Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2022. № 10.

DOI: http://doi.org/10.32702/2307-2156.2022.10.12
УДК 35-027.21:351.86](477)

О. В. Коваленко,
аспірант кафедри глобальної та національної безпеки, Київський національний університет імені Тараса Шевченка
ORCID ID: https://orcid.org/0000-0001-8350-6442

ТЕОРЕТИЧНІ ЗАСАДИ ПРОЕКТУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

O. Kovalenko,
Postgraduate student of the Department of Global and National Security, Taras Shevchenko National University of Kyiv

THEORETICAL PRINCIPLES OF DESIGNING THE CYBER SECURITY SYSTEM OF UKRAINE

Метою статті є наукове обґрунтування теоретичних засад проектування системи забезпечення кібербезпеки України.

Для вирішення завдань дослідження використовувалися загальні та спеціальні методи наукового пізнання, а також системно-структурний метод і метод соціального проектування.

Обґрунтовано, що проектування системи забезпечення кібербезпеки України має здійснюватися в рамках загальної теорії систем,

інституційної теорії, теорій державного та публічного управління, теорій національної безпеки, інформаційної безпеки і кібербезпеки, теорій гібридної, інформаційної та кібернетичної війн. При цьому проектування системи забезпечення кібербезпеки має ґрунтуватися на системній, інноваційній та інституціональній, нормативно-правовій парадигмах проектувальної діяльності.

З метою удосконалення системи забезпечення кібербезпеки України в сучасних умовах російсько-української війни, необхідним є впровадження в публічно-управлінську практику перспективної моделі згаданої системи, яка містить такі складові, як-от: функціональна, інформаційна, інституційна моделі.

The purpose of the article is the scientific substantiation of the theoretical foundations of the design of the cyber security system of Ukraine.

General and special methods of scientific knowledge, as well as the system-structural method and the method of social design, were used to solve the research tasks.

It is substantiated that the design of Ukraine's cyber security system should be carried out within the framework of the general theory of systems, institutional theory, theories of state and public administration, theories of national security, information security and cyber security, theories of hybrid, information and cyber warfare. At the same time, the design of the cyber security system should be based on systemic, innovative and institutional, normative and legal paradigms of design activity.

In order to improve the system of ensuring cyber security of Ukraine in the modern conditions of the Russian-Ukrainian war, it is necessary to introduce into public management practice a perspective model of the mentioned system, which contains such components as: functional, informational, institutional models.

The prospective functional model of the Ukrainian cyber security system is represented by three blocks: reflexive, organizational and managerial, and

instrumental block.

We present the promising information model of the Ukrainian cyber security system in five blocks: regulatory, situational, conceptual, mathematical models, a model for the development of options for management solutions in the field of cyber security.

The prospective institutional model of Ukraine's cyber security system structurally includes the following mechanisms: cyber security information security mechanism, information and analytical security response mechanism for cyber security threats; a mechanism for ensuring managerial interaction of cyber security entities; the mechanism for ensuring the communication of cyber security entities; the mechanism of scientific and methodological provision of responding to cyber security threats, the mechanism of information and technological provision of responding to cyber security threats.

Ключові слова: *національний кіберпростір, державна політика у сфері кібербезпеки, система забезпечення кібербезпеки, механізми забезпечення кібербезпеки, Україна.*

Keywords: *national cyberspace, state policy in the field of cybersecurity, cybersecurity system, cybersecurity mechanisms, Ukraine.*

Постановка проблеми. У Законі України «Про основні засади забезпечення кібербезпеки України» [1] визначено пріоритетні цілі, завдання системи кібербезпеки України, в Стратегії кібербезпеки України [2] визначено напрями забезпечення кібербезпеки України в умовах російсько-української війни.

Ця обставина й визначає ***зв'язок загальної проблеми з найбільш важливими науковими та практичними завданнями*** дослідження проблем проектування системи забезпечення кібербезпеки України.

Аналіз останніх досліджень і публікацій. Результати аналізу наукових публікацій дозволяють констатувати, що проблеми проектування

систем забезпечення національної безпеки у різних сферах суспільної діяльності, й зокрема у сфері кібербезпеки, досліджувались у працях вітчизняних науковців: С. Кримський обґрунтував методологічні засади проектної діяльності [3, с. 134-147]; Ю. Сурмін обґрунтував структуру проектної діяльності [4]; В. Абрамов обґрунтував теоретичні засади проектування системи безпеки [5, с. 146-150], М. Шевченко обґрунтував теоретичні засади проектування системи інформаційної безпеки [6]; В. Бухарєв [7] та І. Діордіца [8] в рамках нормативно-правової парадигми проектної діяльності розглянули питання проектування системи кібекрбезпеки та системи її забезпечення.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість робіт, в яких досліджуються проблеми теорії та практики проектної діяльності у сфері національної безпеки України можна констатувати обмаль праць, які були б присвячені розгляду питання теоретичних засад проектування системи забезпечення кібербезпеки України.

Саме тому **мета цієї статті** полягає у науковому обґрунтуванні теоретичних засад проектування системи забезпечення кібербезпеки України.

Для вирішення завдань дослідження використовувалися загальні та спеціальні методи наукового пізнання. За допомогою системно-структурного методу визначено основні складові перспективної моделі системи забезпечення кібербезпеки. Метод соціального проектування дозволив обґрунтувати теоретичні засади проектування системи забезпечення кібербезпеки.

Виклад основного матеріалу. Аналіз наукової літератури [3-10] дозволяє зробити висновок, що проектування системи забезпечення кібербезпеки України має здійснюватися в рамках загальної теорії систем, інституційної теорії, теорій державного та публічного управління, теорій національної безпеки, інформаційної безпеки і кібербезпеки, теорій

гібридної, інформаційної та кібернетичної війн. При цьому проектування системи забезпечення кібербезпеки має ґрунтуватися на таких парадигмах проектувальної діяльності, як-от:

системна парадигма в рамках якої мають бути визначені основні складові перспективної моделі системи забезпечення кібербезпеки;

інноваційна парадигма в рамках якої проектування перспективної моделі системи забезпечення кібербезпеки має розглядатися як сукупність інноваційних змін (модернізація) вже існуючої вказаної системи;

інституціональна парадигма в рамках якої проектування перспективної моделі системи забезпечення кібербезпеки розглядається як інституціональне моделювання та впровадження інституціональної моделі системи забезпечення кібербезпеки в публічно-управлінську практику у сфері національної безпеки.

Для розв'язання проблем, пов'язаних із вдосконалення системи забезпечення кібербезпеки України в сучасних умовах, необхідним є впровадження в публічно-управлінську практику у сфері національної безпеки перспективної моделі згаданої системи, яка містить такі складові, як-от: функціональна, інформаційна, інституційна моделі.

Вимоги до перспективної функціональної моделі системи забезпечення кібербезпеки України визначаються: нагальною необхідністю впровадження у вітчизняну практику кризового реагування на загрози національній безпеці стандартів НАТО щодо кризового реагування у сфері національної безпеки і оборони й неопрацьованістю підходів щодо їх впровадження; трансграничним характером загроз кібербезпеці України в умовах російсько-української війни, що передбачає комплексне поєднання заходів реактивного і проактивного реагування на вказані загрози.

Перспективна функціональна модель системи забезпечення кібербезпеки України передбачає функціонування вказаної системи у двох режимах:

проактивне реагування на потенційні загрози кібербезпеці – це головне завдання кризового менеджменту у сфері кібербезпеки;

реактивне реагування на реальні загрози кібербезпеці – це часткове завдання кризового менеджменту у сфері кібербезпеки;

Перспективну функціональну модель системи забезпечення кібербезпеки України нами представлено трьома блоками:

Рефлексивний блок: державно-політичний механізм, що представляє собою сукупність процесів, які ініційовані та реалізовані органами державної влади задля досягнення кінцевого результату у вигляді теоретичного обґрунтування засад політико-правового проектування та державного конструювання системи забезпечення кібербезпеки, а також засад практики гарантування кібербезпеки; інформаційно-аналітичний механізм та механізм науково-методичного забезпечення реагування на загрози кібербезпеці.

Організаційно-управлінський блок: правовий, організаційно-адміністративний, інституційний механізми, механізми розробки та реалізації державної політики у сфері кібербезпеки, механізми кадрового, адміністративного, технічного, фінансового та ресурсного забезпечення.

Інструментальний блок: механізм державного реагування на загрози кібербезпеці; механізм запобігання загрозам кібербезпеці; механізм партнерства і співробітництва з питань забезпечення кібербезпеки; механізм інтеграції національного кіберпростору у світовий інформаційний простір; механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки, які використовуються у комплексі з метою забезпечення кібербезпеки.

Інформаційна модель системи забезпечення кібербезпеки України характеризує ступінь невизначеності, яка притаманна системі чи системній проблемі державного реагування на загрози кібербезпеці, рівень наших знань про них, про проблеми в знаннях і шляхах їх усунення.

Інформаційна модель системи забезпечення кібербезпеки України у загальних рисах може бути представлена схемою руху управлінської

інформації: аналіз (опис) → діагностування (передбачення) → цілевизначення / цілереалізація → планування → програмування (як конкретизація програмування) → рішення → контроль на виконанням рішення → зворотній зв'язок (уточнення рішення або нове рішення на основі нових даних аналізування, діагностування, прогнозування і т. ін.).

Вимоги до перспективної інформаційної моделі системи забезпечення кібербезпеки України визначаються:

необхідністю застосування воєнно-політичним керівництвом держави в умовах російсько-української війни релевантних знань в галузях державного управління, національної безпеки і оборони, кібервійни та геополітичного інформаційного протиборства задля оперативного прийняття обґрунтованих рішень у сфері реагування на загрози кібернетичного характеру та не сформованістю бази відповідних релевантних знань;

суперечностями, що існують сьогодні в системі інформаційно-аналітичної діяльності у сфері забезпечення кібербезпеки, а саме: між новітніми викликами й загрозами кібербезпеці в умовах трансформацій безпекового середовища і відсутністю належного інформаційно-аналітичного інструментарію опрацювання практичних проблем державного реагування України як необхідної умови ефективного функціонування системи кібербезпеки;

необхідністю впровадження стандартів НАТО, а саме протоколів реагування у вітчизняну публічно-управлінську практику реагування на загрози кібербезпеці та не розробленістю паспортів загроз кібербезпеці та технологій реагування на них.

Перспективна інформаційна модель системи забезпечення кібербезпеки України передбачає:

1) комплексне застосування в інтересах реактивного та проактивного реагування на загрози кібербезпеці первинної, вищої, масової, військової та

безпекової, стратегічної та ситуаційної аналітики. Технології вказаних видів аналітики докладно розглянуто в [10];

2) розробку паспортів загроз кібербезпеці та технологій реагування на них.

Є сенс зауважити, що первинна аналітика включає в себе моніторинг та ситуаційний аналіз із використанням комп'ютерних технологій обробки великих інформаційних масивів з проблематики кібербезпеки України.

Первинна аналітика виконує управлінську функцію, яка передбачає збирання та опрацювання інформації з проблем кібербезпеки – забезпечує інформацією всі етапи управлінського циклу на стратегічному, тактичному та оперативному рівнях управління кібербезпекою: підготовку, ухвалення державно-управлінських рішень у сфері кібербезпеки і контроль за їх реалізацією.

Вища аналітика, на яку працює весь інструментарій первинної аналітики, включає в себе кваліфікований аналіз практичних проблем забезпечення кібербезпеки, й зокрема загрози кібернетичного характеру, прогноз їх розвитку, вироблення сценаріїв державного реагування на них.

Вища аналітика виконує функції:

а) діагностичну – спрямована на отримання об'єктивної картини безпекової ситуації, діагнозу вказаної ситуації;

б) прогностичну, яка дає можливість виявляти тенденції розвитку безпекової ситуації, прогнозувати наслідки прийнятих державно-управлінських рішень з урахуванням їхнього впливу на зміни в безпековому середовищі і включає в себе підфункції:

стратегічного прогнозування майбутнього безпекового середовища – передбачає розробку прогнозів в межах від 5-10 до 20-30 років, найчастіше до 15 років;

середньотермінового прогнозування майбутнього безпекового середовища – передбачає розробку прогнозів в межах 1-5 років;

поточного прогнозування майбутнього безпекового середовища –

передбачає розробку прогнозів в межах до 1 року;

в) інструментальну – забезпечує прийняття державно-управлінських рішень у сфері кібербезпеки;

г) експертно-консультативну – забезпечує виконання експертно-аналітичних робіт, обумовлених цілями та завданнями забезпечення кібербезпеки, здійснення соціальної експертизи нормативних правових актів з метою виявлення потенційних загроз кібербезпеці, здійснення експертної оцінки чинників ризику, здатних створювати ситуації критичного характеру у сфері національної безпеки;

д) координаційну – спрямована на оцінку рівня кібербезпеки у різних сферах, досягнутого системою забезпечення кібербезпеки на поточний момент, встановлення доцільної взаємодії між структурними компонентами системи забезпечення кібербезпеки в процесі її функціонування за допомогою передачі інформації, оцінку результативності дій щодо нейтралізації виявленої загрози кібербезпеці та визначення витрат на ці дії, оцінку ефективності функціонування системи забезпечення кібербезпеки у відповідній сфері;

е) аналітичну – спрямована на формування цілісної системи наукового знання у сфері кібербезпеки, експертно-аналітичної професійної діяльності в згаданій сфері;

ж) контролю – передбачає здійснення стратегічного та оперативного контролю виконання визначених завдань по забезпеченню кібербезпеки.

Перспективну інформаційну модель системи забезпечення кібербезпеки України нами представлено п’ятьма блоками:

1 блок. Нормативно-правова модель: чинне законодавство, на основі якого формуються та функціонують система кібербезпеки та її складова – система забезпечення кібербезпеки.

2 блок. Ситуативна модель: блок даних – організація достовірної, компактної і вагової інформації про загрози кібербезпеці; блок ситуацій – оцінка достатності опису загроз кібербезпеці.

3 блок. Концептуальна модель**:** блок цілі – формулювання цілей державного реагування на виявлені загрози кібербезпеці; блок вибору – вибір критерію оптимальності дій державного реагування на загрози кібербезпеці.

4 блок. Математична модель: система математичних співвідношень, які описують процес забезпечення кібербезпеки.

5 блок. Модель розробки варіантів управлінських рішень у сфері забезпечення кібербезпеки, у рамках яких визначаються пріоритетні напрями політики реагування на загрози кібернетичного характеру, а також пріоритети розвитку системи забезпечення кібербезпеки.

Розглянемо перспективну інституційну модель системи забезпечення кібербезпеки України.

Вимоги до перспективної інституційної моделі системи забезпечення кібербезпеки України визначаються потребою в обґрунтуванні та розбудові механізмів забезпечення кібербезпеки в умовах динамічного безпекового середовища і відсутністю ефективних напрямів реалізації цього процесу на практиці.

Перспективна інституційна модель системи забезпечення кібербезпеки України структурно має містити такі механізми, як-от:

механізм інформаційного забезпечення кібербезпеки – це сукупність процесів, ініційованих і реалізованих суб’єктами забезпечення кібербезпеки через наявні інструменти управління, комплексна дія яких спрямована на надання посадовим особам центральних органів виконавчої влади відомостей, необхідних для виконання покладених на них завдань у сфері забезпечення кібербезпеки в умовах виникнення і розвитку кризових ситуацій, що загрожують національній безпеці;

механізм інформаційно-аналітичного забезпечення реагування на загрози кібербезпеці – це сукупність процесів, ініційованих і реалізованих суб’єктами забезпечення кібербезпеки щодо діагностування й прогнозування тенденцій розвитку загроз кібербезпеці, розробки варіантів

управлінських рішень щодо реагування на виявлені загрози кібернетичного характеру та оцінка наслідків їх прийняття для гарантування кібербезпеки;

механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки – це сукупність процесів, ініційованих і реалізованих суб'єктами забезпечення кібербезпеки спрямованих на створення умов для об'єднання зусиль керівництва органів виконавчої влади в напрямі своєчасного та адекватного реагування на загрози кібернетичного характеру згідно єдиного задуму гарантування кібербезпеки;

механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки – це сукупність процесів, ініційованих і реалізованих суб'єктами забезпечення кібербезпеки з метою створення умов для інформаційної взаємодії, яка зорієнтована на обмін необхідною та релевантною аналітичною інформацією про загрози кібернетичного характеру між згаданими суб'єктами;

механізм науково-методичного забезпечення реагування на загрози кібербезпеці – це сукупність процесів, ініційованих і реалізованих науковими установами та суб'єктами забезпечення кібербезпеки з метою формування бази релевантних знань про загрози кібернетичного характеру та державне реагування на них;

механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці – це сукупність процесів, ініційованих і реалізованих суб'єктами забезпечення кібербезпеки з метою формування умов безпечного використання інформаційних та аналітичних технологій в інтересах реагування на загрози кібернетичного характеру.

На наше переконання, очікуваними результатами впровадження перспективних моделей системи забезпечення кібербезпеки України, а саме функціональної, інформаційної та інституційної моделей, стане:

створення інституційних спроможностей суб'єктів забезпечення кібербезпеки на стратегічному, оперативному та тактичному рівнях, що

забезпечить своєчасне і адекватне реактивне та проактивне реагування на загрози кібербезпеці;

імплементована організаційна структура системи забезпечення кібербезпеки України відповідатиме стандартам НАТО у сфері кризового реагування;

технічне оснащення відповідних підрозділів сектору безпеки й оборони для ефективної реалізації функцій системи забезпечення кібербезпеки України забезпечить інтеграцію з іншими системами кризового реагування Української держави;

механізм інформаційно-аналітичного забезпечення реагування на загрози кібербезпеці та механізм обмін аналітичними даними між суб'єктами забезпечення кібербезпеки функціонують і включені до загальнодержавної системи забезпечення національної безпеки України.

Висновки.

1. Обґрунтовано, що проектування системи забезпечення кібербезпеки України має здійснюватися в рамках загальної теорії систем, інституційної теорії, теорій державного та публічного управління, теорій національної безпеки, інформаційної безпеки і кібербезпеки, теорій гібридної, інформаційної та кібернетичної війн. При цьому проектування системи забезпечення кібербезпеки має ґрунтуватися на системній, інноваційній, інституціональній, нормативно-правовій парадигмах проектувальної діяльності.

2. З метою удосконалення системи забезпечення кібербезпеки України в сучасних умовах російсько-української війни, необхідним є впровадження в публічно-управлінську практику перспективної моделі згаданої системи, яка містить такі складові, як-от: функціональна, інформаційна, інституційна моделі.

Перспективну функціональну модель системи забезпечення кібербезпеки України нами представлено трьома блоками:

Рефлексивний блок: державно-політичний механізм, інформаційно-

аналітичний механізм, механізм науково-методичного забезпечення реагування на загрози кібербезпеці.

Організаційно-управлінський блок: правовий, організаційно-адміністративний, інституційний механізми, механізми розробки та реалізації державної політики у сфері кібербезпеки, механізми кадрового, адміністративного, технічного, фінансового та ресурсного забезпечення.

Інструментальний блок: механізм державного реагування на загрози кібербезпеці; механізм запобігання загрозам кібербезпеці; механізм партнерства і співробітництва з питань забезпечення кібербезпеки; механізм інтеграції національного кіберпростору у світовий інформаційний простір; механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки, які використовуються у комплексі з метою забезпечення кібербезпеки.

Перспективну інформаційну модель системи забезпечення кібербезпеки України нами представлено п’ятьма блоками:

1 блок. Нормативно-правова модель: чинне законодавство, на основі якого формуються та функціонують система кібербезпеки та її складова – система забезпечення кібербезпеки.

2 блок. Ситуативна модель: блок даних – організація достовірної, компактної і вагової інформації про загрози кібербезпеці; блок ситуацій – оцінка достатності опису загроз кібербезпеці.

3 блок. Концептуальна модель**:** блок цілі – формулювання цілей державного реагування на виявлені загрози кібербезпеці; блок вибору – вибір критерію оптимальності дій державного реагування на загрози кібербезпеці.

4 блок. Математична модель: система математичних співвідношень, які описують процес забезпечення кібербезпеки.

5 блок. Модель розробки варіантів управлінських рішень у сфері забезпечення кібербезпеки, у рамках яких визначаються пріоритетні напрями політики реагування на загрози кібернетичного характеру, а також пріоритети розвитку системи забезпечення кібербезпеки.

Перспективна інституційна модель системи забезпечення кібербезпеки України структурно має містити такі механізми, як-от: механізм інформаційного забезпечення кібербезпеки, механізм інформаційно-аналітичного забезпечення реагування на загрози кібербезпеці; механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки; механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки; механізм науково-методичного забезпечення реагування на загрози кібербезпеці, механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці.

Перспективи подальших досліджень вбачаємо у конструюванні інституційної матриці управління кібербезпекою України.

Література

1. Про основні засади забезпечення кібербезпеки України. Закон України № 1263-VIII від 05.10.2017 р. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

2. Про Стратегію кібербезпеки України : Указ Президента України № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836. (дата звернення: 12.02.2022 р.). Назва з екрану.

3. Кримський С.Б. Запити філософських смислів. К.: ПАРАПАН, 2003. 240 с.

4. Сурмин Ю.П. Социальное проектирование в кризисном обществе: методологический аспект. *Вісник Національної академії державного управління при Президентові України*. 2014. № 3. С. 5-17.

5. Абрамов В.І. Духовність суспільства: методологія системного вивчення: монографія. К.: КНЕУ, 2004. 236 с.

6. Шевченко М.М. Теоретико-методологічні засади розбудови системи інформаційної безпеки України. *День інформаційного суспільства – 2016*: матеріали щоріч. наук.-практ. конф. за міжнар. участю, Київ, 19

трав. 2016 р. / за заг. ред. д-ра держ. упр., проф. А.І. Семенченка. К.: НАДУ, 2016. С. 267-269.

7. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юрид. наук : 12.00.07 / Сумський держ. ун-т. Суми, 2018. 221 с.

8. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109-116.

9. Костенко Д.М.. Формування мережевої архітектури публічного управління в контексті забезпечення національної безпеки: дис. … докт. філософії: спец. 281 / НАДУ. К., 2021. 245 с.

10. Соколов В.А. Інституалізація аналітичної діяльності в системі забезпечення національної безпеки: зарубіжний та вітчизняний досвід: монографія. К. : НАДУ, 2021. 375 с.

References

1. Verkhovna Rada of Ukraine (2017), The Law of Ukraine “About the main principles of ensuring cyber security of Ukraine”, Vidomosti Verkhovnoi Rady, vol. 45.

2. President of Ukraine (2016), Decree “About the Cyber Security Strategy of Ukraine”, available at: https://www.president.gov.ua/documents/962016-19836 (Accessed 12.02.2022).

3. Kryms'kyj, S.B. (2003), Zapyty filosofs'kykh smysliv [Philosophical questions], PARAPAN, Kyiv, Ukraine.

4. Surmyn, Yu.P. (2014), “Social design in a crisis society: methodological aspect”, Natsional'noi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy, vol. 3, pp. 5-17.

5. Abramov, V.I. (2004), Dukhovnist' suspil'stva: metodolohiia systemnoho vyvchennia [Spirituality of society: methodology of systematic study], KNEU, Kyiv, Ukraine.

6. Shevchenko, M.M. (2016), “Theoretical and methodological

principles of building the information security system of Ukraine", Den' informatsijnoho suspil'stva – 2016: materialy schorich. nauk.-prakt. konf. za mizhnar. uchastiu [Information Society Day - 2016: materials of the annual scientific and practical conference with international participation], NADU, Kyiv, Ukraine, pp. 267-269.

7. Bukhariev, V.V. (2018), "Administrative and legal principles of ensuring cyber security of Ukraine", Ph.D. Thesis, Sums'kyj derzh. un-t. Sumy, Ukraine.

8. Diorditsa, I. (2017), "Cyber security system: essence and purpose", Pidpryiemnytstvo, hospodarstvo i pravo, vol. 7, pp. 109-116.

9. Kostenko, D.M. (2021), "Formation of the network architecture of public administration in the context of ensuring national security", Ph.D. Thesis, NADU, Kyiv, Ukraine.

10. Sokolov, V.A. (2021), Instytualizatsiia analitychnoi diial'nosti v systemi zabezpechennia natsional'noi bezpeky: zarubizhnyj ta vitchyznianyj dosvid [Institutionalization of analytical activity in the national security system: foreign and domestic experience], NADU, Kyiv, Ukraine.

Стаття надійшла до редакції 20.10.2022 р.