УДК 323.28:351.74(477)
DOI https://doi.org/10.32782/2663-6170/2023.34.12

ІНСТИТУЦІЙНІ ОСОБЛИВОСТІ ФОРМУВАННЯ ТА ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: АНАЛІЗ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

INSTITUTIONAL FEATURES OF THE FORMATION AND FUNCTIONING OF INFORMATION SECURITY IN UKRAINE: ANALYSIS AND DEVELOPMENT PROSPECTS

Воробець Н.Р.,
аспірант кафедри політології
Прикарпатського національного університету імені Василя Стефаника

Дана наукова стаття присвячена аналізу інституційних особливостей формування та функціонування системи інформаційної безпеки в Україні. У статті висвітлюються ключові аспекти інформаційної безпеки як невід'ємної складової сучасної системи управління. Також зазначається, що інформаційна безпека входить до більш широкого розуміння питань національної безпеки в цілому.

Також проведено дослідження поточного стану інформаційної безпеки в Україні, спрямованості розвитку та основних викликів, з якими стикається країна в цій важливій сфері, зокрема в умовах збройної агресії росії проти України. Розкриваються загрози та ризики, пов'язані з безпекою інформаційного простору, а також висвітлюється інституційний підхід до розв'язання цих проблем, пов'язаних з інформаційною безпекою.

Окрім того, дана стаття підкреслює значущість синергії діяльності державних органів, приватного сектору та громадськості для створення ефективної стійкої системи інформаційної безпеки. Досліджується роль державних органів, законодавства та міжнародного співробітництва у формуванні ефективної системи інформаційної безпеки в Україні, а також висвітлюються перспективи подальшого розвитку в цій галузі. Увага також приділяється фактору, що успішність інформаційної політики державних структур міряється не лише відповідністю міжнародним стандартам та правилам, але й здатністю захищати особливі національні інтереси, вирішувати актуальні виклики та протистояти гострим загрозам.

Зокрема, виділяються такі перспективи розвитку системи інформаційної безпеки в Україні, як постійне вдосконалення законодавчої бази, активна співпраця з міжнародними партнерами, розвиток компетентності фахівців у сфері інформаційної безпеки та впровадження інноваційних технологій.

Результати цього дослідження можуть бути корисними у подальших дослідженнях з даної проблематики, може використовуватися як методологічна база подальшого опрацювання проблем інформаційної безпеки, а також у навчальному процесі.

Ключові слова: інформаційна безпека, інституційні особливості, національна безпека, кіберзагрози, інформаційні технології, інформаційний простір.

This scientific article is devoted to the analysis of institutional features of the formation and functioning of the information security system in Ukraine. The article highlights key aspects of information security as an integral component of a modern management system. It is also noted that information security is part of a broader understanding of national security issues as a whole.

Research was also conducted on the current state of information security in Ukraine, the direction of development and the main challenges the country faces in this important area, in particular in the context of Russia's armed aggression against Ukraine. The threats and risks related to the security of the information space are revealed, and the institutional approach to solving these problems related to information security is highlighted.

In addition, this article emphasizes the importance of synergy between the activities of government bodies, the private sector and the public to create an effective and sustainable information security system. The role of state bodies, legislation and international cooperation in the formation of an effective system of information security in Ukraine is studied, as well as the prospects for further development in this field are highlighted. Attention is also paid to the fact that the success of the information policy of state structures is measured not only by compliance with international standards and rules, but also by the ability to protect special national interests, solve current challenges and confront acute threats.

In particular, such prospects for the development of the information security system in Ukraine as continuous improvement of the legislative framework, active cooperation with international partners, the development of the competence of specialists in the field of information security and the introduction of innovative technologies are highlighted.

The results of this study can be useful in further research on this issue, can be used as a methodological basis for further processing of information security problems, as well as in the educational process.

Key words: information security, institutional features, national security, cyber threats, information technologies, information space.

Постановка проблеми. У сучасному світі інформаційні технології здобувають все більш визначальне значення в усіх сферах життя, включаючи економіку, політику, науку, та соціокультурні аспекти. Інформаційний простір стає основним ресурсом для забезпечення розвитку суспільства та держави в цілому. Однак разом зі зростанням значення інформаційних технологій зростає і ризик їх неправомірного використання, зокрема, для здійснення кібератак, дестабілізації

політичної ситуації, поширення дезінформації, та інших негативних явищ.

Україна, як суверенна держава, також не залишається осторонь цих тенденцій, зокрема у боротьбі з російською агресією її інформаційна безпека стає об'єктом зростаючої загрози. Постійні кібератаки на важливі інформаційні системи, спроби впливу на суспільний дискурс через масові медіа та соціальні мережі, а також широке поширення дезінформації ставлять під загрозу національну безпеку та стабільність держави. Так, однією із найактуальніших проблем сучасної України є аналіз інституційних особливостей формування та функціонування інформаційної безпеки в контексті глобалізації, розбудови інформаційного суспільства та зміни комунікаційних парадигм. Дослідження сучасного стану системи інформаційної безпеки в Україні, виявлення прогалин у законодавчій базі, ефективності діяльності інституцій, які забезпечують інформаційну безпеку, а також перспективи розвитку цієї системи є важливими завданнями наукової спільноти та практиків в сфері інформаційної безпеки в Україні.

Виділення невирішених раніше частин загальної проблеми. При дослідженні інституційних особливостей формування та функціонування інформаційної безпеки в Україні слід акцентувати увагу на декількох ключових аспектах. Важливо визначити необхідність підвищення кваліфікації фахівців з інформаційної безпеки. Швидкі технологічні зміни та поява нових загроз вимагають, щоб спеціалісти у цій галузі постійно оновлювали свої знання та навички. А також, слід зосередити увагу на залученні широкої громадськості до процесів інформаційної безпеки. Це допоможе підвищити рівень громадської свідомості щодо цих питань і створити сприятливі умови для взаємодії між різними суб'єктами системи безпеки в країні. Разом з тим, створення ефективних механізмів захисту інформації та визначення ролі інституцій є важливим аспектом вирішення цієї загальної проблеми.

Формулювання цілей статті (постановка завдання). Мета статті полягає в дослідженні інституційних аспектів забезпечення інформаційної безпеки в Україні, аналізі існуючих проблем та перспектив подальшого розвитку системи інформаційної безпеки.

Зокрема можна виокремити такі завдання:

1) Проаналізувати інституційні особливості формування та функціонування системи інформаційної безпеки в Україні.

2) Аналіз ключових аспектів інформаційної безпеки як невід'ємної складової сучасної системи управління.

3) Дослідити поточний стан інформаційної безпеки в Україні, спрямованість розвитку та основні виклики, пов'язані з інформаційною безпекою в умовах збройної агресії Росії проти України.

4) Визначити перспективи подальшого розвитку системи інформаційної безпеки в Україні.

Аналіз останніх досліджень та публікацій. В сучасному українському теоретичному, аналітичному та дослідницькому дискурсі, зверненому до проблематики інформаційної безпеки, можна спостерігати доволі високу активність науковців, адже ця проблематика сьогодні і раніше була та залишається як теоретичною, так і практичною. Зокрема, у численних роботах таких вчених, як Захаренко К.В., Кононенко О.М., Почепцов Г.Г., Нашинець-Наумова А.Ю. Кормич Б.А., Романенко Є.О., та інших, активно досліджуються аспекти інформаційної безпеки в Україні. Проте з огляду на складність та багатогранність дослідження функціонування інформаційної безпеки в країні, ця проблематика потребує подальшого розвитку.

Виклад основного матеріалу дослідження. Усвідомлення важливості інформаційної безпеки у сучасних умовах стає необхідністю, оскільки дана сфера не тільки впливає на функціонування державних і громадських інституцій, але і має безпосередній вплив на повсякденну життєдіяльність громадян. Зростання залежності суспільства від інформаційних технологій призводить до посилення ризиків та загроз, які стосуються кібербезпеки та безпеки інформаційного простору.

Для вдосконалення інформаційної безпеки в Україні та ефективного протидії сучасним викликам і загрозам, необхідно звернути увагу на деякі ключові аспекти:

Інтегрована стратегія: Розроблення та впровадження інтегрованої національної стратегії інформаційної безпеки, яка об'єднує зусилля державних та недержавних структур, академічних колективів та бізнес-спільноти. Ця стратегія повинна враховувати міжнародний контекст і передбачати взаємодію з іншими країнами для обміну інформацією та спільних проектів у сфері кібербезпеки.

Законодавчі зміни: Вдосконалення законодавства, що стосується інформаційної безпеки, з урахуванням сучасних технологій та викликів. Важливо забезпечити прозорий та ефективний механізм реагування на кіберзагрози.

Громадянська освіта: Запровадження програм громадянської освіти, спрямованих на збільшення обізнаності громадян щодо кібербезпеки, дезінформації та цифрової безпеки. Поширення знань про методи захисту персональних даних та безпечного використання інформаційних технологій.

Міжнародне співробітництво: Активна участь в міжнародних ініціативах та організаціях, спрямованих на спільну боротьбу з кіберзагрозами та підвищення інформаційної безпеки. Обмін досвідом, технічними засобами та інформацією з іншими країнами [4, с. 196–197].

Так, інформаційна безпека є невід'ємною частиною сучасного суспільства, яке стикається зі

зростаючою кількістю кіберзагроз, кібератак та зростаючою інформаційною експансією. Україна, як суверенна держава, також виявляється у центрі цього геополітичного сприйняття, зокрема в час військової агресії яку веде росія проти України. Тому належне формування та функціонування системи інформаційної безпеки має важливе значення для забезпечення національної безпеки та стабільності.

Україна сьогодні зазнає серйозних викликів у сфері інформаційної безпеки. Кіберзагрози, дезінформація, інформаційна експансія на критичну інфраструктуру стають все більш частими, загрожуючи національній безпеці та соціальній стабільності країни.

Однією з головних перешкод у формуванні та функціонуванні системи інформаційної безпеки є відсутність єдиного і чіткого правового положення щодо її забезпечення. Законодавство України повинно максимально встигати за світовими тенденціями а також викликам та загрозам, які постають перед Україною, що стосуються інформаційної безпеки, а також забезпечити його ефективну реалізацію та виконання. Крім того, потрібно створити нові нормативні акти, спрямовані на протидію сучасним загрозам та викликам, з якими стикається країна.

Інституційний аспект формування та функціонування інформаційної безпеки передбачає впровадження ефективної системи координації та співпраці між різними органами влади, правоохоронними організаціями, а також приватним сектором та громадськими організаціями. Важливим кроком у розвитку інформаційної безпеки є створення національного центру кібербезпеки. Даний центр має бути централізованою інстанцією, яка координуватиме діяльність всіх інституцій, що займаються безпекою в інформаційному просторі. Такий підхід дозволить забезпечити швидку та ефективну реакцію на загрози та виклики, а також уникнути дублювання зусиль та збільшити координацію між різними структурами. Також важливим завданням даного органу має бути не лише реакція на поточні загрози, але й передбачення майбутніх ризиків та аналіз тенденцій у сфері інформаційної безпеки [3].

Однак, перебудова існуючої інфраструктури державних інститутів інформаційної безпеки України потребує застосування принципу стримувань і противаг, при якому державні органи повинні підлягати громадському контролю, бути відкритими для комунікації, прозорими в своїх рішеннях і звітності, а також зрозумілими для міжнародних партнерів. Одночасно, перед державою з'являється ряд нових викликів, пов'язаних з розвитком соціальних мереж та існуючою загрозою, з боку російської федерації.

Серед цих завдань можна виокремити структуризацію віртуальних спільнот у вітчизняних соціальних мережах, розуміння їх впливовості та можливостей, а також пошук і вироблення адекватних реакцій на реальні та потенційні загрози, які можуть ховатися у віртуальному громадянському просторі. Крім того, необхідно розвивати доступні механізми державного регулювання цього соціального феномену, дотримуватися демократичних взірців та традицій у відповідній сфері.

Розбудова інфраструктури державних інститутів інформаційної безпеки повинна відбуватися з урахуванням вищезгаданих викликів і завдань. Важливо забезпечити ефективний контроль за діяльністю державних органів в цій сфері, а також сприяти їх активній співпраці з громадськістю та міжнародними партнерами. Тільки таким чином Україна зможе ефективно забезпечити інформаційну безпеку в даних умовах, які постали перед нею і вирішити поставлені завдання.

Особливу увагу слід приділити розвитку інформаційної грамотності в усіх верств населення. Це може бути досягнуто шляхом проведення інформаційних кампаній, навчальних програм у школах та вищих навчальних закладах, а також проведення тренінгів та семінарів для державних службовців, бізнес-лідерів та громадських активістів. Чим більше людей розуміють важливість безпеки в інформаційному просторі та вміють захищати свою інформацію, тим ефективніше буде боротися з тими загрозами, що існують та постають перед суспільством і державою [1, с. 69–70].

Стверджується, що в сучасній системі інформаційної безпеки громадянське суспільство та мас медіа відіграють важливу роль. Так, подано аргументовану тезу про те, що найвразливіше середовище для інформаційних операцій агресивного характеру формується серед пересічних людей, які проявляють апатію до політики, пасивні у соціальних справах, відтіняють нігілістичні настанови, та мають обмежений обсяг знань та стеснений світогляд.

Основною інформаційною загрозою національній безпеці визначається маніпуляція суспільною свідомістю. Це дестабілізуючий вплив як на інформаційну структуру країни, так і на її інформаційні ресурси та суспільство загалом. Зокрема, інформаційні операції можуть спрямовуватися на поширення недостовірної або перекрученої інформації, створення маніпулятивних кампаній для впливу на громадську думку, збурення суспільної стабільності, а також спричинення дезінформації та паніки.

Громадянське суспільство та мас медіа мають великий потенціал у протидії цим інформаційним загрозам. До прикладу, одразу після повномасштабного вторгнення Росії в Україну у лютому 2022 року стартував телемарафон «Єдині новини». Цей марафон об'єднав державний канал «Рада», Суспільне мовлення та великі комерційні канали – ICTV/СТБ, 1+1, Інтер та «Україна 24» (піз-

ніше замінений на канал-новачок «Ми-Україна»). Канали розділили між собою ефірний час.

На самому початку російського вторгнення, телемарафон «Єдині новини» забезпечив задоволення життєво важливих потреб суспільства. Однак з часом, ситуація в країні стабілізувалась, медіа адаптувались, а кількість дезінформації зменшилась. З цього моменту телемарафон став задовольняти передусім потребу влади в контролі інформації у наймасовішому традиційному медіа – телебаченні [8].

Таким чином, роль незалежних мас медіа в цьому процесі надається великого значення, адже їх об'єктивний підхід та перевірка фактів є важливою складовою правильного інформаційного ландшафту. А активна участь громадськості у виявленні та розкритті дезінформації може забезпечити посильний контроль за поширенням недостовірної інформації.

Тому, громадянське суспільство має відігравати активну роль у сприянні інформаційній грамотності, підвищенні критичного мислення, та популяризації фактичної та об'єктивної інформації. ЗМІ з свого боку повинні дотримуватися професійних етичних стандартів та принципів, аби забезпечити якісну та достовірну інформацію своїм читачам, глядачам та слухачам.

До інституційних особливостей формування та функціонування інформаційної безпеки в Україні також слід віднести ініціативи щодо розвитку національних кадрових резервів, забезпечення професійної підготовки та підвищення кваліфікації фахівців з інформаційної та кібербезпеки. Завдання даного напрямку полягає в забезпеченні належного рівня компетентності та експертизи кадрів, які відповідають викликам сучасності та здатні ефективно протистояти загрозам інформаційної безпеки [6, с. 29–30].

Одним із таких завдань полягає у створенні національних кадрових резервів: адже це один із важливих кроків у розвитку інформаційної безпеки, що полягає у формуванні національних кадрових резервів з кваліфікованими фахівцями. Це можливо досягти шляхом впровадження спеціальних програм та стипендіальних грантів для студентів, які обирають напрям інформаційної безпеки. Додатково, співпраця з університетами та вищими навчальними закладами з метою залучення талановитих студентів до вивчення інформаційної безпеки може стати ефективним інструментом для створення обізнаних та мотивованих фахівців у цій галузі [5, с. 190–191].

Наступне завдання полягає у підвищенні професійної підготовки. Швидкі зміни в інформаційній сфері вимагають постійного підвищення кваліфікації фахівців з інформаційної та кібербезпеки. Для цього варто створити спеціалізовані навчальні центри, семінари, тренінги та майстер-класи, що дозволить працівникам у галузі інформаційної безпеки вчитися новим методам протистояння інформаційним та кіберзагрозам, а також сприятимуть обміну досвідом між фахівцями. Крім того, можна активізувати зв'язок із міжнародними організаціями та використовувати їхні ресурси для надання доступу до передових знань та технологій в галузі інформаційної безпеки.

Третє завдання полягає в створенні та зміцненні зв'язку держави з приватним сектором, зокрема компаніями, що спеціалізуються на інформаційних технологіях та кібербезпеці. Взаємодія з такими компаніями є важливим елементом створення міцної інформаційної безпеки в країні. Уряд повинен сприяти розвитку співпраці з приватними компаніями, підтримуючи обмін досвідом, передовими технологіями та розробками у сфері кібербезпеки. Такі партнерства можуть забезпечити створення інноваційних рішень для захисту інформації та підвищити рівень інформаційної безпеки в усіх сферах діяльності.

Важливим елементом успішної реалізації даного завдання є також співпраця з ІТ кластером. ІТ кластер - це об'єднання інноваційних ІТ компаній, стартапів, університетів, дослідницьких центрів та інших зацікавлених сторін з метою спільної розробки технологій, впровадження проектів та стимулювання розвитку галузі [5, с. 188].

Партнерство з ІТ кластером може забезпечити наступні переваги для інформаційної безпеки в Україні:

1. Розробка інноваційних технологій: ІТ кластер об'єднує талановитих фахівців із різних сфер інформаційних технологій. Завдяки цьому, можна спрямувати зусилля на розробку та впровадження передових технологій кібербезпеки, які відповідають сучасним викликам і є більш ефективними у протидії кіберзагрозам.

2. Обмін досвідом та знаннями: Партнерство з ІТ кластером сприяє обміну досвідом та знаннями між різними компаніями та експертами. Це дозволяє впроваджувати передові практики, реагувати швидко на нові загрози та вдосконалювати стратегії кіберзахисту.

3. Розвиток співпраці та інтеграція ресурсів: ІТ кластер об'єднує різні організації і компанії з різноманітними компетенціями. Це дозволяє залучити додаткові ресурси для розвитку проектів інформаційної безпеки, включаючи інвестиції, наукові дослідження та доступ до новітніх технологій.

4. Прискорення розвитку проектів: Взаємодія з ІТ кластером дозволяє прискорити реалізацію проектів, оскільки об'єднання ресурсів та компетенцій дозволяє швидше втілювати ідеї в життя і реагувати на загрози в інформаційному просторі.

Україна, як країна, що активно розвивається та має розвинутий інформаційний сектор, який сьогодні піддається постійним атакам з боку росії,

стикається з необхідністю ефективного захисту своїх інформаційних ресурсів. Для досягнення цієї мети важливо залучити міжнародну співпрацю та взаємодію з іншими країнами та міжнародними організаціями.

На сьогоднішній день багато країн активно співпрацюють з Україною у сфері інформаційної безпеки, створюючи різноманітні міжнародні партнерства, обмін досвідом та інформацією, а також розробляючи спільні стратегії забезпечення інформаційної безпеки. Україна також бере участь у цих ініціативах, співпрацюючи з різними країнами та міжнародними організаціями.

Одним із ключових партнерів є Європейський союз, країни Великої сімки, НАТО, Рада Європи, та ін. з яким Україна підписала ряд угод та меморандумів про співпрацю в сфері інформаційної та кібербезпеки. Ці угоди сприяють обміну інформацією про нові загрози та інциденти, забезпечують взаємодопомогу у розслідуванні інцидентів в інформаційному та кіберпросторі, а також сприяють спільним навчанням та тренуванням персоналу [7].

Партнерства з іншими країнами та міжнародними організаціями дають змогу Україні більш швидко та ефективно реагувати на нові та складні загрози, які часто оперують глобально і мають транскордонний характер. Обмін інформацією про потенційні загрози та досвід у розслідуванні атак в інформаційному та кіберпросторі дозволяє покращити дії при виявленні, ліквідації та уникненні подібних інцидентів. Так, міжнародні організації можуть надавати фахову підтримку та консультації у створенні національних центрів кібербезпеки та впровадженні передових практик у сфері захисту інформації.

Проте, важливо зазначити, що міжнародне співробітництво також може стикатися з певними викликами і обмеженнями. Наприклад, різні правові та культурні норми між країнами можуть ускладнювати обмін інформацією та спільну реакцію на атаки та загрози. Також можуть існувати проблеми з недостатньою довірою між деякими державами, що ускладнює роботу над спільними проектами.

Усі ці виклики потребують уваги та обговорення, однак важливо розвивати міжнародну співпрацю в галузі інформаційної безпеки, знаходячи оптимальні рішення для спільної боротьби з загрозами інформаційному просторі та підвищення загального рівня кібербезпеки.

А успішне забезпечення національного інформаційного продукту потребує всебічної державної підтримки та надання пріоритетності його створенню та поширенню як в межах України, так і за її межами. Цей інформаційний продукт має бути сприянням загальнолюдським цінностям та сприяти інформаційному розвитку людства, включаючи обмін з іноземними партнерами нашими поглядами, підходами та механізмами боротьби з новітніми викликами, спрямованими на підірвання демократичних цінностей та свободи слова в інформаційному просторі, які можуть виникати через деструктивні дії інших держав [2, с. 118].

Лише шляхом об'єднаних зусиль та глобальної співпраці можна досягти успіху в цій важливій сфері інформаційної безпеки. Мета України – розвивати національний інформаційний продукт, що відображатиме цінності та сприятиме просуванню позитивних змін у світі, сприяючи миру, розумінню та співпраці між країнами.

Висновки. Подальший розвиток інформаційної безпеки у країні є надзвичайно важливою задачею, що потребує спільних зусиль всіх зацікавлених сторін. Сьогодні в умовах війни в Україні існує стала необхідність посилення уваги до інституційних засад інформаційного простору та кібербезпеки, адже вони визначають стратегічний курс та спрямованість розвитку цієї сфери. Забезпечення інформаційної безпеки не може обмежуватися окремими діями або ізольованими проектами, а потребує комплексного підходу та системного управління. Інституційні зміни, засновані на об'єктивних дослідженнях та аналізі, дозволять збалансувати зусилля та забезпечити ефективне використання ресурсів для запобігання кіберзагрозам та реагування на них.

Особлива увага має надаватися забезпеченню координації між різними структурами влади, державними органами, науково-дослідними інституціями, приватним сектором та громадськістю. Тільки шляхом гармонійної співпраці всіх сторін можна створити сильну та стійку систему інформаційної безпеки. Необхідно виробити механізми обміну досвідом, інформацією, а також створити ефективні комунікаційні канали для оперативного реагування на кіберзагрози.

Окрім внутрішніх заходів, міжнародне співробітництво сьогодні також має велике значення для забезпечення інформаційної безпеки. Україна має активно взаємодіяти з іншими країнами, міжнародними організаціями та партнерами для обміну досвідом, найкращими практиками та спільного реагування на глобальні виклики та загрози. Лише через співпрацю та об'єднані зусилля країни можуть бути більш успішними у захисті від кібернападів та створенні стабільного та безпечного інформаційного простору.

У подальшому розвитку інформаційної безпеки в Україні, особливу увагу слід звертати на постійне вдосконалення законодавчої бази, підвищення освітнього рівня населення з питань інформаційної безпеки та підтримку інноваційних технологій. Ці кроки допоможуть забезпечити сталість і стійкість інформаційної безпеки України в умовах швидкого розвитку технологій, в умовах військового протистояння та змін в інформаційному просторі.

Загалом, успішне формування та функціонування системи інформаційної безпеки в Україні потребує суцільного підходу та спрямованих на результат дій з урахуванням зовнішніх викликів, загроз та інституційних особливостей. Це зумовлено тим, що інформаційна безпека стає все більш важливою складовою сучасного суспільства та надзвичайно необхідною для забезпечення збереження, стабільності та розвитку країни. Виконання зазначених рекомендацій дозволить стати Україні більш стійкою та впевненою в своїй здатності протистояти існуючим та майбутнім загрозам, а також буде сприяти розвитку інформаційної технологічної індустрії та економіки загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондар І.Р. Інформаційна безпека як основа національної безпеки Mechanism of Economic Regulation. – 2018. № 1. С. 68–75.
2. Бойко М.С., Єгоров І.І. Інформаційна безпека держави: проблеми та шляхи вирішення. Київ: НАУ, 2017. 238 с.
3. Кондратюк І.І., Котик О.В. Інформаційна безпека: проблеми та шляхи вирішення : монографія: Київ: "Ін Юре", 2018. С. 5–18.
4. Кононенко О. М. Інформаційна безпека: теорія та практика (навчальний посібник) О. М. Кононенко. Київ: КНЕУ, 2018. 280 с.
5. Мельник С.В. Понятійно-категоріальний аппарат у системі професійної підготовки майбутніх фахівців з кібербезпеки Інформаційні технології і засоби навчання. 2016. Т. 55. № 5. С. 187–197.
6. Троян С. С. Інформаційно-безпекова політика Європейського Союзу. Зовнішні справи : суспільно-політичний журнал. 2019. № 2/3. С. 28–32.
7. A new strategic agenda for the EU (2019-2024). European Council. URL: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/
8. Russia’s war on Ukraine: Timeline of cyber-attacks. European Parliament. 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf