***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. 2024. № 5.***

**DOI: http://doi.org/10.32702/2307-2156.2024.5.4**

**УДК 351.86**

*Г. П. Ситник,*

*д. держ. упр., професор, завідувач кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби, Київський національний університет імені Тараса Шевченка*

*ORCID ID: https://orcid.org/0000-0002-3083-5733*

*Н .Г. Клименко,*

*д. держ. упр., доцент, професор кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби, Київський національний університет імені Тараса Шевченка*

*ORCID ID: https://orcid.org/0000-0001-5223-8166*

*І. О. Горєліков,*

*студент 2 курсу ОПП «Стратегічний менеджмент у сфері національної безпеки» Навчально-наукового інституту публічного управління та державної служби, Київський національний університет імені Тараса Шевченка*

*ORCID ID: https://orcid.org/0009-0005-3723-1771*

# ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ, ЯК ЇЇ СКЛАДОВОЇ: ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

*H. Sytnyk,*
*Doctor of Sciences in Public Administration, Full Professor, Head of the Department of Global and National Security of Educational and Scientific Institute of Public Administration and Civil Service,*
*Taras Shevchenko National niversity of Kyiv*
*N. Klymenko,*
*Doctor of Sciences in Public Administration, Associate Professor, Professor of the Department of Global and National Security of Educational and Scientific Institute of Public Administration and Civil Service,*
*Taras Shevchenko National University of Kyiv*
*I. Horielikov,*
*Student of the 2nd year of the educational and professional program "Strategic management in the field of national security" of Educational and Scientific Institute of Public Administration and Civil Service,*
*Taras Shevchenko National University of Kyiv*

# THE PUBLIC POLICY OF ENSURING INFORMATION SECURITY AND CYBER SECURITY AS ITS COMPONENT: PROBLEMS AND WAYS TO SOLVE THEM

*У статті досліджено державну політику забезпечення інформаційної безпеки в Україні, її зв'язок з кібернетичною безпекою. Визначено загальні засади безпеки інформації та досліджено вплив інформаційних технологій на зростання кіберзлочинів. Проаналізовано статистику збитків, яких завдає кіберзлочинність у світі. Відзначено існуючі проблеми та заходи, які запроваджуються спеціалізованими структурами зарубіжних країн та міжнародними структурами безпеки для боротьби з кіберзлочинністю та для захисту інформації.*

*В ході проведеного дослідження були визначенні основні регулюючі органи України в сфері інформаційної та кібернетичної безпеки. На підставі чинного законодавства проаналізовано повноваження суб'єктів забезпечення*

*інформаційної та кібернетичної безпеки.*

*За підсумками дослідження змісту державної політики забезпечення інформаційної безпеки в Україні, кібернетичної безпеки як її складової, та кола завдань суб'єктів її реалізації, визначено заходи протидії загрозам інформаційної безпеки, реалізація яких, на думку авторів, сприятиме створенню комплексної системи забезпечення інформаційної безпеки України:*

*- забезпечення інформації безпеки в Україні в умовах воєнного стану повинно стати пріоритетом Міністерства цифрової трансформації, яке разом з відповідними органами має створити надійний інформаційний тил країни, забезпечивши цілковиту гарантію захисту від проникнення ворога в інформаційний простір України;*

*- актуальним є врахування міжнародного досвіду щодо забезпечення інформаційної безпеки та кібербезпеки, як її складової, передусім країн-членів НАТО;*

*- в умовах розвитку новітніх технологій забезпечення інформаційної та кібернетичної безпеки є надскладним завданням, тож запропонована нами сукупність заходів протидії загрозам інформаційної безпеки, реалізація яких сприятиме створенню комплексної системи забезпечення інформаційної безпеки України з метою створення безпечного інформаційного простору.*

*Перспективами подальших розвідок у даному напрямі автори вбачають визначення єдиних методологічних засад щодо розробки політики інформаційної безпеки.*

*The article examines the state policy of ensuring information security in Ukraine, its connection with cyber security. The general principles of information security are defined and the influence of information technologies on the growth of cybercrimes is investigated. The statistics of damages caused by cybercrime in the world are analyzed. Existing problems and measures introduced by specialized structures of foreign countries and international security structures to combat cybercrime and to protect information are noted.*

*In the course of the conducted research, the main regulatory bodies of*

*Ukraine in the field of information and cyber security were determined. On the basis of the current legislation, the powers of subjects of information and cyber security were analyzed.*

*According to the results of the study of the content of the state policy of ensuring information security in Ukraine, cyber security as its component, and the range of tasks of the subjects of its implementation, measures to counter threats to information security have been determined, the implementation of which, according to the authors, will contribute to the creation of a comprehensive system of ensuring information security in Ukraine:*

*- provision of security information in Ukraine under martial law conditions should become a priority of the Ministry of Digital Transformation, which, together with relevant bodies, should create a reliable information backbone of the country, providing a complete guarantee of protection against enemy penetration into the information space of Ukraine;*

*- it is relevant to take into account the international experience in ensuring information security and cyber security, as its component, primarily of NATO member countries;*

*- in the conditions of the development of the latest technologies, ensuring information and cyber security is an extremely difficult task, so we have proposed a set of measures to counter threats to information security, the implementation of which will contribute to the creation of a comprehensive system of ensuring information security of Ukraine with the aim of creating a safe information space.*

*The authors see the definition of uniform methodological principles for the development of information security policy as prospects for further research in this direction.*

***Ключові слова:*** *інформаційна безпека, кібербезпека, новітні технології, державні та недержавні інституції, суб'єкти забезпечення, державна політика, цифрові технології.*

***Keywords:*** *information security, cyber security, the latest technologies, state and non-state institutions, security entities, public policy, digital technologies.*

***Постановка проблеми.*** Сьогодні в умовах розвитку інформаційних технологій та штучного інтелекту загрози для інформаційної безпеки стрімко зростають. Тому не лише комерційним компаніям, але й урядам країн потрібно переосмислити ставлення до інформаційної безпеки та вжити відповідних заходів для мінімізації кількості кібератак та задля запобігання кіберзлочинам. Зазначене свідчить про важливість формування та реалізації адекватної сучасних загрозам та небезпекам державної політики забезпечення інформаційної безпеки та кібербезпеки, як її складової та визначення ефективних заходів щодо протидії загрозам у цій сфері в Україні, що й обумовлює актуальність проведення відповідного дослідження.

***Аналіз останніх досліджень і публікацій.*** Дослідження проблем інформаційної та кібернетичної безпеки в сучасних умовах інтенсифікації глобалізаційних процесів, розвитку інформаційно-комунікаційних технологій та російсько-української війни приділяють увагу науковці різних галузей.

Так, П. Біленчук, Л. Борисова, І. Неклонський, В. Собина своє дослідження присвятили систематизації відомостей про інформаційну безпеку людини, суспільства та держави та визначенню шляхів її забезпечення, у тому числі за допомогою технічного захисту. Автори розглядають інформацію як особливий об’єкт правового регулювання інформаційної безпеки та юридичної відповідальності за порушення правових норм щодо захисту державної таємниці та конференційної інформації [1].

Т. Ткачук досліджує фундаментальні засади, особливості та відмінності правового забезпечення інформаційної безпеки в Україні та європейських державах. Ним здійснено порівняльний аналіз правових норм щодо забезпечення інформаційної безпеки та на цій основі розроблено концептуальні правові засади забезпечення інформаційної безпеки держави й надано практичні рекомендації щодо вдосконалення механізмів її забезпечення в Україні [2].

У монографії О. Панченка інформаційна безпека розглядається в причинно-наслідковому зв’язку з турбулентними явищами у різних сферах життєдіяльності людини (природа, суспільство, інформаційне середовище). Дане дослідження здійснюється через призму державного управління, де центром цілепокладання є особистість. Автором розглядається стан державного управління в умовах суспільно-інформаційної турбулентності, а також комунікаційні, правові, медико-психологічні аспекти забезпечення інформаційної безпеки [3].

В. Шемчук розглядає інформаційну безпеку держави й інформаційну війну в контексті російсько-української війни 2014-2023 рр. та ґенези національної стійкості [4].

Л. Веселова акцентує увагу на історичних аспектах формування та аналізі сучасного стану адміністративно-правового забезпечення кібернетичної безпеки. Авторка узагальнює міжнародний досвід щодо формування безпекового середовища та стійкості суспільства в умовах гібридизації міжнародних відносин та висловлює пропозиції удосконалення адміністративно-правового забезпечення кібернетичної безпеки в Україні в умовах гібридної війни [5].

***Формулювання цілей статті (постановка завдання*).** Мета статті полягає у дослідженні змісту державної політики забезпечення інформаційної безпеки та кібербезпеки, як її складової, та суб’єктів її реалізації, а також розробці рекомендацій щодо комплексу заходів, спрямованих на підвищення її ефективності в Україні.

***Виклад основного матеріалу дослідження.*** У сучасну цифрову епоху, коли значні обсяги інформації передаються через Інтернет, інформаційна безпека стала ключовим елементом для державних, не державних інституцій та приватних осіб. Водночас ескалація країною-агресором кіберзагроз, цілеспрямоване та масштабне використання кібератак зумовили необхідність

розбудови більш ефективної системи інформаційної безпеки в кіберпросторі [5] і поставили на порядок денний питання пошук шляхів забезпечення інформаційної безпеки в умовах глобалізації та російсько-української війни.

Стратегія інформаційної безпеки визначає інформаційну безпеку як «складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [6].

Оскільки кібербезпека невід’ємно пов’язана з інформацією та комунікаційним середовищем, то вітчизняне законодавство визначає її як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [7].

Множина факторів, які породжують небезпеки інформації досить значна, серед яких, зокрема втручання у приватне життя, крадіжка персональних даних, втрата комерційної та конфіденційної інформації, репутаційні збитки. Ці небезпеки в цілому можуть призвести до вкрай негативних наслідків у всіх сферах життєдіяльності інститутів держави, суспільства та кожної людини (індивіда). Так, внаслідок кібератак за останні декілька років було втрачено близько 1% світового ВВП [8]. При цьому грошові збитки від кібератак стрімко зростають (рис. 1).

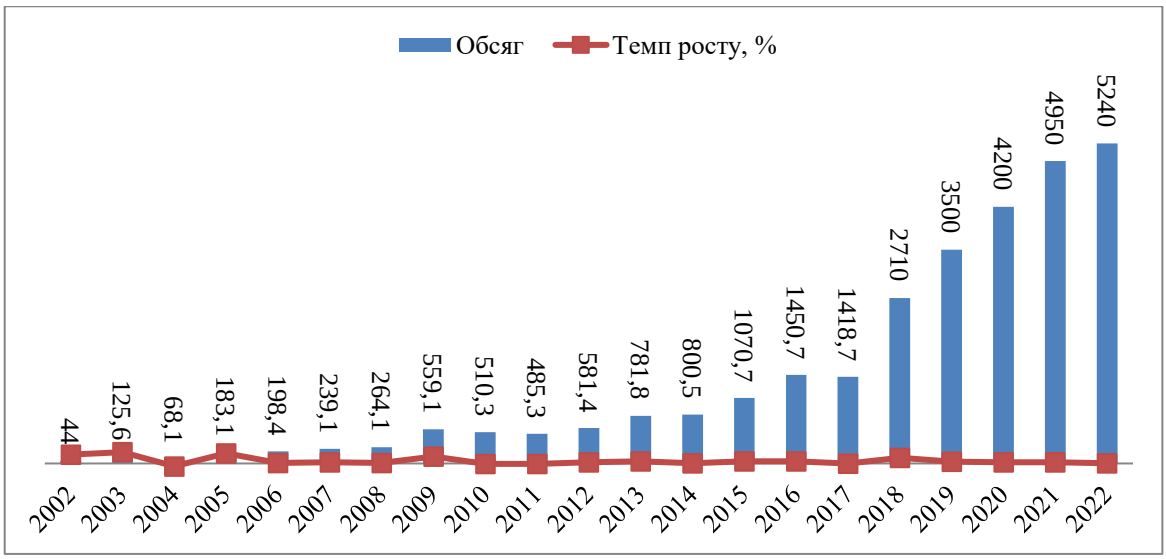


**Рис. 1. Темп зростання грошових збитків від кібератак за період 2002-2022 рр., млн дол.**

*Джерело: [9].*

Отже, інформаційна безпека має вирішальне значення для функціонування сучасного суспільства. Тому захист інформації від несанкціонованого доступу, крадіжки чи знищення є одним з найважливіших завдань бізнесу, державних та недержавних інституцій. Тож урядові та неурядові організації в усьому світі вживають заходів щодо посилення інформаційної безпеки та захисту від кібератак.

У 2018 році Європейське агентство мережевої та інформаційної безпеки (ENISA) опублікувало звіт, в якому ідентифіковано декілька ключових ризиків інформаційної безпеки, таких як атаки на критичну інфраструктуру, використання технології блокчейну зі злочинною метою та атаки на хмарні системи. У відповідь на зростання загроз країни всього світу вживають значну кількість заходів щодо посилення захисту своїх інформаційних систем. Зокрема, у Польщі Агентство внутрішньої безпеки (ABW) працює з різними установами для підвищення поінформованості про небезпеку кіберзагроз та заходи щодо їх запобігання. Агентство проводить навчання для бізнесу та державних установ, а також організовує інформаційні кампанії з інформаційної безпеки. У 2020 році Агентство запустило спеціальний сайт «Безпечна компанія», на якому представлені практичні поради та інформація

щодо інформаційної безпеки для бізнесу.

Інші країни також здійснюють аналогічні кроки, зокрема:

у США Національний інститут стандартів і технологій (NIST) розробив структуру кібербезпеки, яка є набором рекомендацій і кращих практик з інформаційної безпеки;

у Європі Європейське агентство мережевої та інформаційної безпеки (ENISA) розробляє рекомендації з інформаційної безпеки та організує навчальні та інформаційні кампанії.

Міжнародні організації також роблять кроки щодо підвищення інформаційної безпеки. Прикладом може бути розроблена НАТО концепція кіберзахисту та проведення навчань серед членів Альянсу з питань інформаційної безпеки.

Разом з тим варто зазначити, що однією із найбільших проблем забезпечення інформаційної безпеки є відсутність єдиних методологічних засад щодо розробки політики інформаційної безпеки. Кожна країна, організація чи компанія має свій підхід до забезпечення інформаційної безпеки. Ці відмінності можуть бути обумовлені багатьма факторами, зокрема культурними, організаційно-правовими, технологічними. Недостатньо гармонізований підхід до забезпечення інформаційної безпеки Значною мірою це призводить до уразливості, якою може скористатися злочинець чи агресор. Тому для країн, організацій чи компаній важливо діяти передусім на основі гармонізованих стандартів інформаційної безпеки [10].

Окремо варто акцентувати увагу на тому, що загрози, пов'язані із розвитком технологій, створюють ще один виклик для інформаційної безпеки, оскільки у кіберзлочинців з'являється все більше можливостей для проведення кібератак. Прикладом є розвиток технології штучного інтелекту, що дозволяє створювати інструменти для проведення більш інтенсивних та ефективних кібератак, зокрема, кількість підключених до мережі пристроїв, таких як пристрої Internet of Things, збільшує кількість потенційних векторів атак. Це вимагає від країн, організацій та компаній постійної роботи над захистом своїх

систем від нових типів загроз [11].

Очевидно, що одним із способів вирішення проблем забезпечення інформаційної безпеки є розробка ефективних систем моніторингу та реагування на загрози. Такі системи дозволяють швидко виявляти кібератаки та вживати відповідних заходів для мінімізації їхніх наслідків. Розвиток компетентності та обізнаності співробітників щодо забезпечення інформаційної безпеки також є визначальною передумовою ефективного захисту інформаційно-комунікаційних систем. Тому необхідно інвестувати у навчання співробітників заходам забезпечення інформаційної безпеки, щоб вони могли ефективно захищати свої системи від кіберзагроз.

Вищевикладене свідчить про те, що забезпечення інформації безпеки та її складової кібернетичної безпеки є пріоритетним завданням інститутів держави в умовах російсько-української війни. У 2022 році Україна зайняла 24 місце в індексі Кібербезпеки поряд з такими країнами як Італія та Малайзія, і входить до 25-ти країн з високим рівнем інформаційного захисту (джерело 8). Це є наслідком, того, що саме збройна агресія РФ стимулювала збільшити рівень кібербезпеки України та захищати країну в інформаційному просторі.

Щодо інституційної складової забезпечення інформаційної безпеки, то сьогодні забезпечення її належного рівня має стати пріоритетом Міністерства цифрової трансформації України, оскільки на нього покладається завдання щодо участі у «формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, …, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку» [12].

Водночас, комплексність реалізації державної політики у цій сфері

покладається на Міністерство культури та інформаційної політики України, яке є «головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері інформаційної безпеки» [13]. При цьому серед принципів діяльності вказаного Міністерства, зокрема: дотримання Конституції та законодавства України, а також загальновизнаних принципів і норм міжнародного права; забезпечення правової рівності усіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу; пріоритетний розвиток вітчизняних сучасних інформаційних і телекомунікаційних технологій [14].

Є й інші державні органи, які опікуються питаннями забезпечення інформаційної безпеки України. У складі Центрального управління СБУ функціонує підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, а серед завдань Державної служби спеціального зв'язку та захисту інформації України: «формування та реалізацію державної політики у сферах … технічного захисту інформації, кіберзахисту, … захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, …, активної протидії агресії у кіберпросторі» [15]. Саме на неї покладено обов'язки щодо «координації діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту; та забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури…» [15].

Державним органом, який відповідає за інформаційну безпеку, є й Департамент кіберполіції Національної поліції України – «міжрегіональний територіальний орган Національної поліції України, який входить до складу кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у боротьбі з кіберзлочинністю» [16]. Крім того,

в Україні створено систему спеціалізованих органів з кібербезпеки, а до боротьби з кіберзлочинністю залучені звичайні слідчі, які проводять розслідування кіберзлочинів під процесуальним контролем прокуратури.

Водночас існує низка проблем щодо забезпечення інформаційної та кібернетичної безпеки в Україні, передусім: брак висококваліфікованих кадрів, відсутність кіберспеціалізації слідчих та прокурорів, невідповідність законодавства сучасним реаліям, складність організації взаємодії суміжних суб'єктів, відсутність новітніх досліджень та розробок.

Одним з напрямів вирішення цих проблем ми пропонуємо створити спеціалізовані слідчі підрозділи та відповідні підрозділи прокуратури з розслідування кіберзлочинів та запровадити відповідну спеціалізацію суддів. Крім того, для координації наукових розробок на базі Українського науково-дослідного інституту спеціальної техніки та судово-медичної експертизи СБУ створити майданчик для постійного обміну досвідом та досягненнями у галузі кібербезпеки.

Результати аналізу заходів щодо забезпечення інформаційної безпеки України дають підстави вважати, що в сучасних умовах рівень інформаційної безпеки України є недостатнім. Тому захист інформаційного суверенітету, формування більш ефективної системи інформаційної безпеки, розробка та реалізація ефективних стратегій та тактик протидії інформаційним та кібернетичним загрозам мають стати пріоритетними завданнями органів державної влади, спеціальних служб та правоохоронних органів та недержавних інституцій. З огляду на викладене, пропонуємо заходи протидії загрозам інформаційної безпеки, реалізація яких, як на нашу думку, сприятиме створенню комплексної системи забезпечення інформаційної безпеки України (рис. 2).

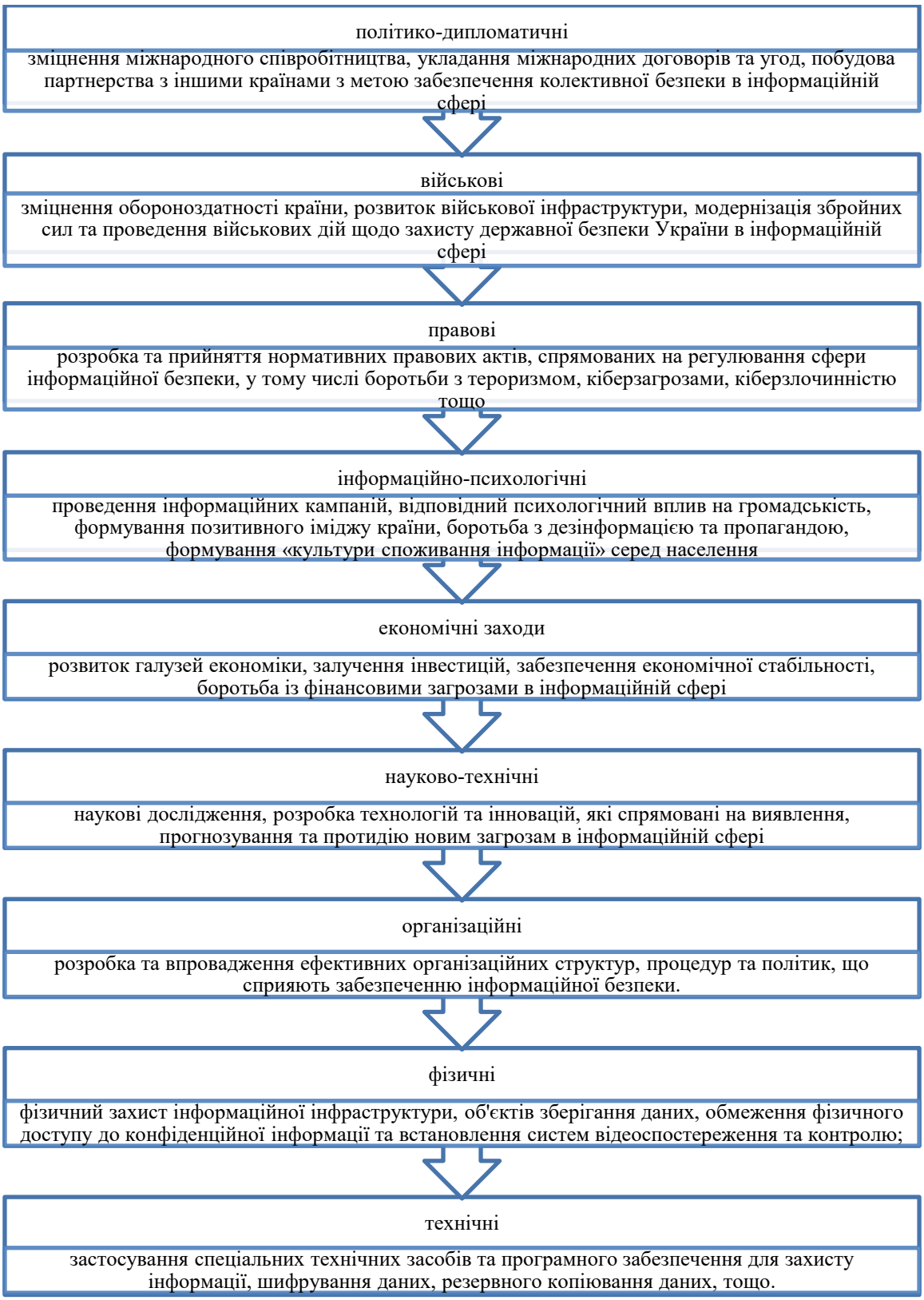


**Рис. 2. Характеристика заходів протидії загрозам інформаційної безпеки**

*Джерело: розробка авторів*

***Висновки та перспективи розвідок у даному напрямі.*** Дослідивши

зміст державної політики забезпечення інформаційної безпеки в Україні, кібернетичної безпеки як її складової, та коло завдань суб'єктів її реалізації, можна зробити наступні висновки:

- забезпечення інформації безпеки в Україні в умовах воєнного стану повинно стати пріоритетом Міністерства цифрової трансформації, яке разом з відповідними органами має створити надійний інформаційний тил країни, забезпечивши цілковиту гарантію захисту від проникнення ворога в інформаційний простір України;

- актуальним є врахування міжнародного досвіду щодо забезпечення інформаційної безпеки та кібербезпеки, як її складової, передусім країн-членів НАТО;

- в умовах розвитку новітніх технологій забезпечення інформаційної та кібернетичної безпеки є надскладним завданням, тож запропонована нами сукупність заходів протидії загрозам інформаційної безпеки, реалізація яких сприятиме створенню комплексної системи забезпечення інформаційної безпеки України з метою створення безпечного інформаційного простору;

- перспективами розвідок у даному напрямі є визначення єдиних методологічних засад щодо розробки політики інформаційної безпеки.

## Література

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

2. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: Монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 411 с.

3. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.

4. Шемчук В.В. Інформаційна безпека держави та інформаційна війна. *Україна під час російсько-української війни 2014-2023 рр.: ґенеза національної стійкості крізь призму наукових досліджень* : монографія / За заг. ред. Б.

Попкова, С. Пєткова. Київ : Вида-во Ліра-К. 2023. С. 140-161.

5. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади: монографія. Видавничий дім «Гельветика», 2021. 488 с.

6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685. URL: https://www.president.gov.ua/documents/6852021-41069

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

8. Hawdon J. Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice.* 2021. № 46(6). p. 837–842.

9. Cyber Crime & Security. Statista Research Department. 2023. URL: https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/

10. Kuhn S. Different Approaches to Information Security Management, in Proceedings of the 38th Hawaii International Conference on System Sciences. Hawaii Island, HI, January 3–6. 2005.

11. Chakrabarti J. Security in the Cloud: Challenges and Opportunities, in Proceedings of the 2010 International Conference on Advances in Computing, *Communications and Informatics.* Miyazaki Japan, June 23–25, 2010.

12. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

13. Деякі питання діяльності Міністерства культури та інформаційної політики : постанова Кабінету Міністрів України від 16.10.2019 р. № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text

14. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

15. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. URL:

https://zakon.rada.gov.ua/laws/show/3475-15#Text

16. Департамент кіберполіції України. Про Департамент. 2024. URL: https://cyberpolice.gov.ua/contacts/

## References

1. Bilenchuk, P.D., Borysova, L.V., Neklonskyi., I.M. and Sobyna V.O. (2018). *Pravovi zasady informatsiinoi bezpeky Ukrainy* [Legal principles of information security of Ukraine], Kharkiv, Ukraine.

2. Tkachuk, T.Iu (2018). *Zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy: pravovyi vymir* [Ensuring information security in the conditions of European integration of Ukraine: legal dimension], TOV «Vydavnychyi dim «ArtEk», Kyiv, Ukraine.

3. Panchenko, O.A. (2020). *Informatsiina bezpeka v epokhu turbulentnosti: derzhavno-upravlinskyi aspekt* [Information security in the era of turbulence: the state-management aspect], KVITs, Kyiv, Ukraine.

4. Shemchuk, V.V. (2023). *Informatsiina bezpeka derzhavy ta informatsiina viina. Ukraina pid chas rosiisko-ukrainskoi viiny 2014-2023 rr.: geneza natsionalnoi stiikosti kriz pryzmu naukovykh doslidzhen* [State information security and information warfare. Ukraine during the Russian-Ukrainian war 2014-2023: the genesis of national stability through the prism of scientific research], Vyda-vo Lira-K, Kyiv, Ukraine.

5. Veselova, L.Iu. (2021). *Kiberbezpeka v umovakh hibrydnoi viiny: administratyvno-pravovi zasady* [Cyber security in the conditions of hybrid warfare: administrative and legal principles],Vydavnychyi dim «Helvetyka», Ukraine.

6. The President of Ukraine (2021), Decree "On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy", available at: https://www.president.gov.ua/documents/6852021-41069 (Accessed April 15 2024).

7. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On the main principles of ensuring cyber security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed April 15 2024).

8. Hawdon, J. (2021), “Cybercrime: Victimization, perpetration, and

techniques”,*American Journal of Criminal Justice*, vol. 46(6), pp. 837–842.

9. Cyber Crime & Security. Statista Research Department (2023), available https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/ (Accessed April 15 2024).

10. Kuhn, S. (2025). "Different Approaches to Information Security Management", Proceedings of the 38th *Hawaii International Conference on System Sciences*. Hawaii Island, HI, January 3–6.

11. Chakrabarti, J. (2010). "Security in the Cloud: Challenges and Opportunities", Proceedings of the 2010 *International Conference on Advances in Computing,Communications and Informatics*, Miyazaki Japan, June 23–25.

12. Cabinet of Ministers of Ukraine (2019), Resolution “Issues of the Ministry of Digital Transformation”, available at: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (Accessed April 15 2024).

13. Cabinet of Ministers of Ukraine (2019), Resolution “Some issues of the Ministry of Culture and Information Policy”, available at: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text (Accessed April 15 2024).

14. Ostroukhov, V.V., Prysiazhniuk, M.M., Farmahei, O.I. and Chekhovska, M.M. (2021). Informatsiina bezpeka [Informational security] Vydavnytstvo Lira-K, Kyiv, Ukraine.

15. The Verkhovna Rada of Ukraine (2006), The Law of Ukraine "About the State Service of Special Communications and Information Protection of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/3475-15#Text (Accessed April 15 2024).

16. Department of Cyber Police of Ukraine. (2024). “About the Department”, available at: https://cyberpolice.gov.ua/contacts/ (Accessed April 15 2024).

*Стаття надійшла до редакції 29.04.2024 р.*