МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ

ОСТРОВИЙ Олексій Володимирович

УДК 351.865:007 (477)

ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

Спеціальність 25.00.02 – механізми державного управління

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата наук з державного управління

Маріуполь – 2019

Дисертацією є рукопис.
Роботу виконано в Донецькому державному університеті управління Міністерства освіти і науки України (м. Маріуполь)

Науковий керівник – доктор економічних наук, професор
БАЛУЄВА Ольга Володимирівна,
Донецький державний університет управління
Міністерства освіти і науки України (м. Маріуполь),
проректор з наукової роботи

Офіційні опоненти: доктор наук з державного управління, професор
ДОВГАНЬ Валерій Іванович,
Національна академія Державної прикордонної
служби України імені Б. Хмельницького
(м. Хмельницький), головний науковий співробітник
науково-дослідного відділу;

доктор наук з державного управління, доцент
ШПАЧУК Віталій Васильович,
Таврійський національний університет
імені В.І. Вернадського (м. Київ), професор кафедри
публічного управління та адміністрування.

Захист дисертації відбудеться *10 жовтня 2019 року* о *13:00* на засіданні спеціалізованої вченої ради Д 11.107.01 у Донецькому державному університеті управління Міністерства освіти і науки України за адресою: 87513, м. Маріуполь, вул. Карпинського, 58.

З дисертацією можна ознайомитись у бібліотеці Донецького державного університету управління Міністерства освіти і науки України за адресою: 87513, м. Маріуполь, вул. Карпинського, 58.

Автореферат розіслано *07 вересня 2019 року.*

Вчений секретар
спеціалізованої вченої ради **В.В. Хороших**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Стрімкий розвиток інформаційно-комунікаційних технологій сприяв формуванню кібернетичного простору, який здійснює значний вплив на соціально-економічне становище України та її національну безпеку.

Однак, інформаційні технології не тільки відкривають певні можливості для розвитку країни, але й створюють ряд викликів та загроз, які активізуються з поширенням таких технологій у політичній, соціальній та економічній сферах, актуалізуючи процеси, пов'язані з забезпеченням кібербезпеки.

В сучасних умовах, для яких є характерним збільшення кількості кібератак та кіберінцидентів, що призводять до фінансових втрат, порушення функціонування інформаційно-телекомунікаційних систем, впливають на стан національної безпеки і оборони країни, перед Україною постало актуальне завдання щодо формування державної політики забезпечення кібернетичної безпеки, як засобу посилення безпеки і надійності інформаційних систем, адекватної сучасним викликам і реаліям, спрямованої на своєчасне виявлення, запобігання й нейтралізацію реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним, національним інтересам на основі комплексного підходу та участі всіх суб'єктів.

Формування державної політики забезпечення кібернетичної безпеки є комплексною методичною проблемою, яка вимагає детального розгляду з метою розробки підходів, методів, інструментів, які дозволяють реалізувати процес управлінської діяльності в цій сфері для збереження відкритості та безпечності кіберпростору.

Питанням формування сучасного кіберпростору та науково-практичних підходів до вирішення проблем в сфері кібербезпеки присвячено праці таких зарубіжних дослідників, як Д. Белл, Б. Гейтс, М. Кастельс, Е. Тофлер та інші.

Проблемам формування державної політики, закладенню теоретичного підґрунтя державного управління в цілому приділено увагу в працях Ю. Ковбасюка, Ю. Комара, В. Токаревої, О. Черниш та багатьох інших.

Теоретико-методичні засади вирішення проблем в сфері державного регулювання процесів кіберезпеки знайшли відображення у працях таких українських науковців, як О. Балуєва, В. Бурячок, С. Гнатюк, І. Діордіца, В. Довгань, В. Ліпкан, А. Семенченко, В. Шпачук та інші.

Однак, незважаючи на широкий спектр результатів досліджень зарубіжних та вітчизняних вчених, слід вказати, що досі залишається невирішеним коло питань, пов'язаних із розробкою, удосконаленням та впровадженням методичних підходів щодо формування державної політики забезпечення кібернетичної безпеки. Отже, постає необхідність у розробці цілісної теоретико-методичної основи для забезпечення кібернетичної безпеки, що має ґрунтуватись на застосуванні дієвих інструментів з урахуванням сучасних ризиків кібератак та кіберінцидентів, спрямованої на формування безпечного кібернетичного простору.

Вагомість і актуальність зазначених питань та їх неповне вирішення у визначених проблемах, відсутність однозначного теоретичного обґрунтування та

відповідних методичних і практичних напрацювань зумовили тему дисертаційної роботи, її мету, задачі і структуру, теоретичну та практичну значущість.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано згідно з тематикою науково-дослідних робіт Донецького державного університету управління Міністерства освіти і науки України за темою «Правові засади діяльності підрозділів поліції органів місцевого самоврядування» (номер державної реєстрації 0110U003043, за період 2015–2018 рр.), а також «Теоретико-методологічні засади розроблення та функціонування механізмів державного управління на центральному, регіональному, галузевому рівнях, в різних сферах суспільного життя» (номер державної реєстрації 0110U002889, за період 2015–2018 рр.), в межах яких автором узагальнено теоретичні основи формування державної політики забезпечення кібернетичної безпеки, поглиблено й аргументовано концепцію формування державної політики забезпечення національної кібернетичної безпеки, запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері кібернетичної безпеки.

Мета і задачі дослідження. Метою дисертаційної роботи є поглиблення теоретичних засад та розвиток науково-методичних і практичних рекомендацій щодо формування державної політики забезпечення кібернетичної безпеки. Для досягнення мети було поставлено і вирішено такі завдання:

узагальнити та систематизувати теоретичні основи формування державної політики забезпечення кібернетичної безпеки;

дослідити зарубіжний досвід державної політики забезпечення кібернетичної безпеки і виявити можливості його адаптації до вітчизняних умов;

удосконалити методичні засади аналітичного забезпечення державного управління кібернетичною безпекою;

розвинути методичні підходи до формування державної політики забезпечення кібернетичної безпеки;

поглибити й аргументувати концепцію формування державної політики забезпечення національної кібернетичної безпеки;

запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері кібернетичної безпеки на основі методів моделювання;

удосконалити механізм формування державної політики забезпечення кібернетичної безпеки.

Об'єктом дослідження є процес формування та реалізації державної політики забезпечення кібернетичної безпеки.

Предметом дослідження є теоретико-методичні, організаційні і науково-практичні засади формування державної політики забезпечення кібернетичної безпеки.

Методи дослідження. Дослідження теоретичних і методичних положень дисертаційної роботи ґрунтуються на загальнонаукових принципах проведення комплексних досліджень, роботах провідних вітчизняних і зарубіжних вчених з питань державної політики забезпечення кібернетичної безпеки.

Методологічною базою дисертаційного дослідження є концептуальні положення сучасної економічної теорії, теорії державного управління, методи системного аналізу, загальнонаукові принципи проведення наукових досліджень.

В процесі дослідження використовувались загальнонаукові та специфічні для економічної науки підходи, методи і прийоми, зокрема: *монографічний, системний аналіз, метод узагальнення, комплексний підхід* – для вивчення теоретичних основ формування державної політики забезпечення кібернетичної безпеки; *метод порівняльного аналізу* – при дослідженні зарубіжного досвіду державної політики кібернетичної безпеки і виявленні можливості його адаптації; *метод конкретизації, статистичний, графічний* – при аналізі рівня розвитку інформаційно-комунікаційних технологій, кіберзагроз та формуванні аналітичного забезпечення державного управління кібернетичною безпекою; *концептуалізація, абстрактно-логічний метод*, *прескриптивний аналіз, теорія множин, теорія графів, сценарне моделювання, когнітивне моделювання* – при формуванні концепції державної політики забезпечення національної кібернетичної безпеки, обґрунтуванні напрямів управлінського впливу в сфері кібернетичної безпеки та удосконаленні механізму формування державної політики забезпечення кібернетичної безпеки.

Правове поле дисертаційного дослідження склали Конституція України, чинні законодавчі та нормативні документи України, що визначають зміст та особливості регулювання інформаційної та кібернетичної безпеки.

Інформаційною базою є матеріали Міністерства внутрішніх справ, Департаменту кіберполіції Національної поліції України, Державного комітету статистики України, Євростату, міжнародних компаній у сфері інформаційної безпеки, роботи вітчизняних та зарубіжних вчених, а також результати власних досліджень автора.

Наукова новизна одержаних результатів полягає у вирішенні наукового завдання поглиблення теоретичних засад та розвитку науково-методичних і практичних рекомендацій щодо формування державної політики забезпечення кібернетичної безпеки, що створює фундаментальне підґрунтя для посилення національної безпеки. Основні результати та ключові положення дисертації, що мають наукову новизну та характеризують особистий внесок автора в розвиток державного управління як науки, полягають у наступному:

удосконалено:

методичні засади формування аналітичного забезпечення державного управління кібернетичною безпекою, які, на відміну від існуючих, передбачають оцінку рівня кібернетичних загроз для регіонів країни та їх розподіл на кластери на основі використання економіко-математичних методів, що дозволяє обґрунтувати напрями державної політики кібербезпеки та диференціювати засоби впливу на рівні регіонів;

концепцію формування державної політики забезпечення національної кібернетичної безпеки, яка, на відміну від існуючої, представляє собою систему теоретичного базису, методичних засад, інструментального забезпечення, побудовану за принципом ієрархії на основі комплексного підходу, що передбачає участь держави (в рамках державної політики в сфері кіберзахисту) та залучення

інших суб'єктів, які працюють в цій сфері на національному та міжнародному рівні (підприємства, корпорації, неурядові організації) до процесів управління, реалізація якої обумовлює зміст механізму формування державної політики забезпечення кібернетичної безпеки та спрямована на формування безпечного кібернетичного простору;

методичний підхід до обґрунтування напрямів управлінського впливу в сфері забезпечення кібернетичної безпеки, який ґрунтується на використанні методу когнітивного моделювання та передбачає аналіз обраних факторів управлінського впливу, формування відповідних сценаріїв, що дозволило виявити певні тенденції змін, які здатні вплинути на рівень кібернетичної безпеки та є базою для науково обґрунтованого коригування існуючої стратегії кібербезпеки з урахуванням факторів впливу та удосконалення механізму формування державної політики забезпечення кібернетичної безпеки;

механізм формування державної політики забезпечення кібернетичної безпеки, що, на відміну від існуючих, являє собою сукупність організаційно-економічних методів і інструментів, які, ґрунтуючись на правових нормах, дозволяють державі, органам місцевого самоврядування і підприємствам зменшити ризики кібератак та кіберінцидентів та реалізація якого дозволить забезпечити формування безпечного кібернетичного простору, що передбачає кібербезпеку особистості, організації та країни в цілому;

дістали подальшого розвитку:

теоретичні підходи формування державної політики забезпечення кібернетичної безпеки шляхом уточнення змісту поняття «державна політика в сфері кібербезпеки» як заснованої на чинних нормативно-правових актах, узгодженої за цілями системи державно-управлінських заходів з боку органів державної влади, спрямованої на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору, мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об'єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі; а також обґрунтування авторського бачення моделі державного управління кібернетичною безпекою, яка містить такі основні складові: управлінську, забезпечуючу, результативну та комплекс засобів і інструментів управлінського впливу та є основою для формування державної політики забезпечення кібернетичної безпеки;

систематизація й узагальнення досвіду зарубіжних країн з питань розробки та реалізації державної політики забезпечення кібернетичної безпеки, що доводить необхідність застосування комплексного підходу до формування безпечного кіберпростору;

методичні підходи до формування державної політики забезпечення кібернетичної безпеки шляхом врегульованого розвитку концепції державно-приватного партнерства, запровадження незалежного аудиту, а також пов'язаних із

ним процесів стандартизації та сертифікації як складових національної системи кібербезпеки України та інструментів формування ефективної державної політики в сфері кіберзахисту, використання потенціалу міжнародного співробітництва в управлінських процесах, які спрямовані на розвиток інформаційного суспільства, своєчасне виявлення, нейтралізацію реальних і потенційних загроз, що виникають у кіберпросторі та запобігання їм.

Практичне значення одержаних результатів дослідження полягає в тому, що теоретичні положення дисертації доведені до рівня практичних рекомендацій і складають методичну основу для забезпечення кібернетичної безпеки на державному, регіональному рівні та рівні підприємств і організацій.

Результати дисертаційного дослідження, наукові висновки, практичні рекомендації автора впроваджені в практику діяльності Департаменту кіберполіції Донецького управління кіберполіції Національної поліції України (довідка б\н від 15.01.2019 р.) в частині залучення кращих західних практик задля посилення міжвідомчого співробітництва та застосування елементів державно-приватного партнерства в сфері кібербезпеки, а також впровадження аналітичного забезпечення управління кібернетичною безпекою.

Результати дослідження знайшли практичне застосування в діяльності Маріупольської міської ради в процесі розробки стратегії розвитку м. Маріуполя на період до 2021 року (довідка б/н від 20.02.2019 р.), зокрема, в частині підвищення ефективності діяльності місцевої влади шляхом впровадження актуальних електронних сервісів місцевого самоврядування та системи управління інформаційною безпекою, що базується на підході до оцінки ризиків під час створення, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалення безпеки інформації.

Науково-методичні розробки автора, практичні висновки і пропозиції дисертаційного дослідження впроваджено в навчальний процес Донецького державного університету управління при викладанні дисциплін «Інформаційне право», «Адміністративне право» (довідка № 10-19/632 від 29.10.2018 р.).

Особистий внесок здобувача. Теоретичні обґрунтування, практичні рекомендації, висновки та пропозиції, які отримані в процесі проведення досліджень, розроблено здобувачем самостійно. Внесок автора в опубліковані колективні роботи конкретизовано у списку публікацій. У друкованих працях, опублікованих у співавторстві, автору дисертації належать: аналіз світового досвіду та доведення необхідності прийняття вітчизняної стратегії забезпечення кібернетичної безпеки [1], пропозиції щодо застосування інструментів державно-приватного партнерства в сфері кібербезпеки [6].

Апробація результатів дослідження. Основні положення й результати дисертації оприлюднено на науково-практичних конференціях: Всеукраїнській науково-практичній конференції «Напрями вдосконалення механізмів державного управління в умовах сучасних реформаційних процесів» (м. Запоріжжя, 2016), ІІ Всеукраїнській науково-практичній інтернет-конференції «Публічне управління та адміністрування: конкурентні виклики сучасності» (м. Львів, 2019), Всеукраїнській науково-практичній конференції «Організаційно-правові аспекти

публічного управління в Україні» (м. Полтава, 2019), Міжнародній науково-практичній конференції «Research and Innovation: Collection of scientific articles» (м. Намур, Бельгія, 2019 р.).

Публікації. Основні положення дисертаційної роботи опубліковано у 12 наукових працях, зокрема, у 7 статтях у наукових фахових виданнях з державного управління, з яких 4 статті у виданнях, що входять до міжнародних наукометричних баз даних, 1 стаття у зарубіжному виданні, 3 публікації у матеріалах конференцій. Загальний обсяг публікацій становить 4,78 др. арк., з яких 3,74 др. арк. належать особисто авторові.

Структура й обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, додатків, списку використаних джерел. Повний обсяг дисертації – 239 сторінок, з них 179 сторінок основного тексту. Робота містить 32 таблиці, у тому числі 4 – на окремих сторінках, 39 рисунків, у тому числі 3 – на окремих сторінках, 6 додатків – на 18 сторінках. Список використаних літературних джерел із 205 найменувань викладено на 26 сторінках.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЙНОЇ РОБОТИ

У **Вступі** обґрунтовано актуальність теми дисертаційної роботи, визначено мету і задачі дослідження, його об’єкт і предмет, методи дослідження, наукову новизну і практичне значення отриманих результатів.

У першому розділі **«Теоретичні основи формування державної політики забезпечення кібернетичної безпеки»** висвітлено теоретичну сутність кібербезпеки в системі забезпечення національної безпеки України; проаналізовано основні аспекти державної політики забезпечення кібербезпеки України; досліджено зарубіжний досвід державної політики забезпечення кібернетичної безпеки.

Теоретичне дослідження сутності кібербезпеки в системі забезпечення національної безпеки України дозволило встановити, що процеси глобалізації, які характерні для сучасного суспільства, зростання кількості загроз і викликів, актуалізували проблеми національної безпеки для більшості країн світу, в тому числі і для України. За таких умов постає необхідність адекватного реагування на існуючі виклики та загрози, тобто запровадження дієвої політики національної безпеки задля забезпечення національних інтересів держави. Її зміст, складові, методи та інструменти значною мірою залежать від сприйняття та розуміння сутності національної безпеки суб’єктами прийняття державних управлінських рішень.

Відзначено, що процеси розвитку інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем сприяли формуванню інформаційного та кібернетичного просторів, які здійснюють значний вплив на соціально-економічний розвиток країни та її національну безпеку. Запровадження у роботу державних структур, підприємств та організацій, життя українського суспільства сучасних інформаційно-телекомунікаційних технологій, призводить до трансформації злочинів, появи їх нових видів.

З’ясовано, що сьогодні Україна зазнає значного впливу інцидентів та атак в кібернетичній сфері. Збереження кіберпростору відкритим та безпечним можливе виключно за рахунок своєчасного виявлення, запобігання й нейтралізації реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним, національним інтересам та застосування комплексного підходу й участі всіх суб’єктів, що актуалізує розробку державної політики в сфері кібербезпеки, формування та реалізацію її основних напрямів.

Аналіз напрацювань науковців стосовно трактування поняття «державна політика» дозволив уточнити зміст поняття «державна політика в сфері кібербезпеки» як заснованої на чинних нормативно-правових актах, узгодженої за цілями системи державно-управлінських заходів з боку органів державної влади, спрямованої на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору, мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об’єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі.

В роботі обґрунтовано авторське бачення моделі державного управління кібернетичною безпекою, яка містить управлінську, організаційно-забезпечуючу, результативну складові, а також комплекс засобів і інструментів управлінського впливу та є основою для формування державної політики забезпечення кібернетичної безпеки, спрямованої на формування безпечного кібернетичного простору (рис. 1).

Визначено такі основні напрями формування державної політики забезпечення кібербезпеки: організаційні, правові, технічні, фінансові, просвітницькі, наукові; уточнено її принципи з урахуванням специфіки і масштабності сучасних кіберзагроз.

Систематизація та узагальнення досвіду зарубіжних країн з питань формування та реалізації державної політики забезпечення кібернетичної безпеки дозволила довести необхідність застосування управлінського впливу на процеси забезпечення кіберзахисту.

За результатами дослідження, проведеного серед керівників підприємств та організацій у різних країнах встановлено, що за показником оцінки кібератаки, як неминучої загрози, серед лідерів – США, Австралія та Німеччина (рис. 2).

Відзначено, що державна політика кібернетичної безпеки у світі виступає засобом посилення безпеки і надійності інформаційних систем держави. Акцентовано увагу на тому, що транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію, що обумовлено не тільки необхідністю ефективної підготовки до кібератак, а й доцільністю своєчасної реакції на них, вироблення узгоджених механізмів запобігання.

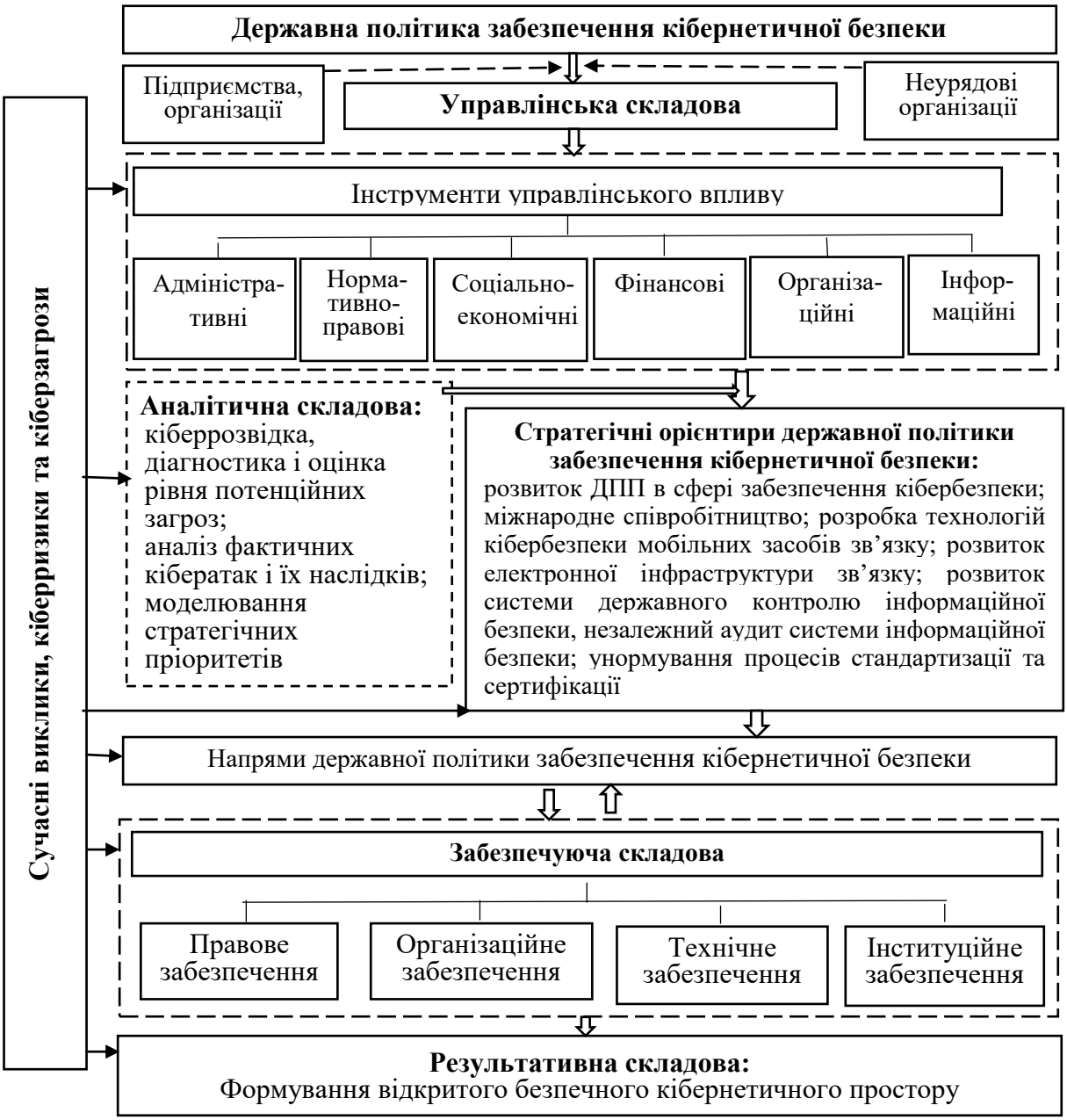

Рис. 1. Модель державного управління кібернетичною безпекою

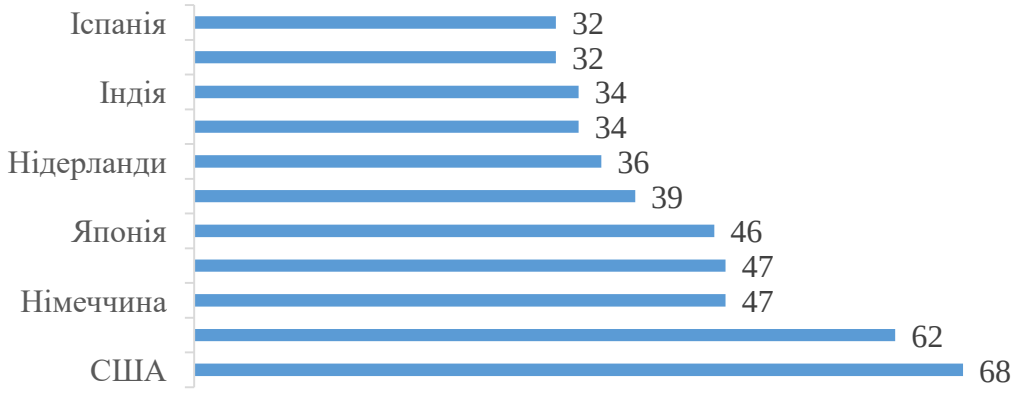

Рис. 2. Оцінка кібератак, як загрози для підприємств та організацій, %*

*Сформовано автором на основі KMPG International Growing pains 2018 Global Outlook

Акцентовано увагу на тому, що формування національної державної стратегії кібербезпеки є основою для вироблення ефективної державної політики.

В другому розділі **«Методичні засади формування державної політики забезпечення кібернетичної безпеки»** проаналізовано рівень кіберзлочинності та оцінено стан державного управління системою кібербезпеки України; удосконалено методичні засади аналітичного забезпечення управління кібернетичною безпекою; запропоновано методичні підходи до формування державної політики забезпечення кібернетичної безпеки.

Аналіз основних статистичних показників, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах та організаціях України, дозволив констатувати зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет та збільшення рівня використання інформаційно-комунікаційних технологій. Серед напрямів використання мережі Інтернет відзначено такі: надсилання чи отримання повідомлень електронною поштою; здійснення телефонних дзвінків за допомогою Інтернет/VoIP-зв'язку або відео-конференцій; отримання інформації про товари та послуги; користування миттєвим обміном повідомленнями та електронною дошкою оголошень; отримання інформації від органів державної влади; здійснення різноманітних операцій з органами державної влади (за винятком отримання інформації); здійснення банківських операцій; доступ до інших фінансових послуг.

Встановлено, що такі тенденції створили не лише передумови для розвитку підприємств та національної економіки в цілому, але й спричинили підвищення рівня злочинності в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (рис. 3). Темп приросту показника за 2014–2017 роки склав 480,8 %, а за 8 місяців 2018 року перевищив рівень 2016 року на 117,9 %.

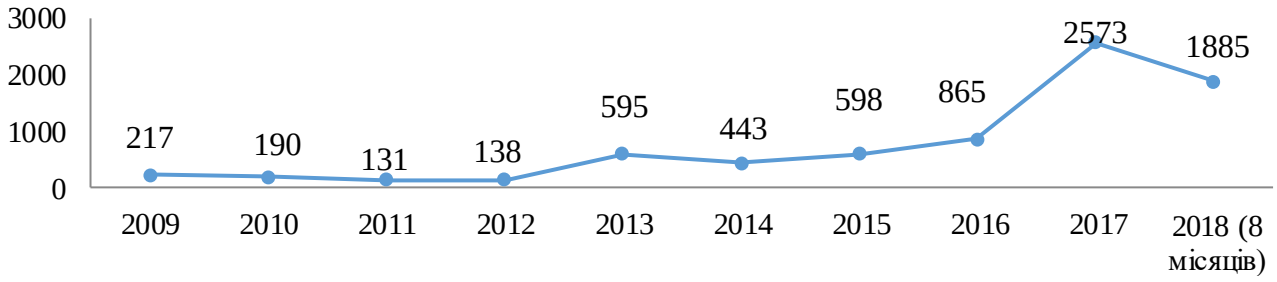

Рис. 3. Динаміка облікованої кіберзлочинності в Україні, кількість злочинів*
*Сформовано автором на основі даних офіційного сайту кіберполіції України

Аналіз структури кіберзлочинів в динаміці дозволив констатувати протягом 2013–2017 років найбільшу частку злочинів, які скоєно за статтею 361 Кримінального Кодексу України: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (від 50 до 77 %). Саме за рахунок цих злочинів спостерігається загальний приріст кіберзлочинів в динаміці.

Встановлено, що з метою виявлення кіберзлочинів вітчизняною кіберполіцією розроблено і впроваджено сучасні методики виявлення, фіксації і дослідження цифрових доказів. Акцентовано увагу на активізації міжнародної співпраці, результати якої у 2018 році полягають у наступному: викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях; підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів (представниками міжнародних компаній у сфері інформаційної безпеки та IT-компаній, поліцією Австралії, Сінгапуру, Катару та інших країн); налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами.

Встановлено, що зростання інформатизації країни та підвищення тиску кібервпливів актуалізує роль держави у забезпеченні кібернетичної безпеки. Акцентовано увагу на тому, що з точки зору розбудови ефективної системи кібербезпеки основоположною є нормативно-правова база для її запровадження, яка представлена міжнародними та національним нормативно-правовими актами.

В роботі запропоновано методичні засади формування аналітичного забезпечення управління кібернетичною безпекою, які передбачають інтегровану оцінку рівня кібернетичних загроз для регіонів країни та їх розподіл на кластери для обґрунтування напрямів державної політики кібербезпеки та диференціювання засобів впливу на рівні регіонів.

На основі методу експертних оцінок обрано та сформовано систему індикаторів для інтегрованої оцінки рівня кібернетичних загроз для регіонів країни, яку згорнуто до інтегрованого показника. Серед таких індикаторів: валовий регіональний продукт на одну особу; капітальні інвестиції в інформацію та телекомунікації; кількість абонентів мережі Інтернет (підприємства та фізичні особи); кількість підприємств, які займаються інноваційною діяльністю (придбання машин, обладнання, програмного забезпечення); кількість абонентів мобільного зв’язку; валова додана вартість інформації та телекомунікацій; зареєстровані кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж електрозв’язку.

На основі порівняльного аналізу парних коефіцієнтів кореляції для сукупності відібраних факторів та кількості зареєстрованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж електрозв’язку доведено значну лінійну залежність між ними.

Розрахунок інтегрованого показника оцінки рівня кібернетичних загроз для регіонів здійснено окремо для кожної області України як середнє значення стандартизованих показників-індикаторів. Визначено рейтингову позицію кожного регіону за інтегрованим показником оцінки рівня кібернетичних загроз, що є підґрунтям для формування стратегічних напрямів державної політики забезпечення кібернетичної безпеки з урахуванням територіальної специфіки.

На основі комплексу ієрархічних та неієрархічних методів, користуючись статистичним пакетом IBM SPSS Statistics, здійснено групування регіонів країни на чотири кластери (табл. 1).

Таблиця 1

Результати кластеризації регіонів України
за рівнем кібернетичних загроз (за даними 2017 р.)

№ кластера	Назва кластеру	Регіон	Значення інтегрованого показника оцінки рівня кібернетичних загроз
1	Регіони з дуже високим рівнем кібернетичних загроз	Луганська	7,022
		Чернігівська	6,234
2	Регіони з високим рівнем кібернетичних загроз	Хмельницька	5,216
		Житомирська	4,826
		Херсонська	4,751
		Чернівецька	4,327
3	Регіони з середнім рівнем кібернетичних загроз	Черкаська	4,013
		Рівненська	3,708
		м. Київ	3,702
		Волинська	3,197
		Сумська	3,076
		Кіровоградська	2,851
		Закарпатська	2,491
4	Регіони з рівнем кібернетичних загроз нижче середнього	Миколаївська	2,194
		Тернопільська	1,755
		Полтавська	1,658
		Івано-Франківська	1,499
		Одеська	1,344
		Донецька	1,303
		Запорізька	1,253
		Харківська	1,164
		Київська	1,158
		Дніпропетровська	1,146
		Львівська	1,086
		Вінницька	1,083

До першого кластеру – з дуже високим рівнем кібернетичних загроз – відносяться Луганська та Чернігівська області (з середнім значенням інтегрованого показника оцінки рівня кібернетичних загроз 7,022 та 6,234 відповідно). Другий кластер включає регіони з високим рівнем кібернетичних загроз: Чернівецьку, Херсонську, Житомирську, Хмельницьку області (граничні значення інтегрованого показника – від 4,327 до 5,216). Кластер 3 об'єднує регіони з середнім рівнем кібернетичних загроз і включає сім областей зі значеннями інтегрального показника від 2,491 до 4,013. Кластер 4 представляють дванадцять регіонів (значення інтегрованого показника від 1,083 до 2,194).

Подальший аналіз отриманих результатів є основою для коригування напрямів державної політики кібербезпеки, диференціації сучасних інструментів кіберрозвідки, визначення найбільш значимих факторів впливу на рівні регіонів та розробки дієвих методів кіберзахисту.

Запропоновано методичні підходи до формування державної політики забезпечення кібернетичної безпеки, які передбачають впровадження комплексного інструментарію, застосування якого сприятиме та стратегічному розвитку національної системи кібернетичної безпеки.

У третьому розділі **«Напрями формування державної політики забезпечення кібернетичної безпеки»** поглиблено концептуальні засади державної політики забезпечення кібернетичної безпеки; сформовано методичний підхід до обґрунтування напрямів управлінського впливу в сфері забезпечення кібернетичної безпеки; удосконалено механізм формування державної політики забезпечення кібернетичної безпеки.

Базуючись на результатах досліджень, в роботі теоретично обґрунтовано концепцію формування державної політики забезпечення національної кібернетичної безпеки, яка представляє собою систему теоретичного базису, методичних засад, інструментального забезпечення, побудовану за принципом ієрархії на основі комплексного підходу, що передбачає участь держави (в рамках державної політики в сфері кіберзахисту) та залучення інших суб'єктів, які працюють в цій сфері (підприємств, корпорацій, неурядових організацій) до процесів управління, реалізація якої спрямована на формування безпечного кібернетичного простору (рис. 4).

Зазначено, що управління процесами кіберзахисту має здійснюватися системно, у відповідності до прийнятої Стратегії кібербезпеки, в якій визначено особливості державної політики та основні стратегічні пріоритети. Проте, формування дієвої державної політики забезпечення кібернетичної безпеки, адекватної сучасним викликам та загрозам, потребує актуалізації цілей та пріоритетів, які мають скласти основу для науково обґрунтованого коригування існуючої стратегії кібербезпеки з урахуванням факторів впливу і спрямування її на формування безпечного кіберпростору.

Доведено доцільність застосування когнітивного підходу, який передбачає здійснення моделювання і формування відповідних сценаріїв, що дозволяє приймати рішення та спрямовувати діяльність в ситуаціях, для яких характерна невизначеність, слабка структурованість проблем та відсутність чіткої визначеної вхідної інформації, що має місце в процесі забезпечення кібернетичної безпеки.

Запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері забезпечення кібернетичної безпеки на основі когнітивного моделювання та сформовано основні його етапи.

Базуючись на результатах експертної оцінки сформовано систему факторів впливу на процеси кібербезпеки. Використовуючи когнітивні технології та систему підтримки прийняття рішень «КАНВА» як засіб їх реалізації, здійснено аналіз обраних факторів впливу, сили зв'язку між ними, що дозволило виявити певні тенденції змін, які здатні вплинути на рівень кіберзахисту.

Побудовано когнітивну модель факторів регуляторного впливу на рівень кібербезпеки та сформовано відповідні сценарії розвитку ситуації в сфері забезпечення кібернетичної безпеки.

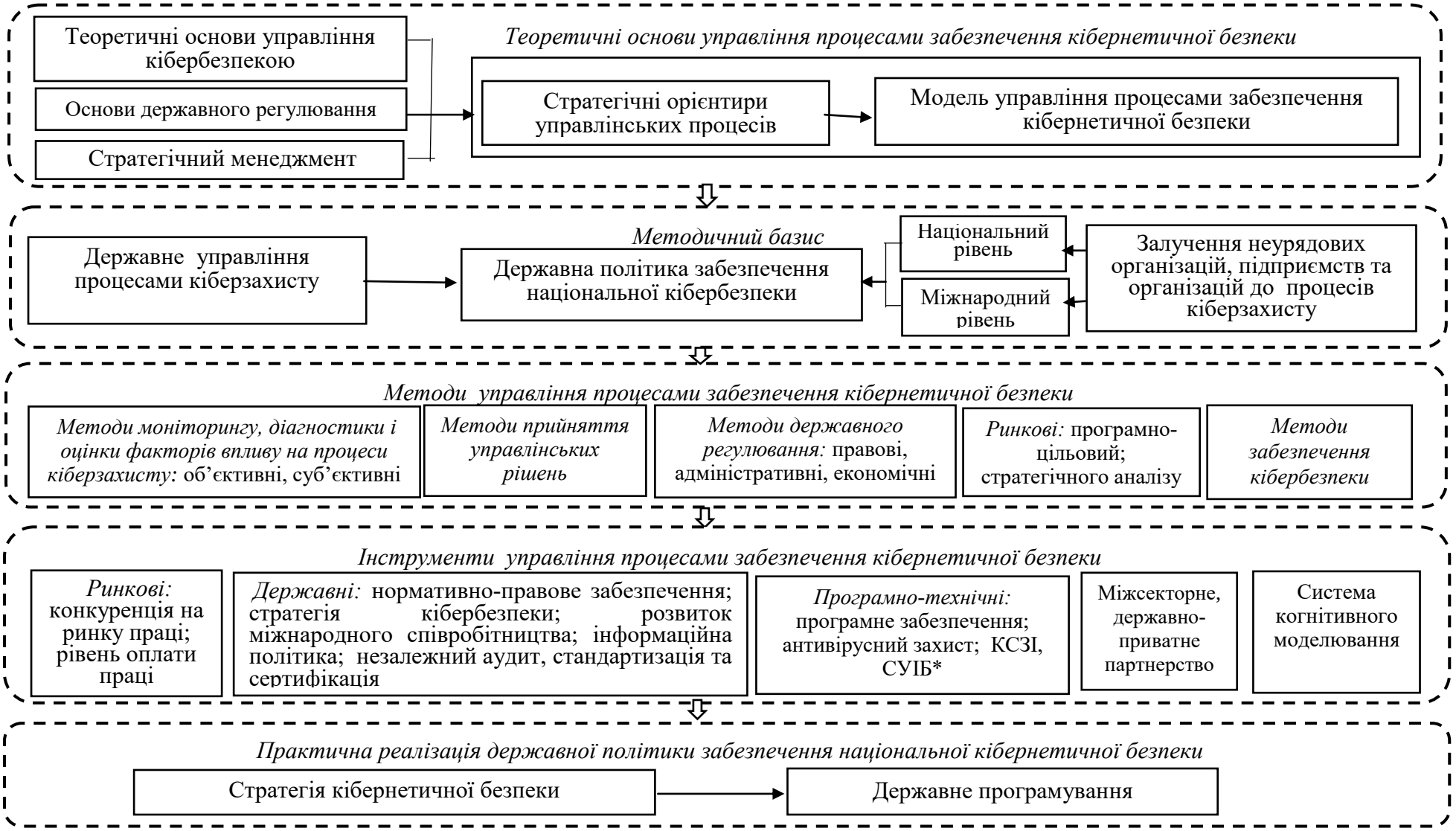

Рис. 4. Концепція формування державної політики забезпечення національної кібернетичної безпеки
* КСЗІ – комплексна система захисту інформації; СУІБ – система управління інформаційною безпекою

Аналіз результатів сценарного моделювання показав доцільність спрямування управлінського впливу за такими напрямами: розвиток державно-приватного партнерства в сфері забезпечення кібернетичної безпеки; запровадження незалежного аудиту систем інформаційної безпеки; унормування процесів стандартизації та сертифікації в сфері кіберзахисту; розвиток міжнародного співробітництва в сфері кібербезпеки та підтримка міжнародних ініціатив, які відповідають національним інтересам України, зростання інвестиційної активності в сфері інформаційно-комунікаційних технологій; розвиток інноваційної діяльності; підвищення рівня інформованості населення стосовно ситуації в сфері кібербезпеки.

Удосконалено механізм формування державної політики забезпечення кібернетичної безпеки, який являє собою сукупність організаційно-економічних методів і інструментів, які, ґрунтуючись на правових нормах, дозволяють державі, органам місцевого самоврядування і підприємствам забезпечити зменшення ризиків кібератак та кіберінцидентів (рис. 5).

З метою реалізації даного механізму та його спрямування на формування безпечного кіберпростору, обґрунтовано доцільність використання програмно-цільового підходу в сфері кіберзахисту та розроблено проект концепції Державної програми забезпечення кібернетичної безпеки.

ВИСНОВКИ

На підставі проведених наукових досліджень у дисертаційній роботі вирішено актуальне науково-практичне завдання у галузі державного управління щодо формування державної політики забезпечення кібернетичної безпеки, що створює фундаментальне підґрунтя для посилення національної безпеки. Результати дослідження дозволяють зробити такі висновки:

1. На основі узагальнення та систематизації теоретичних основ формування державної політики забезпечення кібернетичної безпеки встановлено, що сьогодні Україна зазнає значного впливу інцидентів та атак в кібернетичній сфері, що обумовлює необхідність своєчасного виявлення, запобігання й нейтралізації реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним, національним інтересам та актуалізує розробку державної політики в сфері кібербезпеки. Уточнено зміст поняття «державна політика в сфері кібербезпеки» як заснованої на чинних нормативно-правових актах, узгодженої за цілями системи державно-управлінських заходів з боку органів державної влади, спрямованої на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору, мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об’єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі. Обґрунтовано авторське бачення моделі державного управління кібернетичною безпекою, яка містить такі основні складові: управлінську, забезпечуючу, результативну, а також комплекс засобів і інструментів

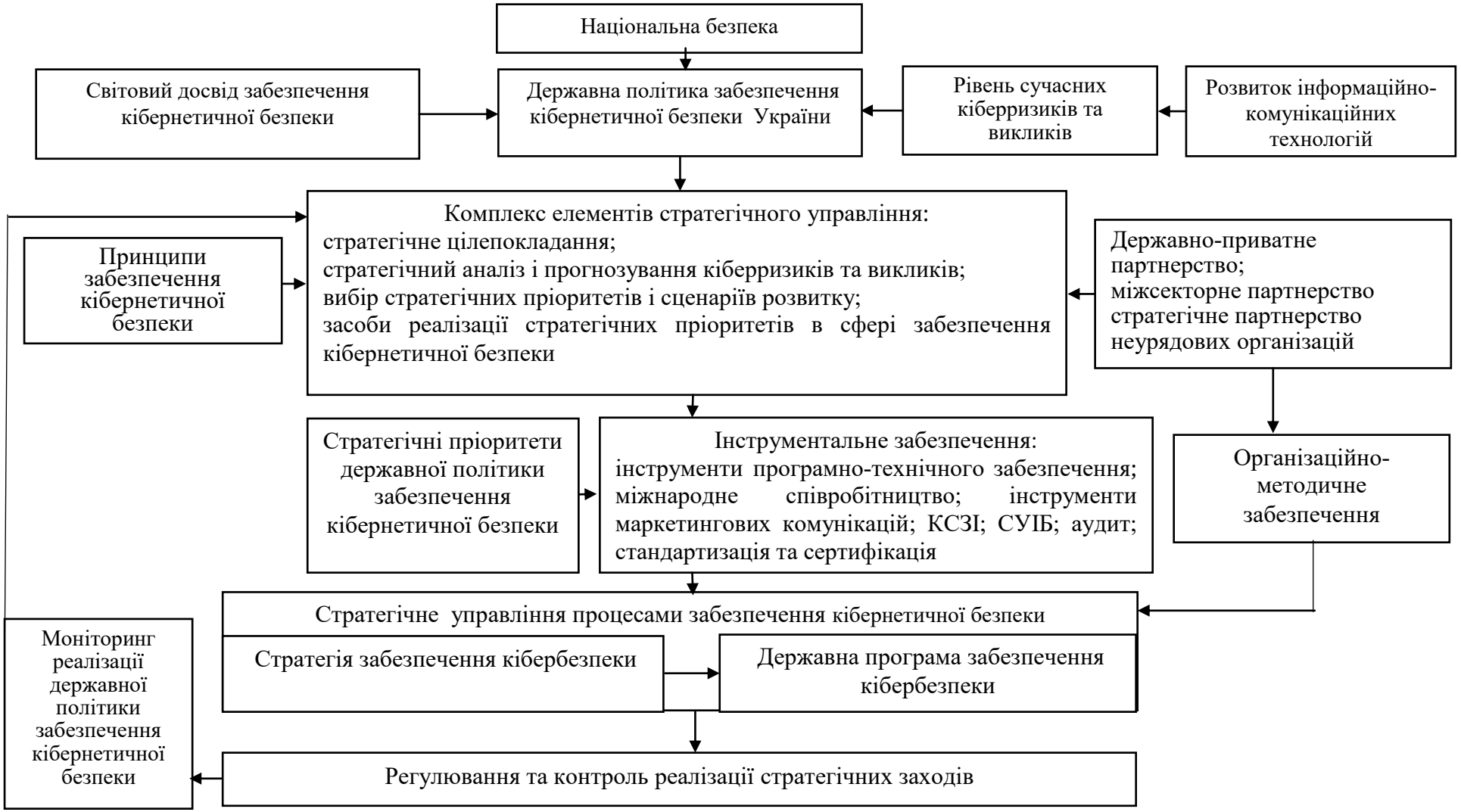

Рис. 5. Структура механізму формування державної політики забезпечення кібернетичної безпеки

управлінського впливу та є основою для формування державної політики забезпечення кібернетичної безпеки, спрямованої на створення безпечного кібернетичного простору.

2. Досліджено зарубіжний досвід державної політики забезпечення кібернетичної безпеки і виявлено можливості його адаптації до вітчизняних умов. Доведено необхідність застосування управлінського впливу на процеси забезпечення кіберзахисту та зазначено, що державна політика країн ґрунтується на гнучких, оперативних стратегіях кібернетичної безпеки. Транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію, що обумовлено не тільки необхідністю ефективної підготовки до кібератак, а й доцільністю своєчасної реакції на них, вироблення узгоджених механізмів запобігання. Акцентовано увагу на тому, що формування національної державної стратегії кібербезпеки є основою для вироблення ефективної державної політики.

3. Удосконалено методичні засади формування аналітичного забезпечення державного управління кібернетичною безпекою. На основі методу експертних оцінок обрано та сформовано систему індикаторів для оцінки рівня кібернетичних загроз регіонів країни, яку згорнуто до інтегрованого показника. На основі порівняльного аналізу парних коефіцієнтів кореляції відібраних факторів і кількості злочинів в сфері інформаційно-комунікаційних технологій доведено значну лінійну залежність між ними. Для кожної області України розраховано інтегрований показник оцінки рівня кібернетичних загроз та з використанням ранжування визначено її рейтингову позицію. На основі поєднання ієрархічних та неієрархічних методів кластеризації, з використанням статистичного пакету IBM SPSS Statistics здійснено групування регіонів країни на чотири кластери, що є базою для коригування пріоритетів державної політики кібербезпеки, обґрунтованого підходу при виборі засобів та інструментів впливу на регіональному рівні.

4. Розвинуто методичні підходи до формування державної політики забезпечення кібернетичної безпеки, які передбачають запровадження моделі державно-приватної взаємодії, втілення сучасної системи стандартизації та сертифікації і методики незалежного аудиту, використання форм міжнародного співробітництва за векторами Україна – ЄС і НАТО з врахуванням національних стратегічних інтересів і підходів країн-партнерів в сфері забезпечення кібернетичної безпеки, з врахуванням її специфіки з метою формування безпечного кіберпростору.

5. Поглиблено й аргументовано концепцію державної політики забезпечення національної кібернетичної безпеки, яка представляє собою систему теоретичного базису, методичних засад, інструментального забезпечення, побудовану за принципом ієрархії на основі комплексного підходу, що передбачає участь держави (в рамках державної політики в сфері кіберзахисту) та залучення інших суб’єктів, які працюють в цій сфері (підприємств, корпорацій, неурядових організацій) до процесів управління. Зазначено, що реалізація цієї концепції спрямована на формування безпечного кібернетичного простору.

6. Запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері кібернетичної безпеки на основі методів

моделювання. На основі експертної оцінки сформовано систему факторів впливу на процеси кібербезпеки. Використовуючи когнітивні технології та як засіб їх реалізації – систему підтримки прийняття рішень «КАНВА», здійснено аналіз обраних факторів впливу, сили зв'язку між ними, що дозволило виявити певні тенденції змін, які здатні вплинути на рівень кіберзахисту. Побудовано когнітивну модель факторів регуляторного впливу на рівень кібербезпеки та сформовано відповідні сценарії розвитку ситуації в сфері забезпечення кібернетичної безпеки, що є базою для науково обґрунтованого коригування існуючої стратегії кібербезпеки з урахуванням факторів впливу та удосконалення механізму формування державної політики забезпечення кібернетичної безпеки;

7. Удосконалено механізм формування державної політики забезпечення кібернетичної безпеки, який являє собою сукупність організаційно-економічних методів і інструментів, які, ґрунтуючись на правових нормах, дозволяють державі, органам місцевого самоврядування і підприємствам забезпечити зменшення ризиків кібератак та кіберінцидентів.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації:

Статті у наукових фахових виданнях та виданнях, внесених до наукометричних баз даних:

1. Балуєва О. В., **Островий О. В.** Європейський досвід забезпечення кібернетичної безпеки. *Менеджер. Вісник Донецького державного університету управління (Серія «Державне управління»*). 2015. №1(69). С. 30–36. (*0,4 др. арк.*).

Особистий внесок: актуалізовано необхідність прийняття національної стратегії забезпечення кібернетичної безпеки з урахуванням положень світового досвіду.

2. Островий О. В. Деякі підходи до удосконалення державної політики забезпечення кібернетичної безпеки України. *Збірник наукових праць ДонДУУ «Сучасні проблеми державного управління в умовах системних змін». Серія «Державне управління».* 2016. Т. XVII, вип. 298. С. 77–85 (*0,5 др. арк*.).

3. Островий О. В. Пріоритетні напрями розвитку кібербезпеки в Україні. *Збірник наукових праць ДонДУУ «Сучасні проблеми державного управління в умовах системних змін». (Серія «Державне управління»).* 2017. Т. XVIII, вип. 302. С. 251–257 (*0,4 др. арк*.).

4. Островий О. В. Дослідження проблематики забезпечення кібернетичної безпеки в роботах українських науковців: джерельний аналіз. *Менеджер. Вісник Донецького державного університету управління (Серія «Державне управління»*). 2018. №1(78). С. 157–164. (*0,56 др. арк.*).

5. Островий О. В. Інструменти державної політики забезпечення кібернетичної безпеки. *Електронне наукове фахове видання «Публічне адміністрування та національна безпека».* 2019. С. 13–21. (*0,6 др. арк.*)

6. Balueva O., **Ostrovoj A.** Development of Public-Private Partnership in the Field of Cyber Defense: European Experience. *International Journal of New Economics, Public Administration and Law* (IJONEPAAL). 2019. С. 8–16. *(0,64 др. арк.).*

Особистий внесок: доведено доцільність формування державної політики кібернетичної безпеки з використанням інструментів державно-приватного партнерства.

7. Ostrovoy A. Main directions for the development of the state policy in the field of cyber security. *Science and society : Fadette editions. 2019.* С. 75–78 (*0,3 др. арк.).*

8. Ostrovoy A. Analysis of the conditions for the state policy formation to ensure kibernetic security in Ukraine. *Public management*. 2019. № 2(17) – March, 2019. P. 296–306 *(0,6 др. арк.).*

9. Островий О. В. Формування механізму державної політики забезпечення кібернетичної безпеки України. *Збірник наукових праць ДонДУУ «Сучасні проблеми державного управління в умовах системних змін» (Серія «Державне управління»).* 2018. Т. XX, вип. 310. С. 136–145 *(0,4 др. арк.).*

Матеріали наукових конференцій:

10. Островий О. В. Проблематика забезпечення кібернетичної безпеки України. *Напрями вдосконалення механізмів державного управління в умовах сучасних реформаційних процесів* : матеріали Всеукраїнської науково-практичної конференції, 23–24 грудня 2016 р. Запоріжжя : Класичний приватний університет, 2016. С. 58–61 (*0,14 др. арк.)*.

11. Островий О. В. Державно-приватне партнерство як інструмент забезпечення кібернетичної безпеки. *Організаційно-правові аспекти публічного управління в Україні* : матеріали VI Всеукраїнської науково-практичної конференції, 23 квітня 2019 р. Полтава : ПолтНТУ, 2019. С. 235–237 (*0,1 др. арк*.).

12. Островий О. В. Кібернетична безпека: державний вимір. *Публічне управління та адміністрування: конкурентні виклики сучасності* : матеріали II Всеукраїнської науково-практичної інтернет-конференції, 01 квітня 2019 р. Львів : ТзОВ «Галицька видавнича спілка», 2019. 1 електрон. Опт. Диск (CD-ROM). С. 64–66 (*0,14 др. арк.*).

АНОТАЦІЯ

Островий О. В. Формування державної політики забезпечення кібернетичної безпеки в Україні. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Донецький державний університет управління, Міністерство освіти і науки України, Маріуполь, 2019.

Дисертацію присвячено поглибленню теоретичних засад та розвитку науково-методичних і практичних рекомендацій щодо формування державної політики забезпечення кібернетичної безпеки. Узагальнено та систематизовано теоретичні

основи формування державної політики забезпечення кібернетичної безпеки. Досліджено зарубіжний досвід державної політики забезпечення кібернетичної безпеки і виявлено можливості його адаптації до вітчизняних умов. Удосконалено методичні засади аналітичного забезпечення державного управління кібернетичною безпекою. Розвинуто методичні підходи до формування державної політики забезпечення кібернетичної безпеки. Поглиблено й аргументовано концепцію формування державної політики забезпечення національної кібернетичної безпеки. Запропоновано методичний підхід до обґрунтування напрямів управлінського впливу в сфері кібернетичної безпеки на основі методів моделювання Удосконалено механізм формування державної політики забезпечення кібернетичної безпеки.

Ключові слова: кібербезпека, кіберзахист, державна політика, державне управління, концепція, механізм державної політики.

SUMMARY

Ostrovyi O. Formation of the state policy of providing cyber security in Ukraine. – Manuscript.

Thesis for obtaining the Degree of Candidate of Sciences in Public Administration by specialty 25.00.02 – Mechanisms of Public Administration. – Donetsk State University of Management, Ministry of Education and Science of Ukraine, Mariupol, 2019.

The dissertation is devoted to extending the theoretical bases and development of scientific and methodical and practical recommendations on formation of the state policy of providing cyber security.

The theoretical bases of forming the state policy of providing cyber security have been generalized and systematized. The content of the concept of "state cyber security policy" has been clarified. The author's vision of the state management model of cyber security has been substantiated, which contains the following main components: managerial, provisional, effective and complex of means and tools of managerial influence and is the basis for forming the state policy of providing cyber security aimed at creation of safe cyber space.

The foreign experience of the state policy of providing cyber security has been researched and the possibilities of its adaptation to domestic conditions have been identified. The necessity of applying managerial influence to the processes of providing cyber defense has been proved and states that the state policy of the countries is based on flexible, operational cyber security strategies. The trans-boundary nature of the threats forces countries to engage in close international cooperation, which is conditioned not only by the need for effective cyber attack preparation but also by the expediency of timely response and the development of concerted prevention mechanisms. Attention has been drawn to the fact that the formation of a national state cyber security strategy is the basis for the effective state policy development.

Methodical principles of forming analytical support for cyber security management have been improved, which ensure an assessment of the cyber threats level within the regions of the country and their distribution into clusters based on the use of economic and

mathematical methods, which allows to substantiate the directions of the state cyber security policy and differentiate the means of influence at the regional level.

Methodical approaches to the state cyber security policy formation through regulated development of the public-private partnership concept, introduction of independent audit, as well as the related standardization and certification processes as components of the national cyber security system of Ukraine and instruments for the effective state policy formation in the cyber defence sphere using the potential of international cooperation and non-governmental organizations in management processes aimed at developing the Information Society, early detection, neutralization of real and potential threats arising in cyberspace and prevention.

The concept of forming a national policy of ensuring national cyber security is extended and substantiated, which is a system of theoretical basis, methodological foundations, instrumental support, built on the principle of hierarchy on the basis of a comprehensive approach, involving state participation (within the state policy in the field of cyber defence) and involvement of other entities operating in this field at national and international levels (enterprises, corporations, non-governmental organizations) to the management processes which implementation creates the content of the state policy mechanism formation of providing cyber security and aims at the safe cyber space formation. A methodological approach to substantiation of directions of managerial influence in the field of cyber security has been proposed, which is based on the use of the method of cognitive modelling and provides analysis of selected factors of managerial influence, formation of appropriate scenarios. This revealed certain trends that could affect the level of cyber security and is the basis for a scientifically sound adjustment of the existing cyber security strategy, taking into account the factors of influence and improvement of the state policy mechanism for ensuring cyber security.

The mechanism of the state policy formation of providing cyber security has been improved, which is a set of organizational and economic methods and tools that, based on legal norms, allow the state, local governments and enterprises to reduce the risks of cyber attacks and cyber incidents; their implementation will allow to secure the cyber security formation.

Keywords: cyber security, cyber protection, public policy, public administration, concept, mechanism of public policy.

ОСТРОВИЙ Олексій Володимирович

Формування державної політики забезпечення кібернетичної безпеки в Україні

Автореферат дисертації на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління

Підписано до друку 05.09.2019. Формат 60×84/16.
Ум. друк. арк. 1,17. Авт. арк. 0,9.
Наклад 100 пр.

Друкарня С. Г. Щербенка «Літерія»
вул. Рокоссовського, 5/3, м. Кривий Ріг, 50027
097-192-20-77
Свідоцтво суб'єкта видавничої справи ДК № 4561 від 13.06.2013 р.