УДК 351.004
DOI https://doi.org/10.32782/TNU-2663-6468/2024.1/54

***Лисенко С.О.***
ПрАТ «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

# ВДОСКОНАЛЕННЯ СТРАТЕГІЧНИХ ПРИНЦИПІВ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ У СКЛАДІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

*Стаття присвячена дослідженню актуальних питань вдосконалення стратегічних принципів державного управління інформаційною безпекою у контексті забезпечення національної безпеки України. В умовах сучасних викликів та загроз, пов'язаних із розвитком інформаційних технологій та кіберзагрозами, ефективне управління інформаційною безпекою стає ключовим елементом національної безпеки.*

*Досліджено основні підходи до формування стратегічних принципів, проаналізовано міжнародний досвід та існуючі нормативно-правові акти України в цій сфері. Деталізовано стратегічні принципи державного управління інформаційною безпекою: адаптивності, комплексності, проактивності, координації, стійкості. Запропоновано рекомендації щодо вдосконалення державної політики, з метою підвищення рівня захисту національних інформаційних ресурсів та критичної інфраструктури, а також забезпечення кібербезпеки в умовах військового стану.*

*Окрему увагу присвячено міжнародному досвіду у сфері управління інформаційною безпекою та проведено аналіз існуючих теорій і стратегій. Окреслено основні проблеми та недоліки поточної системи державного управління інформаційною безпекою в умовах війни та гібридних загроз.*

*Подальші результати дослідження можуть бути використані для розробки та реалізації ефективної стратегії державного управління інформаційною безпекою, що включає вдосконалення наявної бази інформації, впровадження передових технологій захисту інформації, підвищення рівня професійної підготовки фахівців у галузі кібербезпеки та посилення міжнародного співробітництва. В статті також підкреслено важливість громадської обізнаності та актуальність підвищення ролі приватного сектору у забезпеченні інформаційної безпеки.*

***Ключові слова:*** *інформаційна безпека, управління інформаційною безпекою, стратегічні принципи, державне управління, національна безпека, безпека України, інформаційні системи, методи захисту.*

**Обґрунтування актуальності обраної теми.** Інформаційна безпека, як система, стала ключовим елементом національної безпеки для сучасних держав. У контексті України, що переживає складну геополітичну ситуацію, ефективне управління інформаційною безпекою є життєво необхідним для захисту державного суверенітету, економічної стабільності та суспільної злагоди. Це вимагає вдосконалення стратегічних принципів державного управління інформаційною безпекою, враховуючи необхідність неочевидних тактичних рухів та постійність, нескінченність стратегії національної безпеки.

Актуальність теми дослідження стратегічних принципів державного управління інформаційною безпекою є надзвичайно важливою в умовах сучасних викликів та загроз, які постають перед Україною. Інформаційна безпека є ключовим елементом національної безпеки, особливо з огляду на швидкий розвиток інформаційних технологій, глобалізацію інформаційного простору та зростання кількості кіберзагроз. Військові конфлікти, гібридні війни та кібератаки стають все більш поширеними інструментами впливу, що використовуються для підриву державних інституцій, економічної стабільності та суспільної безпеки.

**Метою статті** є всебічне дослідження та аналіз стратегічних принципів державного управління інформаційною безпекою у складі національної безпеки України, а також розробка рекомендацій щодо їх вдосконалення, з урахуванням сучасних викликів та загроз.

**Виклад основного матеріалу.** Сучасна інформаційна безпека охоплює широкий спектр питань,

включаючи захист критичної інфраструктури, протидію кіберзагрозам, забезпечення інформаційної стійкості та захист від інформаційних операцій, спрямованих на дестабілізацію суспільства. У зв'язку з цим, необхідно постійно розвивати та вдосконалювати стратегічні принципи державного управління інформаційною безпекою, щоб вони були здатні відповідати сучасним викликам та загрозам.

Теорія стратегії неочевидних дій Ліддела Гарта акцентує увагу на важливості використання непередбачуваних та інноваційних тактичних підходів у військовій та інформаційній сферах. Для України це означає необхідність розробки таких стратегічних принципів, які б враховували динамічні зміни в середовищі загроз та забезпечували гнучкість у відповідях на них. Використання неочевидних дій дозволяє уникнути прямої конфронтації та знаходити ефективні способи нейтралізації загроз, що є особливо актуальним у контексті інформаційної безпеки України [1].

Концепція нескінченної стратегії Шеллінга підкреслює необхідність постійного адаптування та вдосконалення стратегічних підходів у відповідь на нові виклики та загрози. У випадку інформаційної безпеки це означає, що держава повинна бути готовою до безперервного вдосконалення своїх методів захисту, а також до постійного моніторингу та аналізу нових загроз. Стратегія безпеки повинна бути постійно-нескінченною, оскільки загрози невпинно еволюціонують, а відповідь на них повинна бути адекватною та своєчасною [2].

Враховуючи значну залежність сучасного суспільства від інформаційних технологій, Україна раз-по-раз стикається з новими викликами та загрозами у сфері інформаційної безпеки. Ці загрози включають кібернапади, інформаційні війни, дезінформацію та інші форми інформаційного впливу, що можуть дестабілізувати суспільство та підривати довіру до державних інститутів. Тому вдосконалення стратегічних принципів управління інформаційною безпекою є необхідною умовою для забезпечення національної безпеки України.

У складі інформаційної безпеки значне місце займає процес захисту інформаційних ресурсів від загроз різного характеру. Основними аспектами інформаційної безпеки є конфіденційність, цілісність та доступність інформації, що випливає із природи інформації та різних етапів її еволюції. Спочатку інформація створюється та передається користувачам. Далі інформацію потрібно зберігати та охороняти її конфіденційність. І на кожному із цих етапів інформацію супроводжують загрози знищення, руйнування, викривлення, викрадення та незаконного розповсюдження. Тому державне управління інформаційною безпекою передбачає комплекс заходів, спрямованих на захист інформаційних систем, запобігання кіберзагрозам та протидію дезінформації [3].

Конфіденційність означає захист інформації від несанкціонованого доступу. Важливо забезпечити, щоб інформація була доступною лише тим особам або системам, які мають відповідні повноваження. Це досягається за допомогою шифрування даних, контрольованого доступу та використання засобів аутентифікації.

Цілісність інформації полягає в забезпеченні її точності та повноти. Інформація не повинна бути змінена або пошкоджена несанкціонованим чином під час зберігання, обробки або передачі. Це включає захист від помилок, зловмисних змін та збоїв у системах. Методи забезпечення цілісності включають використання контрольних сум, цифрових підписів та алгоритмів хешування.

Доступність означає, що інформація та інформаційні системи повинні бути доступними в будь-який час, коли це потрібно уповноваженим користувачам. Це вимагає захисту систем від атак, спрямованих на відмову в обслуговуванні (DDoS), а також забезпечення резервного копіювання даних та планів відновлення після аварій [4].

Державне управління інформаційною безпекою включає розробку та впровадження політик, стандартів та процедур, спрямованих на захист інформаційних систем. Це включає встановлення технічних засобів захисту, таких як міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень (IDS/IPS), а також засоби управління вразливостями.

Запобігання кіберзагрозам вимагає комплексного підходу, включаючи моніторинг мережевої активності, аналіз загроз, регулярне оновлення програмного забезпечення та проведення навчань для персоналу. Ключовим елементом є створення і підтримка кібербезпекових операційних центрів (SOC), які можуть швидко реагувати на інциденти.

Протидія дезінформації є важливим аспектом інформаційної безпеки, особливо в умовах сучасних гібридних загроз. Це включає виявлення та нейтралізацію фейкових новин, інформаційних атак і пропаганди, спрямованих на дестабілізацію суспільства. Важливими заходами є підвищення медіаграмотності населення, розвиток механізмів швидкого спростування неправдивої інформації та співпраця з медіа.

Пропонується розглянути наступні стратегічні принципи державного управління інформаційною безпекою, що мають свої ознаки та визначення.

Принцип адаптивності – здатність системи безпеки швидко реагувати на зміну загроз та впроваджувати нові технології та методи захисту.

2. Принцип комплексності – інтеграція всіх аспектів інформаційної безпеки, включаючи технологічні, організаційні та правові заходи.

3. Принцип проактивності – акцент на випереджувальні дії та заходи, спрямовані на запобігання загрозам до їх реалізації.

4. Принцип координації – забезпечення взаємодії між різними державними структурами та приватним сектором у сфері інформаційної безпеки.

5. Принцип стійкості – створення умов для швидкого відновлення та продовження функціонування інформаційної інфраструктури після атак або збоїв.

Вдосконалення стратегічних принципів державного управління інформаційною безпекою є критично важливим для забезпечення національної безпеки України. Врахування концепцій неочевидних дій та нескінченності стратегічного підходу дозволить створити ефективну систему захисту, здатну протистояти сучасним загрозам та викликам.

Системний підхід та інтеграція в управлінні інформаційною безпекою має бути інтегрованим у загальну систему національної безпеки. Це включає координацію дій між різними державними органами, приватним сектором та громадянським суспільством.

Адаптивність та гнучкість, означає, що в умовах швидко змінюваних загроз стратегія управління інформаційною безпекою має бути гнучкою та адаптивною. Це дозволить оперативно реагувати на нові виклики та змінювати тактику в залежності від ситуації [5].

Вимога до постійного вдосконалення та навчання для забезпечення ефективної інформаційної безпеки декларує необхідність постійно вдосконалювати технології, методи та навички фахівців. Регулярні навчання та тренінги, а також наукові дослідження у сфері інформаційної безпеки є критично важливими.

Важливо забезпечити прозорість дій державних органів у сфері інформаційної безпеки та їх підзвітність суспільству. Це сприятиме підвищенню довіри громадян та зміцненню соціальної згуртованості.

Варто розглянути ще одну групу принципів державного управління, які стосуються неочевидних тактичних та стратегічних дій у сфері інформаційної безпеки. Зазначені принципи пропонуються автором, як складні та різноманітні, що мають певні особливості. За способом застосування їх можна класифікувати за наступними видами: превентивні заходи та проактивність, асиметричні відповіді, психологічні операції та інформаційна підтримка.

Превентивні заходи та проактивність є ключовими елементами сучасних принципів управління інформаційною безпекою. Замість традиційного реактивного підходу, орієнтованого на подолання наслідків кіберінцидентів, сучасні стратегії акцентують увагу на попередженні загроз і вразливостей до їх реалізації. Такий принцип має низку переваг, серед яких зменшення ризиків, підвищення стійкості інформаційних систем та зниження витрат на усунення наслідків атак [6].

До вказаних заходів можна віднести моніторинг та аналіз потенційних загроз, що виражається в наступному.

Постійний моніторинг: для забезпечення інформаційної безпеки необхідно здійснювати постійний моніторинг мережевої активності та системних подій [7]. Це включає виявлення аномалій, підозрілої активності та можливих загроз у реальному часі.

2. Аналіз загроз: використання сучасних інструментів та технологій для аналізу загроз, таких як системи виявлення вторгнень (IDS), аналітичні платформи та штучний інтелект. Це дозволяє визначити патерни та тенденції, які можуть вказувати на потенційні атаки.

3. Інформаційний обмін: співпраця з іншими державними та приватними організаціями для обміну інформацією про кіберзагрози. Це включає участь у міжнародних мережах обміну інформацією та спільних розслідуваннях інцидентів.

Розробка та впровадження захисних механізмів теж представляють собою ефективні заходи в державному управлінні інформаційною безпекою і складається з наступного.

Оцінка вразливостей: регулярне проведення аудитів безпеки та тестування на проникнення для виявлення вразливих місць у системах та мережах. Це дозволяє виявити потенційні слабкі місця до того, як ними скористаються зловмисники.

2. Розробка політик безпеки: створення та впровадження політик безпеки, які визначають правила та процедури захисту інформації [8]. Це включає правила доступу, використання шифрування, управління паролями та інші заходи.

3. Навчання та підготовка персоналу: регулярні тренінги та навчання для співробітників щодо найкращих практик інформаційної безпеки. Це допомагає підвищити обізнаність та здатність персоналу реагувати на потенційні загрози.

4. Технологічні рішення: впровадження сучасних технологічних рішень, таких як багатофакторна аутентифікація, шифрування даних, фаєрволи та антивірусні системи. Ці рішення сприяють зміцненню захисту інформаційних ресурсів.

5. Планування на випадок інцидентів: розробка планів реагування на інциденти, що включають детальні інструкції для швидкого та ефективного реагування на кіберінциденти [7]. Це дозволяє мінімізувати вплив атак та швидко відновити нормальну роботу систем .

Систематичний підхід до проактивності в державному управління включає кілька основних вимог для дієвості стратегічних принципів.

Інтеграція безпеки у процеси: впровадження безпеки на всіх етапах життєвого циклу інформаційних систем та додатків, від проектування до експлуатації. Це дозволяє враховувати аспекти безпеки ще на стадії розробки.

Безперервне покращення: регулярний перегляд та оновлення стратегій та політик безпеки відповідно до нових загроз та технологій. Це дозволяє підтримувати високий рівень безпеки в умовах динамічно змінюваного середовища.

Співпраця з експертами: залучення фахівців з кібербезпеки для проведення регулярних оцінок та надання рекомендацій щодо покращення захисту. Це забезпечує незалежний погляд на стан безпеки та допомагає виявити приховані ризики.

Зрештою, застосування превентивних заходів та проактивності в державному управлінні інформаційною безпекою дозволяє знизити ризики кіберзагроз, забезпечити стійкість інформаційних систем та зберегти довіру громадян до державних інституцій. Зазначене критично важливо для захисту національної безпеки України в умовах сучасних викликів та загроз.

Державне управління інформаційною безпекою не може бути разовою акцією, воно має бути постійним процесом. В сучасному світі, де інформаційні загрози постійно еволюціонують, стратегія безпеки повинна бути нескінченною та динамічною. Це вимагає створення системи безперервного моніторингу, аналізу та вдосконалення. Постійне оновлення знань, технологій та методів захисту є ключовим фактором успіху у боротьбі з інформаційними загрозами.

Заходи, що підтримують нескінченність стратегічних принципів державного управління безпекою можуть розкрити сенс самого принципу.

Постійний моніторинг і аналіз, як група заходів включають регулярне спостереження за потенційними та існуючими загрозами, а також аналіз тенденцій та моделей у кіберпросторі [9]. Це потребує постійного оцінювання слабких місць у системах інформаційної безпеки для їх швидкого усунення та підвищення рівня захисту.

Динамічне оновлення забезпечується заходами для використання новітніх технологій і методів захисту, таких як штучний інтелект, машинне навчання та блокчейн, для посилення інформаційної безпеки. Регулярний перегляд і вдосконалення політик безпеки, процедур реагування на інциденти та планів відновлення після атак.

Навчання та підвищення обізнаності суб'єктів інформаційної безпеки складаються з освіти та тренінгів. Організація постійних навчальних програм для співробітників та громадськості з метою підвищення обізнаності про інформаційні загрози та методи захисту. Проведення регулярних симуляційних вправ для перевірки готовності до кіберінцидентів та вдосконалення навичок реагування.

Інформаційна співпраця відноситься до заходів забезпечення нескінченості стратегічних принципів інформаційної безпеки [10]. До неї відносять взаємодію з міжнародними партнерами та організаціями для обміну інформацією про загрози та найкращі практики захисту. Також тут доцільна співпраця з приватними компаніями та науково-дослідними установами для розвитку новітніх технологій захисту та впровадження інновацій.

Визначимо переваги нескінченості стратегічних принципів безпеки, до яких можна віднести наступні. Гнучкість і адаптивність полягає в постійному оновленні стратегій та методів, що дозволяє швидко адаптуватися до нових загроз та змін у кіберпросторі. Підвищення стійкості являє собою безперервний процес моніторингу та вдосконалення і сприяє підвищенню стійкості інформаційних систем до атак, знижуючи ризик їх успішного здійснення. Зниження ризиків досягається регулярним оновленням знань і технологій, що допомагає зменшити ризик експлуатації вразливостей та забезпечити вищий рівень захисту. Нарешті, зміцнення довіри досягається завдяки постійному інформування громадськості про заходи безпеки. Підвищення обізнаності сприяє зміцненню довіри до державних інституцій та їх здатності захищати національні інтереси.

**Висновки та перспективи подальших досліджень.** Вдосконалення стратегічних принципів державного управління інформаційною безпекою є критично важливим для забезпечення національної безпеки України. В сучасних умовах, де інформаційні загрози стають все більш складними та різноманітними, стратегія інформаційної безпеки повинна бути нескінченною та динамічною. Це вимагає інтеграції, адаптивності, постійного вдосконалення та прозорості у діяльності державних органів. Використання неочевидних тактичних і стратегічних дій, що забезпечують постійність стратегії безпеки є необхідними умовами для ефективного протистояння інформаційним загрозам та забезпечення стабільності у країні.

Врахування концепцій неочевидних тактичних дій та нескінченності стратегічного підходу дозволить створити ефективну систему захисту, здатну протистояти сучасним загрозам та викликам. Це завдання вимагає комплексного підходу, постійного моніторингу та адаптації до нових умов, що виникають у глобальному інформаційному просторі.

Ключовими елементами описаних стратегічних принципів є: необхідність безперервного спостереження за потенційними загрозами, аналізу вразливостей та адаптації до нових ризиків; використання найсучасніших технологій та методів захисту, регулярне оновлення політик та процедур для забезпечення найвищого рівня безпеки; постійна освіта та тренінги для співробітників і громадян, проведення симуляцій та вправ для підвищення готовності до кіберінцидентів; тісна взаємодія з міжнародними партнерами, обмін інформацією про загрози та найкращі практики захисту, а також партнерство з приватним сектором для впровадження інновацій.

Лише за умови реалізації цих принципів можна забезпечити ефективний захист інформаційних ресурсів, підтримувати національну безпеку та сприяти стабільності та злагоді в суспільстві. Використання асиметричних відповідей, психологічних операцій та інформаційної підтримки дозволить зміцнити стійкість суспільства до дезінформації та інших форм інформаційного впливу, що є важливим для забезпечення довіри громадян до державних інституцій.

Таким чином, впровадження нескінченної та динамічної стратегії інформаційної безпеки є життєво необхідним для захисту національних інтересів України в умовах сучасного глобального інформаційного простору. Подальші дослідження у сфері інформаційної безпеки мають бути спрямовані на розробку нових технологій захисту, вивчення поведінки загроз та розвиток методів психологічного впливу на суспільство. Важливо також продовжувати вивчення досвіду інших країн та адаптувати найкращі практики до українських реалій.

**Список літератури:**

1. Латишев К. Стратегія непрямих дій Б. Г. Ліддела Гарта: вчення «алхіміка війни» з Туманного Альбіону. *Пломінь*. URL: https://plomin.club/strategy-indirect-approach-liddell-hart/

2. Schelling T. (1960) The Strategy of Conflict, *Harvard University Press*. pp. 212

3. Закон України Про національну безпеку (*Відомості Верховної Ради (ВВР)*, 2018, № 31, ст.241) *Офіційний веб-сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

4. A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. *Scalable Computing: Practice and Experience*. 2019. Volume 20, Number 4, pp. 669–685. URL: https://doi.org/10.12694/scpe.v20i4.1569

5. Beebe, N.L., and Rao, V.S. Improving Organizational Information Security Strategy Via MesoLevel Application of Situational Crime Prevention to the Risk Management Process. *Communications of the Association for Information Systems (26:17)*. 2010. P. 329–358.

6. ISO 27001:2005 «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги». *Національний Стандарт України*. URL: https://dnaop.com/html/62498/doc-%D0%94%D0%A1%D0%A2%D0%A3_ISO_IEC_27001_2015

7. Ільницька У. Інформаційна безпека Україна: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Вип. 2. С. 27–32.

8. Саричев Ю.О. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління. *Вісник НАДУ при Президентові України (Серія "Державне управління")*. 2017. № 3. С. 120–126.

9. Богданович В.Ю. Методика формування та управління інтегрованим потенціалом протидії загрозам воєнного характеру для забезпечення визначеного рівня воєнної безпеки держави / В.Ю. Богданович, І.Ю. Свида, А.М. Сиротенко. *Сучасні інформаційні технології у сфері безпеки та оборони: Зб. наук. пр. НУОУ ім. Івана Черняховського*. 2018. № 2(32). С. 81–86.

10. Білоусенко, О. (2022). Що таке інформаційно-психологічні операції і як їх розпізнати. *ms. detector. media. URL:* https://ms.detector.media/manipulyatsii/post/29009/2022-02-23-shcho-take-informatsiyno-psykhologichni-operatsii-i-yak-ikh-rozpiznaty/

**Lysenko S.O. IMPROVEMENT OF STRATEGIC PRINCIPLES OF STATE MANAGEMENT OF INFORMATION SECURITY AS PART OF NATIONAL SECURITY OF UKRAINE**

*The article is devoted to the study of topical issues of improving the strategic principles of public administration of information security in the context of ensuring the national security of Ukraine. In the context of modern challenges and threats associated with the development of information technology and cyber threats, effective information security management is becoming a key element of national security.*

*The article examines the main approaches to the formation of strategic principles, analyses international experience and existing Ukrainian regulations in this area. The strategic principles of public administration of information security are detailed: adaptability, complexity, proactivity, coordination, and sustainability. Recommendations are offered to improve the state policy in order to increase the level of protection of national information resources and critical infrastructure, as well as to ensure cybersecurity in martial law.*

*Particular attention is paid to international experience in the field of information security management and an analysis of existing theories and strategies. The main problems and shortcomings of the current system of public administration of information security in the context of war and hybrid threats are outlined.*

*Further results of the study can be used to develop and implement an effective strategy for public administration of information security, including improving the existing information base, introducing advanced information security technologies, increasing the level of professional training of cybersecurity specialists and strengthening international cooperation. The article also emphasises the importance of public awareness and the relevance of enhancing the role of the private sector in ensuring information security.*

***Key words:*** *information security, information security management, strategic principles, public administration, national security, security of Ukraine, information systems, protection methods.*