Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Категорія «Б», Наказ Міністерства освіти і науки України від 28.12.2019 №1643)
www.dy.nayka.com.ua | № 6 2020 р. | 25.06.2020

DOI: 10.32702/2307-2156-2020.6.102

УДК 351.86:659.3. 4:004](477)

О. В. Коваленко,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою,
Національна академія державного управління при Президентові України
ORCID ID: 0000-0001-8350-6442

КОНЦЕПТУАЛЬНІ ЗАСАДИ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ ДЕРЖАВНОГО БУДІВНИЦТВА

O. Kovalenko
Postgraduate student of the Department of European integration and globalization and management of national security, National Academy of Public Administration under the President of Ukraine

CONCEPTUAL FUNDAMENTALS OF THE DEVELOPMENT OF THE NATIONAL CYBER SECURITY SYSTEM OF UKRAINE AT THE CURRENT STAGE OF STATE BUILDING

Метою статті є обґрунтування концептуальних засад розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва.
Для вирішення завдань дослідження використовувалися методи аналізу і синтезу, системно-ситуаційний підхід.
Встановлено, що з причин складності кібернетичної сфери в умовах інформаційної глобалізації, трансграничного характеру сучасних загроз кібербезпеці та гібридної війни проти нашої держави існує нагальна необхідність розвитку системи забезпечення кібербезпеки України.
Обґрунтовано, що концептуальними засадами розвитку національної системи кібербезпеки України є ідеї паспортизації загроз кібербезпеки і технологізації державного реагування на загрози кібербезпеці, які розроблялися вітчизняними науковцями.
Доведено, що важливими напрямами розвитку національної системи кібербезпеки України є розробка паспортів загроз кібербезпеці, технологій державного реагування на виявлені загрози кібербезпеці та впровадження їх у державно-управлінську практику.

The purpose of the article is to substantiate the conceptual foundations of the development of the national cybersecurity system of Ukraine at the present stage of state building.
Methods of analysis and synthesis, system-situational approach were used to solve the research problems.
It is established that the implementation of the tasks defined in the official discourse of Ukraine on the development of the national cybersecurity system requires a comprehensive scientifically sound methodology. This methodology should take into account the multifaceted complex nature of the problems of cybersecurity of the Ukrainian state, Ukrainian society and citizens of Ukraine in the context of information globalization and a dynamic security environment.

It is proved that the ideas of certification of cybersecurity threats and technologicalization of state response to threats in this area serve as a theoretical basis for improving the national cybersecurity system of Ukraine, namely the state mechanism for monitoring cybersecurity threats and the mechanism of state response to identified cybersecurity threats.
In order to improve the state mechanism for monitoring cybersecurity threats, it is proposed to develop and implement cybersecurity threat passports in public administration practice, which should include the following sections: general characteristics of cybersecurity threats; characteristics of the possible development of cybersecurity threats; activities of cybersecurity actors to respond to threats.
In order to improve the mechanism of state response to identified cybersecurity threats, it is proposed to develop and implement in the practice of public administration technology of state response to cybersecurity threats, which includes the following structural elements: a holistic theoretical concept that reflects the patterns of cybersecurity; the object of cybersecurity and the subject of public administration influence; algorithm of state-administrative influence on the object of cybersecurity; technological methods and means of state-administrative influence on the object of cybersecurity; element of control of the result of application of this technology.

Ключові слова: *кібербезпека; державне управління кібербезпекою; система кібербезпеки; система забезпечення кібербезпеки; загрози кібербезпеці; паспорт загроз кібербезпеці; технологія державного реагування на загрози кібербезпеці.*

Keywords: *cybersecurity; state management of cybersecurity; cybersecurity system; cybersecurity system; cybersecurity threats; cybersecurity threats passport; technology of state response to cybersecurity threats.*

Постановка проблеми в загальному вигляді. Дослідження державно-управлінських проблем забезпечення кібербезпеки України обумовлено відсутністю єдиних підходів серед вітчизняних науковців щодо теоретико-методологічного обґрунтування засад розбудови та функціонування національної системи забезпечення кібербезпеки в умовах інформаційної глобалізації та динамічного безпекового середовища.

Ця обставина й визначає ***зв'язок загальної проблеми з найбільш важливими науковими та практичними завданнями дослідження*** питання ідентифікації та структурування проблем моніторингу загроз кібербезпеці держави та адекватного державного реагування на них.

Аналіз останніх досліджень та публікацій. Аналіз досліджень та публікацій науковців щодо теоретико-методологічного обґрунтування засад класифікації та моніторингу загроз кібербезпеці України, а також державного реагування на ці загрози [1-5] дозволяє констатувати відсутність єдиного підходу до розуміння сутності, соціального призначення та завдань інформаційно-аналітичного забезпечення державної політики у сфері кібербезпеки, технологій державного реагування на загрози кібербезпеці. Недостатня наукова обґрунтованість засад інформаційно-аналітичного забезпечення та державного реагування обумовлюють необхідність синтезування теоретичних положень щодо організації та здійснення вказаних видів діяльності у сфері забезпечення кібербезпеки України.

Виділення невирішених раніше частин загальної проблеми. Аналіз нормативно-правової бази України в галузі кібербезпеки [6; 7] дозволяє констатувати наявність в офіційному дискурсі визначення переліку загроз кібербезпеці України, а також правових засад моніторингу загроз кібербезпеці та державного реагування на них. Проте, наразі аналітична діяльність та державне реагування у цій сфері безпеки не набули ознак системності, що значно знижує рівень ефективності системи забезпечення кібербезпеки Української держави.

Метою статті є обґрунтування концептуальних засад розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва.

Для вирішення завдань дослідження нами використовувалися: методи аналізу і синтезу – для осмислення питань виявлення та ідентифікації загроз кібербезпеці, державного реагування на виявлені загрози; порівняльного аналізу – при вивченні зарубіжного досвіду у сфері забезпечення кібербезпеки; системно-ситуаційний підхід – для дослідження технологічного аспекту реалізації функції управління, зокрема для удосконалення методики моніторингу загроз кібербезпеці та технології реагування на виявлені загрози кібербезпеці.

Виклад основного матеріалу. В Законі України «Про основні засади забезпечення кібербезпеки України» [6] та Стратегії кібербезпеки України [7] визначено засади державної політики у сфері кібербезпеки

щодо розвитку національного кіберпростору та національної системи кібербезпеки. Проте, аналіз результатів реалізації вказаної політики дозволяє констатувати, що наразі існує нагальна необхідність впровадження в державно-управлінську практику у цій сфері наукових розробок вітчизняних вчених, а саме науково обґрунтованих методик розробки паспортів загроз національній безпеці [8] та технологій державного реагування на загрози національній безпеці [9]. Зауважимо, що в зазначених методиках реалізовано ідеї паспортизації загроз національній безпеці та технологізації державного реагування на виявлені загрози національній безпеці. На нашу думку, ці ідеї мають значний евристичний потенціал й дозволять розв'язати низку проблем забезпечення кібербезпеки України на сучасному етапі державного будівництва. В контексті вище зазначеного варто навести слова П. Копніна, котрий писав: «Наукова зрілість, характер ідей є першою необхідною передумовою для її успішної реалізації; наявність необхідних технічних засобів – друга умова, її втілення у дійсність. Сукупність того й іншого призводить до того, що в практиці суб'єкт створює об'єкт, який найбільш повно відповідає ідеям, цілям, людській суспільній природі» [10, с. 296].

Саме тому, вбачається за доцільне, розробити відповідні паспорти загроз кібербезпеці України з метою подальшої технологізації процесу реагування на виявленні загрози у цій сфері. Зауважимо, що паспорт (матриця) загрози – це документ, який передбачає ідентифікацію (оцінку) подій, явищ, процесів, інших чинників, що створюють небезпеку реалізації життєво важливим національним інтересам України, характеристику їх можливого розвитку (масштаб, тенденції розвитку, можливі наслідки для національної безпеки), а також визначення основних організаційно-правових та інших механізмів щодо діяльності суб'єктів забезпечення національної безпеки з реагування на загрози (моніторинг, запобігання, превентивні дії, локалізація тощо) [8, с. 27-31].

Не претендуючи на системний розгляд всієї сукупності показників кібербезпеки, пропонуємо обмежитися скороченою процедурою ідентифікації та моніторингу за індикаторами лише в основних ділянках кібернетичного простору, які визначені в офіційному дискурсі державного управління кібербезпекою, а саме [6; 7]:

1) загроз кібербезпеці, що актуалізуються через дію таких чинників, як:

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки»;

2) кіберзлочинів, що поділяються на наступні категорії:

а) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, зокрема:

незаконний доступ, наприклад, шляхом злому, обману і іншими засобами;

нелегальне перехоплення комп'ютерних даних;

втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на критичну інформаційну інфраструктуру;

зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів;

б) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів;

в) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

г) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і книг.

Використовуючи напрацювання вітчизняних науковців в царині паспортизації загроз національній безпеці [8] пропонуємо наступну структуру паспорту загроз кібербезпеці:

І. Загальна характеристика загрози кібербезпеці.

1.1. Структура загрози кібербезпеці: вказуються складові загрози кібербезпеці, а також аналізу мають підлягати можливі події, процеси та інші чинники, що створюють небезпеку реалізації життєво важливим національним інтересам України в кіберпросторі.

1.2. Об'єкти загрози кібербезпеці: об'єкти загрози визначаються відповідно їх спрямованості проти реалізації життєво важливих національних інтересів у кіберпросторі.

1.3. Джерела загроз кібербезпеці: визначаються явища, процеси, події та інші чинники, а також суб'єкти які створюють небезпеку реалізації національних інтересів України в кіберпросторі.

ІІ. Характеристика можливого розвитку загрози кібербезпеці.

2.1. Масштаб загрози кібербезпеці: вказуються просторовий розмах зовнішніх та внутрішніх чинників, що в змозі перешкоджати реалізації національних інтересів України в кіберпросторі, вказується можливий взаємозв'язок з іншими загрозами кібербезпеці, що, за певних умов може спричинити каскадний ефект руйнування критичної інформаційної інфраструктури та комунікаційних систем.

2.2. Тенденції розвитку загрози кібербезпеці: надається коротка довідка про динаміку розвитку рівня загрози кібербезпеці.

2.3. Можливі наслідки реалізації загрози кібербезпеці: вказується короткий прогноз наслідків реалізації виявленої загрози для об'єкта кібербезпеки, а також для критичної інформаційної інфраструктури та комунікаційних систем загалом.

ІІІ. Діяльність суб'єктів забезпечення кібербезпеки по реагуванню на виявлену загрозу.

3.1. Суб'єкти забезпечення кібербезпеки: мають бути стисло описані, виходячи із норм чинного законодавства основні функції, завдання, повноваження, сфери відповідальності, особливості діяльності суб'єктів забезпечення кібербезпеки, підпорядкованих їм сил і засобів щодо виявлення, запобігання, прогнозування, нейтралізації (пониження рівні) загрози (її складових), ліквідації наслідків реалізації загрози.

Згідно чинного законодавства функціональними органами державної влади, які безпосередньо залучаються до виконання завдань щодо забезпечення кібербезпеки є: Служба безпеки України, Антитерористичний центр при Службі безпеці України, Національна поліція, Державна служба спеціального зв'язку та захисту інформації, Національний координаційний центр кібербезпеки при РНБО України, Генеральний штаб Збройних сил України, розвідувальні органи [6; 7].

3.2. Ресурсне забезпечення: вказуються особливості організації ресурсного забезпечення (фінансового, матеріально-технічного, інформаційного тощо) діяльності суб'єктів забезпечення кібербезпеки по реагуванню на виявлену загрозу, сили і засоби що додатково можуть залучатися, їх розподіл та порядок використання.

3.3. Способи і методи реагування на загрозу кібербезпеки: визначається алгоритм дій суб'єктів забезпечення кібербезпеки, підпорядкованих їм сил і засобів, а також тих, які можуть залучатися додатково щодо реагування на загрозу, їх розподіл, порядок, способи і методи використання.

Наразі у сфері забезпечення кібербезпеки України гостро стоїть питання технологізації державного реагування на загрози національним інтересам в кіберпросторі. Саме тому, пропонуємо розробити технологію державного реагування на загрози кібербезпеці. Це, на нашу думку значно підвищить ефективність діяльності суб'єктів забезпечення кібербезпеки у цій сфері.

В науковій літературі [9] під поняттям «технологія державного реагування на загрози національній безпеці» розуміється процес цілеспрямованого державно-управлінського впливу на субстрат загроз з метою зниження рівня загроз національним інтересам. В залежності від стадії реалізації загроз національним інтересам вітчизняні дослідники виокремлюють такі спеціальні технології державного реагування на загрози як: профілактика та протидія, яка в свою чергу передбачає: попередження, припинення та локалізацію дії загроз національним інтересам.

Технологія державного реагування на загрози національній безпеці структурно включає в себе такі елементи, як [9]: цілісну теоретичну концепцію, яка відображає: закономірності функціонування об'єкту впливу; об'єкт і предмет державно-управлінського впливу; алгоритм державно-управлінського впливу; технологічні способи і засоби перетворення предмету; елемент контролю результату застосування цієї технології.

Відповідно, першою складовою технології державного реагування на загрози кібербезпеці є теоретична концепція державного реагування на загрози національним інтересам в кіберпросторі. Ця концепція включає в себе систему ідей і принципів дії, методи державного реагування на загрози кібербезпеці. В цій концепції також може бути виділена група причинних чинників викликів, ризиків, загроз і небезпек кібербезпеці. Так, аналіз результатів наукових досліджень проблем інформаційного протиборства, а також проблем державного реагування на загрози кібербезпеці України [9] дозволяє побудувати базову модель загроз кібербезпеці, яка структурно включає в себе такі моделі як: модель загроз безпеці персональних даних, модель кіберзлочинів, модель загроз терористичного характеру, модель загроз кібербезпеці об'єктам критичної інфраструктури, модель загроз кібербезпеці комунікаційним системам та інші.

Таким чином, базова модель загроз кібербезпеці дозволяє визначити перелік потенційних та реальних загроз у цій специфічній сфері.

Друга складова технології державного реагування на загрози кібербезпеці – це:

1) об'єкт державно-управлінського впливу – субстрат загроз кібербезпеці: особа, її права і свободи в кіберпросторі; суспільні організації, які вступають у взаємовідносини між собою та з державою; держава, її інформаційний суверенітет та національний кіберпростір;

2) головний суб'єкт забезпечення кібербезпеки є Українська держава, яка разом із інститутами громадянського суспільства та бізнесом здійснює державну політику у сфері кібербезпеки;

3) предмет державно-управлінського впливу – процес перетворення і трансформації субстрату загроз кібербезпеці, а саме: профілактика та протидія.

Третя складова технології державного реагування на загрози кібербезпеці – це алгоритм реагування, який передбачає послідовне застосування технологічних способів, методів і засобів реагування з метою мінімізації рівня загроз кібербезпеці.

Алгоритм державного реагування на загрози кібербезпеці містить такі операційні ланцюги: формулювання проблеми забезпечення кібербезпеки (виявлення проблеми, оцінка проблеми) моніторинг небезпек і загроз кібербезпеці ідентифікація та оцінка рівня загроз кібербезпеці розробка варіантів нейтралізації загрози кібербезпеці оцінка варіантів нейтралізації загрози кібербезпеці вибір оптимального варіанту за обраним критерієм прийняття рішення про нейтралізацію загрози кібербезпеці підготовка та всебічне забезпечення реалізації державно-управлінського рішення щодо реагування на загрозу кібербезпеці вплив на загрозу (нейтралізація загрози) оцінка рівня загрози після впливу на неї системи забезпечення кібербезпеки вибір оптимального варіанту за обраним критерієм досягнення запланованого результату.

Четверта складова технології державного реагування на загрози кібербезпеці – це технологічні способи реагування на загрози, тобто правила, відповідно до яких здійснюється весь комплекс заходів щодо реагування на виявлені загрози кібербезпеці.

П’ята складова технології державного реагування на загрози кібербезпеці – це засіб перетворення предмету, що передбачає застосування комплексних чи часткових методик реагування на виявлені загрози кібербезпеці.

Шоста складова технології державного реагування на загрози кібербезпеці – це контроль досягнутого результату по нейтралізації виявленої загрози кібербезпеці.

Таким чином, вказана технологія є надійним інструментом у процесі вирішення завдань забезпечення кібербезпеки України.

Висновки.

1. Встановлено, що виконання завдань визначених в офіційному дискурсі України щодо розвитку національної системи кібербезпеки потребують комплексної науково обґрунтованої методики. В цій методиці має бути враховано багатоаспектний комплексний характер проблем забезпечення кібербезпеки Української держави, українського суспільства та громадян України в умовах інформаційної глобалізації і динамічного безпекового середовища.

2. Доведено, що ідеї паспортизації загроз кібербезпеці та технологізації державного реагування на виявленні загрози у цій сфері слугують теоретичною основою удосконалення національної системи кібербезпеки України, а саме державного механізму моніторингу загроз кібербезпеці та механізму державного реагування на виявлені загрози кібербезпеці.

3. З метою удосконалення державного механізму моніторингу загроз кібербезпеці запропоновано розробити та упровадити в державно-управлінську практику паспорти загроз кібербезпеці, до складу яких мають входити такі розділи: загальна характеристика загрози кібербезпеці; характеристика можливого розвитку загрози кібербезпеці; діяльність суб’єктів забезпечення кібербезпеки щодо реагування на загрози.

4. З метою удосконалення механізму державного реагування на виявлені загрози кібербезпеці запропоновано розробити та упровадити в практику державного управління технологію державного реагування на загрози кібербезпеці, до складу яких входять такі структурні елементи: цілісна теоретична концепція, яка відображає закономірності функціонування об’єкту кібербезпеки; об’єкт кібербезпеки і предмет державно-управлінського впливу; алгоритм державно-управлінського впливу на об’єкт кібербезпеки; технологічні способи і засоби державно-управлінського впливу на об’єкт кібербезпеки; елемент контролю результату застосування цієї технології.

Перспективи подальших досліджень вбачаємо у дослідженні структури та функцій, завдань системи забезпечення кібербезпеки України.

Список використаних джерел:

1. Бурячок В.Л., Богуш В.М. Кібербезпека та захист критичної інформаційної інфраструктури. *Ukrainian Scientific Journal of Information Security.* 2014. № 2. С. 119–148.
2. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юрид. наук : 12.00.07 / Сумський держ. ун-т. Суми, 2018. 221 с.
3. Гаращенко Ю. В. Державна політика у сфері кібербезпеки України. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2019. № 1. Т. 30 (69). С. 140-145.
4. Дубов. Д. В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети.* 2013. № 4. С. 119–127.
5. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. 233 с.
6. Про основні засади забезпечення кібербезпеки України. Закон України № 1263-VIII від 05.10.2017 р. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
7. Про Стратегію кібербезпеки України [Електронний ресурс]: Указ Президента України № 96/2016. Режим доступу : https://www.president.gov.ua/documents/962016-19836. (дата звернення: 12.12.2019 р.). Назва з екрану.
8. Обґрунтування концептуальних та організаційно-правових засад розробки паспортів загроз національній безпеці України : навч.-метод. посіб. / [Г.П. Ситник, В.І. Абрамов, М.М. Шевченко та ін.] за заг. ред. Г.П. Ситника К.: НАДУ, 2012. 52 с.

9. Шевченко М.М. Поняття «технологія державного реагування на загрози національній безпеці»: смисловий простір соціально-філософського змісту. *Філософія науки: традиції та інновації*. 2017. № 2 (16). С. 183-196.

10. Копнин П.В. Диалектика как логика и теория познания : монография. М.: Изд-во «НАУКА», 1973. 324 с.

References.

1. Buriachok, V.L. and Bohush, V.M. (2014), "Cybersecurity and critical information infrastructure protection", *Ukrainian Scientific Journal of Information Security*, vol. 2, pp. 119–148.

2. Bukhariev, V.V. (2018), "Administrative and legal principles of cybersecurity of Ukraine", Abstract of Ph.D. dissertation, 12.00.07, Sumskyi derzh. un-t. Sumy, Ukraine, P. 221.

3. Harashchenko, Yu. V. (2019), "State policy in the field of cyber security of Ukraine", *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Derzhavne upravlinnia*, issue 1, vol. 30 (69), pp. 140-145.

4. Dubov,. D. V. (2013), "Strategic aspects of cybersecurity in Ukraine", *Stratehichni priorytety*, vol. 4, pp. 119–127.

5. Cybersecurity in Ukraine: legal and organizational issues: materials all-Ukrainian. scientific-practical conf., Odessa, October 21, 2016, ODUVS, Odessa, Ukraine, P. 233.

6. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the basic principles of cybersecurity in Ukraine", *Vidomosti Verkhovnoi Rady*, vol. 45, art. 403.

7. President of Ukraine (2016), Decree of the President of Ukraine " On the Strategy of Cyber Security of Ukraine", available at: https://www.president.gov.ua/documents/962016-19836 (Accessed 12 Dec 2019).

8. Sytnyk, H.P. Abramov, V.I. Shevchenko, M.M. and others (2012), *Obgruntuvannia kontseptualnykh ta orhanizatsiino-pravovykh zasad rozrobky pasportiv zahroz natsionalnii bezpetsi Ukrainy: navch.-metod. posib.* [Substantiation of conceptual and organizational-legal bases of development of passports of threats to national security of Ukraine], NADU, Kyiv, Ukraine, P. 52.

9. Shevchenko, M.M. (2017), "The concept of "technology of state response to threats to national security": the semantic space of socio-philosophical content", *Filosofiia nauky: tradytsii ta innovatsii*, vol. 2 (16), pp. 183-196.

10. Kopnin, P.V. (1973), *Dialektika kak logika i teorija poznanija: monografija* [Dialectics as logic and the theory of knowledge: monograph], Izd-vo «NAUKA», Moscow, Russia, P. 324.

Стаття надійшла до редакції 20.06.2020 р.