УДК 351.861.3:004.056

Д. І. Прокопович-Ткаченко, В. П. Звєрєв, І. М. Козаченко

СУЧАСНИЙ ВИКЛИК ЦИФРОВОГО СВІТУ І РОЛЬ НАЦІОНАЛЬНОГО КООРДИНАЦІЙНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Проаналізовано роль Національного координаційного центру кібербезпеки у формуванні системи захисту держави. Оцінено його ефективність у протидії таким сучасним загрозам, як кібератаки та інформаційна агресія. Визначено також ключові функції Національного координаційного цетру кібербезпеки: моніторинг загроз, координація суб'єктів кібербезпеки, упровадження новітніх технологій.

Запропоновано напрями вдосконалення національної системи кібербезпеки й забезпечення цифрової стійкості держави. Наголошено на необхідності гармонізації законодавства з міжнародними стандартами. Акцентовано увагу на важливості співпраці державних і приватних інституцій у сфері кіберзахисту.

Ключові слова: *інформація, безпека, кіберзагрози, моніторинг, інфраструктура, технології, стандарти.*

Постановка проблеми. Стрімкий розвиток цифрових технологій супроводжується появою нових загроз, які впливають на інформаційну безпеку держави. Зокрема, збільшення кількості та складності кібератак створює серйозні виклики для захисту критичної інформаційної інфраструктури [1]. Використання інформаційно-комунікаційних технологій у державному управлінні, фінансовій сфері та обороні значно підвищує ризики несанкціонованого доступу до інформації, маніпулювання даними й порушення функціонування державних систем [2]. У зв'язку з цим виникає необхідність розроблення комплексних стратегій кіберзахисту, які передбачають ефективний моніторинг загроз, координацію між суб'єктами кібербезпеки та впровадження сучасних технологій захисту [3].

Національний координаційний центр кібербезпеки (НКЦК) відіграє ключову роль у забезпеченні інформаційної безпеки України. Він координує заходи, спрямовані на захист державної кіберінфраструктури, протидію кібератакам та гармонізацію національних стандартів із міжнародними вимогами [4]. Однак зростання складності кіберзагроз вимагає постійного вдосконалення методів аналізу, прогнозування й нейтралізації потенційних атак. Такі технології, як штучний інтелект, аналіз великих даних, автоматизовані системи кіберзахисту, стають важливими інструментами у боротьбі з цифровими загрозами [5]. Проте ж ефективність заходів кібербезпеки залежить не лише від технологічних рішень, а й від нормативно-правового забезпечення, міжнародного співробітництва та кадрового потенціалу [6].

Аналіз останніх досліджень і публікацій. Проблематика інформаційної безпеки та кіберзахисту державних структур є предметом численних наукових досліджень. У значній кількості праць здійснено аналіз сучасних кіберзагроз, оцінювання ефективності заходів протидії та розроблення стратегічних підходів до забезпечення інформаційної безпеки.

На дедалі більшій ролі державних органів у створенні механізмів оперативного виявлення та нейтралізації загроз наголошує М. Гуцалюк [3]. На його думку, розвиток інформаційно-комунікаційних технологій значно посилює уразливість державних структур перед кібератаками, тому необхідне постійне вдосконалення національної системи кіберзахисту.

Питання інтеграції міжнародного досвіду у сферу інформаційної безпеки України розглядає Є. Захаров, зазначаючи, що співпраця з такими міжнародними організаціями, як НАТО та ЄС, сприяє підвищенню ефективності кіберзахисту через адаптацію провідних світових практик до національних реалій [4].

Важливим аспектом кібербезпеки І. Лосєв вважає використання штучного інтелекту та аналізу великих даних для прогнозування загроз [5]. У своєму дослідженні він обґрунтовує, що застосування автоматизованих систем моніторингу дають змогу значно скоротити час реагування на інциденти та підвищити загальну ефективність кіберзахисту державних структур.

Водночас у низці праць наголошується на необхідності вдосконалення нормативно-правової бази у сфері кібербезпеки. Так, на думку О. Нестеренка [6], швидкий розвиток цифрових технологій потребує регулярного оновлення законодавства для ефективної протидії новітнім загрозам.

Отже, робимо висновок, що одним із ключових викликів у сфері кібербезпеки є необхідність підвищення рівня координації між державними органами, розширення міжнародного співробітництва та впровадження інноваційних технологій для захисту критичної інформаційної інфраструктури. У цьому контексті діяльність Національного координаційного центру кібербезпеки має стратегічне значення для забезпечення інформаційної безпеки держави.

Метою статті є комплексний аналіз ролі Національного координаційного центру кібербезпеки у забезпеченні інформаційної безпеки держави в умовах сучасних цифрових викликів, а також дослідження його функцій і завдань щодо координації між державними органами, приватним сектором і міжнародними партнерами.

Особливу увагу приділено питанням моніторингу та аналізу кіберзагроз, розвитку нормативно-правової бази, упровадженню сучасних технологій кіберзахисту, зокрема штучного інтелекту та аналізу великих даних для прогнозування атак [2]. Окремо розглядається вплив міжнародного досвіду та стратегій співробітництва України з ЄС та НАТО у сфері кібербезпеки [3].

Результати дослідження дають змогу сформулювати практичні рекомендації щодо вдосконалення механізмів кіберзахисту, зокрема в аспекті зміцнення координації між суб'єктами кібербезпеки, посилення технічних можливостей НКЦК та адаптації міжнародних стандартів до національної практики [4].

Виклад основного матеріалу. Дослідження функціонування Національного координаційного центру кібербезпеки як головного елемента управління інформаційною безпекою держави здійснено на основі міждисциплінарного підходу, що включає методи системного аналізу, математичного моделювання, оброблення великих даних і машинного навчання.

Для оцінювання ефективності роботи НКЦК застосовано метод системного аналізу, який дає змогу розглянути Центр як частину складної кібербезпекової інфраструктури, що взаємодіє з державними органами, приватним сектором і міжнародними партнерами. Використано методику моделювання взаємодії суб'єктів кібербезпеки для аналізу впливу Центру на загальну стійкість національної інформаційної інфраструктури. У моделюванні кіберзагроз і прогнозуванні атак застосовуються методи штучного інтелекту й машинного навчання, що дає змогу оцінювати поточні тенденції та передбачати розвиток загроз у цифровому просторі. Використано алгоритми кластерного аналізу і глибокого навчання для виявлення закономірностей у кіберінцидентах. Оцінювання вразливості критичної інформаційної інфраструктури здійснювалося методами математичного моделювання, зокрема побудовою моделей атак, та сценарного аналізу, що уможливлює розроблення адаптивних механізмів реагування. Застосовано ймовірнісні моделі оцінювання ризиків для аналізу потенційних загроз у реальному часі. Під час оцінювання інформаційної взаємодії між НКЦК та іншими суб'єктами кібербезпеки використовувалися методи мережевого аналізу для виявлення ключових вузлів інформаційного обміну та оцінювання ефективності координаційних механізмів. Проведено аналіз потоку даних між державними структурами, приватними компаніями та міжнародними партнерами для виявлення можливих точок уразливості. Оцінювання відповідності законодавчої бази міжнародним стандартам здійснювалося методами порівняльного аналізу, що уможливило виявлення розбіжностей між чинними нормативно-правовими актами України і рекомендаціями таких міжнародних організацій, як ЄС і НАТО. Результати дослідження ґрунтуються на аналізі відкритих джерел, зокрема звітів міжнародних організацій, наукових публікацій, аналітичних матеріалів та офіційних документів державних органів, що дало змогу забезпечити об'єктивність і наукову обґрунтованість висновків.

Ключовими функціями Національного координаційного центру кібербезпеки є моніторинг кіберзагроз, розроблення стратегій захисту та інтеграція таких сучасних технологій, як штучний інтелект і аналіз великих даних [3]. Завдяки цьому НКЦК відіграє провідну роль у побудові стійкої екосистеми кібербезпеки, яка здатна ефективно реагувати на сучасні виклики, прогнозувати потенційні загрози й координувати міжвідомчу взаємодію [4].

Особлива увага приділяється впровадженню адаптивних механізмів управління, що дають змогу системі швидко реагувати на зміни у зовнішньому середовищі, мінімізуючи ризики для держави [5]. У цьому контексті гармонізація нормативно-правової бази з міжнародними стандартами також відіграє вирішальну роль у підвищенні ефективності заходів кіберзахисту [6].

Отже, НКЦК виступає не лише як головний координаційний орган, але й як інтеграційний елемент, що забезпечує узгодженість дій усіх суб'єктів системи інформаційної безпеки. Його діяльність

спрямована на зміцнення стійкості держави до кібератак, формування безпечного інформаційного середовища та створення стратегічно орієнтованої моделі кіберзахисту [7].

У сучасному цифровому світі стрімкий розвиток інформаційно-комунікаційних технологій створює нові можливості для державного, економічного й соціального розвитку, водночас супроводжуючись численними викликами та загрозами для інформаційної безпеки. Захист критичної інформаційної інфраструктури, протидія кібератакам та інформаційній агресії стали ключовими напрямами забезпечення національної безпеки. Складна система інформаційної безпеки держави ґрунтується на інтеграції різних елементів (технології, процеси, людські ресурси та інфраструктура), що взаємодіють у єдиній екосистемі. У цьому контексті особливої актуальності набуває визначення ролі Національного координаційного центру кібербезпеки як головної ланки складної системи інформаційної безпеки держави [1]. Розглянемо його основні функції. Глибоке розуміння цих функцій є підґрунтям для аналізу ефективності та перспектив подальшого розвитку системи кібербезпеки України [2].

Національний координаційний центр кібербезпеки виконує також низку важливих функцій, які забезпечують інтеграцію та узгодженість дій суб'єктів системи кібербезпеки, спрямованих на захист інформаційного простору держави. Одна з ключових функцій полягає у постійному моніторингу кіберзагроз: виявлення потенційних атак, аналіз шкідливого програмного забезпечення, оцінювання рівня ризиків для державної інформаційної інфраструктури [3]. Центр забезпечує цілодобовий моніторинг кіберпростору, використовуючи передові технології аналізу великих даних і штучного інтелекту для оперативного виявлення загроз [5]. Завдяки цьому НКЦК може прогнозувати розвиток атак і своєчасно впроваджувати заходи захисту.

Національний координаційний центр кібербезпеки відіграє провідну роль у захисті критичної інформаційної інфраструктури держави. Здійснюються розроблення стандартів безпеки, тестування систем на вразливості та впровадження сучасних захисних механізмів [4]. Особлива увага приділяється захисту енергетичних, фінансових, транспортних і комунікаційних систем, які є об'єктами найпотужніших кібератак [3]. У своїй діяльності Центр також ґрунтується на міжнародному досвіді і стандартах, що сприяє підвищенню рівня захищеності інфраструктури [6]. Одне з головних завдань НКЦК полягає в забезпеченні координації між державними структурами, приватним сектором, академічними установами й міжнародними партнерами. Центр узгоджує дії різних суб'єктів кібербезпеки для ефективного обміну інформацією щодо загроз, уникнення дублювання функцій і підвищення ефективності спільних заходів [1]. Особливо важливою є співпраця з міжнародними організаціями (НАТО та ЄС), що дає змогу Україні адаптувати найкращі практики й технології.

НКЦК активно займається аналізом поточних загроз і прогнозуванням їх розвитку. Для цього Центр використовує інструменти аналізу великих даних, штучного інтелекту й машинного навчання [5]. Це робить можливим не лише оцінювання поточних тенденцій у сфері кіберзагроз, але й створення моделей для прогнозування можливих атак у майбутньому. Такі інструменти важливі для стратегічного планування і визначення пріоритетів у сфері кібербезпеки [7].

У межах моделювання інформаційної безпеки держави як складної техногенної системи пропонується розглядати Національний координаційний центр кібербезпеки головним елементом управління, котрий впливає на всі компоненти системи. НКЦК виступає інтегратором і регулятором, що забезпечує координацію між складниками системи, підтримуючи її функціональну цілісність та адаптивність до зовнішніх і внутрішніх загроз. У контексті технічної інфраструктури НКЦК має забезпечувати постійний моніторинг усіх її елементів: сервіси, сервери, мережі зв'язку та системи захисту включно. Центр упроваджує механізми автоматичного виявлення вразливостей і оновлення захисних засобів, що дає змогу мінімізувати ризики, пов'язані з неправильними налаштуваннями чи відсутністю оновлень. Для цього активно використовуються такі сучасні технології, як штучний інтелект та аналіз великих даних. В організаційних процесах НКЦК відіграє роль стратегічного координатора, забезпечуючи узгодженість підходів до управління ризиками, розроблення політик безпеки та планування реагування на інциденти. Центр запроваджує навчальні програми для підвищення компетенції персоналу, який відповідає за інформаційну безпеку, та контролює дотримання стандартів безпеки в усіх секторах. Особливу увагу НКЦК приділяє людському фактору, адже персонал є важливим елементом у системі інформаційної безпеки. Центр упроваджує стандарти безпечної поведінки, програми навчання та механізми оперативної підтримки користувачів. Здійснюються також заходи щодо запобігання внутрішнім загрозам, пов'язаним із діяльністю інсайдерів чи зловмисників. Отже, НКЦК виконує критично важливу роль у забезпеченні взаємодії між

усіма елементами системи інформаційної безпеки держави, створюючи умови для її функціональної стійкості та ефективного реагування на сучасні виклики.

На рисунку 1 зображено структуру Національного координаційного центру кібербезпеки як головного елемента управління у складній моделі інформаційної безпеки держави.

Рисунок 1 – Структура НКЦК та ключові елементи

Національний коорднаційний центр кібербезпеки міститься в центрі системи і впливає на всі її компоненти, забезпечуючи координацію, моніторинг та управління ризиками. Технічна інфраструктура (сервери, мережі зв’язку та системи захисту) підпадає під постійний моніторинг із боку НКЦК. Центр забезпечує виявлення вразливостей, запровадження сучасних технологій і контроль за стабільністю технічних засобів захисту. Організаційні процеси, які охоплюють управління ризиками, формування політик безпеки та планування реагування на інциденти, координуються НКЦК для забезпечення інтеграції стандартів і узгодженості дій між усіма суб’єктами кібербезпеки. Людський фактор становить важливий складник, що охоплює навчання персоналу, підтримку безпеки та моніторинг дій користувачів. НКЦК забезпечує упровадження навчальних програм, стандартів поведінки та мінімізацію ризиків, пов’язаних із людськими помилками. Такі інформаційні ресурси, як критичні дані, канали зв’язку та секретна інформація, захищаються через постійний контроль із боку НКЦК, що забезпечує їх збереження та недоступність для зловмисників. Зовнішні загрози, зокрема кібератаки, геополітичні ризики й екологічні виклики, аналізуються і прогнозуються, НКЦК організує протидію цим загрозам. Отже, НКЦК відіграє ключову роль у формуванні інтегрованої системи захисту інформації, забезпечуючи її адаптивність і стійкість до сучасних викликів.

Розвиток технологічної бази для протидії постквантовим загрозам є одним із ключових напрямів удосконалення Національного координаційного центру кібербезпеки. З огляду на потенційну небезпеку, яку становлять постквантові обчислення, НКЦК має адаптувати існуючі системи безпеки до нових викликів. Ідеться про впровадження криптографічних алгоритмів, стійких до квантових атак, що дасть змогу забезпечити захист критичних даних навіть у разі зламу традиційних методів шифрування. Потребують також інтегрування квантові генератори випадкових чисел, які підвищують надійність ключів шифрування.

У рамках розвитку самоорганізуючих і адаптивних механізмів НКЦК має впроваджувати системи автоматичного моніторингу та реагування на кіберзагрози, які базуються на технологіях штучного інтелекту та машинного навчання. Завдяки цьому Центр зможе не лише оперативно виявляти і нейтралізувати загрози, але й адаптувати існуючі політики безпеки до змін у цифровому середовищі. Важливим складником є створення децентралізованих мереж безпеки на базі блокчейн-технологій, які забезпечують надійність і стійкість систем до зовнішніх впливів.

Центр також повинен активізувати співпрацю з міжнародними партнерами для обміну досвідом у протидії постквантовим загрозам та інтеграції кращих світових практик у національну систему кібербезпеки. Потребує вдосконалення законодавча база у сфері інформаційної безпеки з огляду на

перспективи розвитку квантових технологій і необхідність інтеграції міжнародних стандартів у національну практику. Це передбачає створення нормативних актів, спрямованих на захист критичної інформаційної інфраструктури від новітніх загроз, а також забезпечення підтримки наукових досліджень у сфері постквантової криптографії та квантових обчислень. Отже, розвиток НКЦК як ключового елемента інформаційної безпеки держави має бути спрямований на створення інтегрованої системи, здатної не лише протистояти сучасним викликам, але й адаптуватися до майбутніх загроз у постквантовому світі.

На схемі (рисунок 2) змодельовано основні процеси реалізації Національного координаційного центру кібербезпеки як головного елемента державної системи кіберзахисту.

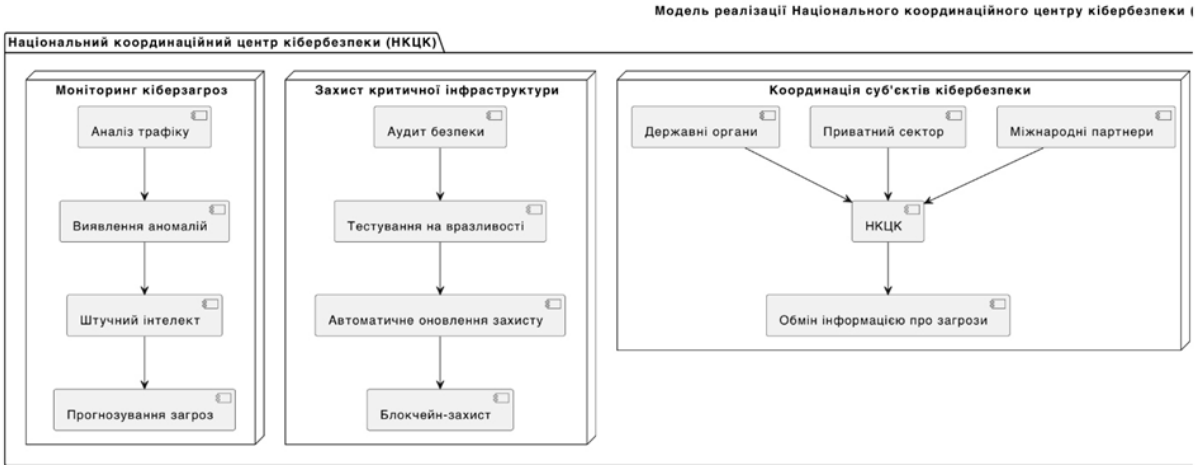

Рисунок 2 – Модель реалізації НКЦК

Моніторинг кіберзагроз здійснюється шляхом аналізу мережевого трафіку, виявлення аномалій за допомогою штучного інтелекту та прогнозування потенційних загроз. Захист критичної інфраструктури забезпечується аудитом безпеки, тестуванням на вразливість, автоматичним оновленням захисту та інтеграцією блокчейн-технологій. Координація суб'єктів кібербезпеки полягає у забезпеченні взаємодії між державними органами, приватним сектором і міжнародними партнерами для обміну інформацією про загрози. Розвиток кадрового потенціалу передбачає створення навчальних програм, сертифікацію фахівців, підвищення кваліфікації та формування експертного середовища. Інтеграція постквантових технологій включає розроблення криптографічних алгоритмів, стійких до квантових атак, квантові генератори випадкових чисел і децентралізовані мережі безпеки. Схема відображає взаємозв'язок між цими компонентами й демонструє, як Національний координаційний центр кібербезпеки виконує функції моніторингу, аналізу, координації та захисту інформаційної інфраструктури держави.

Отже, Національний координаційний центр кібербезпеки є головним елементом системи кібербезпеки держави, який забезпечує моніторинг загроз, захист критичної інфраструктури, координацію міжсекторальної взаємодії та прогнозування майбутніх викликів [1, 2]. Його діяльність сприяє формуванню безпечного цифрового середовища, яке відповідає сучасним викликам.

Висновки

Національний координаційний центр кібербезпеки являє собою ключовий елемент національної системи кібербезпеки, забезпечуючи координацію між державними органами, приватним сектором і міжнародними партнерами. Аналіз сучасних тенденцій у сфері інформаційної безпеки свідчить про необхідність удосконалення механізмів моніторингу кіберзагроз, інтеграції передових технологій і розроблення ефективних стратегій реагування на кібератаки. Упровадження штучного інтелекту й аналізу великих даних дає змогу значно підвищити рівень кіберзахисту, сприяючи проактивному виявленню загроз та оперативному ухваленню рішень. Розширення повноважень Національного координаційного центру кібербезпеки у сфері захисту критичної інформаційної інфраструктури вимагає інтеграції постквантових технологій і розроблення нових криптографічних методів, стійких до атак квантових комп'ютерів. Використання квантових генераторів випадкових чисел і децентралізованих систем безпеки на основі блокчейну є перспективними напрямами для зміцнення

інформаційного захисту держави. Водночас упровадження цих технологій потребує значних фінансових вкладень і створення відповідної нормативно-правової бази, яка регламентуватиме їх використання.

Одним із головних викликів у розвитку Національного координаційного центру кібербезпеки залишається забезпечення ефективної взаємодії між усіма суб'єктами кібербезпеки. Новітній підхід передбачає створення централізованої платформи для обміну інформацією про кіберзагрози, що забезпечить оперативне реагування на потенційні атаки й запобігатиме їх негативним наслідкам. Координація між державним сектором, бізнесом і науковими установами відіграє вирішальну роль у розбудові стійкої кіберекосистеми.

Підготовка кадрів у сфері кібербезпеки потребує окремої уваги, оскільки дефіцит висококваліфікованих фахівців є одним із ключових чинників, який обмежує розвиток ефективної системи захисту. Необхідним вбачається впровадження спеціалізованих освітніх програм, сертифікація експертів і створення умов для безперервного професійного розвитку.

Отже, Національний координаційний центр кібербезпеки відіграє провідну роль у забезпеченні інформаційної безпеки держави, проте його подальший розвиток потребує комплексного підходу. Ідеться про технологічні інновації, удосконалення нормативно-правового регулювання, розширення міжнародної співпраці та посилення кадрового потенціалу. Інтеграція сучасних методів аналізу загроз, автоматизація процесів реагування та адаптація до таких викликів майбутнього, як постквантові загрози, дадуть змогу Україні створити ефективну та стійку систему кіберзахисту, здатну протистояти сучасним загрозам цифрового світу.

Перелік джерел посилання

1. Булашенко А. В., Бруй М. Інформаційна безпека : *зб. тез доп. Наук.-метод. конф. викладачів, співробітників, студентів*, Суми, 28 квіт. 2010 р. Суми : СумДУ, 2010. Ч. 2. С. 13–16. URL: https://surl.lu/zflugg (дата звернення: 08.02.2025).
2. Потапенко О. К. Державна інформаційна політика та безпека. *Вісник Київського національного університету імені Тараса Шевченка. Філософія. Політологія.* 2011. № 102. С. 48–51.
3. Гуцалюк М. Інформаційна безпека у сучасному суспільстві. *Право України.* 2005. № 7. С. 71–74.
4. Захаров Є. Інформаційна безпека: що захищаємо? *Свобода висловлювань і приватність.* 2013. № 4. С. 3–6.
5. Лосєв І. Інформаційна безпека: як укріпити. *День*. 2014. № 82–83. С. 19.
6. Нестеренко О. Свобода інформації чи інформаційна безпека? *Свобода висловлювань і приватність*. 2011. № 1. С. 3–9.
7. Althobaiti O. S., Dohler M. (2020). Cybersecurity Challenges Associated With the Internet of Things in a Postquantum World. *IEEE Access*, vol. 8. DOI: 10.1109/ACCESS.2020.3019345.
8. Батечко О., Цимбаленко Н. В. Інформаційна безпека підприємства. *Наукові розробки молоді на сучасному етапі*: тези доп. XV всеукр. наук. конф. молодих учених та студентів, Київ, 28–29 квіт. 2016. Київ, 2016. URL: https://surl.li/vrykvu (дата звернення: 09.02.2025).
9. Адміністрація. Національний кластер кібербезпеки. 2023. URL: https://surl.li/qmqkwt (дата звернення: 09.02.2025).
10. Глушков В. Інформаційна безпека (соціально-правові аспекти). *Право України*. 2010. № 9. С. 311–313.
11. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8 (58). С. 11–18.
12. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р. № 242-2016 URL: https://surl.li/dyvbwc (дата звернення: 09.02.2025).
13. Zawoad S., Hasan R. Proof of past data possession in Cloud Forensics. Proceedings of International Conference on Cyber Security (USA, New York, December 14–16, 2012). URL: https://arxiv.org/abs/1211.4328 (дата звернення 10.02.2025).
14. Weber R. (2010). Internet of Things – New Security and Privacy Challenges. *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30. DOI: 10.1016/j.clsr.2009.09.008.
15. Соловій Г. Р. Міжнародна інформаційна безпека: польський досвід, *Актуальні проблеми міжнародних відносин*. 2006. № 65, ч. 1. С. 45–47.

16. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ* (серія юридична). 2023. № 1. С. 28–35. DOI: 10.32782/2311-8040/2023-1-4.

17. Conti M., Dehghantanha A., Franke K., Watson S. (2018). Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, vol. 78, pp. 544–546. DOI: 10.1016/j.future.2017.09.007.

18. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2024. № 18. Ст. 76. URL: https://surl.li/enchzc (дата звернення: 08.02.2025).

19. Маракова І. І., Сиропятов О. А. Інформаційна безпека комплексних систем зв'язку. *Ukrainian Information Security Research Journal*. 2006. Т. 8. Вип. 4 (31). URL: https://surl.li/qmopwp (дата звернення 11.02.2025).

20. Суббот А. Інформаційна безпека суспільства. *Віче.* 2015. № 8 (388). С. 29–31.

21. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. (2015). Security, Privacy and Trust in Internet of Things: *The Road Ahead. Computer Networks*, vol. 76, pp. 146–164. DOI: 10.1016/j.comnet.2014.11.008.

Стаття надійшла до редакції 07.03.2025 р.

UDC 351.861.3:004.056

D. Prokopovych-Tkachenko, V. Olenchenko, V. Zvieriev, I. Kozachenko

MODERN CHALLENGES OF THE DIGITAL WORLD AND THE ROLE OF NCCC IN ENSURING STATE INFORMATION SECURITY

The rapid advancement of digital technologies presents new opportunities for economic, social, and cultural development while simultaneously generating numerous threats that negatively impact national security. Information security, as an integral part of national security, is a crucial element in countering modern threats, such as cyberattacks, information warfare, and disruptions in critical infrastructure. In this context, the National Coordination Center for Cybersecurity (NCCC) plays a key role in coordinating, integrating, and managing measures aimed at ensuring state information security. The NCCC performs a range of vital functions, including cybersecurity threat monitoring, analysis of emerging trends in the cybersecurity domain, incident response, and the implementation of protective strategies. The center coordinates collaboration between government agencies, the private sector, academic institutions, and international partners. A significant focus is placed on developing security standards for critical information infrastructure, threat forecasting, and establishing effective cybersecurity mechanisms. The expansion of NCCC's responsibilities is accompanied by the adoption of cutting-edge technologies, such as artificial intelligence, process automation, and big data analytics for risk assessment. The center is also actively engaged in improving the legislative framework governing cybersecurity to align with international standards. Effective coordination between cybersecurity stakeholders minimizes redundancy and enhances the overall efficiency of the cybersecurity system.

Keywords: *information, security, cyber threats, monitoring, infrastructure, technology, standards.*

Прокопович-Ткаченко Дмитро Ігорович – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки, Університет митної справи та фінансів
https://orcid.org/0000-0002-6590-3898

Звєрєв Володимир Павлович – кандидат технічних наук, старший науковий співробітник, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет
https://orcid.org/0000-0002-0907-0705

Козаченко Ігор Миколайович – начальник підрозділу Державного центру кіберзахисту, Державна служба спеціального зв'язку та захисту інформації України
https://orcid.org/0000-0002-0774-7284