The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Received: *April 7, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *May 25, 2026* | **Published Online:** *August 5, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.2.20

Формування алгоритму системного оцінювання та стратегічного планування у сфері національної безпеки

Василь Школяренко
кандидат технічних наук, старший науковий співробітник
Воєнна академія імені Євгенія Березняка
04050, вулиця Юрія Іллєнка, 81, Київ, Україна
e-mail: vasyl1970@yahoo.com
ORCID: 0000-0001-8274-2232

Анотація. У статті досліджено теоретико-методологічні засади формування алгоритму системного оцінювання та стратегічного планування у сфері національної безпеки в умовах зростання багатовимірних загроз і високої невизначеності безпекового середовища. Стаття має на меті розробити механізм комплексного оцінювання й перспективного планування в галузі національної безпеки шляхом поєднання новітніх методологій, аналізу ризиків, узгодження дій між відомствами та гнучкого менеджменту. В основу дослідження покладено системний, ризик-орієнтований, інституційний, сценарний та адаптивний підходи, які дозволяють комплексно аналізувати безпекове середовище, взаємозв'язки між загрозами, спроможностями держави та механізмами стратегічного управління, причому системний підхід трактує національну безпеку як взаємопов'язану систему політичних, військових, економічних, інформаційних, соціальних, кібернетичних та інфраструктурних компонентів, ризик-орієнтований підхід використовується для ідентифікації, класифікації та пріоритизації загроз на основі ієрархічного аналізу ризиків, оцінювання ймовірності реалізації загроз, масштабу їх наслідків, швидкості ескалації та рівня вразливості системи, а принцип адаптивного управління забезпечує постійне оновлення рішень, коригування цілей і ресурсів залежно від змін безпекового середовища, що в сукупності формує комплексний, міждисциплінарний та доказовий підхід до розробки алгоритму системного оцінювання та стратегічного планування у сфері національної безпеки. Обґрунтовано необхідність переходу від фрагментарного реагування на окремі виклики до комплексного, адаптивного та доказового стратегічного управління. Визначено сутність понять "оцінювання", "системне оцінювання" та "стратегічне планування", а також розкрито їх взаємозв'язок у межах єдиного управлінського циклу. Доведено, що системне оцінювання виступає інформаційно-аналітичною основою стратегічного планування, забезпечуючи своєчасне виявлення загроз, оцінювання ризиків, аналіз спроможностей держави та підтримку процесу ухвалення управлінських рішень. На основі аналізу сучасних наукових підходів, міжнародного досвіду та ризик-орієнтованих методів запропоновано алгоритм системного оцінювання й стратегічного планування у сфері національної безпеки. Алгоритм охоплює послідовність взаємопов'язаних кроків: ідентифікацію проблеми, вивчення стратегічного середовища, збирання і верифікацію даних, оцінювання загроз і ризиків, встановлення зацікавлених сторін, аналіз їх центрів тяжіння, формування стратегічних цілей і показників результативності, оцінювання ресурсів, критичний аналіз спроможностей, розроблення та вибір стратегічних альтернатив, планування реалізації, застосування стратегії, моніторинг, оцінювання та

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

адаптивне коригування рішень. Особливу увагу приділено використанню сучасних аналітичних інструментів, зокрема SWOT-аналізу, сценарного моделювання, PESTLE-, STEEPLEMS-, CoG-аналізу, багатокритеріального оцінювання, ризик-аналізу та DIME-підходу. Визначено роль міжвідомчої координації, ситуаційної обізнаності, стратегічних комунікацій і цифрових технологій у забезпеченні стійкості сектору безпеки й оборони. Наголошено на важливості інтеграції штучного інтелекту та прогнозної аналітики у процеси оцінювання ризиків і підтримки ухвалення стратегічних рішень. Запропонований алгоритм дозволяє забезпечити цілісність стратегічного управління, підвищити ефективність використання ресурсів, покращити адаптивність державної політики та посилити спроможність держави реагувати на сучасні гібридні загрози.

Ключові слова: національна безпека; системне оцінювання; стратегічне планування; ризик-аналіз; загрози; стратегічне середовище; адаптивне управління; сектор безпеки й оборони.

Вступ (Introduction)

Сучасне безпекове середовище характеризується високим рівнем невизначеності, динамічністю та багатовимірністю загроз. Поєднання воєнних, кібернетичних, інформаційних, економічних та соціальних викликів вимагає переходу від фрагментарного реагування до системного стратегічного управління у сфері національної безпеки. Особливої актуальності це набуває для України в умовах воєнного стану, коли ефективність державної політики безпосередньо залежить від здатності інтегрувати оцінювання ризиків, прогнозування загроз та стратегічне планування в єдиний управлінський алгоритм.

У науковій літературі поняття “оцінювання” розглядається як процес визначення стану, результативності, рівня ефективності або ступеня відповідності певного об’єкта встановленим критеріям, показникам чи цілям. У сфері національної безпеки оцінювання спрямоване на аналіз ризиків, загроз, вразливостей та спроможностей держави щодо забезпечення стійкості й захисту національних інтересів. В. Ду та Х. Чен запропонували комплексний метод прогнозування ризиків для оборонного планування, що ґрунтується на імовірнісному міркуванні та ієрархічному аналізі [1], що є важливим для формування обґрунтованих стратегічних альтернатив у сфері оборони та безпеки.

Водночас сучасні виклики потребують переходу від фрагментарного оцінювання окремих загроз до системного оцінювання, яке базується на комплексному аналізі взаємопов’язаних елементів безпекового середовища. Системне оцінювання доцільно визначати як інтегрований процес збирання, аналізу, інтерпретації та узагальнення інформації про стан безпеки держави, що здійснюється з урахуванням взаємозалежності політичних, економічних, військових, соціальних, інформаційних, технологічних та інших факторів. Його метою є формування цілісного бачення загроз, ризиків і спроможностей держави для забезпечення обґрунтованого ухвалення стратегічних рішень.

Важливість системного оцінювання зумовлюється й тим, що сучасне безпекове середовище характеризується високим рівнем невизначеності. Як зазначають Дж. Бахші та М. Ефатманешнік, безпекові системи функціонують у контексті постійної взаємодії складних факторів, тому оцінювання має враховувати не лише наявні ресурси, а й здатність держави адаптуватися до змін і діяти в умовах нестабільності [2]. У цьому контексті особливого значення набувають адаптивність, міжвідомча координація та ситуаційна обізнаність.

Системне оцінювання враховує каскадний характер сучасних загроз, коли криза в одній сфері здатна спричинити дестабілізацію інших секторів. Так, кібератаки можуть впливати на функціонування критичної інфраструктури, інформаційні операції – на суспільну стійкість і політичну стабільність, а економічні ризики – на обороноздатність держави. Саме тому

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

системне оцінювання має здійснюватися в межах єдиної логіки комплексної безпеки.

Системне оцінювання виконує низку ключових функцій у сфері національної безпеки. По-перше, воно забезпечує своєчасне виявлення загроз і ризиків. По-друге, дозволяє визначати рівень готовності сектору безпеки й оборони до реагування на кризові ситуації. По-третє, створює інформаційно-аналітичне підґрунтя для формування державної політики та ухвалення стратегічних рішень. Крім того, системне оцінювання сприяє підвищенню ефективності використання ресурсів, координації діяльності суб'єктів та адаптації управлінських механізмів до змін безпекового середовища. З. Здравков та А. Атіпова запропонували методологію оцінювання системи національної безпеки. [3]. Цей підхід орієнтований на комплексне вивчення структури, функцій і результативності системи.

В умовах цифровізації та розвитку штучного інтелекту системне оцінювання дедалі більше інтегрується з сучасними технологіями оброблення даних, прогнозної аналітики та підтримки ухвалення рішень. Дослідження І. Адабара та співавторів доводять, що надійні системи штучного інтелекту можуть суттєво підвищити якість стратегічного аналізу та ситуаційної обізнаності, а також забезпечення кіберстійкості [4]. Аналогічно М. Гоффер та співавтори наголошують на важливості використання ШІ-технологій для виявлення кіберзагроз і захисту критичної інфраструктури [5]. С. Хідаятулла, А. Супріяді, І. Пурванто та Г. Сапутро аналізують реформування національної оборонної політики із застосуванням ШІ. Автори наголошують, що ШІ може підвищити якість стратегічного ухвалення рішень, однак його використання має супроводжуватися етичним регулюванням і належним інституційним контролем [6].

Когнітивні й комп'ютерні аспекти управління ситуаціями розглядають К. Бацлавський та його співавтори, зокрема, питання ситуаційної обізнаності, підтримки ухвалення рішень та оброблення складної інформації у динамічних середовищах. Такі напрацювання мають значення для побудови систем стратегічного оцінювання, оскільки дозволяють поєднати когнітивні моделі аналізу з цифровими інструментами моніторингу та прогнозування [7].

Логічним продовженням системного оцінювання виступає стратегічне планування, оскільки саме результати оцінювання формують основу для визначення стратегічних цілей, пріоритетів і механізмів реагування. Стратегічне планування у сфері національної безпеки доцільно розглядати як цілеспрямований процес формування довгострокових цілей, визначення шляхів їх досягнення, розподілу ресурсів та координації діяльності суб'єктів сектору безпеки й оборони з метою забезпечення стійкості та захисту національних інтересів.

Тобто системне оцінювання і стратегічне планування перебувають у тісному взаємозв'язку та утворюють єдиний управлінський цикл. Системне оцінювання забезпечує інформаційно-аналітичну основу стратегічного планування, тоді як стратегічне планування трансформує результати оцінювання у конкретні рішення. Як зазначає Т. Тагарєв, ефективна оборонна політика має базуватися на поєднанні оцінювання загроз, аналізу спроможностей і визначення критеріїв адаптивності, стійкості та реалізації стратегії [8].

Отже, у сучасних умовах системне оцінювання стає необхідною передумовою для ефективного стратегічного планування у сфері національної безпеки.

Огляд літератури (Literature review)

Проблематика системного оцінювання та стратегічного планування у сфері національної безпеки активно досліджується у сучасній науковій літературі, що зумовлено ускладненням безпекового середовища, поширенням гібридних загроз, зростанням ролі штучного інтелекту та необхідністю підвищення адаптивності державної політики.

М. Миколайчук та співавтори досліджують концептуальні засади аналізу й прогнозування загроз національній безпеці в сучасних умовах. У центрі їхньої уваги

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

перебувають методи виявлення загроз, прогнозування їх розвитку та формування управлінських відповідей. Це дослідження є важливим для обґрунтування необхідності прогнозної компоненти в системі стратегічного оцінювання [9].

Т. Паламарчук та співавтори розглядають стратегічні передбачення і механізми випереджального реагування у контексті національної безпеки. Автори підкреслюють значення сценарного аналізу, раннього попередження та адаптивного планування для запобігання кризам і підвищення стійкості держави [10].

Х. Пірес та Л. Гімарайнш запропонували модель динамічного оцінювання цілей і загроз у контексті протиповітряної оборони. Їхнє дослідження демонструє важливість оперативного оновлення оцінки загроз, пріоритизації цілей та ухвалення рішень у режимі високої невизначеності [11].

А. Сергейте аналізує вплив збирання розвідувальної інформації, аналізу ризиків і сценарного планування на формування оборонної політики. Автор доводить, що якість оборонної політики залежить від системного поєднання розвідувальних даних, оцінювання ризиків та моделювання можливих сценаріїв розвитку подій [12].

О. Маслій та Р. Галушка досліджують ієрархічний аналіз ризиків і загроз економічній безпеці України в умовах воєнного стану. Автори акцентують на необхідності ранжування загроз за рівнем їхнього впливу, ймовірністю реалізації та наслідками для стійкості держави. Їхній підхід є важливим для формування ризик-орієнтованої моделі стратегічного планування, оскільки дозволяє визначати пріоритети державного реагування в умовах обмежених ресурсів [13].

У працях, присвячених використанню штучного інтелекту у сфері безпеки, особлива увага приділяється питанням довіри, етичного врядування та захисту від нових технологічних ризиків. Праця Х. Сейфович, А. Врчіч Амар і А. Авдович присвячена психологічним аспектам сприйняття реальності та впливу фантазійної схильності на психологічне життя й здоров'я. Її положення можуть бути використані в контексті аналізу інформаційно-психологічної безпеки, соціальної стійкості та вразливості населення до маніпулятивних впливів [14].

З вищевикладеного випливає, що сучасна наукова думка зосереджується на кількох ключових напрямах: аналізі спроможностей сектору безпеки й оборони, застосуванні сценарного планування, ризик-орієнтованому оцінюванні загроз, використанні штучного інтелекту та формуванні адаптивних механізмів стратегічного управління. Водночас недостатньо розробленим залишається питання інтеграції цих підходів у єдиний алгоритм.

Тому метою цієї статті є формування алгоритму системного оцінювання та стратегічного планування у сфері національної безпеки на основі інтеграції сучасних методологічних підходів, ризик-аналізу, міжвідомчої координації та адаптивного управління.

Методологічна основа (Methodological Framework)

В основу дослідження покладено системний, ризик-орієнтований, інституційний, сценарний та адаптивний підходи, які дозволяють комплексно аналізувати безпекове середовище, взаємозв'язки між загрозами, спроможностями держави та механізмами стратегічного управління.

Ключовим є системний підхід, відповідно до якого національна безпека розглядається як взаємопов'язана система політичних, військових, економічних, інформаційних, соціальних, кібернетичних та інфраструктурних компонентів. Ризик-орієнтований підхід використовується для ідентифікації, класифікації та пріоритизації загроз. Його застосування ґрунтується на положеннях ієрархічного аналізу ризиків, оцінювання ймовірності реалізації загроз, масштабу їх наслідків, швидкості ескалації та рівня вразливості системи.

Методологічна основа дослідження також спирається на принцип адаптивного

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

управління, відповідно до якого система стратегічного планування має забезпечувати постійне оновлення рішень, коригування цілей і ресурсів залежно від змін безпекового середовища. Запропонована методологічна основа забезпечує комплексний, міждисциплінарний та доказовий підхід до формування алгоритму системного оцінювання та стратегічного планування у сфері національної безпеки.

Результати і обговорення (Results and Discussions)

Для вироблення ефективної державної політики національної безпеки слід використовувати алгоритм, який забезпечить послідовність оцінювання, інтеграцію даних і узгодження рішень між інституціями сектору безпеки й оборони. Алгоритм доцільно будувати на низці базових принципів, які забезпечують його наукову обґрунтованість і практичну придатність у сфері національної безпеки. Передусім ідеться про принцип цілісності, що передбачає розгляд безпеки не як суми окремих напрямів, а як взаємопов'язаної системи політичних, військових, економічних, соціальних, інформаційних і технологічних компонентів. Такий підхід дозволяє бачити причинно-наслідкові зв'язки між загрозами та враховувати каскадні ефекти рішень. Не менш важливим є принцип доказовості, відповідно до якого стратегічні рішення мають спиратися на перевірені дані, результати оцінювання ризиків, моделювання сценаріїв і фахові експертні висновки. Це мінімізує суб'єктивність, посилює якість прогнозів і підвищує аргументованість вибору пріоритетів.

Алгоритм має бути адаптивним, тобто передбачати можливість швидкого уточнення цілей, заходів і ресурсів у разі зміни загроз, появи нових ризиків або трансформації операційного середовища. Адаптивність дає змогу підтримувати актуальність стратегії в умовах невизначеності та гібридних впливів. В основі також має лежати принцип субсидіарності та багаторівневого врядування, який означає узгодження рішень між національним, регіональним і місцевим рівнями та розподіл відповідальності відповідно до повноважень і спроможностей. Це забезпечує реалістичність виконання стратегічних завдань і врахування специфіки територій.

Окремо слід підкреслити принцип координації та сумісності, що спрямований на узгодження політик між органами влади, суб'єктами сектору безпеки й оборони та партнерами. Його реалізація знижує ризики фрагментації, дублювання функцій і суперечливих рішень, підвищуючи цілісність державної безпекової політики. Нарешті, алгоритм має відповідати принципу підзвітності та прозорості, закладаючи механізми контролю, комунікації та зворотного зв'язку в межах можливого з огляду на режим доступу до інформації. Це створює умови для підвищення довіри до стратегічних рішень, контролю їх реалізації та своєчасного коригування на основі результатів оцінювання.

Алгоритм системного оцінювання політики й стратегічного планування у сфері національної безпеки доцільно визначити як структуровану послідовність аналітичних і управлінських кроків (табл. 1.). Такий алгоритм поєднує логіку системного аналізу, ризик-орієнтованого управління, стратегічного планування, міжвідомчої координації та програмно-цільового підходу.

Розглянемо послідовно кожний крок.

Крок 1. Ідентифікація та постановка проблеми. Перший крок алгоритму є базовою складовою стратегічного планування у сфері національної безпеки, оскільки саме на цьому етапі визначаються предмет аналізу, його межі, цілі та критерії оцінювання. Фактично формується початкова рамка стратегування: які загрози вважаються пріоритетними, які сфери безпеки охоплюються, які суб'єкти залучаються до процесу та які результати мають бути досягнуті.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Таблиця 1. Блок-схема алгоритму системного оцінювання і стратегічного планування у сфері національної безпеки

Процедурні кроки	Методи та інструменти	Вихідні дані	Результати
Крок 1. Ідентифікація та постановка проблеми	Структуризація проблеми; дерево проблем; SMART-цілі	Запит / доручення; чинні стратегічні документи; попередні оцінки ризиків; правові рамки	Чітко сформульована стратегічна проблема; межі аналізу; критерії успіху; остаточне визначення групи експертів для проведення стратегічного планування
Крок 2. Вивчення стратегічного середовища	STEEPLEMS-аналіз; PESTLE; факторний аналіз; foresight	Геополітичні тренди; соціально-економічні показники; міжнародні звіти; безпекові прогнози	Визначені ключові фактори впливу; сценарії розвитку середовища; безпекові тенденції
Крок 3. Збирання даних і формування інформаційного поля	Data mapping; Delphi-опитування; аудит і верифікація даних; пріоритизація вимог до розвідувальної інформації та відповідне планування розвідки	Статистика; розвіддані (у межах допуску); соціологія; міжнародні індекси; дані КІ	Узгоджений операційний портрет безпекового середовища; консолідована база даних
Крок 4. Визначення та оцінювання зацікавлених сторін	Аналіз стейкхолдерів; мережевий аналіз; діаграми впливу акторів; аналіз ланцюгів відповідальності	Перелік акторів з оцінкою їх інтересу і впливу; повноваження органів; протоколи взаємодії; меморандуми; карта партнерств	Карта акторів; розподіл ролей і відповідальності; пропозиції з міжвідомчої координації
Крок 5. Аналіз центрів тяжіння	CoG-аналіз (аналіз центру тяжіння); визначення критичних можливостей, потреб і вразливостей	Дані про спроможності, потреби та вразливості ключових акторів; перелік умов, дій та заходів, які необхідно встановити чи провести	Визначені центри тяжіння; критичні вразливості; напрями впливу та захисту
Крок 6. Оцінювання власних засобів (ресурсів) /Діагностика спроможностей сектору безпеки та оборони	DIME-analysis; ресурсний аудит; capability assessment	Бюджетні дані; людський капітал; список спроможностей; міжнародна підтримка	Оцінка доступних ресурсів; виявлені ресурсні обмеження; карта наявних інструментів впливу
Крок 7: Критичне оцінювання ситуації	SWOT-analysis	Систематизація своїх сильних та слабких сторін, зовнішні загрози та можливості	Карта спроможностей; виявлені “вузькі місця”; перелік критичних прогалин і пріоритетів посилення
Крок 8. Формування стратегічних цілей, пріоритетів та KPI	Програмно-цільовий підхід; KPI-analysis; логічні моделі	Оцінка ризиків; gap-аналіз; ресурсні обмеження; пріоритизація національних інтересів	Дерево цілей; стратегічні пріоритети; система показників результативності
Крок 9. Розроблення альтернативних стратегій	AHP; MAUT; дерево рішень; аналіз чутливості	Сценарії; критерії оцінки; оцінка ресурсів і ризиків; експертні висновки	Альтернативні стратегії
Крок 10. Оцінювання альтернативних стратегій та аналіз ризиків	Сценарний аналіз; воєнна гра; red teaming; матриця ризиків; крос-імпакт; критеріальний аналіз; порівняльний аналіз	База загроз; тренди; карти інцидентів; індикатори вразливості; оцінки альтернативних варіантів за критеріями	Пріоритизований реєстр загроз; профілі ризиків; карти каскадних ефектів; рекомендації щодо вибору оптимальної стратегії
Крок 11. Вибір оптимальної стратегії та розроблення плану реалізації (ресурси, інструменти, дорожня карта)	Управління програмами; бюджетування; стандартизація	Обрана стратегія; план заходів; фінансові та кадрові ліміти; правові зміни	Деталізований план реалізації; механізми координації; протоколи обміну даними
Крок 12. Застосування стратегії	Стратегічні комунікації; кризовий менеджмент; управління змінами	Затверджені програми; координаційні механізми; оперативні рішення	Реалізація стратегічних заходів; підтримання стійкості системи; адаптація до змін
Крок 13. Моніторинг, оцінювання	KPI-моніторинг; аудит; експертне оцінювання; red teaming	Звіти; індикатори; реєстр інцидентів; результати навчань	Оцінка ефективності стратегії; виявлені відхилення; оновлені аналітичні висновки
Крок 14. Адаптивне коригування стратегії	Adaptive governance; lessons learned; сценарне оновлення	Результати моніторингу; нові ризики; кризові сценарії	Коригування стратегії; оновлення ризик-реєстру

Налаштування обговорення є важливою складовою цього кроку. Попри те, що політика традиційно визначає загальні орієнтири для стратегії, на практиці стратегічне планування

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

рідко здійснюється за умов повної визначеності. Саме тому першочерговим завданням є досягнення спільного розуміння того, яких результатів необхідно досягти та чому це має стратегічне значення. Для цього доцільним є проведення відкритого експертного обговорення, під час якого аналізуються природа проблеми, її причини, наслідки та взаємозв'язок із національними інтересами держави. Такі дискусії дозволяють сформувати узгоджене бачення проблеми, визначити її пріоритетність і виявити інформацію, необхідну для подальшого стратегічного аналізу.

Ідентифікація проблеми ґрунтується на розумінні того, що сучасні загрози мають комплексний і взаємопов'язаний характер. Вони можуть проявлятися у вигляді кіберзагроз, інформаційних впливів, криз критичної інфраструктури, економічної нестабільності чи безпекових викликів воєнного характеру. Тому стратегічна проблема розглядається не як окремий інцидент, а як системне порушення стійкості держави та її інституцій.

Важливим завданням є розмежування симптомів, причин і наслідків проблеми. Симптомами можуть бути зростання кількості кібератак, перебої у роботі інфраструктури або зниження рівня суспільної довіри. Причинами виступають внутрішні слабкості системи: технологічна застарілість, кадровий дефіцит, прогалини у правовому регулюванні чи недостатня міжвідомча координація. Наслідки ж відображають реальний вплив загроз на функціонування держави – економічні втрати, порушення роботи критичних систем, соціальну напругу та послаблення національної стійкості.

Для забезпечення ефективності стратегічного планування проблема має бути сформульована в категоріях вимірюваності та керованості. Це дозволяє перейти від загальних декларацій до конкретних цілей, індикаторів і механізмів оцінювання результатів політики. Наприклад, замість абстрактного завдання "посилення кібербезпеки" доцільніше визначати конкретні параметри: скорочення часу реагування на інциденти, підвищення рівня захищеності критичної інфраструктури чи посилення спроможностей до відновлення систем після атак.

Після визначення проблеми формується рамка оцінювання, яка охоплює часові горизонти, рівні безпеки та сфери аналізу. Короткострокова перспектива орієнтована на оперативне реагування, середньострокова – на розвиток інституційних спроможностей, а довгострокова – на підвищення стратегічної стійкості держави. Одночасно визначаються рівні безпеки – національний, регіональний і місцевий, оскільки одна й та сама загроза може мати різний характер і наслідки залежно від масштабу управління.

Окрему увагу приділяють визначенню обмежень стратегічного планування. До них належать правові норми, ресурсні можливості, кадровий потенціал, технічні спроможності та інституційні бар'єри. Урахування таких обмежень дозволяє уникнути формування нереалістичних стратегій, які неможливо реалізувати на практиці.

Завершальним елементом першого кроку є формування ключових аналітичних запитань і критеріїв успішності політики. Вони мають визначати, які загрози є критичними, які вразливості мають найбільший вплив на стійкість системи, які ресурси доступні та яким чином оцінюватиметься результативність державної політики. Критеріями успішності доцільно вважати ефективність реагування, рівень координації, стійкість системи, адаптивність і здатність до відновлення після кризових ситуацій.

Крок 2. Вивчення стратегічного середовища. Після визначення суті проблеми наступним важливим кроком є аналіз стратегічного середовища, у межах якого необхідно з'ясувати, яким чином сама проблема впливає на безпекову ситуацію та як зовнішні й внутрішні чинники можуть впливати на можливості її вирішення. У сучасних умовах національна безпека формується під впливом великої кількості взаємопов'язаних процесів, тому стратегічне середовище слід розглядати комплексно та динамічно.

У практиці стратегічного аналізу не існує єдиного універсального підходу до оцінювання

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

середовища безпеки. Проте ефективність дослідження значно підвищується при використанні структурованих моделей аналізу, які дозволяють систематизувати фактори впливу та виявити їхній взаємозв'язок. Однією з найбільш поширених і результативних моделей є STEEPLEMS, що охоплює соціальні, технологічні, економічні, екологічні, політичні, правові, етичні, військові та безпекові аспекти стратегічного середовища.

Соціальний вимір дає можливість оцінити рівень суспільної стійкості, демографічні процеси, соціальні настрої та довіру населення до державних інституцій. Технологічний компонент дозволяє визначити вплив цифровізації, розвитку штучного інтелекту, кіберзагроз і новітніх технологій на безпекову сферу. Економічний аспект охоплює фінансову стійкість держави, ресурсні можливості та економічні ризики. Водночас політичні й правові чинники визначають ефективність державного управління, стан політичної системи, стабільність інституцій та нормативно-правові умови реалізації безпекової політики.

Окреме значення мають військові та безпекові фактори, оскільки саме вони формують рівень готовності держави до реагування на зовнішні й внутрішні загрози. Не менш важливими є екологічні та етичні аспекти, які дедалі більше впливають на сучасне безпекове середовище, особливо в умовах глобальних криз, інформаційних впливів та гуманітарних викликів.

Під час аналізу кожного з факторів важливо не обмежуватися лише їх описом, а намагатися зрозуміти практичні наслідки для національної безпеки, використовуючи інструмент факторного аналізу. Саме тому ключовим елементом цього кроку є постійне критичне осмислення: як певний фактор може вплинути на реалізацію стратегії, які ризики або можливості він створює та яким чином змінює загальне безпекове середовище. Такий підхід дозволяє перейти від простого переліку чинників до формування аналітичних висновків і прогнозів.

Важливу роль у процесі вивчення стратегічного середовища відіграють експерти – як внутрішні, так і зовнішні. Їх залучення дозволяє врахувати різні точки зору, уникнути однобічності оцінок та підвищити якість стратегічного аналізу. Особливо це важливо в умовах невизначеності та швидкої трансформації загроз, коли ефективність державної політики значною мірою залежить від здатності своєчасно виявляти нові тенденції та адаптуватися до змін.

У результаті цього кроку мають бути визначені ключові стратегічні фактори – тобто ті чинники, які найбільше впливають на реалізацію стратегії, захист національних інтересів і забезпечення стійкості держави. Подальше групування цих факторів та узагальнення отриманих висновків створюють основу для оцінювання ризиків, формування стратегічних цілей і вибору оптимальних напрямів державної політики у сфері національної безпеки.

Крок 3. Наступний крок алгоритму передбачає створення цілісної інформаційної бази для подальшого оцінювання загроз, аналізу ризиків і вибору стратегічних рішень у сфері національної безпеки. Якщо попередні кроки визначають сутність проблеми та особливості стратегічного середовища, то на цьому кроці формується інформаційне підґрунтя, на основі якого здійснюється подальший аналіз.

Основною метою є об'єднання даних із різних джерел у єдиний інформаційний простір, де інформація є узгодженою, перевіреною та придатною для аналітичної роботи. У сфері національної безпеки це особливо важливо, оскільки різні органи влади та структури сектору безпеки і оборони працюють із неоднаковими форматами даних і процедурами їх збирання. Саме тому формування інформаційного поля потребує не лише технічної сумісності, а й чіткої координації між суб'єктами стратегування.

Інформаційне поле охоплює широкий спектр джерел: офіційну державну статистику, адміністративні реєстри, аналітику сектору безпеки й оборони, матеріали розвідувального характеру, результати правоохоронної діяльності та моніторинг кризових процесів. Важливу

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

роль відіграє також інформація з відкритих джерел, яка містить дані медіа, соціальних мереж, аналітичних центрів, міжнародних організацій і наукових досліджень. Такі джерела дозволяють оперативно відстежувати зміни безпекового середовища та виявляти нові тенденції.

Окреме значення мають соціологічні дослідження та моніторинг громадської думки, оскільки рівень суспільної довіри, соціальної стійкості та готовності населення до кризових ситуацій безпосередньо впливає на національну безпеку. Водночас аналіз кіберінцидентів і стану критичної інфраструктури дозволяє оцінити реальний рівень кіберстійкості держави, визначити вразливі елементи системи та пріоритетні напрями захисту.

Для забезпечення якості стратегічного аналізу дані мають проходити перевірку, узгодження та систематизацію. Це передбачає виявлення суперечностей між джерелами, оцінювання достовірності інформації та дотримання вимог щодо захисту даних і режиму секретності. У результаті формується єдина картина безпекового середовища, яка відображає ключові загрози, вразливості, ресурси та спроможності держави. Саме така узгоджена інформаційна база створює основу для подальшого стратегічного оцінювання та ухвалення обґрунтованих управлінських рішень.

Крок 4. Визначення та оцінювання зацікавлених сторін. Цей крок алгоритму спрямований на визначення ключових акторів у системі забезпечення національної безпеки, серед яких не останньою чергою – зовнішні, та оцінювання їхньої ролі у формуванні (впливу на формування) й реалізації стратегічних рішень. У цьому контексті система розглядається як взаємопов’язане середовище, у межах якого реалізується стратегія та взаємодіють державні й недержавні суб’єкти.

До зацікавлених сторін можуть належати органи сектору безпеки й оборони, центральні та місцеві органи влади, суб’єкти критичної інфраструктури, приватний сектор, міжнародні партнери, громадські організації, медіа, а також потенційні противники чи інші актори, які прямо або опосередковано впливають на безпекову політику. Сучасні загрози мають комплексний характер, тому ефективність державної політики значною мірою залежить від врахування взаємодії між цими суб’єктами.

Після визначення кола учасників здійснюється оцінювання їхніх повноважень, ресурсів, інтересів та рівня впливу на процес реалізації стратегії. Особливу увагу приділяють співвідношенню двох показників: рівня впливу актора на систему, ступеня його зацікавленості у вирішенні проблеми.

Такий підхід дозволяє визначити ключових партнерів, потенційних союзників чи противників або суб’єктів, здатних блокувати реалізацію політики. Актори, які мають високий рівень впливу та значний інтерес, потребують першочергової уваги в процесі стратегічного планування.

Важливо також оцінювати можливу поведінку кожного учасника в різних сценаріях розвитку ситуації. Для цього аналізуються його політичні цілі, мотивація, доступ до ресурсів, здатність впливати на ухвалення рішень і потенційна реакція на кризові процеси.

На основі отриманих результатів формується карта взаємодії, яка відображає інформаційні, управлінські та ресурсні зв’язки між учасниками системи.

Результатом цього кроку має стати узгоджена модель координації, яка визначає ключових стейкхолдерів, їхні ролі, зони відповідальності та механізми взаємодії. Це створює основу для подальшого формування реалістичних стратегічних рішень і забезпечує керованість політики у сфері національної безпеки.

Крок 5. Аналіз центрів тяжіння. Ті учасники системи, які мають значний рівень впливу та високий інтерес до проблеми, потребують особливої уваги, оскільки саме від взаємодії з ними або здатності ефективно їм протидіяти часто залежить успішність реалізації стратегії. Для глибшого розуміння ролі таких акторів доцільно застосовувати аналіз центру тяжіння.

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Поняття “центр тяжіння” походить із військово-стратегічної теорії К. фон Клаузевіца, який визначав його як “місце, де сконцентрована вся рушійна сила, від якої все залежить” [15]. У сучасному стратегічному плануванні цей підхід використовується для виявлення ключового елемента, що забезпечує актору його силу, стійкість або здатність впливати на розвиток ситуації. Метою такого аналізу є визначення основної характеристики або ресурсу, який забезпечує суб’єкту можливість досягати своїх цілей у конкретних умовах. Центрами тяжіння можуть бути суспільна підтримка, політична легітимність, згуртованість союзників, економічні ресурси, технологічна перевага, військовий потенціал, інформаційний вплив або авторитет стратегічного лідера. У різних ситуаціях саме ці фактори визначають стійкість актора та його здатність впливати на безпекове середовище (рис.1).

Після визначення центрів тяжіння стратегія має бути спрямована, з одного боку, на захист власних критично важливих елементів і підтримку партнерів, а з іншого – на зниження спроможностей противника або нейтралізацію його ключових переваг. Такий підхід дозволяє концентрувати ресурси на найбільш важливих напрямах і підвищує ефективність рішень.

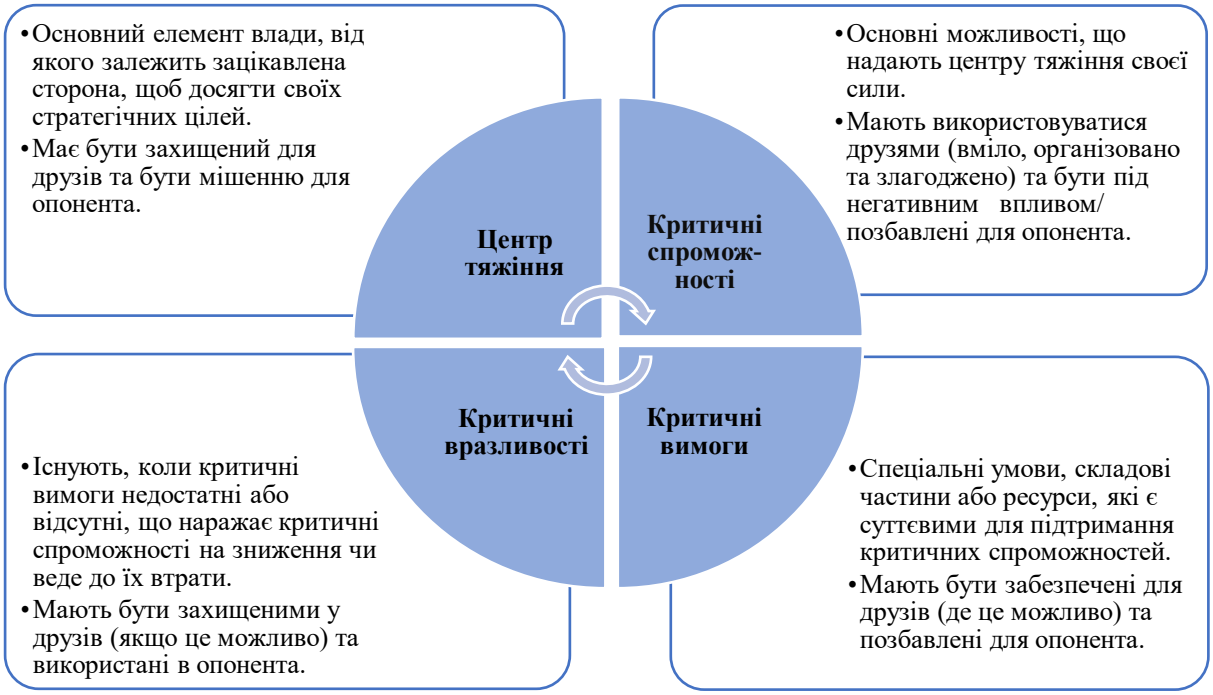


Рисунок 1. Аналіз центру тяжіння

На практиці визначити центр тяжіння не завжди просто. Тому доцільно спочатку аналізувати критичні можливості, потреби та вразливості кожного актора. Це допомагає зрозуміти, від чого залежить його стійкість, які ресурси є для нього ключовими та які фактори можуть посилити або послабити його позиції. Водночас аналіз центрів тяжіння не є одноразовою процедурою. У процесі розвитку кризових ситуацій, зміни безпекового середовища та появи нових факторів оцінювання може переглядатися. Це дозволяє адаптувати стратегію до нових умов і підтримувати її актуальність у динамічному середовищі.

Крок 6. Оцінювання власних засобів (ресурсів) / Діагностика спроможностей сектору безпеки та оборони. Для системного аналізу наявних ресурсів та інструментів, які можна використати з метою досягнення бажаного результату, доцільно використовувати підхід DIME, який охоплює чотири основні групи інструментів впливу: дипломатичні, інформаційні, військові, економічні (табл. 2).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Таблиця 2. DIME-підхід – аналіз чотирьох основних груп інструментів впливу

Дипломатичні засоби	Інформаційні засоби	Військові засоби	Економічні засоби
Дипломатична мережа, міжнародні організації, міжнародне право, союзи	Розвідувальні агенції, стратегічні комунікації, психологічні операції, інформаційні операції	Збройні сили, правоохоронні органи, агенції захисту кордону тощо	Структури іноземної допомоги, торговельна та фінансова політика, стимули, санкції

Кожен із цих інструментів виконує окрему функцію у забезпеченні національної безпеки, проте найбільшу ефективність вони демонструють у поєднанні та взаємодії. Саме тому на цьому етапі важливо оцінити, які різні засоби можуть бути використані для впливу на противників, підтримки союзників, зміцнення міжнародного партнерства та формування сприятливого стратегічного середовища.

Дипломатичні інструменти передбачають міжнародне співробітництво, переговори, участь у міжнародних організаціях і механізмах безпеки. Інформаційні засоби охоплюють стратегічні комунікації, протидію дезінформації, кіберкомунікацію та формування суспільної стійкості. Військовий компонент пов'язаний із оборонними спроможностями, стримуванням агресії та готовністю до реагування. Економічні інструменти охоплюють фінансову стійкість, санкційну політику, підтримку критичної інфраструктури та ресурсне забезпечення сектору безпеки і оборони. Водночас оцінювання ресурсів не обмежується лише визначенням наявних можливостей. Не менш важливо враховувати існуючі обмеження – політичні, правові, фінансові, технологічні або міжнародні. Частина ресурсів може бути недоступною через дефіцит фінансування, обмежені кадрові спроможності, міжнародні зобов'язання або використання цих ресурсів в інших напрямах державної політики.

Окремої уваги потребує оцінювання реалістичності застосування певних інструментів. Наприклад, використання військових засобів може залежати від міжнародної підтримки, політичної легітимності або міжнародно-правових рішень. Аналогічно інформаційні чи економічні заходи мають оцінюватися з точки зору їхнього потенційного впливу, ефективності та можливих побічних наслідків. У результаті – формується реалістичне розуміння ресурсного потенціалу держави, визначаються сильні та слабкі сторони наявних інструментів, а також встановлюються межі можливого стратегічного реагування. Це дозволяє забезпечити збалансованість між стратегічними цілями та фактичними спроможностями держави у сфері національної безпеки.

Крок 7. Критичне оцінювання ситуації. На цьому кроці аналізується "наскільки система готова протидіяти загрозам". Критичне оцінювання ситуації передбачає поєднання результатів попереднього аналізу та застосування SWOT-аналізу для визначення: сильних сторін системи, слабких місць, можливостей розвитку, зовнішніх загроз. Сильні сторони відображають наявні переваги держави – ефективні інституції, міжнародну підтримку, стійку систему управління, оборонні спроможності чи технологічний потенціал. Слабкі сторони пов'язані з внутрішніми обмеженнями: кадровими проблемами, нестачею ресурсів, недостатньою координацією або вразливістю критичної інфраструктури. Можливості визначають напрями, у яких держава може посилити свої позиції через партнерства, модернізацію чи впровадження нових технологій, тоді як загрози охоплюють фактори, що можуть перешкоджати досягненню стратегічних цілей.

У межах цього кроку оцінюються інституційні, кадрові, технологічні, правові та фінансові спроможності сектору безпеки й оборони. Особлива увага приділяється ефективності міжвідомчої координації, готовності до кризового реагування, рівню цифровізації, кіберстійкості та здатності системи діяти в умовах невизначеності. Важливим елементом є аналіз "вузьких місць" – факторів, які стримують ефективність навіть за наявності

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

ресурсів. Це можуть бути затримки ухвалення рішень, розриви в обміні інформацією, дублювання функцій або недостатня взаємосумісність інформаційних систем. Виявлення таких проблем дозволяє визначити напрями, де навіть незначні зміни можуть суттєво підвищити ефективність системи безпеки.

Окрему увагу приділяють оцінюванню рівня зрілості ключових функцій безпеки: кризового реагування, кіберзахисту, стратегічних комунікацій, управління інцидентами та безперервності діяльності. Такий підхід дозволяє не лише виявити недоліки, а й визначити потенціал розвитку та пріоритети модернізації. Результатом має стати узагальнений профіль спроможностей сектору безпеки й оборони, який відображає сильні сторони системи, критичні вразливості, рівень готовності до реагування та перспективні напрями розвитку.

Крок 8. Формування цілей, пріоритетів і показників результативності. Цей крок є переходом від аналітичного оцінювання до практичного стратегічного управління, оскільки саме тут результати попереднього аналізу трансформуються у систему цілей, пріоритетів і показників ефективності політики, а з нею і стратегії національної безпеки.

Формування стратегічних цілей має ґрунтуватися на національних інтересах держави та враховувати реальні ресурсні й інституційні можливості. Цілі мають бути спрямовані на забезпечення суверенітету, стійкості державних інституцій, захист населення та безперервність функціонування критичних систем. Водночас надмірно загальні або нереалістичні цілі знижують ефективність стратегічного планування та ускладнюють реалізацію політики.

Доцільним є використання ієрархічного підходу до цілепокладання. На стратегічному рівні визначаються довгострокові орієнтири розвитку системи безпеки, наприклад, підвищення стійкості до гібридних загроз або посилення адаптивності сектору безпеки й оборони. Операційні цілі конкретизують ці напрями через визначення необхідних змін у спроможностях, процедурах чи координаційних механізмах. Реалізація таких цілей здійснюється через програми та конкретні заходи з визначенням відповідальних суб’єктів, ресурсів і строків виконання.

Важливою складовою цього кроку є формування системи показників результативності. Вони мають забезпечувати можливість оцінювання прогресу реалізації та своєчасного коригування стратегії. Показники результатів відображають реальний вплив політики на рівень безпеки, зокрема зменшення ризиків, скорочення часу реагування на інциденти або підвищення рівня стійкості критичної інфраструктури. Показники характеризують готовність системи безпеки до реагування на загрози, рівень міжвідомчої координації, розвиток технологічних рішень та ефективність управлінських процедур.

Окрему увагу слід приділяти якості індикаторів. Вони мають бути чіткими, вимірюваними, порівнюваними у часі та придатними для практичного використання. Надмірна кількість формальних показників ускладнює моніторинг і знижує ефективність управління. У підсумку цей крок формує цілісну систему стратегічних цілей, пріоритетів і критеріїв оцінювання, яка створює основу для подальшої реалізації, моніторингу та адаптації політики національної безпеки і стратегії її реалізації в умовах динамічних загроз.

Крок 9. Розроблення альтернативних стратегій. Основним завданням цього кроку є формування стратегічних альтернатив, яке ґрунтується на результатах попередніх кроків. Альтернативи можуть відрізнятися за масштабом заходів, рівнем ризику, обсягом ресурсів та швидкістю досягнення результатів.

У межах стратегічного планування доцільно виокремлювати кілька типових варіантів:

- мінімальна альтернатива – орієнтована на підтримання базової функціональності системи за рахунок обмежених і переважно реактивних заходів;
- базова альтернатива – передбачає поступове посилення спроможностей через модернізацію процесів і координації;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

- посилена альтернатива – спрямована на масштабні реформи, технологічний розвиток та суттєве підвищення стійкості системи;
- інноваційна альтернатива – базується на впровадженні цифрових технологій, аналітики даних і нових моделей взаємодії з партнерами.

Крок 10. Оцінювання альтернативних стратегій та аналіз ризиків. Після формування альтернатив здійснюється їх порівняльне оцінювання. Для цього використовуються методи багатокритеріального аналізу, SWOT-аналіз, воєнна гра, порівняльний аналіз, сценарне моделювання, дерева рішень та аналіз витрат і вигід. Такі підходи дозволяють оцінити ефективність стратегічних варіантів рішень, рівень ризику, ресурсні потреби та відповідність національним інтересам.

Отримані на попередньому кроці стратегічні альтернативи матимуть свої переваги та недоліки, але виявити це на практиці досить складно, адже це є спробою передбачити, як інші гравці, швидше за все, будуть діяти і як найімовірніше зміниться навколишнє середовище, коли варіант стратегії почне реалізовуватися. Можливо найефективніший спосіб отримати як мінімум деяке розуміння цього полягає в тому, щоб провести воєнну гру, в якій оцінити кожну альтернативу у різних сценаріях. Дуже небезпечно обмежуватися лише розглядом ситуацій, які дають ідеальний результат. Замість цього слід розглянути широкий спектр ситуацій, зокрема найбільш “небезпечних” і найбільш імовірних. “Червона команда”, що складається з внутрішніх і зовнішніх експертів, які грають за противників і в цілому за зовнішнє середовище, має вирішальну роль на цьому етапі аналізу, особливо в забезпеченні обґрунтованого пояснення того, як інші актори ймовірно реагуватимуть на імплементацію того чи іншого курсу дій.

Частиною цього аналізу є також розгляд загроз та аналіз ризиків. Як тільки кожна альтернатива буде обґрунтована достатньо детально, її слід перевірити на відповідність критеріям, які оцінюють потенційну успішність майбутньої стратегії. Критерії передбачають “прийнятність”, “здійсненність”, “придатність”, “стійкість” та “адаптивність”. Хоча це суб’єктивно, кожну стратегічну альтернативу необхідно кількісно-якісно оцінити за цими критеріями та, виходячи з результатів оцінювання, охарактеризувати її переваги та недоліки.

Оцінювання ризиків передбачає послідовну процедуру: ідентифікацію загроз, їх класифікацію, аналіз причин і наслідків, визначення вразливостей та пріоритизацію з урахуванням наявних спроможностей реагування. У сучасних умовах загрози рідко існують ізольовано – вони взаємопов’язані та можуть створювати каскадні ефекти, впливаючи одночасно на військову, економічну, енергетичну, інформаційну та кібернетичну сфери. Саме тому оцінювання має здійснюватися в межах комплексного підходу до безпеки та мати оцінку ризиків 2-го та 3-го порядків. Окремого значення набуває оцінювання кіберзагроз і захисту критичної інфраструктури. Сучасні дослідження свідчать, що кібератаки можуть мати масштабні наслідки для державного та військового управління, енергетики, зв’язку та систем життєзабезпечення. Використання ШІ-технологій для виявлення та прогнозування кіберзагроз підвищує ефективність системи реагування та ситуаційної обізнаності.

Результатом цього кроку алгоритму має стати матриця ризиків, яка відображає співвідношення між імовірністю реалізації загроз та масштабом їх наслідків. На її основі визначаються критичні загрози, формуються стратегічні пріоритети та обґрунтовуються подальші управлінські рішення.

Важливим елементом є оцінювання чутливості стратегії до змін зовнішнього середовища. Це дозволяє визначити, наскільки обрана альтернатива залишатиметься ефективною в умовах ескалації загроз, ресурсних обмежень або зміни міжнародної ситуації.

Крок 11. Вибір оптимальної стратегії та розроблення плану реалізації: ресурси, інструменти та дорожня карта. Цей крок передбачає презентацію висновків з оцінювання альтернативних стратегій вищому політичному керівництву, де результатом стає вибір оптимальної стратегії або комбінованого варіанта, який найбільше відповідає стратегічним цілям держави. Цей крок забезпечує перехід від стратегічного вибору до практичної реалізації

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

політики національної безпеки. Саме тут стратегія трансформується у систему конкретних управлінських дій із визначенням виконавців, ресурсів, строків і очікуваних результатів. План реалізації передбачає деталізацію стратегічних цілей через програми, підпрограми та окремі заходи. Для кожного напряму визначаються відповідальні органи, співвиконавці та механізми координації. Такий підхід дозволяє уникнути дублювання функцій, розмиття відповідальності та міжвідомчих конфліктів, що особливо важливо у сфері національної безпеки.

Важливим елементом є ресурсне забезпечення стратегії. На цьому кроці оцінюються фінансові, кадрові, технологічні та матеріально-технічні ресурси, необхідні для реалізації політики. Джерелами підтримки можуть виступати державний бюджет, міжнародна допомога, спеціальні програми та державно-приватне партнерство. Реалістичне ресурсне планування дозволяє підвищити ефективність реалізації стратегії.

Окрему увагу приділяють нормативному та організаційному забезпеченню. Передбачаються необхідні зміни до законодавства, процедур і стандартів, що створюють умови для реалізації стратегічних рішень, особливо у сферах кібербезпеки, захисту критичної інфраструктури та міжвідомчої взаємодії.

Не менш важливим є налагодження координації між органами влади, сектором безпеки й оборони, місцевим самоврядуванням і партнерами. Для цього визначаються механізми обміну інформацією, регламенти взаємодії та відповідальні координаційні структури.

Крок 12. Застосування стратегії. Ефективність стратегії у сфері національної безпеки залежить не лише від якості її розроблення, а й від здатності держави забезпечити її практичну реалізацію. Для цього стратегія має бути зрозумілою, послідовною та переконливою як для внутрішньої аудиторії, так і для міжнародних партнерів. Надмірна складність або перевантаження деталями можуть ускладнювати сприйняття стратегічних рішень. Важливо, щоб логіка стратегії була чіткою та доступною, а її цілі – зрозумілими для всіх учасників процесу реалізації. Саме це формує довіру до державної політики, сприяє суспільній підтримці та посилює міжнародну легітимність стратегічних рішень.

Не менш важливим є формування сприятливого стратегічного середовища для реалізації політики. Успішна стратегія передбачає не лише реагування на загрози, а й активне створення умов, які посилюють позиції держави та розширюють її можливості. Це передбачає розвиток партнерств, зміцнення інституційної стійкості, підготовку ресурсів і підтримання готовності до кризових ситуацій. У сучасному безпековому середовищі особливого значення набуває здатність до адаптації. Ефективні стратегічні рішення мають враховувати можливість швидких змін, непередбачуваних подій та нових ризиків.

Крок 13. Моніторинг і оцінювання. Моніторинг і оцінювання забезпечують постійний зворотний зв’язок між стратегічними цілями, реалізацією політики та фактичними результатами у сфері національної безпеки. На цьому кроці відстежуються визначені показники результативності, рівень досягнення цілей, динаміка загроз, стан спроможностей сектору безпеки й оборони, а також ефективність міжвідомчої взаємодії.

Моніторинг дозволяє своєчасно виявляти відхилення від запланованих параметрів, а оцінювання – глибше аналізувати, чи справді реалізовані заходи зменшують ризики, підвищують стійкість системи та забезпечують очікуваний результат. Важливо перевіряти не лише виконання заходів, а й правдивість початкових припущень, на яких будувалася стратегія. Для цього доцільно використовувати систему індикаторів, аудит, експертні оцінки та, за потреби, механізм “червоної команди”, що допомагає виявити слабкі місця й уникнути надмірного оптимізму в реалізації політики. Результатом цього кроку має стати об’єктивне розуміння того, що працює ефективно, які рішення потребують уточнення, де виникають управлінські або ресурсні проблеми та які нові ризики необхідно врахувати.

Крок 14. Адаптивне коригування стратегії. Адаптивне коригування є завершальним, але не фінальним у логіці стратегічного циклу кроком. Воно передбачає перегляд цілей, пріоритетів, заходів і ресурсів з урахуванням результатів моніторингу, оцінювання та змін у безпековому середовищі. Оскільки загрози можуть швидко трансформуватися, стратегія не

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

має залишатися статичною; її необхідно регулярно уточнювати відповідно до нових даних і реального розвитку подій.

Ключовим завданням є пошук балансу між збереженням обраного курсу та необхідністю його перегляду. Якщо обставини змінюються, стратеги мають ставити питання: "що це означає для реалізації стратегії?" і, за потреби, повертатися до попередніх кроків аналізу. Такий підхід відповідає логіці адаптивного стратегічного управління. Це дозволяє підтримувати актуальність стратегії, підвищувати її стійкість до непередбачуваних змін і забезпечувати ефективне досягнення цілей національної безпеки.

Висновок (Conclusion)

Отже, алгоритм системного оцінювання й стратегічного планування у сфері національної безпеки виступає методологічною рамкою. Унікальність запропонованого алгоритму системного оцінювання й стратегічного планування у сфері національної безпеки полягає у його цілісному, інтегрованому характері та принципово відмінній логіці побудови стратегічного процесу. Такий підхід дозволяє розглядати національну безпеку не як статичний набір документів або реактивних заходів, а як динамічний процес управління ризиками та розвитком спроможностей в умовах постійної невизначеності.

Принциповою особливістю алгоритму є його орієнтація на доказове стратегування та інтеграцію сучасних аналітичних і цифрових інструментів у архітектуру управління безпекою. Водночас алгоритм узгоджує дії національного, регіонального та місцевого рівнів. Його циклічний і адаптивний характер забезпечує можливість постійного перегляду пріоритетів, оновлення стратегічних рішень та коригування політики відповідно до зміни безпекового середовища, що принципово відрізняє цей підхід від лінійних моделей стратегічного планування.

Рекомендації (Recommendations)

Для підвищення ефективності державної політики у сфері національної безпеки доцільно впроваджувати системний алгоритм оцінювання та стратегічного планування, заснований на ризик-орієнтованому підході, міжвідомчій координації та адаптивному управлінні. Важливим напрямом подальшого розвитку є інтеграція цифрових технологій, систем прогнозної аналітики та штучного інтелекту у процеси моніторингу, оцінювання загроз і підтримки ухвалення стратегічних рішень.

Конфлікт інтересів (Conflict of Interest)

Автор заявляє про відсутність конфлікту інтересів під час підготовки та написання цієї статті.

Використані джерела

1. Du, W. W., & Chen, X. W. (2024). A comprehensive risk prediction method for defense mission planning based on probabilistic reasoning and hierarchical analysis. *Complex Engineering Systems*, *4*, 9. http://dx.doi.org/10.20517/ces.2024.15
2. Bakhshi, J., & Efatmaneshnik, M. (2024). *The interplay of capability and complexity in military context: definitions, challenges, and implications* (p. 133–162). https://doi.org/10.1080/14702436.2024.2415715
3. Zdravkov, Z., & Atipova, A. (2025). Methodology for assessment of a national security system. *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, *5*, 349–352. https://doi.org/10.17770/etr2025vol5.8480
4. Adabara, I., Olaniyi Sadiq, B., & Nuhu Shuaibu, A. (2025). Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment. *F1000Research*, *14*, 905. https://doi.org/10.12688/f1000research.169927.1
5. Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., & Hasan, R.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

(2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. *Journal of Posthumanism*, *5* (3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965

6. Hidayatullah, S., Supriyadi, A. A., Purwanto, I. E. D., & Saputro, G. E. (2025). Reformulating National Defense Policy Through Artificial Intelligence: Enhancing Strategic Decision Making and Ethical Governance. *Journal of Social Work and Science Education*, *6* (1), 180–200. https://doi.org/10.52690/jswse.v6i1.1069
7. Baclawski, K., Kozak, M., Bellman, K., D'Aniello, G., Ruvinsky, A., & Ferreira Barreto, C. D. S. (Eds.). (2023). *Proceedings of Conference on Cognitive and Computational Aspects of Situation Management 2023*, *102*, 172–177. https://doi.org/10.29007/vnzb
8. Tagarev, T. (2025). Formulating Defense Policy: Main Considerations and Evaluation Criteria. *Connections: The Quarterly Journal*, *24* (3), 9–35. https://doi.org/10.11610/Connections.23.4.12
9. Mykolaichuk, M., Petrukha, N., Akimova, L., Pozniakovska, N., Hudenko, B., & Akimov, O. (2025). Conceptual principles of analysis and forecasting threats to national security in modern conditions. *Sapienza: International Journal of Interdisciplinary Studies*, *6* (2), e25029. https://doi.org/10.51798/sijis.v6i2.985
10. Palamarchuk, T., Zavoritnya, H., Iemelianov, V., Lehkyi, S., & Taran, Y. (2025). Theoretical and methodological approach for strategic foresight and advanced response in the national security context. *Sapienza: International Journal of Interdisciplinary Studies*, *6* (2), e25039. https://doi.org/10.51798/sijis.v6i2.944
11. Pires, H. B., & Guimarães, L. N. F. (2024). Dynamic Multi-Target Three-Way Threat Assessment in the Context of Air Defense. *IEEE Access*, *12*, 141397–141413. https://doi.org/10.1109/ACCESS.2024.3468248
12. Sarjito, A. (2024). The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation. *International Journal Administration, Business & Organization*, *5* (2), 27–46. https://doi.org/10.61242/ijabo.24.396
13. Маслій, О., & Галушка, Р. (2025). Ієрархічний аналіз ризиків і загроз економічній безпеці України в умовах воєнного стану. *Економічний простір*, *198*, 69–75. https://doi.org/10.30838/EP.198.69-75
14. Sejfović, H., Vrcić Amar, A., & Avdović, A. (2023). Fantasy proneness in one's psychological life and health: observational study with impact analysis. *SCIENCE International Journal*, *2* (4), 101–106. https://doi.org/10.35120/sciencej0204101s
15. Clausewitz, C. *On War* (p. 596–597). (1976). (Eds. Michael Howard and Peter Paret). Princeton University Press.

References

1. Du, W. W., & Chen, X. W. (2024). A comprehensive risk prediction method for defense mission planning based on probabilistic reasoning and hierarchical analysis. *Complex Engineering Systems*, *4*, 9. http://dx.doi.org/10.20517/ces.2024.15
2. Bakhshi, J., & Efatmaneshnik, M. (2024). *The interplay of capability and complexity in military context: definitions, challenges, and implications* (p. 133–162). https://doi.org/10.1080/14702436.2024.2415715
3. Zdravkov, Z., & Atipova, A. (2025). Methodology for assessment of a national security system. *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, *5*, 349–352. https://doi.org/10.17770/etr2025vol5.8480
4. Adabara, I., Olaniyi Sadiq, B., & Nuhu Shuaibu, A. (2025). Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment. *F1000Research*, *14*, 905. https://doi.org/10.12688/f1000research.169927.1
5. Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Critical Infrastructure. *Journal of Posthumanism*, *5* (3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965
6. Hidayatullah, S., Supriyadi, A. A., Purwanto, I. E. D., & Saputro, G. E. (2025). Reformulating National Defense Policy Through Artificial Intelligence: Enhancing Strategic Decision Making and Ethical Governance. *Journal of Social Work and Science Education*, *6* (1), 180–200. https://doi.org/10.52690/jswse.v6i1.1069
7. Baclawski, K., Kozak, M., Bellman, K., D'Aniello, G., Ruvinsky, A., & Ferreira Barreto, C. D. S. (Eds.). (2023). *Proceedings of Conference on Cognitive and Computational Aspects of Situation Management 2023*, *102*, 172–177. https://doi.org/10.29007/vnzb
8. Tagarev, T. (2025). Formulating Defense Policy: Main Considerations and Evaluation Criteria. *Connections: The Quarterly Journal*, *24* (3), 9–35. https://doi.org/10.11610/Connections.23.4.12
9. Mykolaichuk, M., Petrukha, N., Akimova, L., Pozniakovska, N., Hudenko, B., & Akimov, O. (2025). Conceptual principles of analysis and forecasting threats to national security in modern conditions. *Sapienza: International Journal of Interdisciplinary Studies*, *6* (2), e25029. https://doi.org/10.51798/sijis.v6i2.985
10. Palamarchuk, T., Zavoritnya, H., Iemelianov, V., Lehkyi, S., & Taran, Y. (2025). Theoretical and methodological approach for strategic foresight and advanced response in the national security context. *Sapienza: International Journal of Interdisciplinary Studies*, *6* (2), e25039. https://doi.org/10.51798/sijis.v6i2.944
11. Pires, H. B., & Guimarães, L. N. F. (2024). Dynamic Multi-Target Three-Way Threat Assessment in the Context of Air Defense. *IEEE Access*, *12*, 141397–141413. https://doi.org/10.1109/ACCESS.2024.3468248
12. Sarjito, A. (2024). The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation. *International Journal Administration, Business & Organization*, *5* (2), 27–46. https://doi.org/10.61242/ijabo.24.396
13. Masliy, O., & Galushka, R. (2025). Hierarchical analysis of risks and threats to the economic security of Ukraine under martial law. *Economic Space*, *198*, 69–75. https://doi.org/10.30838/EP.198.69-75
14. Sejfović, H., Vrcić Amar, A., & Avdović, A. (2023). Fantasy proneness in one's psychological life and health: observational study with impact analysis. *SCIENCE International Journal*, *2* (4), 101–106. https://doi.org/10.35120/sciencej0204101s
15. Clausewitz, C. *On War* (p. 596–597). (1976). (Eds. Michael Howard and Peter Paret). Princeton University Press.

Formation of an algorithm for systemic assessment and strategic planning in the area of national security

Vasyl Shkoliarenko
PhD in technical science, Senior Researcher
Military academy named after Yevhenii Berezniak
04050, Yurii Illienko Street, 81, Kyiv, Ukraine
e-mail: vasyl1970@yahoo.com
ORCID: 0000-0001-8274-2232

Abstract. The article explores the theoretical and methodological principles of forming an algorithm for system assessment and strategic planning in the area of national security in the context of growing multidimensional threats and high uncertainty of the security environment. The article aims to develop a mechanism for comprehensive assessment and strategic planning in the field of national security by combining modern methodologies, risk analysis, interagency coordination, and

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

adaptive management. The study is based on systemic, risk-oriented, institutional, scenario-based and adaptive approaches, which allow for a comprehensive analysis of the security environment, the interrelations between threats, state capabilities and strategic management mechanisms, whereby the systemic approach treats national security as an interconnected system of political, military, economic, informational, social, cybernetic and infrastructural components, the risk-oriented approach is used to identify, classify and prioritise threats on the basis of hierarchical risk analysis, assessment of the probability of threat realisation, the scale of their consequences, the speed of escalation and the level of system vulnerability, and the principle of adaptive management ensures continuous updating of decisions, adjustment of goals and resources depending on changes in the security environment, which collectively forms a comprehensive, interdisciplinary and evidence-based approach to the development of an algorithm for systemic assessment and strategic planning in the field of national security.The need to transition from a fragmented response to individual challenges to complex, adaptive and evidence-based strategic management is substantiated. The essence of the concepts of "assessment", "system assessment" and "strategic planning" is determined, and their relationship within a single management cycle is revealed. It is proven that system assessment serves as an information and analytical basis for strategic planning, ensuring timely detection of threats, risk assessment, analysis of state capabilities and support for the process of making managerial decisions. Based on the analysis of modern scientific approaches, international experience and risk-oriented methods, an algorithm for system assessment of policy and strategic planning in the field of national security is proposed. The algorithm covers a sequence of interconnected stages: problem identification, study of the strategic environment, data collection and verification, threat and risk assessment, stakeholder analysis, determination of centers of gravity, formation of strategic goals and performance indicators, resource assessment, critical analysis of capabilities, selection of strategic alternatives, implementation planning, strategy application, monitoring, evaluation and adaptive adjustment of decisions. Particular attention is paid to the use of modern analytical tools, in particular SWOT analysis, scenario modeling, PESTLE, STEEPLEMS, and CoG analysis, multi-criteria assessment, risk analysis and DIME approach. The role of interdepartmental coordination, situational awareness, strategic communications and digital technologies in ensuring the sustainability of the security and defense sector is determined. The importance of integrating artificial intelligence and predictive analytics into the processes of risk assessment and supporting strategic decision-making is emphasized. The proposed algorithm allows to ensure the integrity of strategic management, increase the efficiency of resource use, improve the adaptability of state policy and strengthen the state's ability to respond to modern hybrid threats.

Keywords: national security; system assessment; strategic planning; risk analysis; threats; strategic environment; adaptive management; security and defense sector.