ОБГРУНТУВАННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМНИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ СТРАТЕГІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

SUBSTANTIATION OF DIRECTIONS FOR IMPROVING SYSTEM MECHANISMS FOR ENSURING STRATEGIC INFORMATION SECURITY MANAGEMENT

УДК 351:004
DOI https://doi.org/10.32782/pma2663-5240-2023.34.36

Лисенко С.О.
д. юр. наук, професор,
директор Інституту безпеки,
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

Стаття присвячена дослідженню стратегічних напрямів удосконалення системних механізмів управління інформаційною безпекою. Підкреслюється важливість міждисциплінарного підходу, який інтегрує правові, соціальні та технологічні рамки для протидії складним загрозам у цифрову епоху. Науковці наголошують на необхідності адаптації заходів безпеки до існуючих та нових загроз, про що свідчить нещодавнє збільшення кількості гібридних та кібератак. Така інтеграція дозволяє національним органам безпеки ефективно і злагоджено реагувати на швидкозмінний ландшафт загроз, що особливо актуально для держав, які стикаються з постійними викликами безпеці.

Обгрунтовано важливість чітко визначених правових структур і протоколів міжвідомчої координації для впорядкування комунікації та покращення часу реагування. Ефективні системи інформаційної безпеки спираються на фундамент правової ясності та процедурної узгодженості між державними органами, що допомагає запобігти дублюванню зусиль і сприяє уніфікованому реагуванню. Крім того, у статті досліджується важлива роль адаптивних систем, які включають розвідку загроз у режимі реального часу та передбачають нові методи атак, підтримуючи проактивну позицію захисту.

Досліджено стратегічні підходи, запропоновані провідними вченими, які виступають за комплексний механізм захисту, що охоплює превентивні та реактивні заходи. Ці стратегії включають ініціативи з обміну даними в режимі реального часу та стандартизовані процедури, які покращують міжвідомчу співпрацю та ефективність реагування. Підкреслюючи багатовимірність інформаційної безпеки, цей підхід відповідає світовим стандартам і посилює стійкість до витонченого характеру сучасних кібернетичних та інформаційних загроз.

Підкреслено гостру потребу в стійкій і адаптивній структурі інформаційної безпеки. Майбутні дослідження заохочуються до розширення цих рамок, зосереджуючись на міжнародному співробітництві і передових технологіях для посилення національної і регіональної оборони. Це гарантуватиме, що механізми інформаційної безпеки залишатимуться гнучкими і здатними протистояти як очікуваним, так і непередбачуваним викликам.

Ключові слова: *інформаційна безпека, стратегічне управління, кіберзагрози, гібридні загрози, міжвідомча координація, розвідка загроз, міждисциплінарний підхід, превентивні заходи, національна безпека, цифрові загрози, міжнародне співробітництво, механізми інформаційної безпеки.*

The article is devoted to the study of strategic directions for improving the systemic mechanisms of information security management. The article emphasises the importance of an interdisciplinary approach that integrates legal, social and technological frameworks to counter complex threats in the digital age. Scholars emphasise the need to adapt security measures to existing and emerging threats, as evidenced by the recent increase in hybrid and cyber attacks. Such integration allows national security agencies to respond effectively and coherently to the rapidly changing threat landscape, which is especially important for states facing constant security challenges.

The importance of clearly defined legal structures and interagency coordination protocols to streamline communication and improve response times is substantiated. Effective information security systems rest on a foundation of legal clarity and procedural consistency among government agencies, which helps prevent duplication of effort and facilitates a unified response. In addition, the article explores the important role of adaptive systems, which include real-time threat intelligence and anticipate new methods of attack, supporting a proactive defence posture.

The article examines strategic approaches proposed by leading scholars who advocate a comprehensive defence mechanism that encompasses preventive and reactive measures. These strategies include real-time data-sharing initiatives and standardised procedures that improve interagency cooperation and response efficiency. By emphasising the multidimensionality of information security, this approach is in line with international standards and strengthens resilience to the sophisticated nature of modern cyber and information threats.

The urgent need for a resilient and adaptive information security framework is emphasised. Future research is encouraged to expand this framework by focusing on international cooperation and advanced technologies to strengthen national and regional defence. This will ensure that information security mechanisms remain flexible and able to withstand both expected and unforeseen challenges.

Key words: *information security, strategic management, cyber threats, hybrid threats, interagency coordination, threat intelligence, interdisciplinary approach, preventive measures, national security, digital threats, international cooperation, information security mechanisms.*

Актуальність теми дослідження. Важливість надійних механізмів захисту інформації ще ніколи не була такою нагальною. В епоху стрімкого технологічного прогресу та ескалації глобальних кіберзагроз, держави стикаються з безпрецедентною потребою захистити своє інформаційне середовище від все більш витончених форм цифрової та інформаційної агресії. Для України це питання є особливо актуальним, оскільки країна сти-

кається з регіональними та міжнародними безпековими викликами, які безпосередньо впливають на її інформаційний суверенітет та цифрову стійкість. У цьому дослідженні розглядаються основні засади та методологічні підходи, необхідні для забезпечення національної інформаційної безпеки, як у теоретичному, так і в практичному аспектах.

У дослідженні підкреслюється необхідність законодавчо регульованого механізму інформаційної безпеки, в якому правові рамки і системна політика слугують для структурування і спрямування захисних зусиль у різних секторах. Поклавши в основу практик безпеки цілісний, заснований на законі підхід, держава може ефективно координувати різні відомства та установи, відповідальні за інформаційну безпеку, тим самим посилюючи свою стійкість до загроз як з боку зовнішніх акторів, так і внутрішніх вразливостей.

Крім того, дослідження відповідає світовим тенденціям, які наголошують на інтеграції функціональних, структурних та діалектичних методів в інформаційній безпеці. Ці підходи надають Україні теоретичний інструментарій для передбачення, адаптації та протидії загрозам, що еволюціонують. Завдяки цьому дослідженню українські механізми інформаційної безпеки готові не лише реагувати на сучасні виклики, але й розвиватися в тандемі з майбутнім розвитком, забезпечуючи довгострокову, стійку основу, яка зміцнює загальний ландшафт безпеки країни.

Метою дослідження є вивчення та визначення теоретико-методологічних засад, необхідних для розробки ефективного державного механізму забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Останні дослідження відображають перехід до міждисциплінарних, проактивних і адаптивних підходів в інформаційній безпеці. Вони підкреслюють важливість узгодженої правової бази, аналізу даних у режимі реального часу, міжнародної співпраці та залучення громадськості у створенні стійкої структури національної безпеки, здатної протистояти складнощам сучасних кібер- та гібридних загроз. Вчені дослідили основні аспекти підходів до визначення інформаційної безпеки та її зміцнення (Біленчук П. Д., Тихомиров О. О., Нашинець-Наумова А. Ю., Перун Т. С., Ткачук Т. Ю., Авер'янова Н.М., А. Баровської. К., Демиденко В., Гончар, С. Ф., Зозуля О.), проте автор даної статті зробив більший акцент обгрунтування напрямків стратегічного управління.

Основний зміст дослідження. Ефективна система безпеки вимагає чітких правових визначень і обов'язків для кожного органу держави-учасниці, що дозволить спростити координацію і час реагування. Різні методологічні підходи сприяють подальшому зміцненню цих основ. Структурно-функціональний підхід, наприклад, поєднує перспективи конкретних дій і загальної системи, дозволяючи кожному компоненту функціонувати в гармонії з більш широкими цілями інформаційної безпеки. Згідно з цим підходом, кожна установа, що займається інформаційною безпекою, наприклад, підрозділи кібербезпеки, розвідувальні органи та регуляторні органи, виконує свою роль, яка узгоджується з більш широким скоординованим планом.

На додаток до структурно-функціоналістського підходу, діалектичний і формально-юридичний методи забезпечують більш всеосяжну основу. Діалектичне міркування розглядає постійну взаємодію між загрозами, що розвиваються, і реакцією держави, в той час як формально-юридичний метод підкреслює відповідність встановленим законам і політиці. Наприклад, використовуючи діалектичний аналіз, відомства можуть прогнозувати майбутні ризики та протидіяти їм на основі поточних моделей загроз [1]. Разом ці підходи гарантують, що механізм державної інформаційної безпеки є одночасно адаптивним і юридично обґрунтованим, здатним вирішувати нові виклики в міру їх виникнення.

Терміни «механізм» і «система» часто вживаються як взаємозамінні, але це дублювання призводить до непослідовності в розумінні та впровадженні ефективної інформаційної безпеки. Чітке розмежування між цими поняттями є важливим для створення послідовних стратегій, які підтримують як законодавчу ясність, так і операційну ефективність. Робота О.О. Тихомирова в цій галузі підкреслює, що інформаційна безпека охоплює поєднання теоретико-методологічних елементів та адміністративно-правових дій, створюючи багатогранний підхід до національної безпеки [2]. Для Тихомирова «механізм» конкретно стосується структурованих процесів і методів в операціях з інформаційної безпеки, тоді як «система» включає в себе більш широкий спектр державних і недержавних суб'єктів, що беруть участь у цьому процесі. Ця різниця допомагає політикам і відомствам краще зрозуміти ролі різних компонентів і підвищує адаптивність практик безпеки.

Наприклад, аналітичні та розвідувальні заходи є частиною «механізму» інформаційної безпеки, оскільки вони включають структуровані процеси, призначені для збору, аналізу та оцінки ризиків для безпеки. Ця діяльність

є систематичною, але функціонує як частина контрольованого механізму в рамках більшої системи державних та інституційних структур. Підрозділ кібербезпеки, який проводить аналіз розвідувальних даних про нові загрози, є частиною механізму безпеки; однак цей підрозділ також функціонує в рамках ширшої системи, яка включає правові рамки, політичні настанови та міжвідомчу співпрацю. Пояснюючи, що розвідувальні заходи є елементами механізму, Тихомиров відрізняє їх від ширших системних функцій, таких як міжвідомча координація і правовий нагляд, які структурують і підтримують всю стратегію безпеки.

Більше того, Тихомиров підкреслює, що змішування цих термінів може призвести до втрати ефективності, оскільки відомства можуть дублювати зусилля або діяти без чітких директив. Коли механізм чітко визначений як процесний, а система - як структурна, кожен суб'єкт може зосередитися на своїх завданнях. Наприклад, Національне агентство кібербезпеки може бути відповідальним за впровадження протоколів кібербезпеки та пом'якшення загроз у режимі реального часу (механізм), тоді як Міністерство інформації здійснює нагляд за системною політикою, яка підтримує ці операції. Визнаючи роль механізму в безпосередніх заходах із забезпечення безпеки, а роль системи - у підтримці та регулюванні цих заходів, держава може впорядкувати операції та покращити узгодженість законодавства, забезпечивши оптимальне узгодження превентивних заходів та заходів реагування.

Така термінологічна ясність необхідна для того, щоб механізм і система безпеки функціонували синергетично, дозволяючи адаптувати юридично обґрунтовані підходи до сучасних викликів інформаційній безпеці. Це забезпечує міцну основу для розробки узгодженої законодавчої бази, оскільки механізми залишаються адаптивними до еволюції загроз, а системи зберігають стабільність завдяки інституційній підтримці. Наприклад, національний механізм кібербезпеки може адаптуватися шляхом інтеграції нових інструментів розвідки загроз і контрзаходів, тоді як система інформаційної безпеки залишається незмінною, забезпечуючи стабільну основу для цих еволюціонуючих механізмів. Завдяки такому структурованому розумінню система може постійно вдосконалюватися для підтримки нових механізмів у міру їх появи, створюючи гнучкий і оперативний підхід до державної інформаційної безпеки.

Хоча законодавчі повноваження визначають ролі різних відомств у забезпеченні державної інформаційної безпеки, практичні проблеми міжвідомчої координації залишаються значною перешкодою. Ці проблеми часто ускладнюють час реагування та знижують загальну ефективність зусиль із забезпечення національної безпеки. Складність координації між різними органами, відповідальними за кібербезпеку, розвідку та законодавчий нагляд, підкреслює гостру потребу в чітких каналах зв'язку та протоколах співпраці для забезпечення єдиного реагування на інформаційні загрози [3]. Без чітких процедур співпраці ефективність заходів реагування на загрози стає обмеженою, оскільки відомства можуть бути не готові діяти швидко, спираючись на розвіддані іншої організації.

Інша проблема виникає через дублювання обов'язків, що може призвести до дублювання, а іноді навіть до конфліктів у стратегіях реагування на загрози. Відомства, відповідальні за моніторинг онлайн-контенту і запобігання поширенню дезінформації, можуть ненавмисно дублювати зусилля, що призводить до неефективності в управлінні критично важливими ресурсами. Коли кілька відомств відстежують схожі загрози без координації, виникає ризик дублювання, що не лише марнотратно витрачає ресурси, а й призводить до плутанини в розподілі ролей. Це підкреслює необхідність чіткого розмежування ролей кожного з відомств для уникнення дублювання дій.

Крім того, відсутність налагоджених каналів комунікації створює проблеми в ситуаціях, що вимагають негайного реагування. Загрози кібербезпеці часто вимагають швидких, скоординованих дій різних секторів, включаючи розвідку, правоохоронні та регуляторні органи. Однак через існуючі прогалини в комунікаційних стратегіях важлива інформація може не доходити до всіх необхідних сторін вчасно, що призводить до затримок у реагуванні, а в деяких випадках - до втрачених можливостей нейтралізувати загрози. Коли кібератаку виявляє одне відомство, запізніле повідомлення інших залучених відомств може сповільнити заходи зі стримування і зробити системи вразливими.

Деякі відомства стикаються з проблемами при координації дій із зовнішніми суб'єктами, такими як компанії приватного сектору або міжнародні організації з кібербезпеки, що ще більше ускладнює ситуацію з безпекою. Приватні компанії, які керують ключовою інфраструктурою, можуть володіти розвідданими про критичні загрози, але їм часто бракує спрощеного протоколу для обміну цією інформацією з державними установами. Якщо приватна телекомунікаційна компанія виявляє порушення, що впливає на національну безпеку даних, вона може зіткнутися з труднощами в ефективній

комунікації з державними органами безпеки через нечіткі протоколи обміну інформацією. Відсутність встановлених процедур співпраці між державними органами та суб'єктами приватного сектору виявляє значну вразливість в управлінні загрозами національній безпеці, особливо в умовах, коли все більше інфраструктури стає оцифрованою і покладається на технології приватного сектору.

Інша практична проблема пов'язана з відмінностями в протоколах безпеки та стандартах обробки даних між різними відомствами. Ці відмінності можуть створювати проблеми сумісності, коли потрібно швидко обмінюватися інформацією. Наприклад, державна розвідувальна служба може класифікувати певні дані як дуже чутливі і обмежити до них доступ, тоді як правоохоронні органи потребують негайного доступу до цих даних для проведення розслідування в режимі реального часу [4]. Коли різні стандарти класифікації даних і протоколи доступу створюють бар'єри для обміну інформацією, скоординовані дії стають проблематичними. Така несумісність протоколів безпеки затримує здатність відомств працювати злагоджено, що підкреслює необхідність стандартизованих практик, які сприяють безперешкодній міжвідомчій співпраці.

У деяких випадках існуюча законодавча база сприяє виникненню цих проблем, будучи або занадто широкою, або занадто конкретною, що обмежує гнучкість відомств у їхніх діях відповідно до потреб у реальному часі. Закони, які жорстко закріплюють певні обов'язки без можливості їх спільного коригування, ускладнюють динамічну адаптацію відомств до своїх ролей. Такий жорсткий розподіл повноважень може завадити відомствам ефективно об'єднувати свої ресурси, тим самим перешкоджаючи колективному реагуванню на нові виклики безпеці.

Для вирішення цих проблем міжвідомчої координації необхідна всеосяжна, чітко визначена система комунікації, яка б відповідала ролям і оперативним потребам кожного відомства. Така система має визначати пріоритети створення систем обміну інформацією в режимі реального часу, чіткого розподілу ролей і стандартизованих протоколів передачі даних для створення цілісної та ефективної структури реагування. Крім того, запровадження регулярних міжвідомчих тренувань та симуляцій, спрямованих на скоординоване реагування на загрози, може посилити здатність відомств до співпраці [5]. Наприклад, періодичні спільні навчання за участю підрозділів розвідки, кібербезпеки та правоохоронних органів можуть значно покращити скоординоване реагування на кіберінциденти, забезпечивши розуміння кожним підрозділом своєї ролі та ширшої стратегічної мети.

Активні військові конфлікти в Україні створюють унікальні та складні виклики для забезпечення надійної інформаційної безпеки. Ці конфлікти викрили критичну роль інформаційної безпеки у захисті національної інфраструктури, оскільки кібернетичні та гібридні загрози все частіше використовуються як інструменти дестабілізації та маніпуляції. Досвід України підкреслює важливість комплексного підходу до інформаційної безпеки, що поєднує стратегії цифрового захисту з традиційними заходами безпеки. Як наслідок, існує нагальна потреба у стійких, згуртованих механізмах безпеки для захисту як від фізичних, так і від цифрових посягань на національний суверенітет. У ситуаціях, коли військові дії поєднуються з кібератаками на урядові системи зв'язку, перебої можуть послабити контроль держави над критично важливими інформаційними каналами, що загрожує громадській безпеці та військовій таємниці. Це середовище подвійних загроз вимагає від України запровадження багаторівневої моделі безпеки, яка включає превентивні та реактивні заходи як для звичайних, так і для цифрових загроз.

Конфлікти в Україні висвітлили появу гібридних загроз, коли цифрові атаки синхронізуються з фізичними операціями для досягнення максимального ефекту. Така гібридна тактика часто націлена на об'єкти критичної інфраструктури, такі як енергетичні системи, транспортні мережі та фінансові установи, що призводить до широкомасштабних руйнувань [6]. Атаки такого характеру показують, що без надійного захисту кібербезпеки здатність країни реагувати на військові операції в реальному часі серйозно підривається. Уроки, винесені з цих скоординованих атак, підкреслюють важливість інтеграції засобів захисту кібербезпеки з наземними військовими стратегіями для забезпечення стійкості.

Вразливості кібербезпеки також посилюються під час конфлікту, оскільки ворожі суб'єкти часто використовують ці періоди для проведення інтенсивних атак. Триваючий військовий конфлікт виявив слабкі місця в державних інформаційних системах, які, якщо їх не усунути, можуть дозволити зловмисникам проникнути в них і скомпрометувати конфіденційні дані. Під час військової ескалації першочерговими цілями стають системи зв'язку, які необхідні для координації військових дій та заходів безпеки цивільного населення. В Україні несанкціонований доступ до цих систем може поставити під загрозу як стратегічне планування, так і громадську безпеку, розкриваючи секретну інформацію супротивникам. Тому посилення кіберзахисту цих комунікаційних мереж стало необхідним для захисту національних інтересів.

Досвід України демонструє, що без зла-

годжених механізмів безпеки інформаційна сфера залишається вразливою. Під час військових операцій державні органи повинні швидко координувати реагування між різними секторами, включаючи уряд, армію та державні служби. Ця потреба в координації в режимі реального часу ускладнюється, коли протоколи безпеки та інфраструктура є фрагментованими. Коли кіберзахист не узгоджується або погано інтегрований з іншими заходами державної безпеки, відомствам стає складно злагоджено реагувати на нові загрози [7]. Такі затримки знижують ефективність реагування, підкреслюючи необхідність уніфікованих систем інформаційної безпеки, які підтримують швидкі, скоординовані дії в усіх секторах.

Характер сучасних військових операцій також вимагає превентивного підходу до інформаційної безпеки. Кіберзагрози стали невід'ємною складовою війни, і ситуація в Україні ілюструє необхідність проактивної оборони, здатної передбачати і пом'якшувати загрози до того, як вони матеріалізуються. У деяких випадках противники використовують соціальні мережі та цифрові платформи для поширення дезінформації та пропаганди, намагаючись вплинути на громадську думку та послабити моральний дух. Така форма цифрових маніпуляцій може дестабілізувати суспільну згуртованість, що підкреслює важливість комплексних стратегій інформаційної безпеки, які включають протидію психологічним та інформаційним загрозам. У відповідь на це українські відомства почали розробляти механізми моніторингу та протидії таким загрозам в Інтернеті, визнаючи, що інформаційна безпека має виходити за межі кібербезпеки і охоплювати ширший цифровий ландшафт.

Виклики, з якими стикається Україна, ще більше підкреслюють важливість міжнародної співпраці у зміцненні інформаційної безпеки. За підтримки міжнародних партнерів Україна реалізує транскордонні ініціативи з кібербезпеки для протидії зовнішнім загрозам. Так, партнерство з міжнародними організаціями з кібербезпеки дозволило Україні отримати доступ до передових розвідувальних даних про загрози та технічних ресурсів, які посилюють її обороноздатність. Спільні зусилля, такі як ці партнерства, демонструють, як міжнародні альянси надають Україні додаткові рівні захисту, особливо від складних кіберзагроз, що походять від державних суб'єктів. Беручи участь у спільних оборонних структурах, Україна краще підготовлена до протистояння різноманітним, складним загрозам, які супроводжують сучасні військові конфлікти.

Відомі вчені в Україні та світі, такі як І. Боднар, С. Гончар, В. Демиденко та О. Зозуля, зробили значний внесок у розуміння та управління інформаційними ризиками. Їхні дослідження підкреслюють необхідність механізмів інформаційної безпеки, які включають поєднання соціального, політичного та правового вимірів. Розглядаючи інформаційну безпеку за допомогою багатовимірного підходу, ці вчені підкреслюють, наскільки взаємопов'язаними стали сучасні ризики безпеки, що вимагає комплексних стратегій, які реагують на різні загрози. Зокрема, Боднар обговорює, як політична стабільність і соціальна стійкість є невід'ємними складовими інформаційної безпеки, припускаючи, що захисні заходи повинні бути чутливими до соціально-політичного контексту, в якому вони діють. Така перспектива заохочує розробку систем інформаційної безпеки, які враховують і адаптуються до суспільних настроїв і політичної динаміки, що впливають на їхню ефективність.

На додаток до поєднання цих сфер, Демиденко вказує на важливість адаптивної структури, яка розвивається у відповідь на швидкі зміни цифрових загроз. З розвитком цифрових технологій змінюються і тактики, які використовують зловмисники. Демиденко стверджує, що статичні або надто жорсткі протоколи безпеки часто не справляються з сучасними кіберзагрозами, які є динамічними і часто непередбачуваними. Системи безпеки повинні постійно оновлюватися, щоб включати нові дані про моделі загроз, такі як зростання кількості атак з вимогами викупу, спрямованих на урядові дані [8]. Наприклад, механізм безпеки, який розвивається шляхом інтеграції розвідданих про загрози в режимі реального часу, буде краще оснащений для виявлення і нейтралізації нових атак, пропонуючи практичну модель адаптивного захисту.

Внесок Гончара підкреслює цінність правової бази, яка підтримує інформаційну безпеку. Правові структури забезпечують основу для впровадження заходів кібербезпеки і визначення ролей різних відомств, що беруть участь у захисті національних даних. Гончар стверджує, що законодавство має уможливлювати швидкі дії та встановлювати чітку підзвітність для різних зацікавлених сторін, що є важливим для скоординованого реагування на інформаційні загрози [9]. Забезпечення чітких повноважень усіх відомств діяти і співпрацювати відповідно до правових норм, робить загальний механізм безпеки більш згуртованим і стійким.

О. Зозуля зосереджується на інтеграції соціально-політичних факторів у стратегії інформаційної безпеки, визнаючи, що громадське сприйняття та комунікація є ключовими для ефективного управління загрозами. У своїх роботах Зозуля висвітлює, як дезінформаційні кампанії або психологічні операції можуть послабити стійкість суспільства та вплинути на національну безпеку. Він виступає за включення стратегій громадської кому-

нікації в інформаційну безпеку для протидії дезінформації та зміцнення суспільної довіри. На практиці Зозуля пропонує, щоб механізми інформаційної безпеки включали моніторинг ЗМІ та інформаційно-просвітницькі програми для боротьби з цифровою дезінформацією [10]. Наприклад, проактивна інформаційно-просвітницька ініціатива, спрямована на боротьбу з неправдивими наративами в соціальних мережах, може зменшити вплив дезінформації, що в кінцевому підсумку зміцнить довіру громадськості до органів безпеки та загальну стабільність держави.

Разом ці дослідження підкреслюють необхідність комплексного, багатогранного підходу в сучасному складному безпековому ландшафті. Їхні роботи ілюструють, як поєднання правових, соціальних і політичних елементів у механізмах інформаційної безпеки створює надійну систему захисту, здатну протистояти різноманітним викликам, що постають перед сучасними цифровими загрозами. Такий підхід відповідає еволюційній природі інформаційної безпеки, оскільки надає пріоритет адаптивності та багаторівневій взаємодії, посилюючи стійкість державних механізмів в управлінні як очікуваними, так і неочікуваними ризиками.

Крім того, ці матеріали показують, що інформаційна безпека - це не просто технічне питання, а комплексний виклик, який вимагає співпраці між різними секторами. Багатовимірний підхід до безпеки, який поєднує технічні засоби захисту з політичною обізнаністю, правовими повноваженнями та залученням громадськості, забезпечує всебічний захист від різноманітних ризиків, з якими стикаються сьогодні. Узгодивши ці елементи, система інформаційної безпеки України може бути краще підготовлена до протистояння складним викликам, гарантуючи, що захисні механізми будуть стійкими, оперативними та здатними підтримувати національну безпеку в цифровому середовищі, що швидко розвивається.

Висновки та перспективи подальших досліджень. У даному досліджені було підтверджено важливість комплексного підходу до забезпечення інформаційної безпеки держави, особливо для країн, які стикаються з гібридними загрозами, як Україна. Воно підкреслює необхідність інтеграції правового, соціального та політичного вимірів у рамках інформаційної безпеки для ефективної протидії складним сучасним цифровим загрозам. Завдяки такій багатовимірній стратегії можна створити надійний, адаптивний механізм захисту, здатний протистояти як поточним, так і новим викликам. Обгрунтовано роль чіткої правової бази та скоординованої міжвідомчої комунікації у скороченні часу реагування та підвищенні загальної стійкості структур інформаційної безпеки. Створення протоколів обміну інформацією в режимі реального часу та стандартизованих процедур управління даними між відомствами має вирішальне значення для цілісної національної безпеки.

Майбутні дослідження можуть бути зосереджені на вдосконаленні адаптивних моделей, які інтегрують розвідку загроз і машинне навчання для проактивного передбачення і пом'якшення загроз. Крім того, поглиблення міжнародної співпраці може надати меншим або вразливим державам доступ до передових ресурсів кібербезпеки і розвідувальних мереж, зміцнюючи таким чином їхню інфраструктуру інформаційної безпеки. Оскільки кіберзагрози продовжують розвиватися, поточні дослідження повинні бути спрямовані на узгодження внутрішньої політики безпеки з глобальними стандартами кібербезпеки для підвищення національної та міжнародної стійкості перед обличчям все більш витончених цифрових загроз.

ЛІТЕРАТУРА:

1. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України : монографія / за ред. П. Д. Біленчука. Харків:2018. 289 с.

2. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / заг. ред. Р. А. Калюжний. *Центр навч.-наук. та наук.-практ. вид. НА СБ України*, 2014. 196 с.

3. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : *Гельветика*, 2017. 168 с.

4. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. … канд. юрид. наук : 12.00.07. Львів, 2019. 268 с.

5. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. ... д-ра юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

6. Авер'янова Н.М. Гібридна війна: російськоукраїнське протистояння. *Науковий журнал «Молодий вчений»*. 2017. № 3(43). С. 30–34.

7. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. К.: *НІСД*, 2016. 109 с.

8. Демиденко В. Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки. *Юридичний часопис НАВС*. 2018. № 1. С. 141–153.

9. Гончар, С. Ф. (2014). Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України: матеріали круглого столу. Київ, *НАДУ при Президентові України (кафедра національної безпеки)*, С. 92-95.

10. Зозуля О. Фейк як інструмент інформаційної війни. *Юридична газета*. 2019. № 19(673). URL: https://yur-gazeta.com/publications/practice/inshe/feyk-yakinstrument-informaciynoyi-viyni.html