ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ
Кафедра: публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на здобуття ступеня освітнього ступеня магістра

на тему:

«ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ»

Виконала: студентка магістратури
за спеціальністю 281 Публічне
управління та адміністрування
Глупак А.В.
(прізвище та ініціали)

Керівник: к.е.н., доцент кафедри
Омельчук Л.В.
(прізвище та ініціали)

Рецензент: _____
(прізвище та ініціали)

Хмельницький – 2020 рік

Анотація

Глупак А.В. Державна політика забезпечення кібернетичної безпеки в Україні - Кваліфікаційна наукова праця на правах рукопису. Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 281 Публічне управління та адміністрування. – Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2020. – 90 с.

Визначено сутність кібербезпеки, уточнено зміст поняття «державна політика в сфері кібербезпеки». Проаналізовано основні статистичні показники, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах та організаціях України, досліджено динаміку показників кіберзлочинності в Україні, їх структуру за обєктом посягання.

Проведено оцінку державної подітики забезпечення кібернетичної безпеки в Україні. Для кожної області України розраховано інтегральний показник оцінки рівня кібернетичних загроз та з використанням ранжування визначено її рейтингову позицію.

Поглиблено й аргументовано концепцію державної політики забезпечення кібернетичної безпеки. 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.

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

Annotation

Glupak A.V. State policy of cyber security in Ukraine - Qualified scientific work on the rights of the manuscript. Master's thesis on obtaining a master's degree in the specialty 281 Public administration and administration. - Khmelnytsky University of Management and Law named after Leonid Yuzkov, Khmelnytsky, 2020. - 90 p.

The essence of cybersecurity is defined, the meaning of the concept of "state policy in the field of cybersecurity" is specified. The main statistical indicators that characterize the level of use of information and communication technologies at enterprises and organizations of Ukraine are analyzed, the dynamics of cybercrime indicators in Ukraine, their structure according to the object of encroachment are investigated.

An assessment of the state policy on cyber security in Ukraine has been made. For each region of Ukraine, an integrated indicator for assessing the level of cyber threats was calculated and its ranking position was determined using ranking.

The concept of the state policy of cyber security is deepened and argued. The mechanism of formation of the state policy of cyber security, 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 risk of cyber attacks and cyber incidents, has been improved.

Keywords: cybersecurity; cyber protection; public policy; governance; concept; mechanism of public policy.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНИХ І УМОВНИХ ПОЗНАЧЕНЬ

ВВП – валовий внутрішній продукт

ДПП – державно-приватне партнерство

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України

ЄС – Європейський Союз

ІКТ – інформаційно-комунікаційні технології

КСЗІ – комплексна система захисту інформації

КМУ – Кабінет Міністрів України

МВС – Міністерство внутрішніх справ

НУО – неурядові організації

СБУ – служба безпеки України

СУІБ – система управління інформаційною безпекою

ВСТУП

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. 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-практичної 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 магістерської роботи, її мету, задачі і структуру, теоретичну та практичну значущість.

Мета і задачі дослідження. Метою магістерської роботи є поглиблення теоретичних засад та розробка практичних рекомендацій щодо формування державної політики забезпечення кібернетичної безпеки. Для досягнення мети було поставлено і вирішено такі **завдання:**

- визначити сутність кібербезпеки в системі забезпечення національної безпеки України

- узагальнити основні аспекти державної політики забезпечення кібербезпеки України;

- провести аналіз рівня кіберзлочинності та оцінку стану державного управління системою кібербезпеки України;

- дослідити аналітичне забезпечення управління кібернетичною безпекою в Україні;

- сформувати концептуальні засади удосконалення державної політики забезпечення кібернетичної безпеки;

- обґрунтувати напрями управлінського впливу в сфері кібернетичної безпеки на основі методів моделювання.

Об'єктом дослідження є процес державного управління кібернетичною безпекою.

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

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

Методологічною базою 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, узагальнення, комплексний підхід* – для вивчення теоретичних основ формування державної політики забезпечення кібернетичної безпеки; *метод конкретизації, статистичний, графічний* – при аналізі рівня розвитку інформаційно-комунікаційних технологій, кіберзагроз та формуванні аналітичного забезпечення державного управління кібернетичною безпекою; *концептуалізація, абстрактно-логічний метод, моделювання* – при формуванні концепції державної політики забезпечення національної кібернетичної безпеки, обґрунтуванні напрямів управлінського впливу в сфері кібернетичної безпеки.

Інформаційною базою є матеріали Міністерства внутрішніх справ, Департаменту кіберполіції Національної поліції України, Державної служби статистики України, Євростату, міжнародних компаній у сфері

інформаційної безпеки, роботи вітчизняних та зарубіжних вчених, а також результати власних досліджень автора.

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

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

1.1 Сутність кібербезпеки в системі забезпечення національної безпеки України

Процеси глобалізації, які характерні для сучасного суспільства, зростання кількості загроз і викликів, актуалізовали 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.

Зазначимо, що сьогодні в колах науковців та практиків приділяться значна увага тлумаченню терміна «національна безпека», що передбачає використання різних підходів для визначення його сутності.

Так, в Законі «Про національну безпеку України» це поняття трактується як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [125].

В. А. Ліпкан визначає національну безпека як сукупність офіційно прийнятих поглядів на цілі і державну стратегію в області забезпечення безпеки особистості, суспільства і держави від зовнішніх і внутрішніх загроз політичного, економічного, соціального, військового, техногенного,

екологічного, інформаційного та іншого характеру з урахуванням наявних ресурсів і можливостей [81, с. 5].

Я. Ю. Кондратьєв акцентує увагу на «здатності нації задовольняти потреби, необхідні для її самозбереження, самовідтворення і самовдосконалення з мінімальним ризиком збитку для базових цінностей її нинішнього стану» [73, с. 1].

Аналіз теоретичних напрацювань та практичного досвіду функціонування системи забезпечення національної безпеки країни дозволив виокремити основні її елементи, які, формують певні підсистеми (рис.1.1).

Рисунок 1.1 - Структура системи забезпечення національної безпеки України

Примітка. Складено автором за даними [68, с. 43; 74; 81]

Зазначимо, що кожна з підсистем забезпечення національної безпеки спрямована на виконання поставлених завдань, що здійснюються на основі реалізації відповідного комплексу заходів відповідно до компетенцій та функцій, які здатен виконувати кожен із суб'єктів, із врахуванням актуальних викликів і загроз, використовуючи сучасні вітчизняні напрацювання у цій сфері та передовий закордонний досвід задля розвитку національних інтересів держави, добробуту її населення і ефективного функціонування системи національної безпеки в цілому.

Слід погодитись з автором дослідження [81], який вказує на той факт, що у більшості випадків національну безпеку ототожнюють з обороною держави, оскільки у сучасному світі військова могутність є одним з чинників її сили. Однак, сьогодні набувають значущості економічні, політичні та інші не силові елементи забезпечення національної безпеки, які виділено в структурі системи.

Слід вказати на той факт, що сьогодні не існує єдиного трактування поняття «кібербезпека», що спричиняє певні дискусії з цієї теми. Так, науковці [87, с. 44], використовуючи соціально-економічний підхід, зазначають, що кібербезпека являє собою «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційнотелекомунікаційних систем». Однак, акцент на функціонуванні інформаційнотелекомунікаційних систем і «сталості розвитку» у даному визначенні та відсутність конкретизації такого впливу, робить це трактування досить широким, зміщуючи його в бік поняття «інформаційна безпека».

Трактування у надто широкому сенсі з використанням соціального підходу дотримується у своїх дослідженнях В.Н. Фурашев, який надає поняття кібербезпеці як «стану здібності людини, суспільства і держави щодо

запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [159, с.167].

На розгляді кібербезпеки як «стану захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж» наголошує О.А. Баранов, визначаючи серед основних факторів небезпеки «негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [7].

На переконання деяких науковців [58], запропоноване О.А. Барановим визначення поняття "кібербезпека" багато в чому є надмірно "конкретизованим", що потенційно може створити перешкоди пов'язані з його використанням у практичній діяльності держави. Крім того, вважаємо доцільним звернути увагу на розгляд автором поняття «кібербезпека» через призму технічного підходу.

Такий же підход використовує В.М. Панченко [110], акцентуючись на безпеці об'єктів, пов'язаних з комп'ютерними технологіями (цифровими мережами) від небажаного або несанкціонованого доступу.

Згідно з затвердженим на законодавчому рівні трактуванням, кібербезпека являє собою «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» [126].

Слід акцентувати увагу на дискусійності цього визначення, на що звертається увага як науковців, так і практиків. Характеризуючи підходи до трактування терміну кібернетична безпека», вважаємо доцільним розглянути основні особливості дефініцій, наведені у ряді національних стратегій деяких країн світу, присвячених даному питанню (табл. 1.1).

Таблиця 1.1. Трактування терміну кібернетична безпека у відповідних національних стратегіях країн світу

Країна	Визначення поняття «кібербезпека»
1	2
Франція	бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними

Продовження табл. 1.1

1	2
Німеччина	деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків
Канада	захист кибersистем від шкідливого неправильного використання та від інших деструктивних атак
Туреччина	захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам
Нідерланди	сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз
Австралія	забезпечення доступності, цілісності та конфіденційності ІКТ Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації [

Примітка. Сформовано атором за даними [39, С.55; 91; 174; 177; 178; 179; 186; 194]

Звертаючи увагу на особливості та різні підходи до трактування поняття «кібербезпека» в ряді національних стратегій слід зазначити, що кожна держава самостійно встановлює основні елементи, об'єкти і суб'єкти кібернетичної безпеки, перелік її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів. спільним для них є забезпечення, формування сукупності заходів (зусиль), спрямованих на запобігання, протидію, мінімізацію ризиків у кіберпросторі.

Узагальнення підходів щодо визначення поняття «кібербезпека» дозволило сформувати її структуру та виокремити певні складові (рис. 1.2), на основні визначення яких вважаємо доцільним звернути увагу.

Зазначимо, що кібернетичні впливи створюють відповідні загрози для об’єктів кібербезпеки, що потребує формування державної політики, яка базується на дієвих методах та інструментах.

На законодавчому рівні визначено, шо кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів [126].

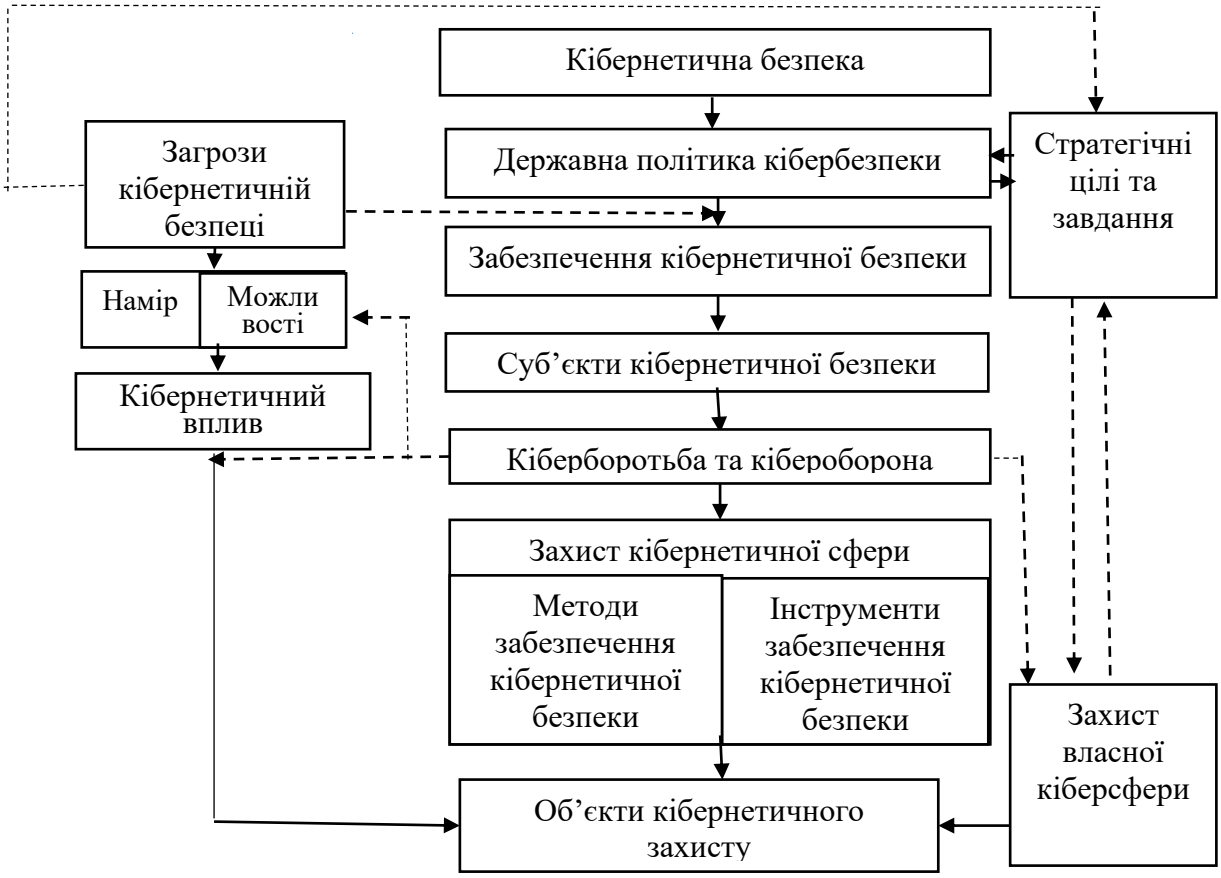

Рисунок 1.3 - Структурна модель кібербезпеки

Примітка. Розроблено автором

Науковці, визначаюючи термін «кіберзагроза», в свою чергу, справедливо роблять акценти не лише на безпеці держави, але звертають увагу на неї, як «протиправні, карані дії суб’єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому» [50; 52]; загрозу «застосування

деструктивних інформаційнопсихологічних впливів на свідомість та психічний стан населення» [141, с.115].

Аналогічні наголоси на «наявних та потенційно можливих явищах і чинниках, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в кібернетичній сфері» було розставлено і у відповідних Проектах Стратегії забезпечення кібернетичної безпеки України [117; 118].

Слід звернути увагу на дослідження І. Діордіци [50, с. 208], який зауважує, що «сутність кіберзагроз становлять їх суб'єкти, а саме суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація».

Тому, спираючись на законодавчу базу [130] необхідно зазначити, що кібернетичні загрози можуть виходити від: окремих злочинців, які мають відповідну підготовку у сфері інформаційних технологій; груп хакерів (в тому числі міжнародних); державних органів інших країн; фінансово-промислових груп і корпорацій; терористичних угруповаанъ та інших. Запровадження у роботу державних структур, підприємств та організацій, життя українського суспільства сучасних інформаційно-телекомунікаційних технологій, призводить до трансформації злочинів, появи їх нових видів.

Як свідчать результати досліджень, на практиці часто виникають суперечки та дискусії стосовно визначення об'єктів впливу для кібер та інформаційної безпеки в частині технічних систем. Тому, в контексті вищезазначеного вважаємо доцільним визначитись з їх розмежуванням (рис. 1.5).

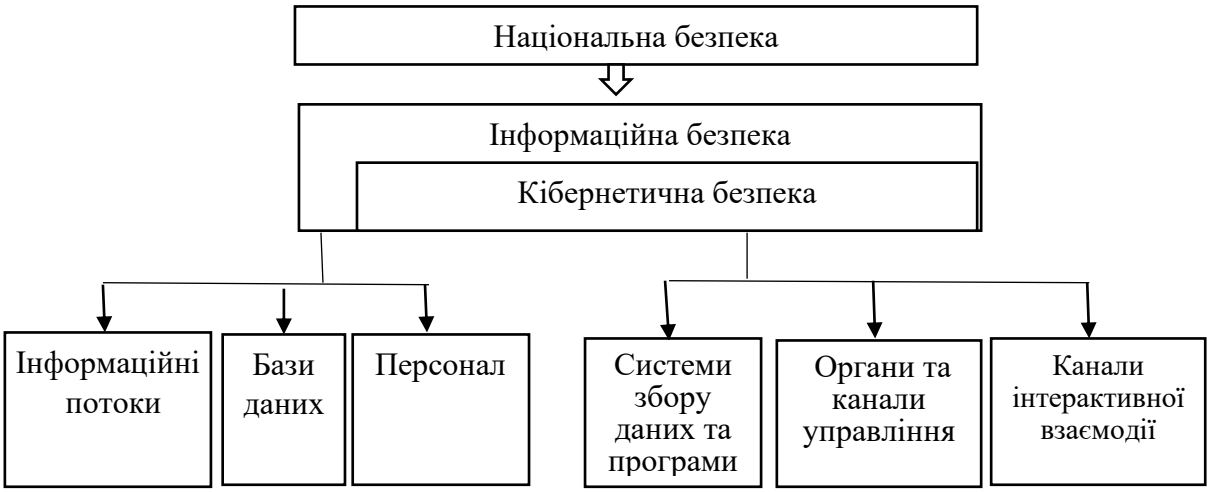

Рисунок 1.4 - Об’єкти впливу інформаційної та кібербезпеки (технічні системи)

Примітка. Сформовано автором за даними [14, с.87; 17, с.47; 38]

Слід вказати, що формування адекватного кіберзахисту являє собою «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [126].

Таким чином, задля збереження кіберпростору відкритим та безпечним представляється доцільним своєчасне виявлення, запобігання й нейтралізація реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним, національним інтересам, що потребує комплексного підходу та участі всіх суб’єктів. Тому існує потреба у розробці державної політики в сфері кібербезпеки, формуванні та реалізації її основних напрямів.

1.2. Основні аспекти державної політики забезпечення кібербезпеки України

Визначаючи основи державної політики забезпечення кібербезпеки, вважаємо необхідним розглянути відповідну дефініцію. Аналіз визначення

поняття «державна політика» дозволив дійти висновку стосовно різноманітності підходів до його трактування різними науковцями.

Зазначимо, що у широкому сенсі вітчизняні дослідники пропонують розглядати державну політику як: «основні принципи, норми та діяльність зі здійснення державної влади» [111, с.24]; «діяльність, результати якої набувають статусу офіційних [167, с. 8]; «сукупність цілей і завдань, що практично реалізується державою» [93, с. 157]; «стратегічну лінію поведінки держави в тих чи інших сферах суспільного життя» [43, с.30]; «сукупність ціннісних цілей, державно-управлінських заходів, рішень і дій, порядок реалізації державно-політичних рішень» [41, с.8]; «набір цінностей, цілей та знарядь, пов'язаних із визначенням суспільних проблем» [40, с. 14].

Аналогічний широкий підхід до трактування терміну «державна політика» використовують і деякі закордонні науковці, визначаючи її як: «складні взаємозв'язки форм влади, типи проблем та організації держав в особливих підсистемах суспільства [29, с. 21]; «заплановану програму цілей, цінностей і дій» [170, с. 80].

Ряд науковців трактує поняття «державна політика» у вузькому сенсі, з більшою конкретизацією цілей, цпроцесів та результатів, визначаючи дефіеніцію, як:

– «пропонований курс діяльності уряду для задоволення потреб чи використання можливостей, сформульований із зазначенням очікуваних результатів та їх впливу на наявний стан справ і конкретне розв'язання проблем» [133, с. 74];

– «дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язання проблем у певній сфері суспільної діяльності» [60, с. 144-145];

– «сукупність організаційних, правових та економічних заходів, які здійснюються державними органами в усіх сферах суспільного життя та реалізуються у напрямах залежно від стратегічних завдань, поставлених перед державою» [9, с. 14].

– «безперервний циклічний процес, що складається із сукупності послідовних дій, взаємодії елементів інститутів з певними функціями, засобів, які спрямовані на досягнення певного наслідку» [79, с. 18];

– «ухвалене на конституційних засадах із залученням громадськості стратегічне рішення з чітким визначенням результатів, яке є засобом забезпечення суспільних потреб у тій чи іншій сфері і реалізується органами державного управління» [109].

Слід погодитись з О.В. Делія, який відзначає складність середовища формування державної політики, його «цілісність, яка поєднує позасоціальну та соцієтальну компоненти та не позбавлена внутрішніх суперечностей», розглядає державну політику з позиції синергетичного підходу, тобто інтерпретує її «як відкриту динамічну систему, основою функціонування якої є постійний енергетичний, ресурсний та інформаційний обмін із зовнішнім середовищем» [40, с.15].

Дослідження різних підходів до трактування поняття «державна політика» дозволило констатувати наряду з їх різноманітністю, визначення її спрямованості на вирішення конкретної суспільної проблеми у певній сфері.

Аналіз напрацювань науковців [145, с. 74; 146; 150, с.84; 160, с. 47; 161, с.31] стосовно трактування поняття «державна політика» дозволило уточнити зміст дефініції «державна політика в сфері кібербезпеки».

Так, вважаємо, що під державною політикою в сфері кібербезпеки слід розуміти засновану на чинних нормативно-правових актах, узгоджену за цілями систему державно-управлінських заходів з боку органів державної влади, спрямовану 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.

Вважаємо доцільним, визначаючи основи державної політики забезпечення кібернетичної безпеки, звернути увагу на структуру відносин в цій сфері і визначити її суб'єкт і об'єкт.

На державному рівні визначено, що суб’єкти забезпечення кібербезпеки у межах своєї компетенції: здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки та інші заходи [126].

Визначаючи суб'єктів державної політики забезпечення кібернетичної безпеки, слід погодитись з думкою І. Діордіци, який звертає увагу на необхідність їх розподілу на дві групи: загальні та спеціалізовані (уповноважені здійснювати боротьбу з кіберзлочинністю та захист об'єктів національної критичної інфраструктури) [49, с.16; 51, с.39].

Вважаємо, що такий підхід є раціональним з точки зору виокремлення функцій та повноважень при формуванні та реалізації державної політики. Основні суб'єкти забезпечення кібернетичної безпеки наведено на рис. 1.8.

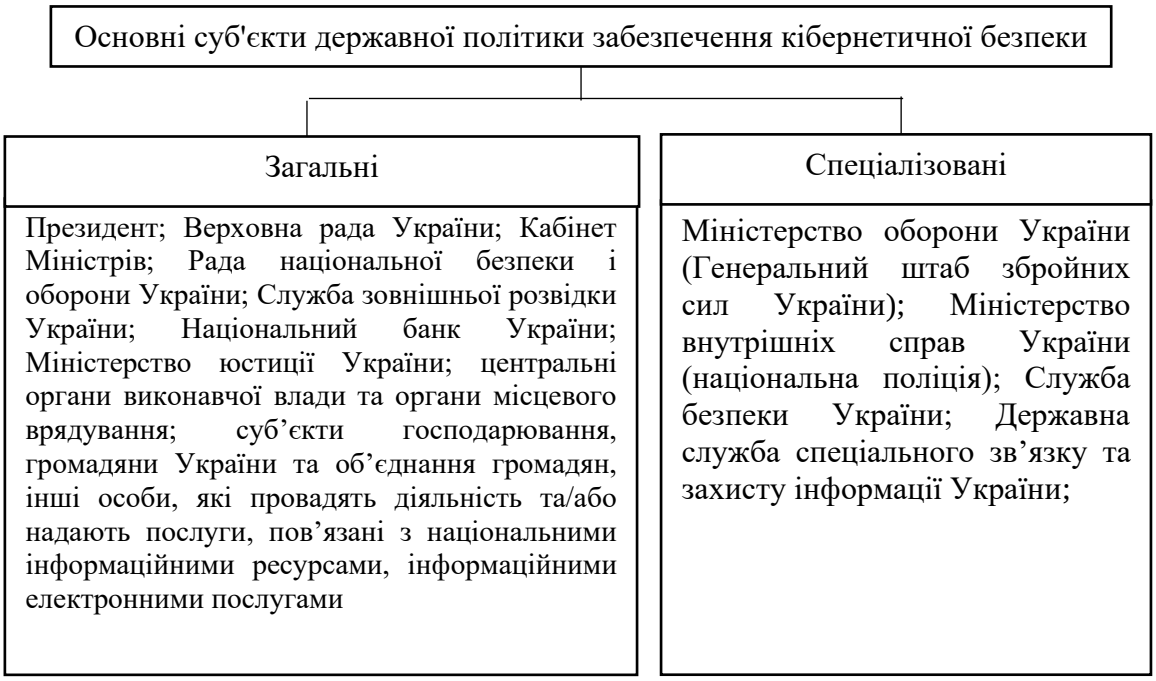

Рисунок 1.5 - Основні суб'єкти державної політики забезпечення кібернетичної безпеки

Складено автором на основі [51, с.40; 129] та удосконалено

Розглянемо більш детально специфіку діяльності визначених спеціалізованих суб'єктів, які складають основу національної системи кібербезпеки з точки зору організаційного виміру.

На законодавчому рівні на Міністерство оборони та Генштаб Збройних сил України покладена зобов'язаність забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі [126].

Серед підрозділів, які відповідальні за забезпечення кібернетичної безпеки країни, слід виокремити війська радіоелектронної боротьби і фахівців Головного управління розвідки. До задачі перших відноситься захист систем управління військами та зброєю від навмисних радіоелектронних перешкод противника, а також порушення роботи інформаційних систем управління противника [30].

Фахівці Головного управління розвідки беруть участь у здійсненні спеціальних заходів щодо забезпечення національних інтересів в

інформаційній сфері (розвідувальні заходи, інформаційне шпигунство, розшукові заходи). Слід підкреслити, що робота Головного управління розвідки в сфері кібернетичної безпеки країни є секретною.

У структурі Міністерства внутрішніх справ України діє спеціальний підрозділ – Департамент кіберполіції, який є міжрегіональним територіальним органом Національної поліції України, входить до структури кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Серед основних його завдань слід виокремити такі: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; Реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів

Служба безпеки України в межах своїх повноважень зобов'язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кіберпросторі, боротися з кібертероризмом і кібершпигунством, проводити таємні перевірки об'єктів критичної інфраструктури [126].

Зазначимо, що у складі Центрального управління СБУ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки), який сприятиме концентрації сил і засобів, оптимізації управлінської діяльності у вирішенні завдань із захисту законних інтересів держави та прав громадян в інформаційній сфері від розвідувально-підривної діяльності іноземних спецслужб, протиправних посягань

організацій, груп і осіб. Робота Департаменту засекречена, проте судити про результати можна за кількістю повідомлень про знешкодження хакерських груп і «телефонних терористів».

ДССЗЗІ є поки єдиною структурою в Україні, яка цілеспрямовано займається питаннями кібернетичної безпеки [98]. Вона створена відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», становить основу національної системи кібербезпеки і приймає участь у формуванні та реалізації державної політики в сфері захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації. На ДССЗІ (разом з СБУ) покладене одне з основних завдань – взаємодія з Міністерством оборони у забезпеченні кіберзахисту інформаційної інфраструктури. Її робота спрямована на захист державної інфраструктури. В контексті дослідження на особливу увагу заслуговують такі підрозділи служби:

Computer Emergency Response Team of Ukraine (CERT-UA). Серед основних його завданнь слід виокремити такі: запобігання, виявлення і усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; консультаційна та методична допомога в питаннях захисту державних інформаційних ресурсів; взаємодія з міжнародними організаціями реагування на несанкціоновані дії (наприклад, з Форумом команд реагування на інциденти безпеки – FIRST) [56, с.112]. На жаль, ресурсів CERT-UA бракує для того, щоб забезпечувати захист не тільки державних інформаційних ресурсів, але й приватних компаній і користувачів;

Центр антивірусного захисту інформації (ЦАЗІ). Його мета - забезпечення єдиної системи антивірусного захисту державних інформаційних ресурсів. Однак, в Україні досі не існує державного проекту зі створення національного антивірусу, що є серйозним упущенням

враховуючи той факт, що в країні вже існують компанії, які володіють антивірусними продуктами високої якості і ефективності.

Крім цього, варто відзначити, що наприкінці червня 2014 року у складі Національної гвардії України було створено Управління інформаційної безпеки, функціями якого є взаємодія та оперативне управління інформаційними потоками в режимі бойової обстановки. Однак, на жаль, й на сьогодні через розбалансованість системи влади координація дій між цими відомствами не перебуває на належному рівні.

У зв’язку з цим вважаємо виправданим зосередити координаційну функцію у сфері забезпечення системи кібернетичної безпеки у ДССЗІ України, яка на сьогодні має найбільший досвід щодо убезпечення державних електронних інформаційних ресурсів.

Слід акцентувати увагу на коригуванні системи загроз у сфері кібернетичної безпеки України відповідно до стандартів НАТО та викликів, з якими стикається Україна сьогодні.

Серед таких викликів слід відзначити гібридні дії екстремістів на сході України, які поєднують у собі активну терористичну діяльність, здійснення інформаційного впливу на свідомість громадян та кіберзлочини. Причому така діяльність здійснюється щонайменше за інформаційної підтримки іноземних джерел.

Слід відзначити, що об'єктами, на які спрямована діяльність суб’єктів, на державному рівні визначено комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об’єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [126].

В контексті проблеми, яка розглядається, цілком слушною є думка В.В. Петрова, який звертає увагу на той факт, що державна політика у сфері забезпечення кібербезпеки дає можливість сформувати ієрархію складових національної системи кібербезпеки, яка має поєднувати в собі комплекс як адміністративно-правових, технічних та організаційних заходів для захисту інформації у воєнній, правоохоронній та спеціальних сферах, так і суто оперативних, розвідувальних і контррозвідувальних заходів [112, с. 128].

Констатуємо, що як діяльність, державна політика забезпечення кібербезпеки може здійснюватися на декількох рівнях, на яких функціонують певні організації та структури (табл. 1.2).

Таблиця 1.2. Рівні державної політики забезпечення кібернетичної безпеки

№	Рівень	Учасники	Характеристика діяльності
1	2	3	4
1	Місцевий	органи місцевого самоврядування, групи та асоціації громадян	передбачає діяльність, пов'язану із захистом життєво важливих інтересів людини та громадянина, суспільства й держави під час використання кіберпростору у сфері функціонування органів місцевого самоврядування; аналіз стану кіберзахисту та дій суб'єктів правовідносин щодо електронних комунікацій, захисту муніципальних інформаційних ресурсів, інформації
2	Регіональний (галузевий)	Державні адміністрації; регіональні центри кібербезпеки СБУ; Галузеві центри управління кібербезпекою	реагування на кібератаки, націлені на державні електронні інформресурси та об'єкти критичної інфраструктури; моніторинг стану кібербезпеки певної галузі, своєчасне інформування про кіберзагрози та обмін інформацією про кіберінциденти із національними центрами кібербезпеки ДССЗЗІ та СБУ
3	Національний	держава як основний інститут формування державної політики забезпечення кібербезпеки	Формування і запровадження державної політики забезпечення кібербезпеки, розробка відповідних національних програм та їх реалізація за допомогою певних механізмів

Продовження табл. 1.2

1	2	3	4
4	Міжнаціональний	Генеральна Ассамблея ООН; ОБСЄ; Центр кібернетичного захисту НАТО; зарубіжні компанії, які спеціалізуються на дослідженні в сфері кіберзахисту (наприклад,	Міжнародна співпраця у сфері кібербезпеки; вироблення спільних підходів до формування комплексу заходів з кібербезпеки; проведення спільних навчань суб'єктів сектору безпеки та формування спільних заходів в рамках законодавства України; обмін інформацією в сфері кібербезпеки (якщоце не протирічить законодавству України); консультативна та дорадча допомога; проведення переговорів у

		Американська компанія «FireEye); Правохоронні органи іноземних держав в сфері кібербезпеки, спеціальні служби (відповідно до укладених договорів); міжнародні організації, які здійснюють боротьбу з кіберзлочинністю; Трастовий фонд Україна-НАТО з питань кібербезпеки	форматі експертних консультацій Україна – НАТО з питань кібербезпеки; створення каналів зв'язку та контактів щодо спільного реагування на загрози у сфері міжнародної інформаційної безпеки; обмін інформацією та співробітництво у правоохоронній сфері з метою розслідування справ, пов'язаних із використанням ІКТ у терористичних та кримінальних цілях; створення механізму співробітництва між уповноваженими органами держав щодо оперативного обміну інформацією та спільного її використання про реальні та потенційні кіберризики та загрози; взаємний обмін технологіями для забезпечення безпеки функціонування критичної інформаційної інфраструктури.

Примітка. Сформовано автором

Необхідно вказати, що управлінська складова включає інструменти відповідного впливу, які розподілено на групи (табл.А.1 додатку А). Зазначимо, що для досягнення резільтату - формування безпечного кібернетичного простору – є необхідним належне правове, організаційне, технічне, інституційне забезпечення, яке є елементами забезпечуючої складової і формується відповідно до сформульованих на основі визначених управлінських орієнтирів напрямів державної політики забезпечення кібернетичної безпеки.

Обгрунтованість управлінських орієнтирів та напрямів державної політики досягається на основі аналітичної складової, яка передбачає використання методів кіберрозвідки, діагностик і оцінку рівня потенційних загроз; аналіз фактичних кібератак і їх наслідків, моделювання стратегічних пріоритетів забезпечення кібернетичної безпеки [101, с.158].

Основні напрями формування державної політики забезпечення кібербезпеки наведено на рис.1.6.

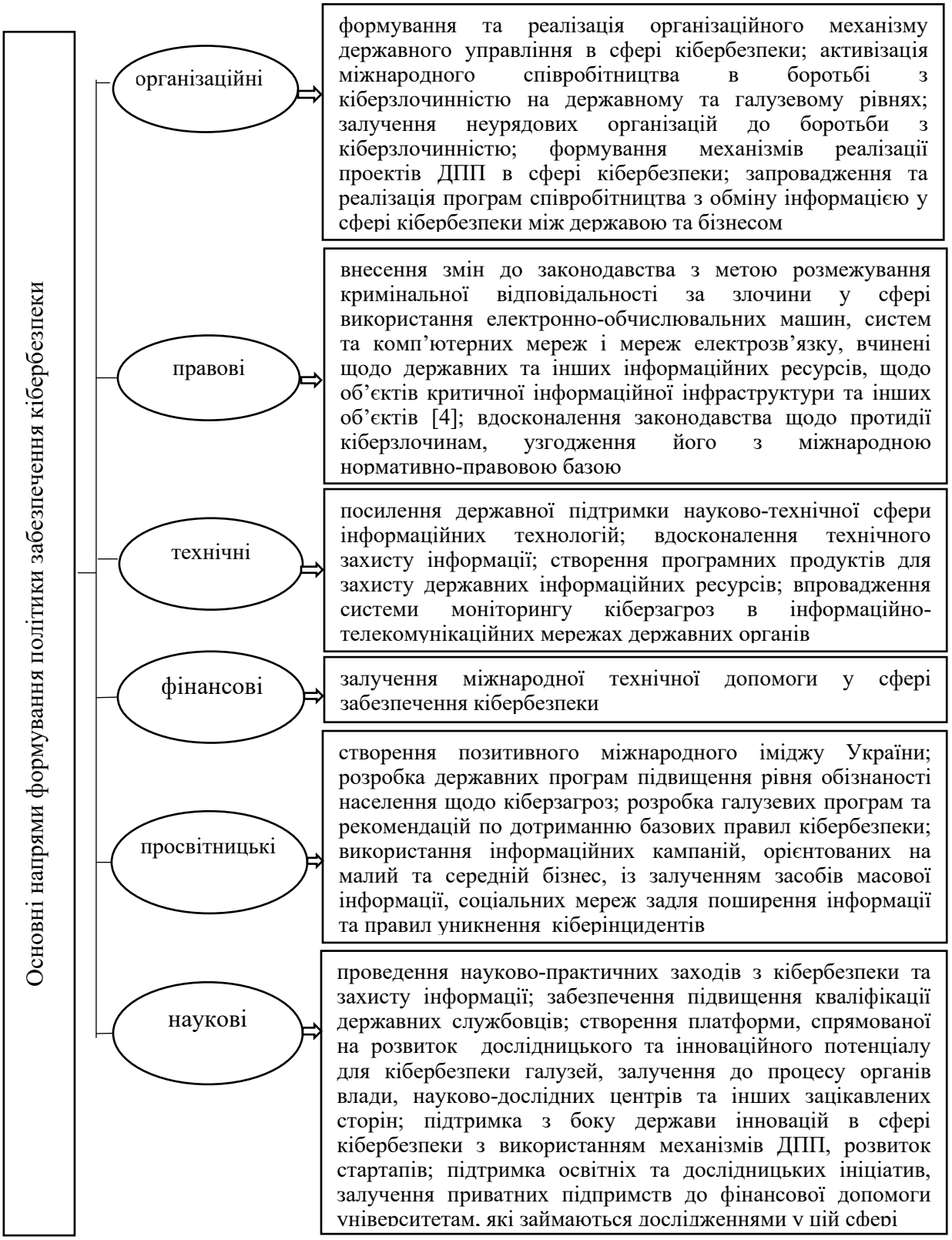

Рисунок 1.6 - Основні напрями формування державної політики забезпечення кібербезпеки

Примітка. Складено автором на основі [5, с.12; 45, с. 84; 80; с.14; 85, с. 112; 129]

Однак, враховуючи специфіку і масштабність сучасних кіберзагроз, задля розв'язання актуальних питань в сфері кіберзахисту, розробки ефективних,

дієвих державно-управлінських рішень та формування адекватної викликам державної політики в зазначеній сфері, ці принципи потребують уточнення та коригування.

Таким чином, систематизація підходів до розуміння державотворчих процесів в цій сфері дозволяє інтегрувати відповідні наукові знання та надає можливість практикам формувати ефективні, раціонально виважені державно-управлінські рішення, спрямовані на комплексне вирішення проблеми кіберзахисту. Реальні прояви кібератак здатні призвести до порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку із цим існуючі загрози вимагають формування та реалізації державної політики забезпечення кібернетичної безпеки, яка має бути спрямована на забезпечення інформаційного суверенітету України у кіберпросторі, створення надійного захисту національного сегменту кіберпростору в умовах антитерористичної операції; зміцнення обороноздатності держави у кіберпросторі; боротьбу з кіберзлочинністю та кібертероризмом; недопущення та запобігання втручанню у внутрішні справи України і припинення посягань на її Інтернет-ресурси з боку інших держав.

РОЗДІЛ 2
СУЧАСНИЙ СТАН РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

2.1. Аналіз рівня кіберзлочинності в Україні

Результати досліджень розвитку мережі Інтернет в Україні свідчать, що 60,7 % населення країни (25,59 млн. осіб) є її користувачами. При цьому, мобільним інтернетом користується 42% населення (18,7 млн. осіб), соціальними мережами - 29% (13 млн осіб), з них за допомогою мобільного телефону у соцмережі виходять 22% населення (9,5 млн.) (табл. 2.1) [181].

Таблиця 2.1

Використання мережі Інтернет та статистика населення в Україні

Рік	Населення кількість, осіб	Користувачі мережі Інтернет		
		Кількість, осіб	рівень проникнення (% до кількості населення)	темп зростання 2000-2018, %
2000	49084600	200000	0,4	X
2006	45833977	5278100	11,5	2639,05
2010	45415596	15300000	33,7	289,87
2018	42153200	25590000	60,7	167,26

Примітка. Сформовано автором за даними [181; 188; 189]

Слід вказати, що світові тенденції зростання рівня проникнення, використання інтернету та соціальних медіа приватними особами і компаніями, є характерними і для України, що, в свою чергу, сприяє розвитку інтернет-бізнесу. Такі факти знайшли своє підтвердження в ряді досліджень.

Так, у 2017 році загальна сума витрат на покупки товарів через електронні платформи склала 1,474 трлн. доларів, що на 16% більше, ніж в 2016 році [181].

Така динаміка назавжди змінила поведінку користувачів, так як прості громадяни і професіонали в області бізнесу все частіше проводять дослідження, приймають рішення про покупки, шукають підтримку і рекомендують бренди в режимі онлайн.

Необхідно констатувати, що найближчим часом в цифровій сфері очікуються найважливіші зміни: аудіовізуальний контент почне переважати над текстом; соціальні відносини і онлайн-суспільства розвиватимуться таким чином, щоб взяти на озброєння ці нові способи взаємодії людей між собою.

Американські дослідники [184] звертають увагу на той факт, що цифрові інновації можуть створити цінний взаємозв'язок між бізнесмоделями, досвідом клієнтів та операційною діяльністю.

Але тісніший взаємозв'язок призводить до посилення вразливості в комп'ютерних мережах та підвищення ризику виникнення кіберінцидентів.

Так, за даними [198], у 2017 році 978 мільйонів дорослих у 20 країнах (де проводилось дослідження) стикалися з глобальною кіберзлочинністю, що складає 44% онлайн-користувачів. В результаті споживачі, які стали жертвами кіберзлочинності, сумарно втратили 172 млрд. доларів (в середньому 142 долари на жертву).

Серед найбільш розповсюджених кіберзлочинів, які було відзначено, слід відзначити наступні:

наявність пристрою, зараженого вірусом чи іншою загрозою безпеці (53%);

проблеми з дебетовими або кредитними картами (38%);

усунення пароля облікового запису (34%);

несанкціонований доступ або хакерство електронної пошти чи облікового запису соціальних медіа (34%);

придбання онлайн, яке виявилося шахрайським (33%);

натискання на шахрайську електронну пошту або надання конфіденційної (особистої / фінансової) інформації у відповідь на шахрайство з електронною поштою (32%).

Зазначимо, що сьогодні експерти [28] звертають увагу на нові кіберзагрози, які пов'язані з масовим розвитком технологій І 4.0, концепція яких передбачає швидкий розвиток та нарощування сегменту технологій четвертої хвилі в економічній і позаекономічній сферах (аж до повного переходу на них). Причому станом на 2018-2019 р.р. цей процес лише розпочався. І на поточному етапі розвитку І 4.0 точкою входу для найбільшої кількості кібератак є персональні, підключені до Мережі портативні пристрої (смартфони, планшети тощо), парк яких набув тотального охоплення і продовжує швидко зростати, збільшуючи можливості кібератаки для зловмисників.

Аналіз основних статистичних показників, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах України (табл.2.2), дозволив констатувати зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет та збільшення рівня використання інформаційно-комунікаційних технологій в своїй діяльності, що проявилось у наступних тенденціях:

зростання кількості комп'ютерної техніки (+2 % у 2017 р. у порівнянні із 2016 р.), підвищення доступу до мережі Інтернет (+2 % у 2017 р.) та збільшення рівня використання інформаційно-комунікаційних технологій у своїй діяльності, зокрема у 2017 р.:

+4 % підприємств, що мали веб-сайт;

+8 % підприємств, які використовували соціальні медіа (соціальні мережі, блоги чи мікроблоги підприємства, веб-сайти з мультимедійним вмістом, засоби обміну знаннями);

+13,6 % підприємств, що купували послуги хмарних обчислень упродовж року;

+3,7 % підприємств, що отримували замовлення через комп'ютерні мережі на продаж товарів або послуг (за винятком замовлень, отриманих електронною поштою);

+4,5 % підприємств, які надавали рахунки-фактури в електронному/паперовому вигляді;

+14 % підприємств, що здійснювали закупівлі через комп'ютерні мережі товарів або послуг (за винятком замовлень, отриманих електронною поштою).

Таблиця 2.2. Використання інформаційно-комунікаційних технологій на підприємствах України

№	Назва показника	2014	2015	2016	2017
1	Кількість підприємств, які використовували комп'ютери, протягом року, од	41165	41597	39540	40327
2	Частка підприємств, які використовували комп'ютери, у % до загальної кількості підприємств, які взяли участь в обстеженні	93,4	95,2	95,1	95,4
3	Кількість підприємств, які мали доступ до мережі Інтернет, од	40111	40747	38825	39572
4	Частка підприємств, які мали доступ до мережі Інтернет, у % до кількості підприємств, які використовували комп'ютери, %	97,4	98,0	98,2	98,2
5	Кількість підприємств, які мали фахівців у сфері ІКТ, од.	7543	8541	10436	10660
6	Кількість підприємств, що мали веб-сайт, який функціонував у мережі Інтернет, од.	13485	18323	15608	16240
7	Кількість підприємств, які використовували соціальні медіа (соціальні мережі, блоги чи мікроблоги підприємства, веб-сайти з мультимедійним вмістом, засоби обміну знаннями, од.	18162	21722	22064	23849
8	Кількість підприємств, що купували послуги хмарних обчислень упродовж року, од., в т.ч.:	1287	2673	3639	4135
	із загальних серверів постачальників послуг	874	967	1506	1832
	серверів постачальників послуг, зарезервованих виключно для обстежуваного підприємства	376	430	665	807
9	Кількість підприємств, які надавали рахунки-фактури в електронному/паперовому вигляді:				
	іншим підприємствам	25312	26010	27919	29171
	державним органам	2540	3465	6582	7238
	приватним споживачам	12345	12869	14302	154733
10	Кількість підприємств, що отримували замовлення через комп'ютерні мережі на продаж товарів або послуг (за винятком замовлень, отриманих електронною поштою)	1573	2489	2503	2596
11	Кількість підприємств, що здійснювали закупівлі через комп'ютерні мережі товарів або послуг (за	5383	5495	7147	8168

	винятком замовлень, отриманих електронною поштою)				

Примітка. Сформовано автором за даними [22; 23]

Серед підприємств, які мали доступ до мережі Інтернет найбільша частка належить до сфери «оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів», переробної промисловості та будівництва.

Серед напрямів використання мережі Інтернет слід відзначити:

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 (додаток Б).

Але такі тенденції створили не лише передумови для розвитку підприємств та національної економіки в цілому, але й спричинили підвищення рівня злочинності в сфері інформаційно-комунікаційних технологій.

За даними дослідження «Всесвітнє дослідження економічних злочинів та шахрайства 2018 року», яке проводиться серед представників українських підприємств та організацій [25], кіберзлочинність входить до п’яти основних видів економічних злочинів та (або) шахрайства в 2018 році. (рис. 2.1).

Рисунок 2.1. - ТОП 5 основних видів економічних злочинів та (або) шахрайства на українських підприємствах та організаціях в 2018 році, %

Примітка. Сформовано автором на основі [25]

За результатами опитування (2018 рік) кількість кіберзлочинів, з якими стикаються підприємства та організації в Україні зростає на 7% в порівнянні з 2016 роком, спричиняючи високі ризики як для різних галузей національної економіки, так і для сфери державного управління.

Від даного виду злочинів, який став одним із найпоширеніших видів економічних злодіянь, посівши 5 місце серед видів шахрайства, постраждав 31% вітчизняних підприємств та організацій, що повністю відповідає загальносвітовим сумним тенденціям (31 % респондентів та 5 місце).

При цьому розвиток технологій призвів до виникнення ряду нових загроз для організацій, серед яких: шкідливе програмне забезпечення, фішинг, сканування мережі та атаки методом підбору паролю.

Слід зазначити, що більше третини українських організацій, що зазнали кібератак, постраждали від наслідків шкідливого програмного забезпечення. Внаслідок кібератак були порушені не тільки бізнес-процеси організацій (51%), а й завдані істотні збитки (рис. 2.2).

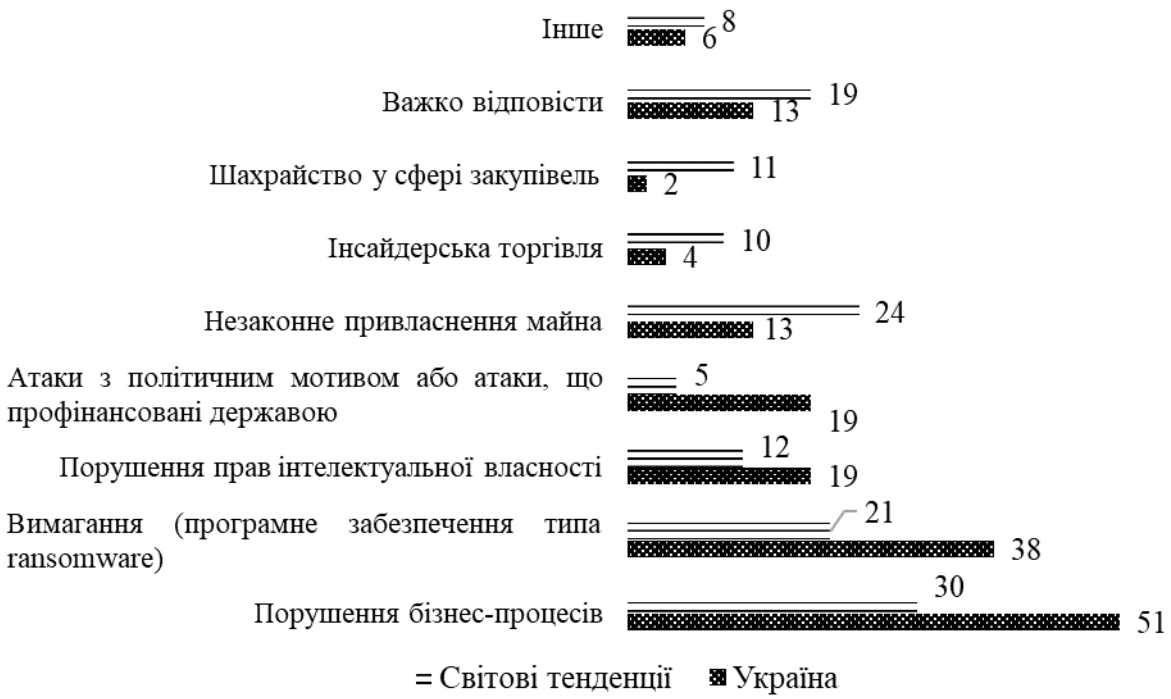

Рисунок 2.2 - ТОП 5 основних видів економічних злочинів та (або) шахрайства на українських підприємствах та організаціях в 2018 році, %

Примітка. Сформовано автором на основі [154]

Слід акцентувати увагу на тому, що за результатами 2018 року, 16% визначили вірогідності того, що їхня організація постраждає від кіберзлочинів у наступні два роки, що свідчить про доцільність приділення максимальної уваги цьому виду економічних злочинів як на рівні підприємств різної форми власності і видів діяльності, так і на рівні формування дієвої державної політики.

Зазначимо, що згідно очікувань українських респондентів, за критерієм суттєвості для організацій з точки зору фінансових збитків або інших наслідків у 2019-2020 р.р., кіберзлочини не лише відзначені у топ 5 видів економічних злочинів та / або шахрайства, а й посіли друге місце, поступаючись лише хабарництву та корупції (рис.2.3).

Рисунок 2.3 - Топ 5 видів економічних злочинів, які, згідно очікувань українських респондентів, будуть найбільш суттєвими для організацій з точки зору фінансових збитків або інших наслідків у наступні два роки

Примітка. Складено автором за даними [25]

Вітчизняні респонденти визнають той факт, що не лише очікують кібервпливи у наступні два роки, а й переконані, що кібератаки будуть найбільш значними для їхніх організацій з точки зору фінансових збитків або інших наслідків. Однак, слід визнати, що більшість підприємств в Україні не лише недостатньо підготовлені до кібератак, а й не розуміють до кінця ризики, які пов’язані з даним видом злочинів.

Враховуючи значущість оцінки ризиків та їх попередження, загальну оцінку ризиків шахрайства протягом 2016-2018 р.р. здійснювали лише 40% опитаних організацій в Україні. При цьому з напряму «вразливість до кіббератак» - 33% (при загальносвітовому показнику – 46 %). Лише кожна третя організація в Україні (31%) має повністю функціонуючу програму кібербезпеки для захисту від кібератак, яка включає наявні та потенційні ризики для організації та план заходів з реагування на інциденти кібербезпеки [25].

Відомості про зареєстровані кримінальні порушення (провадження) та результати їх розслідування, узагальнюються у звітності за формою №1 «Єдиний звіт про кримінальні правопорушення», яка формується щомісячно накопичувальним підсумком з початку звітного періоду (року) за регіоном вчинення злочину на підставі даних, внесених до Єдиного реєстру досудових розслідувань користувачами інформаційної системи, у розрізі розділів та статей Кримінального кодексу України, а про осіб, які їх вчинили – у

звітності за формою №2 «Єдиний звіт про осіб, які вчинили кримінальні правопорушення», за закінченими розслідуванням кримінальними провадженнями.

Так, зазначимо, що кількість злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, починаючи з 2014 року постійно зростала, сягнувши у 2017 році цифри 2573 злочини (рис.2.4). Темп приросту за 2014-2017 роки склав 480,8%. За 8 місяців 2018 року цей показник вже перевищив рівень 2016 року на 117,9 %.

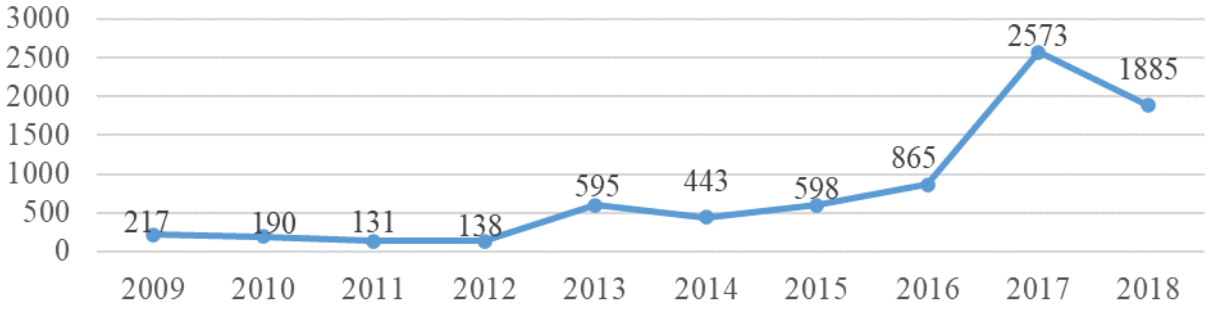

Рисунок 2.4 - Динаміка облікованої кіберзлочинності в Україні, кількість злочинів

Примітка. Сформовано автором за даними [76, с. 157; 107]

Такі тенденції склалися під впливом ряду факторів. Серед основних з них слід відзначити наступні: значні темпи інформатизації суспільства; технічне відставання правоохоронної системи та необхідність її реформування; недостатній рівень фінансування заходів з кіберзахисту.

Випереджаюче зростання зареєстрованих кіберзлочинів, вплинуло на збільшення їх питомої ваги у загальній кількості злочинів в Україні, зберігаючи тенденції підвищення від 0,08 % у 2014 році до 0,51 у 2018, що є найвищим показником, починаючи з 2009 року (рис.2.5).

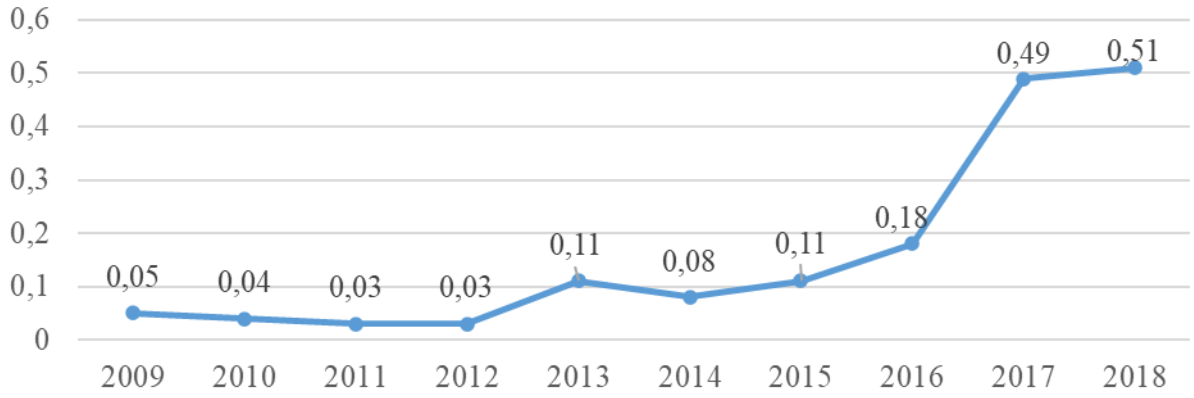

Рисунок 2.5 - Питома вага кіберзлочинів у загальній кількості зареєстрованих в Україні злочинів в динаміці, %

Примітка. Сформовано автором за даними [76, с. 157; 107]

Слід констатувати, що у 2018 році увагу працівників кіберполіції було зосереджено на розслідуванні злочинів, вчинених у сфері високих інформаційних технологій. Так протягом року працівники Департаменту кіберполіції були залучені до розслідування більше 11 тис. кримінальних проваджень. При цьому їх структура наведена на рис. 2.6.

. При цьому, необхідно вказати на той факт, що за територіями найбільша кількість злочинів у 2017 році була зосереджена у місті Києві, Київській, Чернівецькій, Львівській областях.

За результатами 2018 року найвища кримінальна активність спостерігалась у м. Києві, а також на території Черкаської, Одеської, Миколаївської та Львівської областей (додаток В, табл. В.1, В.2).

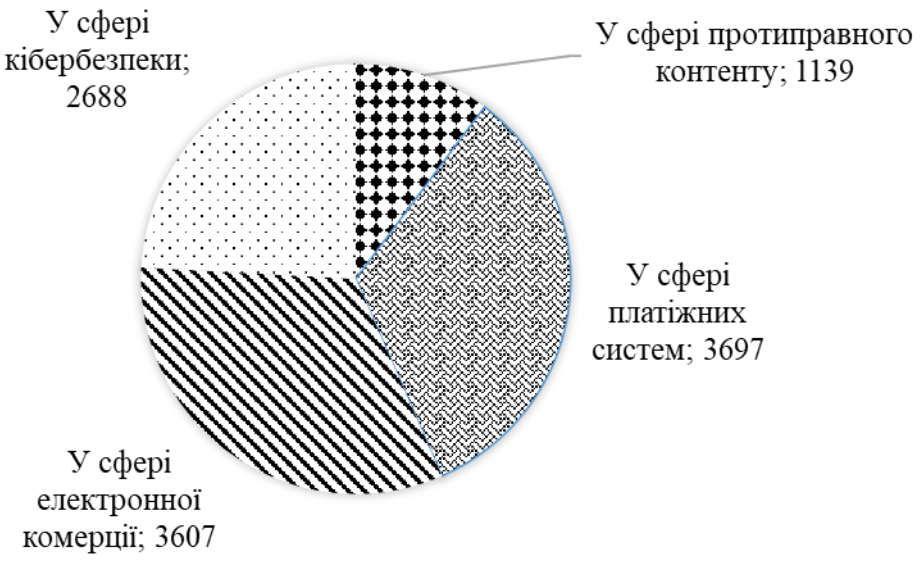

Рисунок 2.6 - Структура кримінальних проваджень, які знаходяться на розслідуванні кіберполіції (2018 р.), одиниць

Примітка. Сформовано автором за даними [107]

Крім того, саме за рахунок цих злочинів спостерігається загальний приріст кіберзлочинів в динаміці.

Аналіз структури кіберзлочинів в динаміці дозволив констатувати на протязі 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 %) (табл.2.3).

Таблиця 2.3. Структура кіберзлочинності за кримінально-правовою ознакою за 2013–2017 рр.

Обліковано кримінальних правопорушень у звітному періоді	2013	2014	2015	2016	2017
1	2	3	4	5	6
Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України)	408	344	432	494	1795
Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України)	12	10	21	15	35
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України)	20	11	59	28	64

Продовження табл. 2.3

1	2	3	4	5	6
Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України)	152	73	75	311	670
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)	2	4	9	15	6
Перешкоджання роботі електронно-обчислювальних	1	1	2	2	3

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України)					
Разом	595	443	598	865	2573

Примітка. Сформовано автором за даними [76, с. 158; 107]

Більш докладний аналіз структури злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, який здійснено на основі статистичної звітності за 2017 рік., дозволив констатувати, що зокрема у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільшу частку становлять ті, відповідальність за які передбачено ст. 361 Кримінального кодексу України – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (69,8 %).

На останньому місці – злочини, передбачені ст. 363-1: перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (0,1 %) (рис. 2.7).

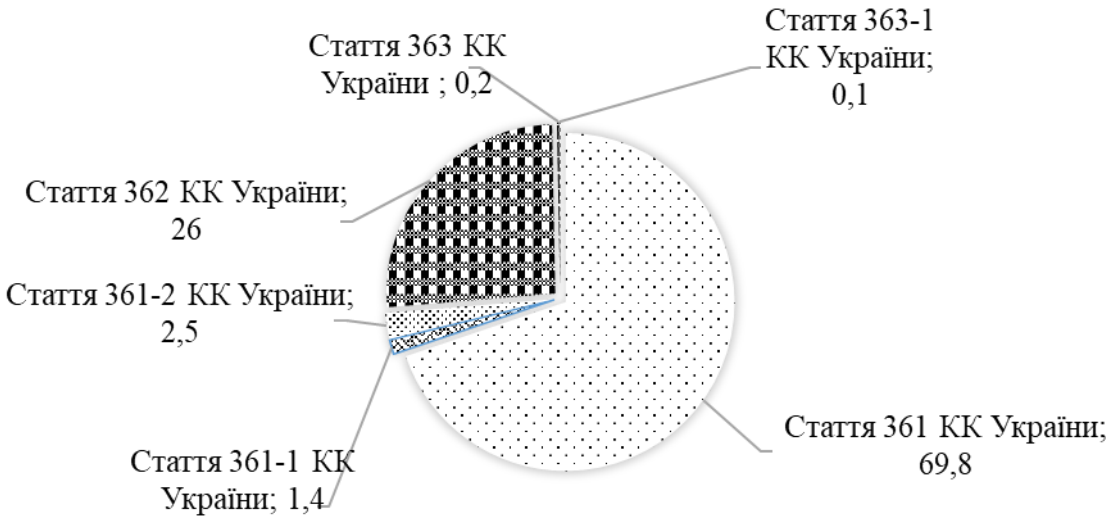

Рисунок 2.7. - Структура злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж

Примітка. Побудовано за даними [107]

Упродовж 2018 року поліцейські виявили 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій.

При цьому найбільше з них – у сфері електронної комерції (рис.2.8).

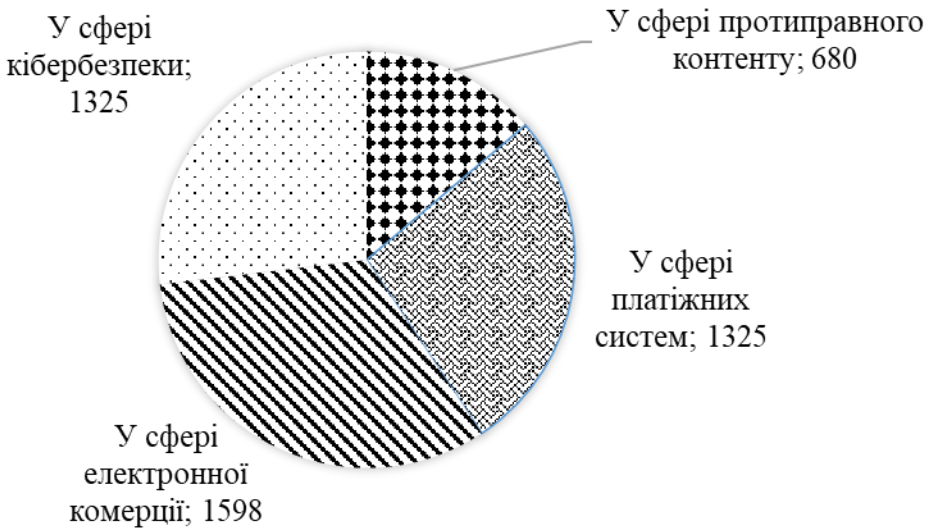

Рисунок 2.9 - Структура виявлених злочинів в сфері високих інформаційних технологій (2018 р.), одиниць

Примітка. Побудовано за даними [107]

Аналіз відомостей про осіб, які вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) (за закінченими розслідуванням кримінальними провадженнями), на основі даних 2017 року, дозволив сформувати «портрет» кіберзлочинця. Основна частка – це особи у віці від 18 до 39 років, які мають повну вищу і базову вищу освіту, що підтверджує їх високий кваліфікаційний рівень (додаток В, табл. В.3, В.4).

За даними 2018 року працівниками поліції викрито більше 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Згідно статистики, більша частина підозрюваних – чоловіки у віці від 25 до 40 років (табл.2.4).

Таблиця 2.4. Розоділ кіберзлочинців за віком та статтю, % (за даними 2018 р.)

Вік	Чоловіки	Жінки
Разом, з них:	67	33
До 25 років	13	6
25-40 років	39	20
40 і більше	15	7

Примітка. Побудовано за даними [107]

Дослідження викритих кіберзлочинів за статтями дозволило констатувати, що основна частка скоєна за статтею 190 Кримінального кодексу України (табл. 2.5).

Таблиця 2.5. Розподіл кіберзлочинців за статтю та видом злочинів

Стать	Стаття Кримінального кодексу України			
	176	190	361	361-1
Разом, осіб, з них:	37	1019	505	55
чоловіки, %	97	67	92	95
жінки, %	3	33	8	5

Примітка. Побудовано за даними [107]

Аналіз структури кіберзлочинів за видами свідчить, що водночас, у сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet (рис.2.9).

Зазначимо, що з метою виявлення кіберзлочинів, українська кіберполіція розробляє і впроваджує у практичну діяльність сучасні методики виявлення, фіксації і дослідження цифрових доказів. Зокрема, упродовж 2018 року спеціалістами з кіберполіції оглянуто та проаналізовано 5,5 петабайтів інформації, яка у подальшому була визначена як цифрові докази. За результатами міжнародної співпраці у 2018 році було викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях.

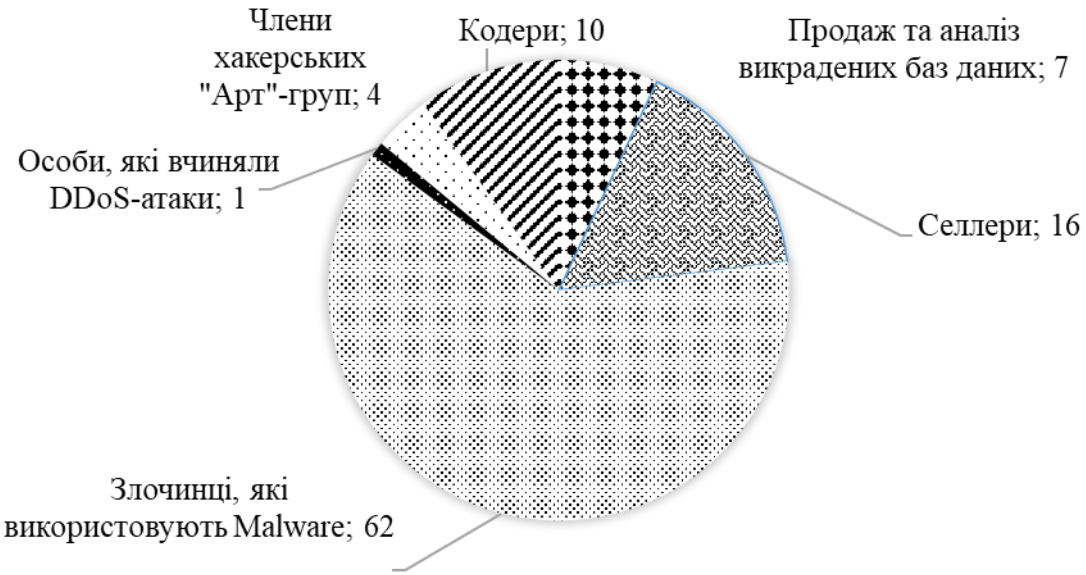

Рисунок 2.9 - Структура виявлених кіберзлочинів за видами (за даними 2018 року), %

Примітка. Побудовано за даними [107]

Слід зазначити, що у 2018 році було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них – представники міжнародних кампаній у сфері інформаційної безпеки та IT-компанії, поліція Австралії, Сінгапуру, Катару та інших країн. Крім того, налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами.

Зростання інформатизації країни та зростання тиску кібервпливів актуалізує роль держави та відповідного державного регулювання у забезпеченні кібернетичної безпеки. Це обумовлено тим, що саме держава визначає політику національної безпеки, сталого розвитку, цифровізації економіки і т.д.

Проведений аналіз показав, що кількість кіберзлочинів в Україні зростає випереджальними темпами, у той час, як правоохоронна система виявилась технічно не готовою до їх запобігання.

Отже, проблема залучення та оптимізації технічних, фінансових та організаційно-управлінських ресурсів, необхідних для ефективного подолання кіберзлочинності в Україні, на сьогоднішній день стає одним із

головних завдань державної політики забезпечення кібернетичної безпеки та є невід'ємною складовою політики національної безпеки.

2.2. Оцінка стану державного управління системою кібербезпеки України

Звертаючи увагу на рівень вітчизняної кібербезпеки слід звернути увагу на відомості про Національний індекс кібербезпеки (NCSI) - глобальний індекс, який вимірює готовність країн до запобігання реалізації фундаментальних кіберзагроз, управління кіберінцидентами, злочинами та масштабними кіберкризами [77, с. 112; 196].

Індекс оцінюється за наступними групами показників, які містять індикатори:

1. Загальні показники кіберезпеки:

розробка політики в галузі кібербезпеки (підрозділ політики кібербезпеки; формат узгодження політики кібербезпеки; стратегія кібербезпеки; план реалізації стратегії кібербезпеки);

аналіз та інформація про кіберзагрози (підрозділ аналізу кіберзагроз; громадські звіти про кіберзагрози публікуються щорічно;в еб-сайт з безпеки та безпеки в кіберпросторі);

освіта та професійний розвиток (компетенції з кібербезпеки в початковій або середній освіті; програма кібербезпеки рівня бакалавра; програма кібербезпеки магістра; програма кібербезпеки рівня доктора наук; професійна асоціація з кібербезпеки);

внесок у глобальну кібербезпеку (конвенція про кіберзлочинність; представництво у форматах міжнародного співробітництва; міжнародна організація з кібербезпеки, яку приймає країна; підвищення потенціалу кібербезпеки для інших країн).

2. Індикатори безпеки бізнесу: захист цифрових послуг; захист основних послуг; служби електронної ідентифікації та довіри; захист персональних даних.

3. Показники управління діяльністю і кризи: відповідь на кіберінциденти; кіберрегулювання кризи; боротьба з кіберзлочинністю; військові кібер-операції

У 2018 році за даним індексом Україна посіла 26 місце зі 131, що свідчить про достатньо високі результати здатності країни розвивати національну політику кіберзахисту, спроможність боротися з кіберзлочинами та надавати послуги електронної ідентифікації та електронного підпису (табл. 2.6).

Талиця 2.6. Перші 30 країн за Національним індексом кібербезпеки (2018 р.)

Місце	Країна	Значення індексу	Місце	Країна	Значення індексу	Місце	Країна	Значення індексу
1	Чехія	90,91	11	Сингапур	80,52	21	Грузія	64,94
2	Естонія	90,91	12	Словакія	79,22	22	Венгрія	64,94
3	Іспанія	89,61	13	Італія	76,62	23	Росія	64,94
4	Литва	88,31	14	Велико-британія	75,32	24	Бельгія	64,94
5	Греція	87,01	15	Малайзія	72,73	25	Ізраіль	64,94
6	Франція	83,12	16	Швейцарія	72,73	26	Україна	63,64
7	Фінляндія	81,82	17	Румунія	71,43	27	Сербія	63,64
8	Данія	81,82	18	Латвія	71,43	28	Ірландія	63,64
9	Нідерланди	81,82	19	Польща	70,13	29	США	63,64
10	Німеччина	80,52	20	Португа-лія	68,83	30	Японія	62,34

Примітка. Складено автором за даними [196]

Слід акцентувати увагу на тому, що з точки зору розбудови ефективної системи кібербезпеки основоположною є нормативно-правова база для її запровадження, яка представлена низкою таких концептуальних нормативно-правових актів:

1. Міжнародні:

Конвенція про кіберзлочинність [72] - основний міжнародний нормативно-правовий акт у сфері боротьби з кіберзлочинністю. Відповідно до її норм країни-учасниці повинні здійснити низку заходів на національному

рівні, спрямованих на боротьбу з кіберзлочинами. Конвенція була затверджена комітетом міністрів Ради Європи у 2001 році і підписана 35 державами (в тому числі не тільки членами Ради Європи, наприклад, її підписантами є США і Японія). Згідно цього документу, країни зобов'язані здійснювати узгоджену політику в сфері боротьби з кіберзлочинністю. Україна ратифікувала цю Конвенцію у 2005 році.

2. Національні:

Конституція України [75], у ст. 17 якої відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього українського народу;

Закон України «Про національну безпеку України» [125], що закріплює основні принципи забезпечення національної безпеки взагалі та інформаційної безпеки зокрема;

Закон України «Про основні засади забезпечення кібербезпеки України, який схвалений у 2017 р. Документом визначено правові та організаційні основи забезпечення державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [126]. Експерти відзначають при формулюванні основних дефініцій врахування термінології ЄС і НАТО, що дозволяє чітко розрізнити види й об'єкти діяльності та зафіксувати сфери відповідальності суб'єктів у цій сфері [137]. Крім того, в Законі відображено такі європейські принципи, як: відкритість, доступність, стабільність і захищеність кіберпростору, а також необхідність взаємодії з приватним сектором і громадянським суспільством у сфері кібербезпеки;

Стратегія національної безпеки України «Україна у світі, що змінюється», що визначає загальні принципи, пріоритетні цілі, завдання і механізми захисту життєво важливих інтересів особистості, суспільства та держави від зовнішніх і внутрішніх загроз;

Стратегія кібербезпеки [129], яка базується на положеннях Конвенції Ради Європи про кіберзлочинність, закладає загальну архітектуру національної системи кібербезпеки і розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки та має на меті створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Серед головних перевага цієї Стратегії слід відзначити: дотримання європейського підходу до забезпечення кібербезпеки як до спільної відповідальності усіх ключових стейкхолдерів; орієнтація на стандарти ЄС та НАТО в сфері забезпечення кібербезпеки замість застосування пострадянських або виключно радянських стандартів; відмова від пріоритету «захисту національного сегменту Інтернету», який є притаманним російському та китайському підходам до кібербезпеки;

Закон України «Про національну безпеку», введений в дію 21 червня 2018 року, в якому визначено, що забезпечення кібербезпеки покладається на Службу безпеки України, а також відзначено особливу роль ДССЗЗІ при формування та реалізації державної політики у сфері кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, Законом передбачено Комплексний огляд сектору безпеки і оборони, який включає проведення, з-поміж інших, «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури» [125].

Однак, слід констатувати, що Воєнною доктриною України, схваленою 24 вересня 2015 року, питання кібероборони фактично не визначено. В документі звертається увага лише на кіберзахист критичної інфраструктури, як частину компетенції ДССЗЗІ [127].

Зазначимо, що в Україні запроваджено ряд важливих кроків в сфері забезпечення кібербезпеки. Серед основних слід виокремити наступні:

ратифікація Конвенції Ради Європи з кіберзлочинності;

розробка Стратегії кібербезпеки;

розвиток мережі команд реагування на комп'ютерні надзвичайні події (CERT) тощо.

Значним кроком у забезпеченні кібербезпеки стало підписання у 2019 р. Меморандуму про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту між Центром кіберзахисту Національного банку України та Державним центром кіберзахисту ДССЗЗІ. Таке співробітництво спрямоване на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту і передбачає наступний комплекс заходів:

здійснення термінового оповіщення про виявленні спроби вчинення кібератак, рівень та складність яких може становити значну загрозу для банківської системи України, критичної інфраструктури та національної безпеки України;

обмін інформацією про результати аналізу виявлених кіберінцидентів та кібератак, рекомендацій та заходів з підвищення рівня кіберзахисту;

обмін технічною, технологічною та довідковою інформацією у сфері забезпечення кіберзахисту;

спільні навчальні, консультативні та суспільно-освітні заходи, обмін набутим досвідом у сфері забезпечення кібербезпеки та кіберзахисту.

Однак, формування та реалізація комплексу заходів у цій галузі потребує доопрацювання.

Слід звернути увагу на результати досліджень [24; 63, с.43; 134, с.88; 143], в яких автори визначають основні проблеми, з якими стикається державна політика в питаннях захисту кіберпростору країни. А саме:

відсутність в Україні єдиної загальнодержавної системи протидії кіберзлочинності та єдиного нормативного документа, який би чітко визначав основні поняття і окреслював зони відповідальності державних структур у сфері кібернетичної безпеки;

застарілість і не систематизованість правових актів з питань національної безпеки містять низку неузгодженостей, не враховують особливості загроз нового типу, у тому числі впливу «гібридної» агресії;

відсутність координації державних структур у сфері кібернетичної безпеки.

З метою вирішення зазначених проблем запропоновано та реалізовано такі заходи:

КМУ ініційований проект Закону України «Про внесення змін до Закону України Про основи національної безпеки України», в якому враховане питання кібернетичної безпеки [131]. Даний документ став результатом тривалої роботи фахівців силових структур країни (СБУ, МВС, Міноборони), метою якого, є «формування основ державної політики в сфері забезпечення кібернетичної безпеки України»;

запропоновані концептуальні підходи до комплексного перегляду законодавства України з питань національної безпеки; надані конкретні рекомендації щодо підготовки нової редакції Закону України «Про основи національної безпеки України» як базового закону у відповідній сфері [24].

Однак, на думку експертів з юридичного управління Верховної Ради України, документ виявився «сируватий» і має бути доопрацьований. Фахівці [168] вважають, що зайва деталізація термінології з приставкою «кібер» «створює негативний прецедент», і взагалі, вже існує відповідна законодавча база.

Крім того, слід констатувати, що одна з проблем в сфері кіберзахисту полягає в тому, що Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово уразливою до кібернетичних загроз і, не в останню чергу, через надмірно широке транслювання іноземних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

Пошук можливих «закладок» у цій продукції практично унеможливлюється через залежність держави від згаданих продуктів, що вийшла на дійсно загрозливий для національної безпеки рівень в усіх сферах.

У зв'язку з цим, розглянувши ситуацію, комплекс проблем у сфері кібербезпеки та рівень загроз національній безпеці, РНБО України визначила ряд заходів, спрямованих на підвищення ефективності протидії актуальним кіберзагрозам і відповідальних суб'єктів.

Серед найбільш важливих з них виокремлено такі: невідкладно забезпечити підготовку законодавчих пропозицій стосовно визначення механізму взаємодії між суб'єктами забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів; забезпечити підготовку законодавчих пропозицій щодо посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах; забезпечити створення єдиних основного та резервного захищених дата-центрів збереження інформації і відомостей державних електронних інформаційних ресурсів; опрацювати питання щодо стимулювання розроблення та впровадження вітчизняного програмного забезпечення для потреб органів державної влади та інших державних органів, підприємств, установ та організацій державної форми власності тощо [128; 138; 168].

Зростання рівня проникнення, використання інтернету та соціальних медіа приватними особами, підприємствами та державними структурами не лише сприяє розвитку, надає можливості освоєння нових сфер діяльності, але й створює загрози через посилення вразливості в комп'ютерних мережах та підвищення ризику виникнення кіберінцидентів.

Зазначені тенденції мають безпосередній вплив на формування та реалізацію державної політики забезпечення кібернетичної безпеки, тому їх відстеження та перманентний аналіз набуває ключового значення для забезпечення національної безпеки в умовах сьогодення.

Зростання кібервикликів та загроз, які продовжують поширюватися на політичне, соціальне та економічне життя суспільства, актуалізують процеси, пов’язані з формуванням і реалізацією державної політики, спрямованої на посилення безпеки і надійності інформаційних систем та створення відкритого безпечного кіберпростору.

Слід звернути увагу, що управління процесами кібернетичної безпеки, прийняття своєчасних, відповідаючих мінливим викликам ефективних рішень має спиратись на потужну дослідницьку базу та потребує належного аналітичного забезпечення.

З метою обґрунтування напрямів державної політики кібербезпеки, диференціювання засобів впливу, відслідковування та своєчасного коригування результатів запровадженого комплексу заходів вважаємо доцільним оцінити рівень кіберзагроз в регіоні.

З використанням методу експертних оцінок визначено такі показники-індикатори, за якими запропоновано оцінити вплив соціально-економічного розвитку на рівень кібернетичних загроз регіонів України та які є складовими інтегрального показника:

ВРП - валовий регіональний продукт на одну особу, грн;

КІ - капітальні інвестиції в інформацію та телекомунікації, млн.грн;

КАІ – кількість абонентів мережі Інтернет (підприємства та фізичні особи), тис. осіб;

ІД – кількість підприємств, які займаються інноваційною діяльністю (придбання машин, обладнання, програмного забезпечення), одиниць;

КАМ - кількість абонентів мобільного зв’язку, тис. осіб;

ВДВ – валова додана вартість інформації та телекомунікацій (у фактичних цінах), млн.грн.;

ЗКП – зареєстровані кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж електрозв’язку, одиниць.

Основні відомості за визначеними факторами наведено у додатку Г,

табл. Г.1.

Слід акцентувати увагу на тому, що перелік даних факторів дещо обмежений тим, що доступ до даних за рядом показників є обмеженим, оскільки вони відносяться до таємниці різного рівня.

З метою стандартизації системи показників, яка характеризує рівень кібернетичних загроз, всю множину необхідно розподілити на дві групи:

- стимулятори. В даному дослідженні серед них відзначено такі: кількість абонентів мережі Інтернет (підприємства та фізичні особи) (Z_1); кількість абонентів мобільного зв'язку (Z_2); валова додана вартість інформації та телекомунікації (у фактичних цінах) (Z_3).

- дестимулятори. В даному дослідженні серед них визначено: валовий регіональний продукт на одну особу (Z_4); капітальні інвестиції в інформацію та телекомунікації (Z_5); кількість підприємств, які займаються інноваційною діяльністю (придбання машин, обладнання, програмного забезпечення) (Z_6).

Розрахунок інтегрального показника здійснюється для кожної області України окремо як середнє значення стандартизованих показників, які характеризують рівень кібернетичних загроз в регіоні. Стандартизовані статистичні показники, які отримано за результатами розрахунків, наведено у додатку Г, табл. Г.2.

Отже зазначимо, що у Дніпропетровській, Донецькій, Львівській, Одеській, Київській, Харківській областях і місті Києві за стандартизованими показниками кількість абонентів мережі Інтернет (підприємства та фізичні особи); кількість абонентів мобільного зв'язку; валова додана вартість інформації та телекомунікації (у фактичних цінах) мають значення вище середнього рівня, що свідчить про значний розвиток інформаційно-комунікаційних технологій і збільшення кількості зареєстрованих злочинів в цій сфері.

Стандартизована оцінка показників «валовий регіональний продукт на одну особу»; «капітальні інвестиції в інформацію та телекомунікації»; «кількість підприємств, які займаються інноваційною діяльністю (придбання

машин, обладнання, програмного забезпечення)» свідчить, що найбільші інвестиції та заходи, які сприяють розвитку галузі спостерігаються у Донецькій, Львівській, Дніпропетровській, Київській, Харківській областях, м. Києві. Найменші – у Луганській, Хмельницькій, Чернівецькій, Рівненській областях.

Використовуючи результати стандартизованої оцінки, отримано інтегральний показник оцінки рівня кібернетичних загроз за регіонами України (2018 рік) (табл.2.7).

Таблиця 2.7. Інтегральні показники оцінки рівня кібернетичних загроз за регіонами України (за даними 2018 р.)

Область	$\overline{Z}$	Відхилення від середнього значення інтегральної оцінки
Луганська	7,022	4,140
Чернігівська	6,234	3,352
Хмельницька	5,216	2,334
Житомирська	4,826	1,944
Херсонська	4,751	1,869
Чернівецька	4,327	1,445
Черкаська	4,013	1,131
Рівненська	3,708	0,826
м. Київ	3,702	0,820
Волинська	3,197	0,315
Сумська	3,076	0,194
Кіровоградська	2,851	-0,031
Закарпатська	2,491	-0,391
Миколаївська	2,194	-0,688
Тернопільська	1,755	-1,127
Полтавська	1,658	-1,224
Івано-Франківська	1,499	-1,383
Одеська	1,344	-1,538
Донецька	1,303	-1,579
Запорізька	1,253	-1,629
Харківська	1,164	-1,718
Київська	1,158	-1,724
Дніпропетровська	1,146	-1,736
Львівська	1,086	-1,796
Вінницька	1,083	-1,799
Середнє значення	**2,882**	**X**

Примітка. Розраховано автором

Констатуємо, що найбільший рівень кібернетичних загроз за сукупністю визначених показників є характерним для Луганської області (інтегральний показник становить 7,022). У групі ризику за рівнем кіберзагроз: Чернігівська, Хмельницька Житомирська, Херсонська області.

Слід акцентувати увагу на тому, що в 11 областях України результат інтегральної оцінки перевищує середній рівень в країні. Найменший рівень кібернетичних загроз - у Вінницькій області (значення інтегрального показника – 1,083). Графічні результати інтегрального показника оцінки рівня кібернетичних загроз за регіонами наведено на рис. 2.10.

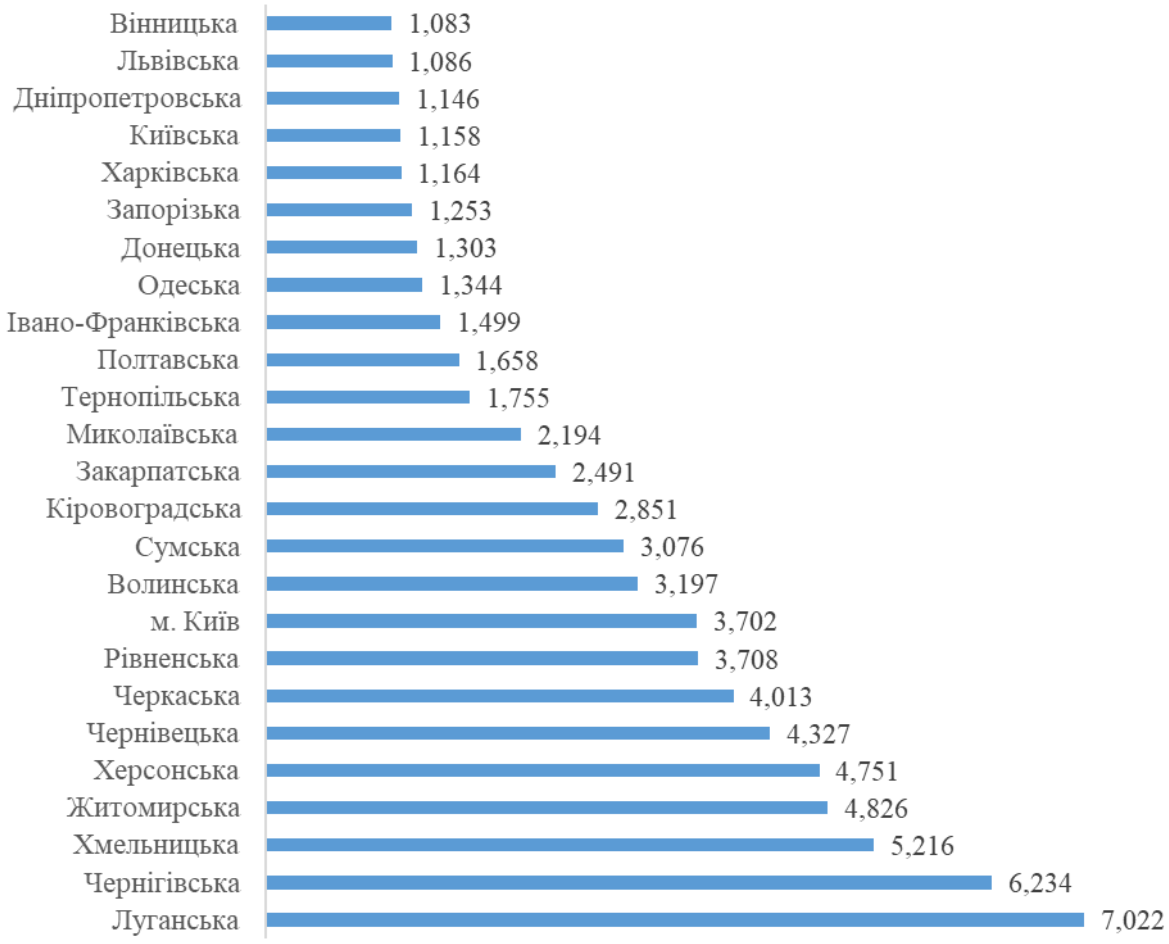

Рисунок 2.10 - Інтегральні показники оцінки рівня кібернетичної загрози за регіонами України (2018 р.)

Примітка. Розраховано автором

Проведені розрахунки склали підґрунтя для визначення місця кожного з регіонів за інтегральним показником оцінки рівня кібернетичних загроз, що має скласти аналітичну базу при формуванні відповідних напрямів державної політики забезпечення кібербезпеки з врахуванням територіальних особливостей.

На основі проведених розрахунків вважаємо доцільним здійснити групування регіонів України в однорідні групи із застосуванням комплексу ієрархічних та неієрархічних методів.

Використання цих методів у комплексі дозволить нівелювати недоліки кожного з цих методів і використати певні переваги. Так, за допомогою ієрархічної групи методів визначено кількість кластерів, неієрархічні методи дозволяють здійснити власне процес кластеризації, не допускаючи перекриття кластерів.

З метою практичної реалізації процесу кластеризації застосовано статистичний пакет IBM SPSS Statistics (табл. 2.8).

Таблиця 2.8. Результати кластеризації регіонів України за рівнем кібернетичних загроз (за даними 2018 р.)

№ кластера	Назва кластеру	Регіон	Значення інтегрального 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

Примітка. Розраховано автором з використанням статистичного пакету IBM SPSS Statistics

Зазначимо, що за результатами кластеризації, на основі розподілу регіонів України за рівнем кібернетичних загроз, виділено чотири кластери:

до першого кластеру – з дуже високим рівнем кібернетичних загроз – Луганська та Чернігівська області (з середнім значенням інтегрального показника оцінки рівня кібернетичних загроз 7,022 та 6,234 відповідно);

другий кластер включає чотири регіони з високим рівнем кібернетичних загроз. Це Чернівецька, Херсонська, Житомирська, Хмельницька області (граничні значення інтегрального 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 інтегрального показника від 1,083 до 2,194.

Запропоновані засади формування аналітичного забезпечення управління кібернетичною безпекою, які передбачають інтегральну оцінку рівня кібернетичного захисту регіонів країни та їх розподіл на кластери, є базою для обґрунтування напрямів державної політики кібербезпеки. Подальший аналіз отриманих результатів є основою для коригування напрямів державної політики кібербезпеки та диференціації засобів впливу на рівні регіонів.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

3.1. Концептуальні засади удосконалення державної політики забезпечення кібернетичної безпеки

Застосування системного погляду до розуміння процесів забезпечення кібербезпеки надало змогу представити концепцію державної політики забезпечення національної кібернетичної безпеки у вигляді системи, яка включає теоретичний базис, методичні засади, інструментальне забезпечення, побудована 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 (підприємства, корпорації, неурядові організації), до процесів управління, реалізація якої спрямована на формування безпечного кібернетичного простору (рис. 3.1).

На відповідних рівнях концепції, спираючись на теоретичні основи управління процесами забезпечення кібернетичної безпеки, методичну базу, користуючись результатами діагностики та моделювання запропоновано пріоритетні напрями державної політики забезпечення кіберзахисту, інструменти реалізації, пропозиції до коригування стратегії та державного програмування.

Акцентуємо увагу на тому, що розвиток державної політики забезпечення кібернетичної безпеки України, враховуючи сучасні загрози, має бути спрямований на:

забезпечення безпечного функціонування об'єктів критичної інформаційної інфраструктури;

розвиток міжнародного співробітництва;

посилення взаємодії у боротьбі з кіберзлочинами вітчизняних правоохоронних, розвідувальних і контррозвідувальних органів;

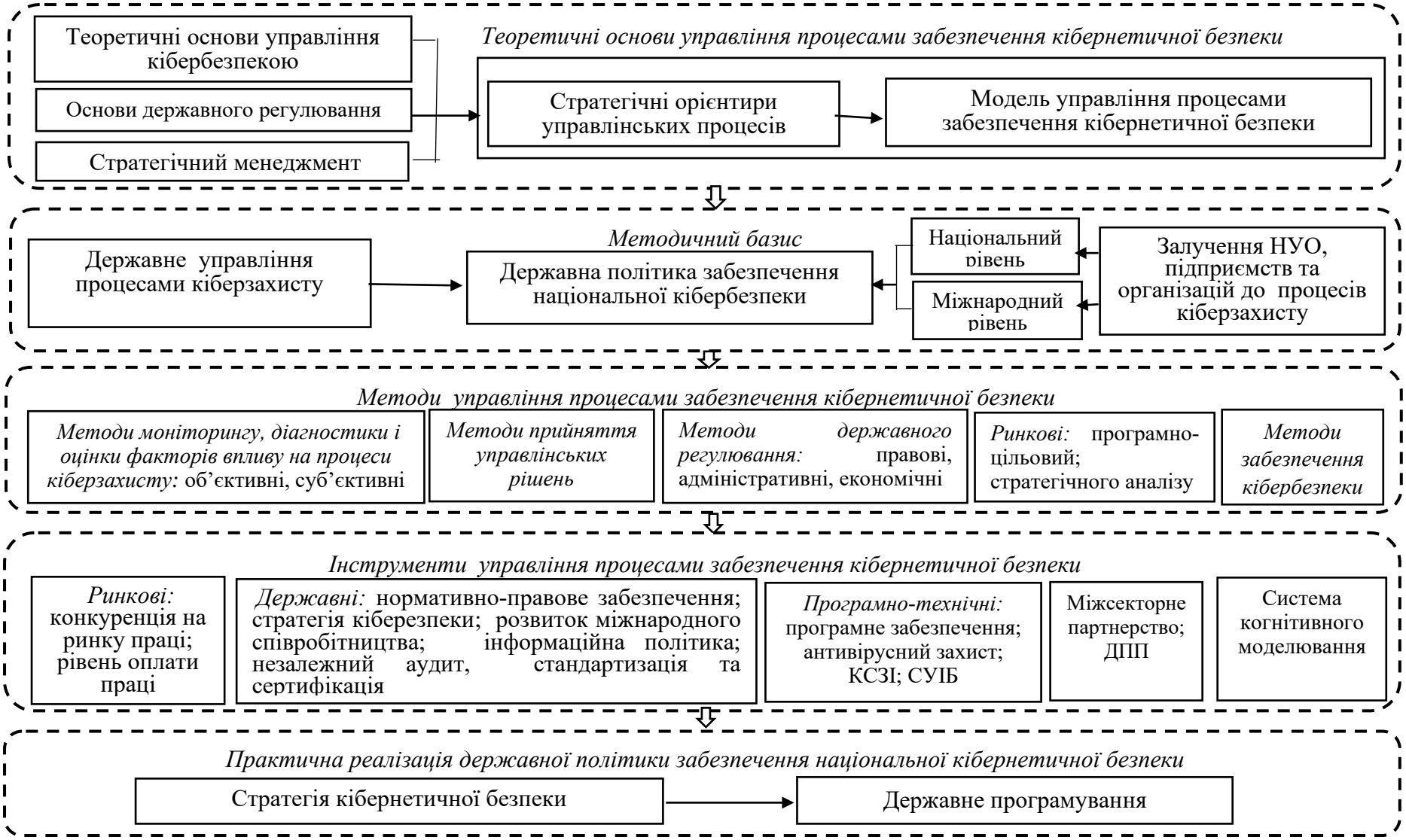

Рисунок 3.1 - Концепція формування державної політики забезпечення національної кібернетичної безпеки

Примітка. Запропоновано автором

використання потенціалу Збройних Сил України при забезпеченні захисту та протидії кіберзагрозам;

розвиток інноваційної діяльності, підтримка наукових досліджень в сфері інформаційних технологій;

підтримка підготовки кваліфікованих фахівців та підвищення кваліфікації користувачів в сфері інформаційних технологій;

удосконалення нормативно-правового забезпечення в сфері кіберзахисту, адаптація законодавства України до норм ЄС та НАТО;

забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних;

використання форм ДПП в сфері кібербезпеки;

використання потенціалу неурядових організацій в формуванні безпечного кіберпростору;

підвищення рівня інформованості суспільства про можливі ризики, виклики та загрози у кіберпросторі, формування комплексу заходів, здатного створити протидію маніпулювання свідомістю та думкою громадян.

Серед засобів провадження державної політики забезпечення національної кібернетичної безпеки слід визначити наступні:

реалізація принципів та положень міжнародних конвенцій та договорів, які ратифіковано Україною в зазначеній сфері;

адаптація законодавчої бази в сфері кіберзахисту до міжнародних стандартів;

формування та реалізація державних та регіональних програм в цій сфері, спрямованих на вирішення сформульованих у Стратегії задань;

створення системи державних органів забезпечити реалізацію державної політики забезпечення кіернетичної безпеки;

залучення аналітичних відділів підприємств недержавної форми власності, неурядових організацій для оперативного виявлення кібернетичних загроз та визначення їх джерел.

Зазначимо, що управління процесами кіберзахисту має здійснюватися системно, в рамках державної політики та на основі відповідної стратегії, оскільки саме такий підхід надає можливість своєчасно приймати ефективні рішення та реагувати інструментами державної політики з врахуванням змін і сучасних кібервикликів.

Слід констатувати, що особливості державної політики в цій сфері та основні стратегічні пріоритети визначені в Стратегії кібербезпеки.

Даним документом визначено такі пріоритети та напрями забезпечення кібербезпеки України [129]:

розвиток безпечного, стабільного і надійного кіберпростору;

кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом; кіберзахист критичної інфраструктури;

розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки;

боротьба з кіберзлочинністю.

Проте, враховуючи сучасні виклики та загрози, які постають перед країною, зазначені стратегічні пріоритети вимагають коригування та поглиблення визначених цільових установок.

В цьому контексті слід відзначити той факт, що експерти [28] звертають увагу на нові кіберзагрози, які пов’язані з масовою імплементацією технологій І 4.0, які можуть спричинити катастрофічні наслідки не лише для національної безпеки, промислового виробництва та економіки загалом, але й для інших суспільних сфер, включаючи приватне життя громадян. Водночас слід наголосити, що відмова від цих технологій означатиме фатальне відставання у розвитку для будь-якої країни чи регіону,

що потребує запровадження адекватних дій в багатьох сферах, і насамперед - в галузі кіберзахисту, що встановлює пріоритетом поєднання швидкої розробки нових адекватних технологій кібербезпеки та формування сучасних інструментів державної політики.

Необхідно вказати, що з метою реалізації сукупності визначених стратегічних пріоритетів та конкретизації заходів, спрямованих на їх досягнення, представляться доцільним формування та запровадження цільових програм. Зауважимо, що реалізація державної політики забезпечення кіберзахисту потребує вирішення комплексу проблем, серед основних з яких слід виокремити фінансування за умов обмеженості ресурсів [100, с. 78].

Тому, з метою залучення фінансових ресурсів і спрямування їх для розв'язання питань в сфері забезпечення кібернетичної безпеки, спираючись на позитивні міжнародні практики в цій сфері, представляється доцільним використання ДПП.

Незважаючи на численні дискурси, досвід багатьох країн свідчить, що інтеграція держави та приватного сектору в боротьбі з кіберзлочинністю, запровадження ДПП в галузі кібербезпеки здатне прискорити її розвиток та створити передумови для посилення національної безпеки [171, с. 10]. Констатуючи існування різних форм ДПП, необхідно відзначити обмеженість практичної реалізації деяких з них, що обумовлено специфікою діяльності в сфері кіберзахисту.

Умови використання окремих базових форм ДПП (з врахуванням галузевої специфіки) при забезпеченні кібернетичної безпеки наведено в табл. 3.1).

Слід констатувати що кожній з зазначених форм притаманні певні недоліки, які обумовлюють складнощі запровадження та обмеження практичної реалізації в сфері забезечення кібернетичної безпеки.

Модель запровадження різних форм ДПП запропонована на (рис. 3.2).

Однак, слід звернути увагу на певні проблеми, які супроводжують запровадження ДПП та уповільнюють процеси, які пов’язані з ним.

Таблиця 3.1. Специфічні умови запровадження форм ДПП в сфері забезпечення кібернетичної безпеки

Форма ДПП	Характеристика форми ДПП	Специфіка використання
1	2	3
Контракт	Характеризується простотою запровадження, що спричиняє широке використання. Передбачає укладання договору між державним органом та приватним партнером на здійснення суспільно необхідних видів діяльності і не призводить до значного економічного ефекту (що часто спричиняє низький інтерес з боку бізнесу)	Можлива при будівництві об’єктів інфраструктури, в т.ч. критичної, створенні програмного забезпечення, розвитку обчислювальних спроможностей
Оренда / лізинг	При оренді з боку приватної сторони здійснюється проектування, будівництво, фінансування, експлуатація власності державного сектора. Лізинг надає право приватному підряднику проектувати, фінансувати, експлуатувати, реконструювати об'єкт державного сектора та в кінці терміну дії договору можливість повернути право власності, або купити за попередньо розрахованою залишковою вартістю об'єкта	При обмеженості ресурсів в приватному секторі представляє певний інтерес. Можлива для запровадження при будівництві інфраструктурних об’єктів та розвитку технічних спроможностей
Аутсорсинг	Держава має можливість передати ряд функцій компанії, яка спеціалізується в цій галузі	побудова комплексних рішень технічного забезпечення; проекти з інформування суспільства щодо кіберризиків; використання можливостей неформальної освіти для підвищення кваліфікації діючих фахівців (тренінгі, семінари, міжнародні стажування; проведення дослідницької та консультативої роботи (залучення науково-аналітичних та консалтингових компаній)
Спільна діяльність	Гнучка форма, для якої характерна взаємодія широкого кола учасників без створення юридичної особи. Здійснюється на основі договору про спільну діяльність. Сторони об’єдуютьі зусилля та майно задля досягнення єдиної мети. Зобов’язання мають не лише майновий, а й чіткий організаційний характер	залучення управлінської експертизи приватного партнера для реалізації складних програм; використання інформаційно-аналітичних підрозділів підприємств для виявлення загроз; формування законопроектів; підготовка кваліфікованих кадрів і поширення серед працівників компаній громадян культури інформаційної та кібернетичної безпеки; спільні інформаційні кампанії, спрямовані на ппідвищення обізнаності стосовно кіберризиків; консультативна діяльність щодо ключових стандартів

		у сфері кібербезпеки; обмін статистичними даними

Продовження табл. 3.1

1	2	3
Технопарк	Значний період окупності. Високий ризик. Існують як експериментальні.	В даній сфері існують обмеження для використання. Є можливим при запровадженні інвестиційних проектів
Концесія	Держава надає право приватному партнеру тимчасово виконувати прописані в договорі функції і надає повноваження для забезпечення ефективного функціонування об'єкта	Має деякі обмеження для використання. Запровадження можливо при створенні або модернізації деяких інфраструктурних об’єктів
Фінансово-промислова група	Розповсюджена форма в окремих сферах економіки.	Використання обмежено специфікою галузі

Примітка. Розроблено автором

Серед основних з них слід виокремити наступні:

на фоні констатації у Законі «Про основні засади забезпечення кібернетичної безпеки України» та відповідній стратегії доцільності запровадження ДПП, недостатньо опрацьовані механізми та процедури застосування його потенціалу;

неврегульованість питання стандартизації у сфері кіберзахисту та інформаційної безпеки, насамперед у частині порядку та меж застосування відповідних українських та/чи міжнародних стандартів (особливо критично для розвитку ДПП за участі об’єктів некритичної інформаційної інфраструктури) [46, с. 54];

відношення значних обсягів інформації в сфері забезпечення кібернетичної безпеки до таємниці різного рівня доступу, що не дає можливості оцінити стан розвитку галузі та наявні проблеми;

нестача довіри між суб’єктами ДПП, що створює бар’єри для надання відповідної інформації та сумісної діяльності в цілому;

відсутність належної інформації з боку державних органів через їх закритість, що унеможливлює співпрацю в рамках ДПП за рядом питань.

Враховучи це, серед основних напрямів державної політики забезпечення кібернетичної безпеки, спрямованої на запровадження ДПП слід відзначити наступні:

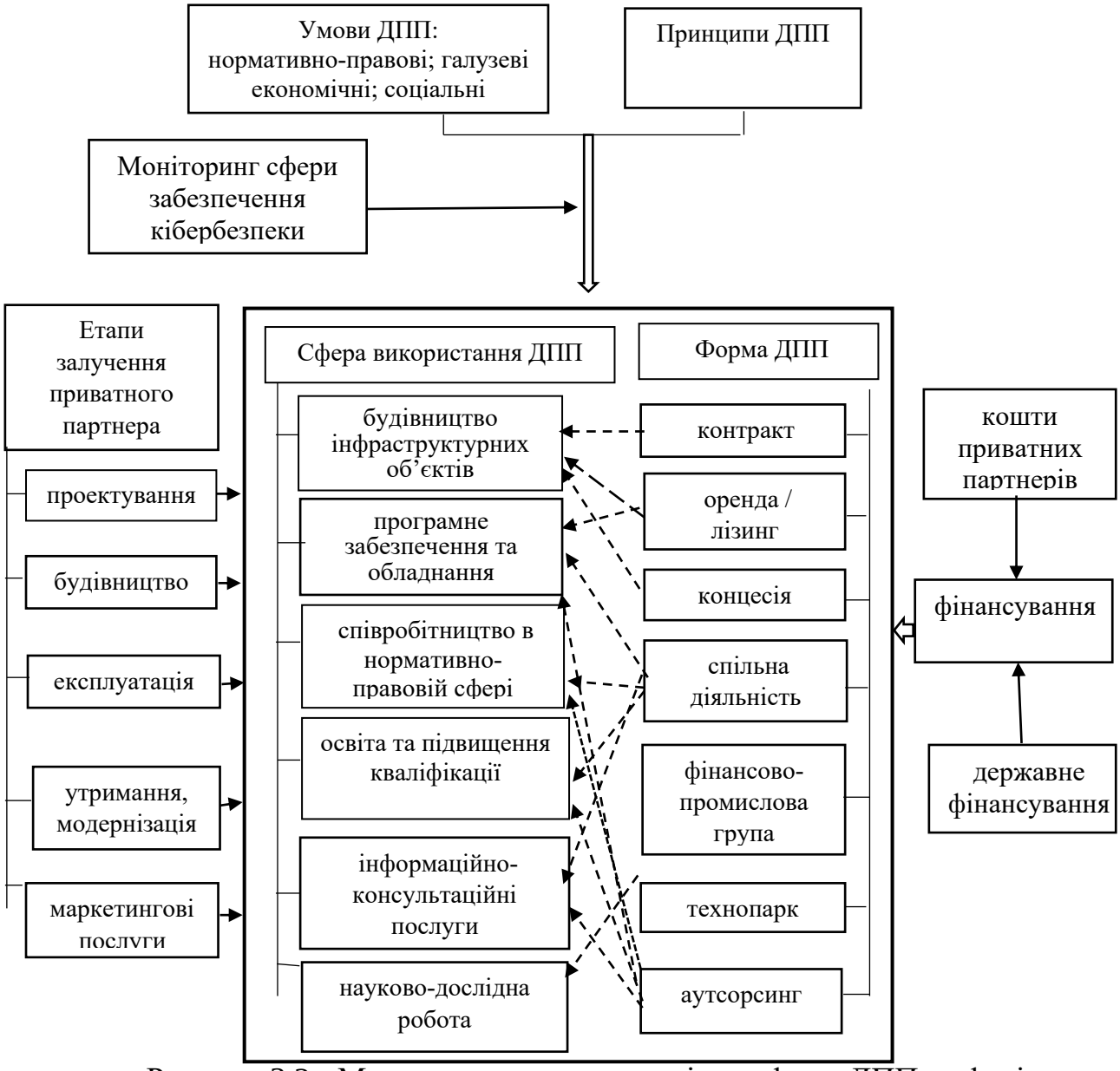

Рисунок 3.2 - Модель запровадження різних форм ДПП в сфері забезпечення кібернетичної безпеки

Примітка. Розроблено автором

розвиток ДПП при формуванні законодавчої бази, створенні відповідних галузевих стандартів в сфері кіберезахисту;

підтримка на урядовому рівні створення системи наукових досліджень та розробок, спрямованих на захист від кіберінцидентів;

запровадження та реалізація програмного підходу щодо побудови ефективного співробітництва з обміну інформацією у сфері кібербезпеки між державою та бізнесом;

створення та підтримка на основі ДПП національної системи обміну даними про кіберінциденти та відповідного реєстру;

створення механізму державної підтримки інновацій в сфері кібербезпеки з використанням механізмів ДПП;

створення системи безперервної освіти та підвищення рівня обізнаності щодо загроз у сфері кібербезпеки із використанням форм ДПП;

започаткування експертних обговорень, комунікаційних платформ, спільних проектів у форматі ДПП для формування довіри між сторонами.

В умовах стрімкого розвитку інформаційно-комунікаційних технологій та існування сучасних викликів та гібридних інформаційних загроз, наявні механізми не дозволяють державним структурам оперативно реагувати на зміни ситуації у кіберпросторі. Тому, представляється доцільним інтеграція зусиль громадянського суспільства в процесах забезпечення кібернетичної безпеки країни.

Зазначимо, що взаємодія між НУО та органами державної влади в сфері забезпечення кібернетичної безпеки здійснюється на основі використання сукупності форм, спираючись на принципи та базуючись на основних аспектах концепції міжсекторного партнерства, яка передбачає рівноправну взаємодію органів державної влади, НУО та підприємств при вирішенні проблем в сфері забезпечення кіберзахисту та належного рівня кібернетичної безпеки (рис. 3.3).

При цьому кожна зі сторін виконує специфічні функції:

органи державної влади здійснюють формування нормативно-правової бази, інституційне та ресурсне забезпечення;

НУО здатні ініціювати проекти, здійснювати функцію контроля за виконанням ініціатив (в тому числі державними органами та бізнесом);

додаткове фінансування, солідарна відповідальність за дотримання законодавства, вирішення ряду проблем (покращення умов праці, створення додаткових робочих місць).

Рисунок 3.3 - Форми взаємодії НУО та державних органів в сфері забезпечення кібернетичної безпеки

Примітка. Розроблено автором

Звертаючи увагу на формування державної політики забезпечення кібернетичної безпеки в умовах співробітництва України з НАТО та ЄС слід відзначити основні напрями його подальшого розвитку. А саме: опрацювання та врахування досвіду ЄС і НАТО при формуванні національної системи сертифікації в сфері забезпечення кібербезпеки, поглиблення державно-приватного партнерства; використання потенціалу Трастового фонду НАТО з кібербезпеки задля посилення технічної складової забезпечення кібернетичної безпеки; формування Плану реагування на надзвичайні ситуації в кіберпросторі; посилення міжвідомчого

співробітництва та ДПП, розробка механізму його практичного застосування; формування системи мотивації для фахівців, зайнятих у сфері кібербезпеки та кібероборони. Слід вказати, що для обґрунтованого формування державної політики забезпечення кібернетичної безпеки запропоновано застосування інструментів моделювання.

3.2. Механізм формування державної політики забезпечення кібернетичної безпеки

Запровадження державної політики представляється доцільним на основі запропонованої концепції, реалізація якої забезпечить змістовне наповнення механізму 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 та спрямований на формування безпечного кіберпростору, що передбачає забезпечення кібербезпеки особистості, організації та країни в цілому (рис. 3.4).

З метою запровадження цього механізму вважається доцільною така послідовність дій:

виявлення проблемних зон в сфері захисту критичної інформаційної інфраструктури або отримання інформації про реальні чи потенційні кіберзагрози;

виявлення джерела, аналіз факторів і причин, які спричиняють такі проблеми;

формулювання цілі та задач в сфері кіберзахисту;

визначення методів, інструментів досягнення поставленої мети;

визначення рівня ризиків, прогнозна оцінка можливості розв’язання зазначених проблем.

Рис. 3.4. Структура механізму формування державної політики забезпечення кібернетичної безпеки

Однак, практична реалізація даного механізму та його спрямування на формування безпечного кіберпростору представляється доцільним на основі програмно-цільового підходу [106, с. 124].

Враховуючи вищевказане, існує потреба у розробці та реалізації Державної програми забезпечення кібернетичної безпеки, яка являє комплекс організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та інших заходів.

Державна програма забезпечення кібернетичної безпеки має базуватись на поточній інформації та аналізу внутрішньодержавного стану. Всі зацікавлені сторони процесу забезпечення кібернетичної безпеки повинні звертатися до офіційних джерел, а також до академічних і галузевих досліджень, які надають відповідні дані, серед них: Євробарометр; ЄВРОПОЛ; статистика щодо кіберзлочинності ООН; управління та агенції національної статистики; інформація про кіберінциденти з різних джерел; галузеві дослідження комерційних фірм.

Зазначимо, що розробка державної програми має ґрунтуватись на системному підході і представляти собою динамічну гнучку модель, яка надає достовірну інформацію про існуючий рівень безпеки та показники вдосконалення і розвитку.

Порядок розробки програми забезпечення кібернетичної безпеки має ґрунтуватись на використанні технологій стратегічного управління (рис. 3.5).

Правову основу державної програми забезпечення кібернетичної безпеки складають:

Кодекс цивільного захисту України, Кримінальний кодекс України;

Закони України «Про національну безпеку України», «Про боротьбу з тероризмом», «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання», «Про об’єкти підвищеної небезпеки», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про державну таємницю», «Про

оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про правовий режим надзвичайного стану», «Про правовий режим воєнного стану»;

Рисунок 3.5. Порядок розробки державної програми забезпечення кібернетичної безпеки

Примітка. Розроблено автором

Указ Президента України від 16 січня 2017 року № 8 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури», Указ Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», Указ Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію

кібербезпеки України», резолюція Ради безпеки Організації об'єднаних націй від 13 лютого 2017 року № 2341 щодо захисту критичної інфраструктури від терористичних атак;

розпорядження Кабінету Міністрів України від 06.12.2017 № 1009 «Про схвалення Концепції створення державної системи захисту критичної інфраструктури».

Паспорт Державної програми забезпечення кібернетичної безпеки наведено в табл. 3.2.

Таблиця 3.2. Паспорт Державної програми забезпечення кібернетичної безпеки

Ініціатор розроблення	МВС України
Розробник програми	Міністерство оборони України
Співрозробники програми	Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, громадські організації
Відповідальний виконавець	Міністерство оборони України
Організації-співвиконавці програми	Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, розвідувальні органи; органи місцевого самоврядування, громадські організації
Мета	забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури України, запобігання проявам актів несанкціонованого втручання, прогнозування та запобігання кризовим ситуаціям з негативним впливом на об'єкти критичної інфраструктури, а також підвищення рівня захисту, удосконалення заходів безпеки від існуючих загроз
Термін реалізації програми	2020-2022
Джерела фінансування та загальний обсяг фінансування, необхідного для реалізації програми	державна фінансова підтримка, кошти державного та місцевих бюджетів; кошти недержавних підприємств та донорських міжнародних організацій. Загальний обсяг фінансування визначається наповненням програми
Очікувані результати виконання	створення державної системи кібернетичної безпеки, запровадження єдиних підходів до організації управління об'єктами критичної інфраструктури на державному та місцевому рівнях, визначення основ взаємодії залучених до забезпечення кібернетичної безпеки державних органів та суб'єктів господарювання, суспільства та громадян
Контроль за виконанням	Поточний моніторинг - Державна служба спеціального зв'язку та захисту інформації України. Контроль – Міністерство оборони України

Примітка. Розроблено автором

Водночас результати реалізації програми на всіх її етапах виступають як основа для подальшого розвитку шляхів удосконалення процесів забезпечення кібернетичної безпеки, визначення векторів подальшого розвитку, розробки відповідних заходів, планів, бюджетів.

Слід звернути увагу на доцільність коригування змісту програми у відповідності до виявлених в процесі розвідувальних дій або визначених в процесі моніторингу нових викликів та загроз в сфері кібернетичного захисту. Термін реалізації програми визначено з врахуванням нагальності та стратегічної важливості проблеми. Мінливість та непередбачуваність ситуації в сфері забезпечення кібернетичної безпеки унеможливило її етапність.

Реалізація програми дозволить забезпечити створення державної системи кібернетичної безпеки, запровадить єдині підходи до організації управління об’єктами критичної інфраструктури на державному та місцевому рівнях, визначить засади взаємодії залучених до забезпечення кібернетичної безпеки державних органів та суб’єктів господарювання, суспільства та громадян.

Ключові напрями реалізації державної програми забезпечення кібернетичної безпеки є: нормативно-правове та управлінсько-інституційне забезпечення; розвиток системи спеціалізованих досліджень та спеціалізованого консультування; налагодження співпраці та координація зусиль на урядовому рівні, серед громадських організацій, а також у межах міжнародних відносин.

Структурні елементи пропонованої державної програми забезпечення кібернетичної безпеки мають наступний вигляд.

На макрорівні – плани захисту та забезпечення кібернетичної безпеки на національному рівні (розробляється Національний план захисту кібернетичного простору, встановлюються вимоги до планування заходів

щодо захисту критичної інфраструктури, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань).

На мезорівні - органами державної влади розробляються і затверджуються галузеві плани та програми з протидії загрозам кібернетичної безпеки. Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури.

На мікрорівні - органи місцевого самоврядування забезпечують розробку, затвердження і виконання місцевих програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Ці програми включають заходи з забезпечення захисту та стійкості критичної інфраструктури, взаємодії суб'єктів системи захисту критичної інфраструктури, забезпечення інформаційної безпеки та кібербезпеки на об'єктах критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури.

Одним із перших кроків державної програми має бути оцінка та перегляд діючої системи управління «зверху-вниз» з макрорівня до мікрорівня. Цей крок проілюструє, наскільки установи та організації користуються та (або) беруть до уваги положення вимог законодавства, регуляторних актів або забезпечення відповідності в частині забезпечення кібернетичної безпеки.

Окремий етап – визначення потенційних фінансового та нефінансового впливу і наслідків кіберзлочинності та кібервійни повинні ґрунтуватися на системному управлінні кібербезпекою та відповідних заходах.

Після визначення потенційного впливу інцидентів, пов’язаних із кібербезпекою, необхідним є визначення загроз та вразливості, що можуть вимагати застосування загальних чи цільових положень систе5ми забезпечення кібернетичної безпеки.

Наступним етапом в процесі реалізації програми забезпечення кібернетичної безпеки є визначення та аналіз всіх загроз та інцидентів, (включаючи ті, що вважаються малоймовірними). Заходи на цьому етапі мають відображати ймовірну можливість того, що кіберзлочинці уникатимуть найочевидніших напрямків атаки, шукаючи менш очевидні напрями або найслабшу ланку ланцюга, а не найбільш ймовірну точку входу.

Окремим положенням програми є створення Національної бази даних об’єктів критичної інфраструктури, яка формується та ведеться Уповноваженим органом у сфері захисту критичної інфраструктури на основі пропозицій суб’єктів державної системи захисту критичної інфраструктури.

Заходи щодо кіберзахисту об’єктів критичної інфраструктури на всіх рівнях, а також захист технологічної інформації, що циркулює в автоматизованих системах об’єктів критичної інфраструктури, здійснюються відповідно до законодавства у сфері захисту інформації та кібербезпеки.

Повноваження суб’єктів державної системи захисту критичної інфраструктури щодо забезпечення кібербезпеки та кіберзахисту об’єктів критичної інфраструктури визначаються законодавством у сфері захисту інформації та кібербезпеки.

Реалізація програми передбачає взаємодію державної системи забезпечення кібернетичної безпеки з іншими системами захисту у сфері національної безпеки.

Для забезпечення стійкості критичної інфраструктури до загроз усіх видів, реалізації національних інтересів, функціонування суспільства та забезпечення соціально-економічного розвитку державна система забезпечення кібернетичної безпеки (у вигляді державного органу -

Ситуаційного центру забезпечення кібербезпеки Служби безпеки України з питань кібератак та кіберінцидентів, що загрожують сталому функціонуванню об'єктів критичної інформаційної інфраструктури) взаємодіє з іншими системами захисту у сфері національної безпеки, а саме:

1) з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, з територіальною та функціональною підсистемами, структурними підрозділами суб'єктів боротьби з тероризмом та Міжвідомчою координаційною комісією Антитерористичного центру при Службі безпеки України з питань боротьби з тероризмом та реагування на загрозу вчинення або вчинення терористичних актів;

2) з правоохоронними органами у сфері протидії злочинності;

3) з об'єднаною цивільно-військовою системою організації повітряного руху України, Українським центром планування використання повітряного простору та регулювання повітряного руху, Командуванням Повітряних Сил, Збройних Сил України з питань:

захисту повітряного простору, протиповітряної оборони важливих державних об'єктів та визначених об'єктів критичної інфраструктури;

взаємодії з припинення протиправних дій повітряних суден, які можуть використовуватися для вчинення терористичних актів у повітряному просторі України проти об'єктів критичної інфраструктури та важливих державних об'єктів;

4) з єдиною державною системою цивільного захисту, з постійно діючими функціональними і територіальними підсистемами та їх ланками, з Державною комісією з питань техногенно-екологічної безпеки та надзвичайних ситуацій та комісіями з питань техногенно-екологічної безпеки та надзвичайних ситуацій Автономної Республіки Крим, областей, м. Києва та Севастополя, з питань попередження, реагування та ліквідації на кризові ситуації на об'єктах критичної інфраструктури;

5) з державною системою фізичного захисту з питань захищеності та охорони ядерних установок, ядерних матеріалів, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів.

Контроль виконання Державної програми забезпечення кібернетичної безпеки передбачено за наступними напрямами:

дотримання визначених термінів;

визначення ефективності заходів;

оцінка ресурсного забезпечення, необхідного для реалізації заходів.

Реалізація державної програми стане важливим кроком на шляху формування ефективної законодавчої бази в сфері забезпечення кібернетичної безпеки, яка на основі вимог міжнародного законодавства та позитивного досвіду зарубіжних країн створить умови для безпечного кібернетичного простору.

ВИСНОВКИ

Таким чином, на підставі проведених наукових досліджень у магістерській роботі вирішено актуальне науково-практичне завдання у галузі державного управління щодо удосконалення державної політики забезпечення кібернетичної 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. Встановлено, що кібербезпека являє собою 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.

2. 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.

3. Проаналізовано основні статистичні показники, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах та організаціях України, що дозволило констатувати зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет та збільшення рівня використання інформаційно-комунікаційних технологій. Відзначено, що кількість злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, починаючи з 2014 року постійно зростала, сягнувши у 2017 році цифри 2573 злочини. Темп приросту за 2014-2017 роки склав 480,8%. За 2018 рік цей показник вже перевищив рівень 2016 року на 117,9 %. Випереджаюче зростання зареєстрованих кіберзлочинів, вплинуло на збільшення їх питомої ваги у загальній кількості злочинів в Україні, зберігаючи тенденції підвищення від 0,08 % у 2014 році до 0,51% у 2018, що є найвищим показником, починаючи з 2009 року. Аналіз структури злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, який здійснено на основі статистичної звітності за 2017 рік., дозволив констатувати, що зокрема у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільшу частку становлять ті, відповідальність за які передбачено ст. 361 Кримінального кодексу України – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (69,8 %).

4. Проведено оцінку державної подітики забезпечення кібернетичної безпеки в Україні. Встановлено, що в Україні запроваджено ряд важливих

кроків в сфері забезпечення кібербезпеки. Серед основних слід виокремити наступні: ратифікація Конвенції Ради Європи з кіберзлочинності; розробка Стратегії кібербезпеки; розвиток мережі команд реагування на комп'ютерні надзвичайні події (CERT) тощо. Значним кроком у забезпеченні кібербезпеки стало підписання у 2019 р. Меморандуму про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту між Центром кіберзахисту Національного банку України та Державним центром кіберзахисту ДССЗЗІ. Таке співробітництво спрямоване на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту.

Для кожної області України розраховано інтегральний 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.

5. Поглиблено й аргументовано концепцію державної політики забезпечення кібернетичної безпеки, яка представляє собою систему теоретичного базису таінструментального 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. 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. 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.

Отже, опрацьовані в цій роботі теоретичні положення та практичні пропозиції можуть підгрунтям для удосконалення механізму розробки та реалізації державної політики забезпечення кібернетичної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абдикеев Н. М., Аверкин А. Н., Ефремова Н. А. Когнитивная экономика в эпоху инноваций. *Вестник РЭА.* 2010. № 1. С. 3-20.

2. Акімова Л. М. Інструменти державного управління забезпечення економічної безпеки держави за суб'єктами економіки держави. *Державне управління та місцеве самоврядування : зб. наук. пр. ДРІДУ НАДУ при Президентові України*. 2018. Вип. № 3(38). С. 53-61.

3. Алексєєв В. М. Теоретичні засади взаємовідносин держави та суспільства в управлінні : монографія. Чернівці : Технодрук, 2012. 392 с.

4. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». К. : НІСД, 2017. 928 с.

5. Бакуменко В., Князєв В., Сурмін Ю. Методологія державного управління: проблеми становлення та подальшого розвитку. *Вісн. УАДУ*. 2003. № 2. С. 11-27.

6. 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.

7. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2(42). URL: http://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya-“kiberbezpeka” (дата звернення: 16.11.18).

8. Бараш Л. Кибербезопасность в Украине. Дискуссия. URL: http:// ko.com.ua/ kiberbezopasnost_v_ukraine_diskussiya_121089. (дата звернення: 18.03.18).

9. Бєлявська С. Ю. Організаційно-правові засади впровадження інновацій у судове управління в умовах інформаційного суспільства в Україні: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: 12.00.07. Київ, 2016. 21 с.

10. Боднар І. Р. Роль держави у формуванні інформаційної політики. Вісник ЛКА. Львів: Видавництво ЛКА. 2011. Вип. 34. Серія економічна. 2011. С. 291-296.

11. Бойко В.О. Досвід Німеччини у функціонуванні платформ державно-приватного партнерства в сфері кібербезпеки. Аналітична записка. Київ: НІСД, 2018. 42 с.

12. Большой экономический словарь: Под ред. А.Н. Азрилияна. – 5-е изд., перераб. и доп. М.: Институт новой экономики, 2002. 830 с.

13. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі. *Наука і оборона.* 2011. № 3. С. 35-42.

14. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

15. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка.* 2011. № 3 (26). С. 104-114.

16. Бурячок В.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. *Захист інформації.* 2013. Том 15, № 1. С. 5-12.

17. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: монографія. К.: НАУ, 2013. 432 с.

18. Бурячок В.Л., Хорошко В.О. Технологія прийняття рішень у складних соціотехнічних системах: монографія; під заг. ред. докт. техн. наук, проф. В.О. Хорошка. К.: ДУІКТ, 2012. 344 с.

19. Валовий регіональний продукт у 2017 році. Державна служба статистики України. URL: http://www.ukrstat.gov.ua/ (дата звернення: 19.02.18).

20. Вдовенко С., Данік Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*, 2019. № 1. С. 18-30.

21. В ЄС створять агентство із кібербезпеки та нові сертифікати для цифрових продуктів URL: https://www.unian.ua/science/2143199-v-es-stvoryat-agentstvo-iz-kiberbezpeki-ta-novi-sertifikati-dlya-tsifrovih-produktiv.html (дата звернення: 18.03.18).

22. Використання інформаційно-комунікаційних технологій на підприємствах України. Статистичний бюлетень за 2016 р. Відповідальна за випуск О. О. Кармазіна. Київ: Державна служба статистики України, 2017. 39с.

23. Використання інформаційно-комунікаційних технологій на підприємствах України. Статистичний бюлетень за 2017 р. Відповідальна за випуск О. О. Кармазіна. Київ: Державна служба статистики України, 2018. 38с.

24. Висновки і рекомендації щодо внесення змін до Закону України «Про основи національної безпеки України»: аналіт. записка Нац. Ін-ту стратегічних досліджень при Президентові України. URL: http://www.niss. gov.ua/articles/1775/ (дата звернення: 10.02.18)

25. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій. Виведення шахрайства з тіні URL: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf (дата звернення: 12.03.19)

26. Гнатенко А. І. Стратегічне планування у сфері державного управління: концептуальні підходи. *Державне управління та місцеве самоврядування: зб. наук. пр*. Дніпропетровськ: Вид-во ДРІ НАДУ , 2013. № 3(18). С. 51- 60.

27. Гнатюк С.Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/kiberbezpek-d3e61.pdf (дата звернення: 16.11.18).

28. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. Аналітичні матеріали. URL: https://www.niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya (дата звернення: 12.01.19).

29. Говлет М., Рамеш М. Дослідження державної політики: цикли та підсистема політики / пер. з англ. Олександра Рябова. Львів: Кальварія, 2004. 264 с.

30. Головне управління зв’язку та інформаційних систем Генерального штабу Збройних сил України; Міністерство оборони України.

URL: http://www.mil.gov.ua/index.ph p?part=department&lang=ua&sub=guz_is (дата звернення: 12.01.19).

31. Горелова Г.В., Захарова Е.Н., Радченко С.А. Исследование слабоструктурированных проблем социально-экономических систем: когнитивный подход : монография. Ростов-на-Дону: Изд-во РГУ, 2006. 332 с.

32. Государственно-частное партнерство в условиях инновационного развития экономики : монография / под ред. А. Г. Зельднера, И. И. Смотрицкой. Москва: ИЭ РАН, 2012. 212 с.

33. Государственные стратегии кибербезопасности. URL: https://www.securitylab.ru/analytics/429498.php. (дата звернення: 12.10.18).

34. Грабовий А. Закон про кібербезпеку та Стратегія кібербезпеки України. *Юрист & Закон.* 2017. № 26 URL: http://uz.ligazakon.ua/ua/magazine_article/ EA010553 (дата звернення: 18.02.17).

35. Грайворонський, М. В. Сучасні підходи до забезпечення кібернетичної безпеки. *Теоретичні і прикладні проблеми фізики, математики та інформатики:* Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, 21-23 травня 2015 р. м. Київ,. Київ : НТУУ «КПІ». 2015. С. 10-17.

36. Грищенко С. Підготовка та реалізація проектів публічноприватного партнерства : практичний посібник для органів місцевої влади та бізнесу. Київ: ФОП Москаленко О.М., 2011. 140 с.

37. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: монографія / за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.

38. Гудзь Ю. Кібербезпека чи інформаційна безпека КО IT для бізнеса. URL: https://ko.com.ua/kiberbezpeka_chi_informacijna_bezpeka_120068 (дата звернення: 29.05.17).

39. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О.С. Попова, 2018. 228 с.

40. Делія О. В. Фізичне середовище державної політики: теоретичний аналіз. *Теорія та практика державного управління*. 2017. № 4(59). С. 12-20.

41. Державна політика / Нац. акад. держ. упр. при Президентові України; ред. кол.: Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови). К.: НАДУ, 2014. 448 с.

42. Державна служба статистики України [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua.

43. Державне регулювання інноваційного розвитку економіки України: стратегічні пріоритети : монографія / за заг. ред. М. А. Латиніна. Х. : Вид-во ХарРІ НАДУ «Магістр», 2014. 320 с.

44. Державне управління в Україні: наукові, правові, кадрові та організаційні засади / за заг. ред. Н.Р. Нижник, В.М. Олуйка. Львів : Львів. політехніка, 2002. 352 с.

45. Державне управління : словн.-довід. / уклад. : В.Д. Бакуменко (кер. твор. кол.), Д.О. Безносенко, І.М. Варвар, В.М. Князєв; за заг. ред. В.М. Князєва, В.Д. Бакуменка. Київ : Вид-во УАДУ, 2002. 228 с.

46. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.

47. Деякі питання організації здійснення державно-приватного партнерства: Постанова КМУ від 11 квітня 2011 р. №384 URL: http://zakon.rada.gov.ua/laws/show/384-2011-п (дата звернення: 25.06.18).

48. Деякі питання щодо забезпечення участі громадськості у формуванні та реалізації державної політики: Постанова КМУ від 03 листопада 2011 р. № 996. URL: http://zakon3.rada.gov.ua/laws/show/ 996-2010-п (дата звернення: 23. 10.18).

49. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. на здобуття наук. ступеня д-ра юридич. Наук : 12.00.07. Запоріжжя, 2018. 40 с.

50. Діордіца І. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. *Підприємництво, господарство і право*. 2017. № 10. С. 206-211.

51. Діордіца І. Поняття та зміст національної системи кібербезпеки. *Національний юридичний журнал: теорія та практика*. 2016. Грудень. С.37-42.

52. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право*. 2017. № 14. С. 99-107.

53. Діордіца І. В. Поняття та зміст кібершпигунства URL: http://goal-int.org/ponyattya-tazmist-kibershpigunstva (дата звернення: 29.05.17).

54. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Видавничий дім «АртЕк», 2017. 107 с.

55. Досвід та перспективи впровадження державно-приватних партнерств в Україні та за кордоном / Б. Винницький, М. Лендьел, Б. Онищук та ін. Київ : К.І.С., 2008. 146 с.

56. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К.: НІСД, 2014. 328 с. URL: //www.niss.gov.ua/content/articles/files/ Dubov_mon-89e8e.pdf (дата звернення: 11.11.18).

57. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. К.: НІСД, 2011. 30 с.

58. Дубов Д. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. URL: http://www.niss.gov.ua/articles/294 (дата звернення: 14.01.18).

59. Европейское агентство по сетевой информационной безопасности (ENISA), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss (дата звернення: 19.12.18).

60. Енциклопедичний словник з державного управління / уклад.: Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін. Київ: НАДУ, 2010. 819 с.

61. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України; наук. ред. колегія: Ю.В. Ковбасюк (голова) та ін. К.: НАДУ, 2011. Т. 4: Галузеве управління / Наук.ред. колегія: М.М. Їжа (співголова), В.Г. Бодров (співголова) та ін. 2011. 648 с.

62. Євсеєв С. П., Рзаєв Х. Н., Мамедова Т. А., Самедов Ф. Г., Ромащенко Н.В. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Кібербезпека: освіта, наука, техніка*. 2018. №2. С. 47- 67.

63. Жиляєв І.Б., Семенченко А.І., Фурашев В.М. Інструменти державного стратегічного управління: національна програма інформатизації. *Інформація і право.* 2018. № 1(24). С. 44-58.

64. Жиляєв І.Б., Семенченко А.І. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. Стратегічні пріоритети. 2017. №4 (45). С. 55-64.

65. Запатрина И. В. Потенциал публично-частного партнерства для развивающихся экономик : монографія. Київ: Издательский дом Союза собственников жилья Украины, 2011. 152 с.

66. Запорожець О. Ю. Кібервійна: концептуальний вимір. *Актуальні проблеми міжнародних відносин.* 2014. Вип. 121. Частина І. С. 80-86.

67. Звонар В. П. Інституційні засади використання механізму міжсекторного партнерства в соціальній політиці України. *Проблеми і перспективи функціонування інноваційної системи держави в умовах глобалізації:* матеріали XIII міжнар. наук.-практ. конф., 27–28 верес. 2007 р., Луцьк / відп. ред. М. І. Карлін. Луцьк : РВВ „Вежа" Волин. держ. ун-ту ім. Лесі Українки, 2007. С. 118–120.

68. Золотар О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

69. Інформаційно-комунікаційні технології в публічному управлінні: словник-довідник / уклад. : В. М. Дрешпак, О. В. Кравцов, С. П. Кандзюба; за заг. ред. В. М. Дрешпака, О. В. Кравцова. Дніпропетровськ: ДРІДУ НАДУ, 2013. 132 с.

70. Кастельс М. Информационная эпоха, общество и культура; Пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.

71. Комар Ю. М. Атрибутивний науковий інструментарій — фундаментальна основа формування інноваційних механізмів державного управління. *Інвестиції: практика та досвід*. 2010. № 17. С. 99-103.

72. Конвенція про кіберзлочинність від 23 листопада 2001 р. *Офіційний вісник України*. 2007. № 65. Ст. 2535.

73. Кондратьєв Я. Ю., Ліпкан В. А. Концепція національної безпеки України: теоретико-правові аспекти зарубіжного досвіду. – К. : Національна академія внутрішніх справ України, 2003. 20 с.

74. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2007. 471с.

75. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

76. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2(19) С. 155-166.

77. Кравчук І. В. Оцінювання державної політики в Україні : монографія. К. : К.І.С., 2013. 272 с.

78. Кулинич А. А. Система когнитивного моделирования «КАНВА» / А. А. Кулинич URL: www.raai.org/kulinich/.../pages/ kanva2003.html (дата звернення: 23.10.18).

79. Купрій В. Процес творення державної політики як об’єкт наукових досліджень. *Політичний менеджмент.* 2007. № 5. С. 15-32.

80. Кучеренко О. О. Державна політика: теоретико-методологічні засади дослідження процесу формування та здійснення : автореф. дис. на здобуття наук. ступеня канд. з держ. упр. Київ, 2000. 20 с.

81. Ліпкан В. А., Ліпкан О. С., Яковенко О. О. Національна і міжнародна безпека в визначеннях та поняттях . К. : Текст, 2006. 256 с.

82. Лісовська Ю.П. Адміністративно-правова діяльність недержавних органів та організацій як структурних елементів системи забезпечення інформаційної безпеки. *Наукові праці МАУП*. 2014. Вип. 2 (41). С. 108-113.

83. Максимов В. И. Когнитивный анализ и управление развитием ситуаций. *Проблемы управления.* 2010. №3. С30-38.

84. Максимов В. И. Корноушенко Е. К., Качаев С. В. Когнитивные технологии для поддержки принятия управленческих решений. URL: www.iis.ru/events/19981130/ maximov.ru.html (дата звернення: 23.10.18).

85. Мартиненко В.М. Державне управління: шлях до нової парадигми (теорія та методологія): Моногр. Х. : Вид-во ХарРІ НАДУ "Магістр", 2003. 220с.

86. Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. *Інформаційна безпека, людина суспільство держава.* 2014. № 3(16). С.56-63.

87. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійнотермінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави*: Матеріали наук.-практ. конф., (22 березня 2011 р.). Київ, Вид-во НА СБ України, 2011. Ч. 2. С. 43-48.

88. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) Стандарт організації України. URL: https://kyianyn. files.wordpress.com/2010/12/nbu-27001.pdf (дата звернення: 18.03.18).

89. Методологія стратегічного планування в умовах глобальних загроз національній безпеці та міжнародній стабільності : монографія / авт. кол. : В. І. Абрамов, Т. В. Запорожець, Р. Р. Марутян та ін. ; за заг. ред. Л. М. Шипілової. Київ : НАДУ, 2018. 232 с.

90. Мостепанюк. А.В. Державно-приватне партнерство як механізм підвищення конкурентоспроможності економіки країни URL: http://www.nbuv.gov.ua/portal/soc_gum/tppe/2011_26/Zb26_38.pdf (дата звернення: 17.04.18).

91. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. URL: www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie (accessed: 17.04.18).

92. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанціонованого доступу» URL: http://am-soft.ua/files/KSZI/2.5-004-99.pdf (дата звернення: 18.03.18).

93. Нижник Н. Р., Дубенко С. Д., Мельниченко В. І. Державне управління в Україні: організаційно-правові засади. – Київ: Вид-во УАДУ, 2002. 164 с.

94. Никольская Л. И., Якимец В. Н. От конфликта к межсекторному партнерству. *Журнал социологии и социальной антропологии.* 2003. Т. 6. № 1. С. 96–112.

95. Нікітін В. В. Ресурсний потенціал становлення громадянського суспільства в Україні : монографія. Х. : Вид-во ХарРІ НАДУ, «Магістр», 2006. 248 с.

96. Обзор стран-членов Евросоюза: нормативные документы, связанные с надежностью работы телекоммуникационных сетей общего доступа. URL:http://www.enisa.europa.eu/activities/Resilience-and-CIIP /national-cyber- ecurity-strategies-ncsss (дата звернення: 12.10.18).

97. Ольвінська Ю. О., Самотоєнкова О.В. Ранговий кореляційний аналіз при дослідженні діяльності малих підприємств. *Економіка підприємства: сучасні проблеми теорії та практики*: збірник матеріалів IV Міжнародної науково-практичної конференції, 2015 р. Одеса, 2015. – С. 279-280.

98. Основні завдання Державної служби спеціального зв'язку та захисту інформації України. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=89831&cat_id=89828 (дата звернення: 18.03.18).

99. 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 .

100. 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.

101. 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.

102. Островий О. В. Інструменти державної політики забезпечення кібернетичної безпеки. *Електронне наукове фахове видання «Публічне адміністрування та національна безпека».* 2019. С. 13–21.

103. 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.

104. 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.

105. 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.

106. 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»).* 2019. Т. XX, вип. 310. С. 123–133.

107. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 11.03.19).

108. Павлюк А. П., Ляпін Д. В. Державно-приватне партнерство як механізм активізації інвестиційної діяльності в Україні. *Стратегічні*

пріоритети: науково-аналітичний щоквартальний збірник Національного інституту стратегічних досліджень. 2012. № 3 (24). С. 38 – 45.

109. Палагнюк Ю. В. «Державна політика» та «публічна політика»: теоретичний аспект. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія". Сер.: Державне управління*. 2012. Т. 181. Вип. 169. С. 63-67.

110. Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека. *Інформаційна безпека людини, суспільства, держави.* 2013. № 2 (12). С. 20–23.

111. Петренко І. Сутність державної політики та державних цільових програм. *Вече*. 2011. №10. С. 23-25. URL: http://www. viche.info/journal/2566/ (дата звернення: 10.11.18).

112. Петров В. В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети : наук.-аналіт. щокварт. зб.* 2013. № 4 (29). С. 127–131.

113. Піроженко Н. В. Механізми становлення та розвиток соціального партнерства органів публічної влади та неурядових некомерційних організацій : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.02. Одеса, 2007. 20 с.

114. Прангишвили И.В. Основы и проблемы когнитивного подхода**.** URL: http:// ipu.web-soft.ru/…/main_katalog_articles.pl (дата звернення: 10.11.18).

115. Програми НАТО «Удосконалення військової освіти» (Defence Education Enhancement Programme, DEEP). URL: https://www.nato.int/cps/en/natohq/news_ 159840.htm?selectedLocale=en (дата звернення: 25.11.18).

116. Про державно-приватне партнерство: Закон України від 01 липня 2010 р. №2404-VI URL: http: // zakon.rada.gov.ua (дата звернення: 25.06.18).

117. Проект Концепції інформаційної безпеки України. URL: http://www.osce.org/uk/fom/175056?download=true (дата звернення: 27.09.17).

118. Проект Стратегії забезпечення кібернетичної безпеки України. URL: www.niss.gov.ua/public/File/2013_nauk_ an_rozrobku/kiberstrateg.pdf (дата звернення: 27.09.17).

119. Про затвердження Кодексу системи передачі: Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 14 березня 2018 р. № 309 URL: https://zakon.rada.gov.ua/laws/show/v0309874-18/ed20180314#n72 (дата звернення: 10.09.17).

120. Про затвердження Порядку надання державної підтримки здійсненню державно-приватного партнерства: Постанова КМУ від 17.березня 2011 р. №279. URL: http://zakon.rada.gov. ua/laws/show/279-2011-п (дата звернення: 25.06.18).

121. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 URL: https://zakon.rada.gov.ua/laws/show/563-2016-п/ed20160823#n16 (дата звернення: 10.09.17).

122. Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2018 рік: Указ Президента України №89/2018 від 28.03.18 р. URL: https://www.president.gov.ua/documents/892018-23882 (дата звернення: 25.11.18).

123. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. *Відомості Верховної Ради України (ВВР),* 1994. N 31. Ст.286.

124. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту: Директива Ради ЄС 2008/114 від 8 грудня 2008 р. URL: https:// zakon.rada.gov.ua/laws/show/984_002-08/ed20081208#n41 (дата звернення: 30.07.17).

125. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. *Відомості Верховної Ради (ВВР).* 2018. № 31. ст.241.

126. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163- YIII. *Відомості Верховної Ради* (ВВР). 2017. № 45. ст.403.

127. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 р. «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 р. № 555/2015 URL: https://zakon.rada.gov.ua/laws/show/555/2015 (дата звернення: 10.02.18).

128. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України від 13 лютого 2017 р. № 32/2017. *Урядовий кур'єр.* 2017. № 28. Ст.232.

129. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента

України від 15 березня 2016 р. № 96/2016 . *Офіц. вісн. України.* 2016. № 23. Ст. 899.

130. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26 лютого 2016 р. № 68/2016 URL: http://zakon3.rada.gov.ua/laws/show/68/2016 (дата звернення: 17.03.18).

131. Про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них: звіт щодо України 2016/DGI/JP/3608 від 3 листопада 2016 р. URL: https://rm.coe.int/16806f3743 (дата звернення: 17.03.18).

132. Пухкал О. Г. Модернізація державного управління в контексті розвитку громадянського суспільства в Україні : монографія. К. : ВПЦ Київськ. ун-т, 2010. 287 с.

133. Романов В. Є., Рудік О. М., Брус Т. М. Державна політика: аналіз та механізми її впровадження. Дніпропетровськ: ДРІДУ НАДУ, 2003. 172 с.

134. Семенченко А.І., Мялковський Д.В., Станіславський Т.В. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. *Інвестиції. Практика та досвід.* 2018. № 18. С.87-94.

135. Сіпайло Л.Г., Сіпайло Н.А. Діяльність неурядових організацій у системі забезпечення інформаційної безпеки країни. *Глобальні та національні проблеми економіки*. 2017. Вип. 18. С.296-299.

136. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. К.: ВБ «Аванпост-Прим», 2012. 214 с.

137. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. URL: https://www.kas.de/veranstaltungen/detaiI/-

/content/ukraine-nato-nichtmilitaerische- zusammenarbeit-als-gemeinsame-antwort-auf-hybride-bedrohungen (дата звернення: 11.02.19).

138. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности. URL: http://www.crime–research.ru/articles /starostina (дата звернення: 10.02.18).

139. Статистичний збірник «Регіони України 2017 р.»; за ред. І.Є. Вернера. Ч.2. Київ: Державна служба статистики України, 2017, 687 с.

140. Статистичний щорічник України за 2016 рік:; За редакцією І. Є. Вернера; Відповідальний за випуск О. А. Вишневська. Київ: Державна служба статистики України, 2017. 611 с.

141. Стратегічні комунікації : словник / за заг. ред. доктора юридичних наук В. А. Ліпкана. К. : ФОП Ліпкан О.С., 2016. 416 с.

142. Стратегічний оборонний бюлетень України. URL: http://zakon3.rada. gov.ua/laws/show/240/2016/paran10#n10ь (дата звернення: 11.02.19).

143. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект. URL: http : // www. nbuv.gov.ua/portal/natural/vkhnu / Pravo / 2009 (дата звернення: 11.01.17).

144. Тертичка В. В. Державна політика: аналіз і впровадження в Україні : автореф. дис. на здобуття наук. ступеня д-ра наук. з держ. управління : 25.00.01. Київ, 2004. 36 с.

145. Тертичка В.В. Державна політика: аналіз здійснення в Україні: монографія. К.: Основи, 2002. 750 с.

146. Тімкін І. Ф., Новікова Н. Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: http : // www. er.nau.edu.ua (дата звернення: 11.05.18).

147. Ткачук Н.А. Кібербезпека у контексті актуальних змін до стратегічних документів у сфері національної безпеки і оборони. *Вісник Прокуратури.* 2016. №3. С.56-64.

148. Ткачук Н.А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки. *Інформація і право.* 2018. Т.4 Вип.27. С. 104-111.

149. Токарева В. І. Про деякі аспекти розвитку механізмів реалізації державної політики у сфері соціально-трудових відносин. *Економіка будівництва і міського господарства*. 2009. №2. С. 75–80.

150. Толуб'як В. С. Єдність державного регулювання і стратегічного управління: аспект сталого розвитку регіонів. *Інвестиції: практика та досвід.* 2018. № 10. С.83-87.

151. Тоффлер Элвин Третья волна. Перевод на русский язык: А. Мирер, И. Москвина-Тарханова, В. Кулагина-Ярцева, Л. Бурмистрова, К. Бурмистров, Е. Комарова, А. Микиша, Е. Руднева, Н. Хмелик. М., 2010, 784с.

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

153. Трансформація політико-управлінських відносин у державах Центрально-Східної Європи в процесі європейської інтеграції: уроки і досвід для України : монографія; за ред. Д. І. Дзвінчука. Івано-Франківськ : Місто НВ, 2013. 488 с.

154. Україна. Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги. URL: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf (дата звернення: 14.03.19).

155. Україна в координатах східного партнерства 2017-2020 р.р. URL: http://eap-csf.org.ua/wp-content/uploads/2017/10/Report_Ukrainian.pdf (дата звернення: 25.11.18).

156. Україна у цифрах 2016. Статистичний збірник; За редакцією І. Є. Вернера; Відповідальний за випуск О. А. Вишневська. Київ.: Державна служба статистики України, 2017. 240 с.

157. Усаченко Л. М. Органи державної влади та неурядові організації регіонів України: сучасні форми та методи взаємодії. *Університетські наукові записки: часоп. Хмельниц. ун-ту упр. та права.* Хмельницький : Вид-во Хмельниц. ун-ту упр. та права, 2008. Вип. 3 (27). С. 358-363.

158. Усаченко Л. Принципи системи взаємовідносин органів державної влади з неурядовими організаціями. URL: http:// www.nbuv.gov.ua/e-journals/Patp/ 2009_2/09 ulmvno.pdf (дата звернення: 25.11.18).

159. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162-169.

160. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. *Інформація і право: науковий журнал.* К.: НДЦПІ НАПрН України, 2012. № 1(4). С.46– 56.

161. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове,*

нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2004. №8. С.30–33.

162. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 312-320.

163. Шилепницький П. І. Державно-приватне партнерство: теорія і практика : монографія. Чернівці : Інститут регіональних досліджень НАН України, 2011. 455 с.

164. Шпачук В.В. Вплив міжнародних організацій на механізми антикризового управління держав. *Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління»*. 2018. Том 29 (68), Вип. 2. С. 124-128.

165. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом. URL: http://www.crime-research.ru/library/chetilov.htm (дата звернення: 11.02.19).

166. Энциклопедический словарь: под ред. Д. И. Валентей. М.: Советская энциклопедия, 1985. 608 с.

167. Юлдашев О. Х. Проблеми вдосконалення державної регуляторної політики в Україні. Київ: МАУП, 2005. 336 с.

168. Янковский А. Що не так з проектом про кібербезпеку та як його вдосконалити. URL: https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci (дата звернення: 18.03.18).

169. Agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats URL: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (accessed: 16.01.19).

170. Anderson J. Public policymaking. N.-Y.: Houghton Mif in Company, 1997. 123 c.

171. 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. C. 8–16.

172. Bell D. The Social Framework of the Information Society. Oxford, 1980, 650 c.

173. BSA - Software Alliance. URL: http://www.bsa.org/about-bsa (accessed: 16.01.19).

174. Canada's Cyber Security Strategy: For a stronger and more prosperous. Canada. – Her Majesty the Queen in Right of Canada, 2010. 14 c. URL: www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (accessed: 15.04.18).

175. Canadian - Government of Canada Publications. URL: http://publications.gc.ca/site/eng/3 (accessed: 11.11.18).

176. CIP Standards. URL: http://www.nerc.com/pa/Stand/Pages/ CIPStandards.aspx. (accessed: 15.02.18).

177. Cyber security strategy. – Commonwealth of Australia. Australia: Australian Government, 2009. URL: www.ag.gov.au/RightsAndProtections/ CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-20for%20website.pdf (accessed: 17.04.18).

178. Cyber Security Strategy for Germany. Berlin : Federal Ministry of the Interior, 2011. 15 c. URL: www.cio.bund.de/SharedDocs/Publikationen/DE/ Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (accessed: 15.04.18).

179. Cyber Security Strategy for Germany. URL: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (accessed: 11.11.18).

180. Cyber Security Strategy of the Czech Republic. URL: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF (accessed: 12.10.18).

181. Digital in 2018: звіт. URL: https://www.slideshare.net/DataReportal/digital-2018-ukraine-january-2018 (дата звернення: 14.04.18).

182. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently. URL: http://web.ebscohost.com (accessed 18.05.17).

183. Gates B. Business and the Speed of Thought: Level 6. London: Pearson Education Limited, 2008. 112 c.

184. Growing pains 2018 Global CEO Outlook. KPMG International. URL: kpmg.com/CEOoutlook (accessed: 11.03.19).

185. Hird progress report on the implementation of the common set of proposals endorsed by EU and NATO. URL: htlps://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018 (accessed: 17.03.19).

186. Information systems defence and security: France's strategy. French Network and Information Security Agency, 2011. C. 23. URL: www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf (accessed:15.04.18).

187. International Strategy for Cyberspace. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 11.12.18).

188. Internet Security Threat Report. 2017. Volume 23 URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en. pdf (accessed: 15.02.19).

189. Internet World Stats. URL: https://www.internetworldstats.com /stats.htm (accessed 18.12.18).

190. ISO/IEC 27000 family - Information security management systems URL: https://www.iso.org/isoiec-27001-information-security.html (accessed: 15.02.18).

191. Luiijf H.A.M., Besseling K., Spoelstra M., de Graaf P. Ten National Cyber Security Strategies: *CRITIS 2011 – 6th International Conference on Critical information infrastructures Security,* September 2011. Berlin, Heidelberg, 2013. P. 55-61.

192. Manley Max Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. *Journal of Strategic Security*. 2015. Volume 8. No. 3. P. 85-98. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article= 1478&context=jss (accessed: 14.02.19).

193. National center of Incident readiness and Strategy for Cybersecurity. URL: http://www.nisc.go.jp/eng/ (accessed: 01.03.18).

194. National Cyber Security Strategies. URL: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_ PATAIS. pdf (accessed: 14.10.18).

195. National Cyber Security Strategy and 2013-2014 Action Plan. Republic of Turkey: Ministry of Transport, Maritime Affairs and Communications, 2013. C. 47. URL: www.ccdcoe. org/strategies/TUR_ CyberSecurity.pdf (accessed: 15.04.18).

196. NCSI. URL: https://ncsi.ega.ee/ncsi-index/?order=rank (accessed:14.03.19).

197. NIST Releases Version 1.1 of its Popular Cybersecurity Framework URL: https://www.nist.gov/ cyberframework/draft-version-11 (accessed: 15.02.18).

198. Norton Cyber Security Insights Report 2017. Global Results 2017. URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf (accessed: 15.02.19).

199. Ostrovoy A. Main directions for the development of the state policy in the field of cyber security. *Science and society : Fadette editions. 2019.* C. 75–78.

200. Ostrovoy A. Analysis of the conditions for the state policy formation to ensure kibernetic security in Ukraine. *Public management*. 2019. № 2(17) – March, 2019.

201. Public Private Partnerships. Cooperative models. URL: https://www.enisa.europa. eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport (accessed: 17.11.18).

202. ROADMAP: Proposal on a European Strategy for Internet Security. URL: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf (accessed: 19.12.18).

203. Stratégie de la France. URL: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011 (accessed: 14.10.18).

204. The G-Cloud framework on the Digital Marketplace. URL: https://www.gov.uk/guidance/the-g-cloud-framework-on-the-digital-marketplace (accessed: 14.02.19).

205. The National Cyber Security Strategy (NCSS). URL: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 (accessed: 18.11.18).

Виконала: студентка магістратури спеціальності 281 Публічне управління та адміністрування заочної форми навчання
«____» грудня 2020 р. _____ Підпис А.В. Глупак Ініціали, прізвище

Науковий керівник
доцент кафедри публічного управління та адміністрування, к.е.н.
«____» грудня 2020 р. _____ Підпис Л.В. Омельчук Ініціали, прізвище

Робота допущена до захисту:
Завідувач кафедри публічного управляння та адміністрування
д.н.держ.упр., доцент
«____» грудня 2020 р. _____ Підпис Е.В. Щепанський Ініціали, прізвище

Додаток А

Таблиця А.1. Інструменти управлінського впливу на процеси забезпечення кібернетичної безпеки

Види інструментів	Характеристика інструментів
Адміністративні	контроль за виконанням законодавства в сфері кіберзахисту; виявлення і припинення незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у кіберпросторі; стандартизація та сертифікація
Соціально-економічні	розвиток соціально-економічних процесів в країні; розширення та модернізація відповідної інфраструктури; інвестування коштів у розвиток новітніх інформаційних технологій і сучасних засобів і систем захисту інформаційних ресурсів
Нормативно-правові	Міжнародні документи у сфері кібернетичної безпеки, які ратифіковано країною; формування національної нормативно-правової бази (Конституція України, кодекси, закони, укази Президента України, постанови та розпорядження КМУ та Верховної Ради України; накази й розпорядження), механізмів її запровадження; узгодження положень законодавства в сфері кібербезпеки з нормами кримінального, адміністративного, цивільного права.
Фінансові	запровадження пільгового кредитування та фінансування проектів, спрямованих на захист критичної інфраструктури
Організаційні	залучення НУО до вирішення проблем в сфері кіберзахисту; формування та реалізація відповідних програм; співробітництво з іншими державами в сфері забезпечення кібернетичної безпеки; підготовка та підвищення квалфікації кадрів; дослідження та імплементація світового досвіду попередження кіберінцидентів та протидії кібератакам; запровадження державноприватного партнерства в сфері забезпечення кібербезпеки; розвиток інфраструктури кіберзахисту; стимулювання освітньої та науководослідної діяльності в сфері кіберзахисту
Інформаційні	дослідження проблем в сфері кіберзахисту; розповсюдження інформації серед громадян щодо безпечної поведінки у кіберпросторі

Примітка. Складено автором на основі [2, с. 54; 10, с.292; 26, с.52; 44; с.49; 54, с.37] та удосконалено

Додаток Б

Таблиця Б.1

Напрями використання мережі Інтернет (за даними 2017 року) *(од)*

	Кількість підприємств, які мали доступ до мережі Інтернет	З них використовували мережу Інтернет для							
		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 фінан-сових послуг
Усього	**39582**	**38929**	**12048**	**34663**	**18704**	**31571**	**20158**	**38227**	**15535**
Переробна промисловість	9917	9792	3215	9012	4927	7958	5049	9604	3952
Постачання електроенергії, газу, пари та кондиційованого повітря	644	637	192	585	305	576	354	629	299
Водопостачання; каналізація, поводження з відходами	1053	1034	169	926	464	913	457	994	431
Будівництво	4041	3977	824	3589	1761	3033	1888	3893	1567
Оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів	9876	9732	3400	8943	4926	7954	5353	9651	3894
Транспорт, складське господарство, поштова та кур'єрська діяльність	3215	3156	937	2676	1415	2489	1539	3074	1254
Тимчасове розміщування й організація харчування	1178	1148	246	980	506	893	580	1123	423
Інформація та телекомунікації	1785	1770	939	1606	1067	1535	1053	1750	805
Операції з нерухомим майном	2550	2483	464	1939	878	1913	1114	2420	815
Професійна, наукова та технічна діяльність	2474	2440	1024	2169	1265	2094	1422	2381	1020
Діяльність у сфері адміністративного та допоміжного обслуговування	2790	2701	613	2181	1160	2163	1316	2651	1055
Надання інших видів послуг	59	59	25	56	30	50	33	57	20

Примітка. Складено автором за даними [23; 42]

Додаток В

Таблиця В.1 Дані про зареєстровані у розрізі регіонів України упродовж 2017 року кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку (ст.ст. 361 - 363-1 КК України) та результати їх досудового розслідування*

Регіон	Зареєстровано	Кримінальні правопорушення, у яких провадження закрито		Обліковано** кримінальних правопорушень у звітному періоді	з них,			Кримінальні правопорушення, за якими провадження направлені до суду (з урахуванням проваджень минулих років)	Виявлено осіб, які вчинили кримінальні правопорушення
		усього	у т.ч. за ч.1 п.п. 1,2,4,6 ст.284 КПК України		кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)	кримінальні правопорушення у провадженнях досудове розслідування у яких зупинено відповідно до ст.280 КПК України			
						коли місцезнаходження підозрюваного невідомо	у зв'язку з виконанням процесуальних дій в межах міжнародного співробітництва		
Україна	**3178**	**605**	**605**	**2573**	**1426**	**77**	**54**	**1076**	**168**
Області									
Вінницька	33	8	8	25	16	0	4	7	7
Волинська	78	1	1	77	9	0	4	66	8
Дніпропетровська	42	5	6	36	25	0	0	12	6
Донецька	87	7	7	80	42	3	0	35	2
Житомирська	23	10	10	13	6	0	2	5	1

Продовження табл.В.1

Закарпатська	38	1	1	37	9	2	2	24	6
Запорізька	20	10	10	10	7	1	1	6	2
Івано-Франківська	146	5	5	141	36	0	0	106	8
Київська	246	85	85	161	154	0	4	5	6
Кіровоградська	45	17	17	28	25	0	1	1	1
Луганська	40	3	3	37	36	0	0	2	2
Львівська	216	15	15	201	36	11	3	155	27
Миколаївська	128	10	10	118	30	0	1	103	6
Одеська	102	17	17	85	38	0	14	34	5
Полтавська	55	8	8	47	10	0	1	36	2
Рівненська	60	10	10	50	25	3	4	28	10
Сумська	19	9	9	10	4	0	1	5	5
Тернопільська	14	5	5	9	9	0	0		
Харківська	60	12	12	48	11	0	1	40	6
Херсонська	41	15	15	26	16	0	0	6	5
Хмельницька	39	3	3	36	8	0	0	30	4
Черкаська	133	9	9	124	17	1	0	108	16
Чернівецька	272	4	4	268	37	27	3	206	18
Чернігівська	32	7	7	25	16	0	2	7	5
м. Київ	1209	328	328	881	804	29	1	49	10

*Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя та частини зони проведення ООС

** Без урахування кримінальних правопорушень, виключених з обліку у зв’язку із закриттям провадження на підставі п.п. 1,2,4,6 ч.1 ст. 284 КПК України

Примітка. Складено автором за даними [107; 142]

Продовження додатка В

Таблиця В.2 Дані про зареєстровані у розрізі регіонів України упродовж січня-березня 2018 року кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку (ст.ст. 361 - 363-1 КК України) та результати їх досудового розслідування*

Регіон	Зареєстровано	Кримінальні правопорушення, у яких провадження закрито		Обліковано** кримінальних правопорушень у звітному періоді	з них,			Кримінальні правопорушення, за якими провадження направлені до суду (з урахуванням проваджень минулих років)
		усього	у т.ч. за ч.1 п.п. 1,2,4,6 ст.284 КПК України		кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)	кримінальні правопорушення у провадженнях досудове розслідування у яких зупинено відповідно до ст.280 КПК України		
						коли місцезнаходження підозрюваного невідомо	у зв'язку з виконанням процесуальних дій в межах міжнародного співробітництва	
1	2	3	4	5	6	7	8	9
Україна	**996**	**14**	**14**	**982**	**486**	**105**	**0**	**516**
Області								
Вінницька	19	1	1	18	6	0	0	14
Волинська	2	0	0	2	2	0	0	1
Дніпропетровська	12	0	0	12	11	0	0	2
Донецька	14	0	0	14	13	0	0	1
Житомирська	4	0	0	4	4	0	0	0
Закарпатська	23	0	0	23	13	0	0	10
Запорізька	17	1	1	16	6	0	0	12

Продовження табл.В.2

1	2	3	4	5	6	7	8	9
Івано-Франківська	11	0	0	11	5	0	0	33
Київська	21	0	0	21	21	0	0	78
Кіровоградська	26	0	0	26	2	0	0	24
Луганська	5	0	0	5	5	0	0	0
Львівська	50	1	1	49	15	3	0	35
Миколаївська	92	0	0	92	79	0	0	13
Одеська	230	1	1	229	45	0	0	184
Полтавська	25	1	1	24	24	0	0	0
Рівненська	65	0	0	65	5	0	0	61
Сумська	4	0	0	4	4	0	0	7
Тернопільська	6	2	2	4	2	0	0	5
Харківська	16	2	2	14	13	0	0	3
Херсонська	21	1	1	20	20	0	0	0
Хмельницька	15	0	0	15	12	0	0	5
Черкаська	148	0	0	148	40	102	0	8
Чернівецька	33	0	0	33	17	0	0	17
Чернігівська	13	0	0	13	13	0	0	0
м. Київ	124	4	4	120	119	0	0	3

*Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя та частини зони проведення ООС

** Без урахування кримінальних правопорушень, виключених з обліку у зв’язку із закриттям провадження на підставі п.п. 1,2,4,6 ч.1 ст. 284 КПК України

Примітка. Складено автором за даними [107; 142]

Продовження додатка В

Таблиця В.3. Відомості про осіб, які вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) за 2017 рік*

Регіон	Виявлено осіб, які вчинили кримінальні право-порушення (з урахуванням минулих років) **	Характеристика виявлених осіб, які вчинили кримінальні правопорушення									
		за віком на час вчинення кримінального правопорушення						за віком на час вчинення кримінального правопорушення			
		16-17 років	18-28 років	29-39 років	40-54 років	55-59 років	60 років і більше	повна вища і базова вища	професійно-технічна	повна загальна середня та базова загальна середня	початкова загальна та без освіти
1	2	3	4	5		7	8	9	10	11	12
Україна	**168**	**4**	**62**	**62**	**34**	**4**	**2**	**100**	**13**	**54**	**1**
Області											
Вінницька	7	0	2	3	2	0	0	3	1	3	0
Волинська	8	0	5	0	3	0	0	6	0	2	0
Дніпропетровська	6	0	1	4	1	0	0	3	2	1	0
Донецька	2	0	1	1	0	0	0	1	0	1	0
Житомирська	1	0	0	0	1	0	0	1	0	0	0
Закарпатська	6	0	2	3	1	0	0	5	0	1	0
Запорізька	2	0	0	0	2	0	0	0	1	1	0
Івано-Франківська	8	0	3	5	0	0	0	5	0	3	0
Київська	6	0	2	1	1	1	1	6	0	0	0
Кіровоградська	1	0	0	0	1	0	0	0	0	1	0
Луганська	2	0	1	0	1	0	0	2	0	0	0
Львівська	27	1	9	14	2	1	0	20	3	4	0
Миколаївська	6	0	1	4	1	0	0	4	0	2	0
Одеська	5	0	2	2	1	0	0	4	0	0	1

Продовження табл. В.3

1	2	3	4	5	6	7	8	9	10	11	12
Полтавська	2	0	1	0	0	1	0	1	0	1	0
Рівненська	10	0	6	3	1	0	0	7	1	2	0
Сумська	5	0	3	1	1	0	0	2	0	3	0
Тернопільська	0	0	0	0	0	0	0	0	0	0	0
Харківська	6	1	2	1	2	0	0	3	0	3	0
Херсонська	5	0	2	1	2	0	0	3	0	2	0
Хмельницька	4	0	1	3	0	0	0	2	0	2	0
Черкаська	16	0	11	4	1	0	0	3	4	9	0
Чернівецька	18	1	1	6	8	1	1	11	0	7	0
Чернігівська	5	0	2	2	1	0	0	0	1	4	0
м. Київ	10	1	4	4	1	0	0	8	0	2	0

*Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя та частини зони проведення ООС

** За закінченими розслідуванням кримінальними провадженнями

Складено автором за даними [107; 142]

Продовження додатка В

Таблиця В.4. Відомості про осіб, які вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) за січень-березень 2018 року *

Регіон	Виявлено осіб, які вчинили кримінальні право-порушення (з урахуванням минулих років) **	Характеристика виявлених осіб, які вчинили кримінальні правопорушення									
		за віком на час вчинення кримінального правопорушення						за віком на час вчинення кримінального правопорушення			
		16-17 років	18-28 років	29-39 років	40-54 років	55-59 років	60 років і більше	повна вища і базова вища	професійно-технічна	повна загальна середня та базова загальна середня	початкова загальна та без освіти
1	2	3	4	5	6	7	8	9	10	11	12
Україна	**63**	**0**	**24**	**3**	**15**	**1**	**0**	**31**	**13**	**18**	**1**
Області											0
Вінницька	2	0	0	2	0	0	0	2	0	0	0
Волинська	2	0	2	0	0	0	0	0	0	2	0
Дніпропетровська	2	0	1	1	0	0	0	1	0	1	0
Донецька	1	0	1	0	0	0	0	0	0	1	0
Житомирська	0	0	0	0	0	0	0	0	0	0	0
Закарпатська	5	0	0	3	2	0	0	3	0	2	0
Запорізька	4	0	4	0	0	0	0	1	1	2	0
Івано-Франківська	1	0	0	1	0	0	0	1	0	0	0
Київська	3	0	1	2	0	0	0	1	0	2	0
Кіровоградська	1	0	0	0	1	0	0	0	1	0	0
Луганська	0	0	0	0	0	0	0	0	0	0	0
Львівська	9	0	2	3	3	1	0	6	2	0	1
Миколаївська	4	0	0	0	4	0	0	0	4	0	0
Одеська	2	0	0	2	0	0	0	2	0	0	0

Полтавська	0	0	0	0	0	0	0	0	0	0	0

Продовження табл. В.4

1	2	3	4	5	6	7	8	9	10	11	12
Рівненська	4	0	1	1	2	0	0	3	0	1	0
Сумська	1	0	1	0	0	0	0	0	1	0	0
Тернопільська	5	0	2	2	1	0	0	4	1	0	0
Харківська	3	0	0	3	0	0	0	1	2	0	0
Херсонська	0	0	0	0	0	0	0	0	0	0	0
Хмельницька	5	0	5	0	0	0	0	1	0	4	0
Черкаська	2	0	0	2	0	0	0	1	1	0	0
Чернівецька	5	0	2	1	2	0	0	3	0	2	0
Чернігівська	0	0	0	0	0	0	0	0	0	0	0
м. Київ	2	0	2	0	0	0	0	1	0	1	0

*Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя та частини зони проведення ООС

** За закінченими розслідуванням кримінальними провадженнями

Складено автором за даними [107; 142]

Додаток Г

Таблиця Г.1. Вихідні дані для аналізу взаємозв’язків соціально-економічного розвитку регіонів та рівня кібернетичних загроз (2017 р.)*

№ з/п	Регіон	Зареєстровані кримінальні правопорушення у сфері використання ЕОМ, одиниць	Валовий регіональний продукт на одну особу, грн	Капітальні інвестиції в інформа-цію та телекому-нікації, млн.грн	Кількість абонентів мережі Інтернет, тис. осіб	Кількість підприємств, які займаються інноваційною діяльністю (придбання машин, обладнання, програмного забезпечення), одиниць	Кількість абонентів мобільного зв’язку, тис. осіб	Валова додана вартість інформації та телекомунікації (у фактичних цінах), млн.грн
1	Вінницька	33	58384	58,72	438,7	12	1470,9	2333
2	Волинська	78	49987	7,04	241,5	9	1276,3	541
3	Дніпропетровська	42	97137	85,81	761,3	40	4238,2	5237
4	Донецька	87	39411	432,52	880,9	18	6604,7	1791
5	Житомирська	23	49737	4,23	336,0	10	1174,0	1149
6	Закарпатська	38	34202	11,24	196,8	7	1458,0	552
7	Запорізька	20	75306	31,76	453,1	18	2382,5	1836
8	Івано-Франківська	146	46312	19,42	225,9	19	1572,1	866
9	Київська	246	90027	34,49	609,1	28	1621,8	2997
10	Кіровоградська	45	55183	7,32	164,8	20	1192,6	525
11	Луганська	40	13883	4,01	282,3	2	3284,7	400
12	Львівська	216	58221	241,06	780,8	37	2765,9	7761
13	Миколаївська	128	60549	11,18	420,4	17	1591,7	1204
14	Одеська	102	62701	289,9	1938,6	27	3221,9	3723
15	Полтавська	55	106248	15,86	296,7	17	2004,7	1058
16	Рівненська	60	42038	6,1	227,9	7	1140,4	611
17	Сумська	19	51419	6,95	201,2	16	1520,2	763
18	Тернопільська	14	38593	14,3	181,8	23	889,3	605
19	Харківська	61	69489	196,34	706,8	63	4121,5	9118
20	Херсонська	41	45532	4,34	213,0	9	1598,5	655
21	Хмельницька	39	49916	4,01	253,2	6	1033,2	735
22	Черкаська	133	59697	5,01	364,5	21	1342,6	1290
23	Чернівецька	272	31509	5,90	137,5	6	1135,0	547
24	Чернігівська	32	5519	4,54	342,7	9	1316,3	992
25	м. Київ	1209	238622	1066,2	2397,1	59	5905,3	63007

*Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя та частини зони проведення ООС
* Складено автором на основі [4; 19; 42; 107; 139; 140; 156]

Продовження додатка Г

Таблиця Г.2. Система стандартизованих показників та інтегральні показники рівня кібернетичних загроз за регіонами України в 2017 році

Область	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	$\overline{Z}$
Вінницька	0,8402	0,6583	0,5288	1,048	1,749	1,667	1,083
Волинська	0,4626	0,5712	0,1226	1,224	14,592	2,222	3,197
Дніпропетровська	1,4582	1,8967	1,187	0,630	1,197	0,500	1,146
Донецька	1,6872	2,9558	0,2672	1,553	0,238	1,111	1,303
Житомирська	0,6436	0,5254	0,2604	1,230	24,286	2,000	4,826
Закарпатська	0,3769	0,6525	0,1251	1,789	9,140	2,857	2,491
Запорізька	0,8678	1,0662	0,4162	0,813	3,235	1,111	1,253
Івано-Франківська	0,4327	0,7036	0,1963	1,321	5,290	1,053	1,499
Київська	1,1667	0,7258	0,6793	0,680	2,979	0,714	1,158
Кіровоградська	0,3157	0,5337	0,1190	1,109	14,034	1,000	2,851
Луганська	0,5407	1,470	0,0910	4,407	25,619	10,000	7,022
Львівська	1,4955	1,2378	1,7591	1,051	0,426	0,541	1,086
Миколаївська	0,8052	0,7123	0,2729	1,011	9,189	1,176	2,194
Одеська	3,713	1,4419	0,8439	0,976	0,354	0,741	1,344

Полтавська	0,5683	0,8972	0,2398	0,576	6,477	1,176	1,658
Рівненська	0,4365	0,5104	0,1385	1,456	16,841	2,857	3,708
Сумська	0,3854	0,6803	0,1729	1,190	14,781	1,250	3,076
Тернопільська	0,3482	0,3980	0,1371	1,585	7,184	0,870	1,755
Харківська	1,3538	1,8445	2,0667	0,881	0,523	0,317	1,164
Херсонська	0,4080	0,7154	0,1485	1,344	23,671	2,222	4,751
Хмельницька	0,4850	0,4624	0,1666	1,226	25,618	3,333	5,216
Черкаська	0,6981	0,6009	0,2924	1,025	20,505	0,952	4,013
Чернівецька	0,2634	0,5079	0,1240	1,942	17,412	3,333	4,327
Чернігівська	0,6564	0,5891	0,2249	11,087	22,628	2,222	6,234
м. Київ	4,5913	2,6428	14,281	0,256	0,096	0,339	3,702

Розраховано автором

Додаток Д

Таблиця Д.1. Порядок агломерації (кластерів) (за даними 2017 р.)*

Етап	Об'єднаний кластер		Коефіцієнти	Етап першої появи кластера		Наступний етап
	Кластер 1	Кластер 2		Кластер 1	Кластер 2	
1	24	25	,000	0	0	6
2	21	22	,000	0	0	4
3	8	9	,000	0	0	15
4	21	23	,000	2	0	6
5	17	19	,002	0	0	7
6	21	24	,005	4	1	11
7	17	20	,005	5	0	11
8	4	5	,006	0	0	16
9	15	18	,009	0	0	12
10	10	11	,015	0	0	13
11	17	21	,032	7	6	17
12	15	16	,045	9	0	17
13	10	12	,085	10	0	19
14	13	14	,088	0	0	19
15	7	8	,095	0	3	18
16	3	4	,184	0	8	21
17	15	17	,218	12	11	22
18	6	7	,291	0	15	21
19	10	13	,531	13	14	22
20	1	2	,621	0	0	23
21	3	6	1,095	16	18	23
22	10	15	2,284	19	17	24
23	1	3	5,582	20	21	24
24	1	10	11,292	23	22	0

*Метод середнього зв'язку між групами

Розраховано автором з використанням статистичного пакету IBM SPSS Statistics

Таблиця Д.2. Начальні та кінцеві центри кластерів

	Кластер							
	1		2		3		4	
	Начальні центри	Кінцеві центри	Начальні центри	Кінцеві центри	Начальні центри	Кінцеві центри	Начальні центри	Кінцеві Центри
VAR00001	7,02	6,63	6,23	4,78	5,22	3,29	1,08	1,39

Розраховано автором з використанням статистичного пакету IBM SPSS Statistics

Таблиця Д.3. Зведений звіт за результатами спостережень*

Спостереження					
Валідні		Пропущені		Разом	
N	%	N	%	N	%
25	100,0	0	0	25	100,0

* використано квадрат євклидової відстані; метод середнього зв'язку (між групами)

Розраховано автором з використанням статистичного пакету IBM SPSS Statistics