроз, оцінку ризиків та розробку стратегічних рішень. В умовах інформаційного суспільства, де обсяг даних зростає експоненціально, а інформація стає головним ресурсом, ефективність аналітичної діяльності багато в чому залежить від її інституціонального забезпечення, тобто від наявності відповідних структур, нормативно-правової бази та технологічного інструментарію [1].

Основними інституціями, що здійснюють аналітичну діяльність у сфері безпеки, є Рада національної безпеки і оборони України (РНБО), Міністерство оборони, Служба безпеки України (СБУ), Державна служба спеціального зв'язку та захисту інформації. Ці структури здійснюють аналіз національних і міжнародних загроз, готують рекомендації для органів державної влади та розробляють політику у сфері безпеки. При РНБО функціонують спеціалізовані аналітичні підрозділи, що займаються прогнозуванням ризиків, аналізом інформаційних загроз та кібербезпеки [3].

Важливу роль у формуванні аналітичних продуктів відіграють незалежні дослідницькі центри, такі як Національний інститут стратегічних досліджень, Центр досліджень армії,

конверсії та роззброєння, а також міжнародні аналітичні установи (RAND Corporation, Chatham House). Такі організації займаються розробкою альтернативних сценаріїв розвитку ситуації, аналізом міжнародного безпекового середовища, а також прогнозуванням можливих загроз для держави.

У сучасних умовах національна безпека неможлива без тісної взаємодії з міжнародними партнерами, такими як НАТО, Європейський Союз, ОБСЄ та спецслужби союзних держав. Аналітична діяльність у сфері безпеки все більше інтегрується в глобальні системи обміну інформацією, що дозволяє оперативно виявляти загрози та реагувати на них у координації з міжнародними структурами [2].

Законодавче регулювання аналітичної діяльності у сфері безпеки базується на таких ключових документах: Закон України "Про національну безпеку", який визначає основні засади організації безпекового сектору та координації аналітичної діяльності. Закон України "Про інформацію", що регламентує порядок збору, обробки та використання інформації в державному управлінні. Концепція інформаційної безпеки України, яка визначає стратегічні напрями розвитку системи аналітичного забезпечення в умовах гібридних загроз [3].

Розвиток нормативно-правової бази є важливим фактором вдосконалення аналітичної діяльності, оскільки ефективність державної безпекової політики значною мірою залежить від законодавчого врегулювання доступу до інформації, міжвідомчої координації та міжнародної співпраці.

Сучасна аналітична діяльність у сфері національної безпеки значною мірою базується на використанні новітніх цифрових технологій: Big Data та штучний інтелект (AI) дозволяють обробляти великі обсяги інформації та прогнозувати можливі загрози шляхом аналізу поведінкових патернів і тенденцій. Кібернетичні аналітичні системи використовуються для виявлення кібератак, аналізу інформаційних маніпуляцій та протидії ворожим впливам. Геоінформаційні системи (GIS) дозволяють здійснювати моніторинг територіальної безпеки, аналізуючи дані із супутників, дронів та інших джерел [6].

Інституціональне забезпечення аналітичної діяльності повинно включати створення та підтримку технологічних платформ, що дозволяють державним органам швидко обробляти інформацію та використовувати її для ухвалення рішень.

Попри розвиток аналітичних інституцій, у цій сфері залишається низка викликів: Нестача кваліфікованих кадрів – аналітична діяльність потребує фахівців з високим рівнем технічних та стратегічних навичок. Фрагментованість інформаційних систем – різні відомства часто працюють із несумісними базами даних, що ускладнює координацію. Інформаційні війни та дезінформація – масові маніпуляції громадською думкою, кібератаки на державні структури та розповсюдження фейкових новин створюють нові виклики для національної безпеки [4]. Залежність від міжнародних аналітичних структур – в умовах глобальної конкуренції важливо розвивати національні інститути аналітики та не покладатися лише на закордонні джерела інформації.

Для підвищення ефективності аналітичного забезпечення національної безпеки необхідно: Створити єдиний інформаційно-аналітичний центр, що координуватиме діяльність різних державних установ та об'єднуватиме дані з усіх безпекових напрямів. Посилити підготовку аналітичних кадрів шляхом розробки спеціалізованих навчальних програм, що поєднують безпекові дослідження, кібернетику та штучний інтелект. Розширити співпрацю з міжнародними аналітичними структурами, забезпечуючи доступ до передових методик аналізу загроз. Удосконалити систему моніторингу інформаційного простору для своєчасного виявлення загроз та інформаційних атак. Інвестувати у технології обробки даних, зокрема у впровадження нейромереж, машинного навчання та предиктивного аналізу [5].

Таким чином, інституціональні засади аналітичної діяльності в умовах інформаційного суспільства повинні поєднувати ефективну державну політику, високий рівень міжвідомчої координації та сучасні цифрові технології. Вдосконалення цієї системи є критично важливим для забезпечення національної безпеки України в умовах глобальних викликів та інформаційних загроз.

Аналітична діяльність у сфері національної безпеки є критичним компонентом стратегічного управління державою, оскільки забезпечує своєчасний збір, обробку, аналіз та інтерпретацію інформації, необхідної для ухвалення рішень. В умовах інформаційного суспільства, де інформаційні потоки збільшуються експоненціально, ефективність цієї діяльності значною мірою залежить від розвиненої інституційної структури, здатної швидко адаптуватися до змін у глобальному безпековому середовищі [1].

Інституційні засади аналітичної діяльності передбачають функціонування розгалуженої мережі державних, наукових, громадських та міжнародних структур, які здійснюють моніто-

ринг загроз, прогнозують розвиток ситуації та формують відповідні рекомендації для органів влади. До ключових інституцій, що забезпечують аналітичну діяльність у сфері національної безпеки України, належать: Державні аналітичні центри (зокрема, Ради національної безпеки і оборони України, аналітичні підрозділи Міністерства оборони, Служби безпеки України, розвідувальних органів). Наукові установи та експертні спільноти, які проводять незалежні дослідження з питань безпеки, оборони, геополітики та інформаційних загроз. Громадянське суспільство – аналітичні платформи, громадські організації та журналістські розслідування, які здійснюють контроль за реалізацією безпекової політики. Міжнародні структури – співпраця з НАТО, Європейським Союзом, ООН, розвідувальними службами партнерських країн у рамках обміну даними та координації дій [3].

В умовах цифровізації та глобальної конкуренції між державами якість аналітичної діяльності визначається рівнем використання передових інформаційних технологій. Тому серед ключових напрямів розвитку аналітичної діяльності можна виділити:

1. Автоматизацію збору та обробки інформації. Використання штучного інтелекту та алгоритмів машинного навчання для аналізу великих даних (Big Data). Інтеграцію автоматизованих аналітичних платформ, що дозволяють швидко ідентифікувати загрози та прогнозувати їхній розвиток [6].

2. Зміцнення міжвідомчої координації. Посилення взаємодії між державними структурами через створення єдиної національної системи інформаційного обміну. Підвищення ефективності комунікації між аналітичними підрозділами різних відомств з метою уникнення дублювання функцій та забезпечення узгоджених дій.

3. Підвищення рівня професійної підготовки аналітиків. Розширення програм підготовки кадрів у сфері стратегічного аналізу, управління інформаційними ризиками та кібербезпеки. Запровадження системи підвищення кваліфікації для працівників аналітичних центрів та силових структур [5].

4. Розвиток інформаційної безпеки та протидія дезінформації. Впровадження національної стратегії боротьби з інформаційними загрозами. Моніторинг кіберпростору та аналіз інформаційних кампаній, спрямованих на дестабілізацію ситуації в країні.

Таким чином, інституціональні засади аналітичної діяльності в умовах інформаційного суспільства передбачають інтеграцію сучасних технологій, посилення координації між суб'єктами безпеки та вдосконалення професійної підготовки аналітиків. Лише системний підхід до розвитку аналітичних структур дозволить забезпечити ефективне управління ризиками та адекватне реагування на виклики національній безпеці.

Висновки. Дослідження проблематики управління проєктами, комунікативного забезпечення та лідерства у сфері національної безпеки в умовах інформаційного суспільства дозволяє зробити ряд важливих висновків. По-перше, ефективне управління безпековими проєктами потребує застосування сучасних методологій, таких як PMBOK, PRINCE2 та Agile. Вони дозволяють підвищити рівень планування, оптимізувати використання ресурсів та забезпечити адаптивність до змін у безпековому середовищі. Важливим аспектом є впровадження цифрових технологій для аналізу загроз, автоматизації процесів управління ризиками та покращення координації між державними структурами [5]. По-друге, комунікативне забезпечення відіграє ключову роль у функціонуванні системи національної безпеки. Використання сучасних інформаційних технологій, стратегічних комунікацій та цифрових платформ дозволяє оперативно реагувати на виклики, здійснювати ефективний обмін інформацією між державними структурами та міжнародними партнерами. Одним із основних викликів у цьому аспекті є необхідність протидії дезінформації та забезпечення кібербезпеки інформаційних ресурсів держави [4]. По-третє, лідерство є визначальним фактором успіху у сфері національної безпеки. В умовах швидкоплинних загроз керівники безпекових структур повинні володіти стратегічним мисленням, здатністю до адаптації, кризовим менеджментом та компетентністю у цифрових технологіях. Особливу роль відіграє розвиток трансформаційного та діджитал-лідерства, яке дозволяє ефективно управляти складними безпековими проєктами та впроваджувати інноваційні рішення [3]. По-четверте, інституціональні засади аналітичної діяльності повинні ґрунтуватися на розвитку технологічних рішень, міжвідомчій координації та посиленні інформаційної безпеки. В умовах глобальної цифровізації національні аналітичні центри мають інтегрувати технології штучного інтелекту, автоматизовані системи аналізу великих даних та алгоритми прогнозного аналізу для ефективного моніторингу загроз [6]. Отже, управління проєктами, комунікативне забезпечення та лідерство у сфері національної безпеки є тісно взаємопов'язаними компонентами, що визначають ефективність реалізації державної безпекової

політики. Для підвищення рівня національної безпеки необхідно впроваджувати міжнародні стандарти управління, розвивати цифрові аналітичні платформи, зміцнювати стратегічні комунікації та формувати компетентне лідерство. Подальші дослідження мають бути спрямовані на розробку методик оцінювання ефективності безпекових програм, інтеграцію штучного інтелекту в процеси аналізу ризиків та удосконалення механізмів міжнародної співпраці у сфері безпеки.

ЛІТЕРАТУРА:

1. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. К.: Університет «Україна», 2014. 417 с.

2. Ситник Г. П., Орел М.Г. С41 Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. Київ: Міжрегіональна Академія управління персоналом, 2021. 372 с.

3. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія / Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с.

4. Соколов В.А., Шевченко М.М. Методологічні підходи до оцінювання ефективності функціонування державного механізму інформаційно-аналітичного забезпечення політики національної безпеки. Інвестиції: практика та досвід. 2020. № 1. С. 148-154.

5. Цепенда І.Є., Кропельницька С.О. (ред.) (2021). Керівництво з управління проектами розвитку: інтерактивний навчальний посібник. Івано-Франківськ: Видавництво "Агенти змін". URL: https://agentyzmin.pnu.edu.ua/wp-content/uploads/2021/04/PM_AgentyZminPNU_Book-1-%D1%81%D1%82%D0%B8%D1%81%D0%BD%D1%83%D1%82%D0%BE.pdf

6. Інновації і трансфер технологій: методи, моделі та механізми управління: колективна монографія / за ред. д.е.н. В.А. Омельяненка. Суми: Інститут стратегій інноваційного розвитку і трансферу знань. 2023. 370 с.