УДК 327.7:061.1 DOI: https://doi.org/10.36930/506801

Арсенович Леонід Антонович
заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрації Державної служби спеціального зв'язку та захисту інформації України, доктор філософії з галузі публічне управління та адміністрування
ORCID: 0000-0001-7081-2838
e-mail: arsen-leon@ukr.net

СУТНІСТЬ КІБЕРБЕЗПЕКИ ЯК НАПРЯМУ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ

Проаналізовано різні зарубіжні підходи та узагальнено найкращі провідні світові практики щодо формування та розроблення стратегій кібербезпеки. Розглянуто комплексну сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку, складовими частинами якої є: аспекти (правовий, економічний, технічний, фінансовий, міжнародний, науковий), сфери забезпечення кібернетичної безпеки (освітня, зовнішньополітична, правоохоронна, науково-технічна, інформаційна, юридична), а також відповідні рівні кібербезпеки (технологічний, нормативно-правовий, функціональний, матеріальний, програмний та організаційний). Розроблено основні напрями формування державної політики у сфері кібербезпеки (координаційно-контрольний, нормативний, профільно-навчальний, інноваційно-дослідницький, інформаційно-розвідувальний, технічного забезпечення, внутрішнього розвитку, зовнішнього розвитку), які у подальшому дадуть змогу вирішувати актуальні питання у сфері кіберзахисту, розробляти ефективні, дієві державні й управлінські рішення та формувати адекватну державну політику в зазначеній сфері.

Ключові слова: державна політика; інформаційні технології; кібербезпека; стратегія; цифровий розвиток.

Постановка проблеми. Науково-технічний прогрес докорінно змінив сучасне суспільство: на сьогодні інформаційні технології відіграють чи не найважливішу роль у розвитку країн та визначенні рівня життя населення. За останні десятиліття інформація стала настільки потужним чинником розвитку суспільства, що привела до утворення нового інформаційного укладу, який сприяє внутрішньодержавній і світовій інтеграції та реінтеграції. Україна на сьогодні міцно стала на шлях упровадження нових технологій.

Упродовж історії людства інформація була і є основою для прийняття рішень на рівнях людини, суспільства та держави. За сучасних умов розвитку інформаційного суспільства інформацію розглядають як товар, що має цінність і боротьба за який постійно триває. Попри це, інформація є ефективним інструментом провідного впливу на соціальні системи – людину, суспільні групи, суспільство за схемою "керівний вплив – бажаний результат".

У сучасному світі значення інформації виходить далеко за межі того змісту, який вкладається в її офіційне визначення як "будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді". Справді пророчі слова Уінстона Черчіля "Хто володіє інформацією, той володіє світом", що стали крилатою фразою, матеріалізуються в демократичних суспільствах на рівні стратегії національної безпеки,

а в державах із тоталітарним режимом стають страшною зброєю в руках правлячої верхівки, спрямованою як проти власних громадян, так і на реалізацію своїх агресивних зазіхань на незалежність і територіальну цілісність суверенних держав. Через такі діаметрально протилежні вектори інформаційної політики різних держав глобальний інформаційний простір стає полем інформаційних конфліктів, а інформаційна компонента переростає у важливий складник національної безпеки.

Аналіз останніх досліджень і публікацій. Ключовим завданням державної кібербезпекової політики дедалі виразніше виступає створення гарантованих умов реалізації національних інтересів у кіберпросторі. Цей процес уможливлюється завдяки розвитку ефективної системи правового регулювання реалізації кібербезпекової політики. Важливим завданням у цьому ракурсі також є формування успішного, кіберграмотного та кіберосвіченого кіберсуспільства, здатного стати рушієм технологічного прориву України у сфері кібербезпеки, каталізатором розвитку держави за умов перманентних трансформаційних змін та інформаційної глобалізації.

Методологію формування та розвитку кібербезпеки як напряму вироблення державної політики цифрового розвитку вже частково закладено в наукових та навчальних працях вітчизняних дослідників, зокрема таких, як: В. Авер'янов, О. Баранов, В. Грохольський, В. Колпаков, П. Лютіков, Р. Мельник тощо.

Окремі положення державної кібербезпекової політики також розглядали і в роботах зарубіжних дослідників: О. Агапова, Ю. Батуріна, О. Гаврилова, В. Копилова, М. Россолова та інших.

Однак, незважаючи на певний масив наукової літератури, питанням забезпечення та реалізації кібербезпеки як напряму вироблення державної політики цифрового розвитку приділяли замало уваги.

Виокремлення невирішених раніше частин загальної проблеми. Інформація є важливим чинником у формуванні безпечного середовища як з погляду людських відносин, так і забезпечення громадської, національної і міжнародної безпеки. Відповідно, інформаційне протиборство – це природний стан в умовах конкуренції сучасного глобалізованого світу, а питанням забезпечення інформаційної та кібернетичної безпеки приділяють особливу увагу в контексті збереження балансу інтересів на рівнях особи, суспільства, держави та міжнародного правопорядку.

Але разом із впровадженням нових технологій і відкриттям величезного інформаційного простору з'являються й невідомі до цього моменту проблеми, серед яких варто назвати, зокрема, кібернетичні злочини, правопорушення, що становлять загрозу не тільки для окремих громадян, а й для державної безпеки країн (з урахуванням сфери впливу технологій).

Через відсутність дієвої системи забезпечення інформаційної безпеки у національному інформаційному просторі України відбувається багато негативних явищ, які створюють реальні та приховані загрози інформаційній безпеці громадянина, суспільству та державі. Це й злочини в різних сферах господарювання та управління, це й хакерські атаки на урядові сайти та банківські бази даних, це й спроби порушити суспільно-політичний лад у суспільстві через поширення дезінформації чи пропаганди. І на сьогодні це

питання є актуальним не тільки для України, а й для всіх інших країн, тому що не розроблено ефективної системи захисту для запобігання вчиненню правопорушень (злочинів) через віртуальний простір або, як зазначають науковці, – кіберпростір. Саме тому кіберпростір не має меж і кордонів, і в ньому будь-хто набуває широких можливостей у сфері його використання. Саме це робить такий простір надзвичайно зручним для здійснення протиправної діяльності.

Метою роботи є розгляд теоретичних підходів до розуміння сутності кібербезпеки як напряму вироблення державної політики цифрового розвитку.

Виклад основного матеріалу. Вперше термін "кібернетика" увів в обіг древньогрецький філософ Платон для позначення мистецтва кормчого (мистецтва управління). У 1834 році французький учений Андре Марі Ампер використав цей термін для позначення науки, якої на той час ще не існувало, – про управління суспільством. Офіційною датою народження кібернетики як окремої науки вважають рік опублікування книги Норберта Вінера "Кібернетика" (1947 р.), у якій він визначив кібернетику як науку "про управління і зв'язок у тварині і машині". У сучасному розумінні кібернетика – це наука про управління, зв'язок і перероблення інформації [1, с. 191].

Об'єктом дослідження сучасної кібернетики є кібернетичні системи, які розглядають абстрактно (безвідносно до їх реальної природи), що дає змогу досліджувати технічні, біологічні, соціальні системи загальними методами. Кібернетичну систему представляють у вигляді сукупності взаємопов'язаних об'єктів – елементів системи, що здатні запам'ятовувати, обробляти інформацію та обмінюватись нею з іншими елементами та зовнішнім світом. Комп'ютер розглядають як універсальний перетворювач інформації, що здатний, запам'ятовуючи структуру іншої кібернетичної системи, виконувати її функції як перетворювача інформації. Саме ця якість робить його найфункціональнішою відомою кібернетичною системою та основним технічним засобом моделювання й вивчення інших кібернетичних систем будь-якої природи [1, с. 191].

На сьогодні чимало вітчизняних і західних фахівців вважають, що слово "cyber" пов'язане з використанням інформаційних технологій і комп'ютерів, тобто пов'язане з кіберпростором та кібербезпекою.

Вважають, що вперше термін "кібербезпека" у сучасному розумінні став використовуватись у 1990-х роках у США, коли ця проблема стала актуальною для країни. Більшість відомих визначень кібербезпеки ототожнюють це поняття виключно із завданнями забезпечення конфіденційності, цілісності та доступності інформації, тобто захистом інформації у кіберпросторі (кіберзахистом активів), не розглядаючи при цьому аспекти інформаційно-психологічного протиборства у кіберпросторі [1, с. 192].

При цьому варто зазначити, що на міжнародному рівні сьогодні досі немає єдиного визначення кібербезпеки. Цей термін, як і інші ключові визначення, які надано у нормативно-правових документах, значно відрізняються. Маючи певні спільні риси, національні стратегії зарубіжних країн, спрямовані на формування безпечного кіберпростору, характеризуються різноманітністю підходів та специфікою заходів, які враховують особливості державної політики [2, с. 64].

У німецькій стратегії під кібербезпекою розуміють бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму. У Польському законодавстві кібербезпеку розглядають як сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору.

Стратегія кібербезпеки США 2011 року (перша редакція була у 2003 році) визначає контекст підходу до розуміння пріоритетів держави, способів досягнення безпечного кіберпростору та боротьби з кібератаками. У якості загроз визначено шантаж та вимагання коштів, шахрайство, крадіжки та експлуатацію дітей, крадіжки інтелектуальної власності. У Канаді стверджують, що для забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають [1, с. 192, 193].

Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

- кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією;
- використання Інтернету у терористичних цілях. Терористичні угрупування використовують Інтернет для пропаганди, збирання коштів і вербування прихильників;
- кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе програмне забезпечення [3].

Відповідно національні законодавства країн, зазвичай, регулюють питання: захисту персональних даних (Канада, Нідерланди); захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (США, Канада, Польща); захисту дітей (США); захисту важливих об'єктів інфраструктури та інформаційних систем (Франція) [3].

Результати дослідження закордонного досвіду формування державної політики забезпечення кібернетичної безпеки дають підстави констатувати, що у середовищі, де постійно з'являються й еволюціонують кібернетичні загрози, державна політика ґрунтується на гнучких, оперативних стратегіях кібернетичної безпеки. При цьому транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію. Така співпраця потрібна не тільки для ефективної підготовки до кібератак, а й для своєчасної реакції на них, вироблення узгоджених механізмів запобігання [2, с. 67].

Серед основних спільних рис закордонних державних стратегій кібербезпеки потрібно виокремити такі:

- побудова урядової моделі, спрямованої на забезпечення кібербезпеки та визначення відповідного механізму (переважно суспільно-державного партнерства), що дає змогу приватним і державним зацікавленим сторонам обговорювати і затверджувати політики, пов'язані з проблемою кібербезпеки;

- планування та визначення регулювальних механізмів, чітке позначення ролей, прав і відповідальності для приватного і державного сектора;
- міжнародне співробітництво, запровадження необхідної законодавчої бази в цій сфері;
- підвищення готовності, зменшення часу реакції на інциденти, розроблення плану відновлення після збоїв і механізмів захисту для об'єктів критичної інфраструктури;
- розроблення системного та інтегрованого підходу до державного управління ризиками;
- формування інформаційних програм, покликаних навчити користувачів новим моделям поведінки та роботи;
- формування програми освіти, яка передбачає навчання ІТ-фахівців і професіоналів у сфері кібербезпеки [2, с. 63, 64].

Можна констатувати, що тільки формування відповідних документів нормативно-правового характеру з цих питань дало змогу зазначеним країнам визначити правові та організаційні засади державної політики у сфері кібербезпеки, її основні принципи та напрями забезпечення.

Треба зазначити, що саме формування національної державної стратегії кібербезпеки, розроблення її механізмів, інструментів та певних заходів з протидії викликам і загрозам, а також затвердження власних стратегічних підходів до реалізації положень стратегії стало основою для вироблення дійової державної політики розвинених країн світу.

В Україні також розпочато процес формування Національної системи кібербезпеки, який розкриває її поняття, визначає основні засади її забезпечення та який здійснюється через нормативно-правові, організаційно-структурні та інші зміни.

І з погляду розбудови ефективної системи кібербезпеки основоположною є нормативно-правова база для її запровадження. У цьому сенсі можна виділити низку концептуальних нормативно-правових актів: Конституція України [4], у ст. 17 якої відзначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу; Конвенція про кіберзлочинність [5], відповідно до норм якої країни-учасниці повинні здійснити низку заходів на національному рівні, спрямованих на боротьбу з кіберзлочинами; Закони України "Про національну безпеку України" [6], "Про основні засади забезпечення кібербезпеки України" [7], Концепція розвитку сектору безпеки і оборони України [8], Стратегія національної безпеки України [9], а також Стратегія кібербезпеки України [10], яка розкриває умови для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Названими нормативними актами база для розбудови системи кібербезпеки не вичерпується, однак за допомогою їх аналізу можна уявити кістяк, на основі якого можливо формувати суб'єктно-об'єктну модель такої системи.

Сфера кібербезпеки складається зі стандартів, норм, стратегій, принципів формування, засобів реалізації, інструментів управління та запобігання ризикам, що в комплексі формує системний інструментарій здійснення захисту інформації та даних у кіберсередовищі [11, с. 112, 113].

За таких умов комплексну сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку унаочнює наведена нижче схема, яку розробив автор (рис. 1).

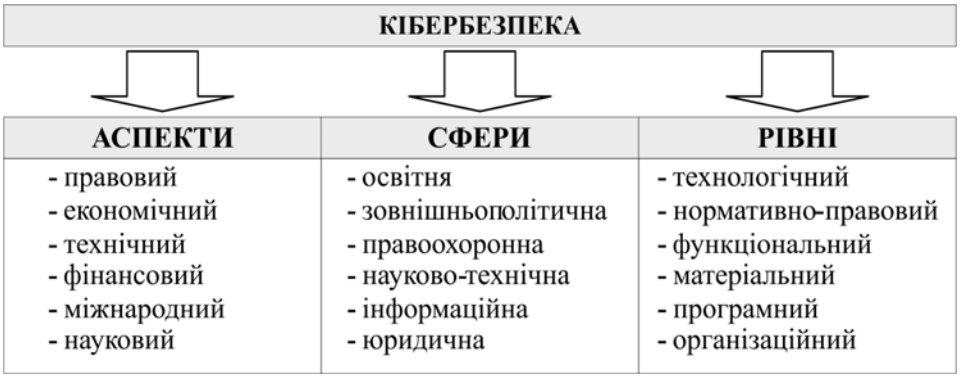

Рис. 1. Комплексна сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку

Формування та ефективна реалізація кібербезпекової політики, в межах якої розглядають правовий, економічний, технічний, фінансовий, міжнародний та науковий аспекти, – є необхідною умовою результативного розвитку кіберсуспільства в Україні.

Так, правовий аспект кібербезпекової політики полягає у виробленні та закріпленні законодавчих дефініцій задля уникнення порізненості та колізії з іншими нормативно-правовими актами, а також уніфікованості правозастосовної практики. Економічний аспект полягає у розвитку економічних процесів у країні, розширенні та модернізації відповідної інфраструктури, інвестуванні коштів у розвиток новітніх інформаційних технологій і сучасних засобів та систем захисту інформаційних ресурсів.

Технічний аспект спрямований на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталого та надійного функціонування комунікаційних і технологічних систем. Фінансовий аспект має на меті запровадження пільгового кредитування та фінансування проєктів, спрямованих на захист кібербезпеки, критичної інфраструктури, освітньої та науково-дослідної діяльності у сфері кіберзахисту.

Міжнародний аспект будується на консультативній та дорадчій допомозі, проведенні переговорів у форматі експертних консультацій Україна – НАТО з питань кібербезпеки, створенні каналів зв'язку та контактів щодо спільного реагування на загрози у сфері міжнародної інформаційної та кібербезпеки. Науковий аспект передбачає створення сприятливих умов для розвитку науки, забезпечення розбудови науково-дослідницької інфраструктури, а також ефективну взаємодію вчених із державним і приватним секторами, стимулювання інновацій та запровадження новітніх технологій.

Зазначимо, що для формування безпечного кібернетичного простору необхідний належний освітній, зовнішньополітичний, правоохоронний, науково-технічний, інформаційний та юридичний супровід, який формується на основі визначених сфер забезпечення кібернетичної безпеки.

Метою освітньої сфери є підготовка фахівців за державним замовленням в обсязі, необхідному для задоволення потреб державного сектора економіки, а також за небюджетні кошти, зокрема для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури.

Метою зовнішньополітичної сфери є співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю. Крім цього, зовнішньополітична сфера забезпечує міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

Правоохоронна сфера, своєю чергою, забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі. Зазначена сфера також здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів та підвищення поінформованості громадян про безпеку в кіберпросторі.

Науково-технічна сфера здійснює вдосконалення технічного захисту інформації, створення програмних продуктів для захисту державних інформаційних ресурсів, впровадження системи моніторингу кіберзагроз в інформаційно-телекомунікаційних мережах державних органів.

Інформаційна сфера проводить дослідження проблем із кіберзахисту, розповсюджує інформацію серед громадян щодо безпечної поведінки у кіберпросторі тощо. Завданням юридичної сфери повинно стати внесення змін до законодавства (для розмежування кримінальної відповідальності за злочини у сфері використання комп'ютерів та комп'ютерних мереж), його вдосконалення (щодо протидії кіберзлочинам), та узгодження з міжнародною нормативно-правовою базою.

Враховуючи специфіку і масштабність сучасних кіберзагроз, комплексну сутність кібербезпеки розкривають відповідні рівні кібербезпеки, які зобов'язані вирішувати актуальні питання кіберзахисту, розробляти ефективні і дієві державно-управлінські рішення та формувати відповідну адекватну політику.

Так, головними завданнями технологічного рівня повинні стати впровадження організаційно-технічної моделі кібербезпеки (як складової частини Національної системи кібербезпеки), а також систем: антивірусного захисту національних інформаційних ресурсів; аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури; виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту; взаємодії команд реагування на комп'ютерні надзвичайні події [7].

Нормативно-правовий рівень передбачає формування національної нормативно-правової бази та механізмів її запровадження (законопроєкти, акти Президента України, Верховної Ради України та Кабінету Міністрів України, нормативно-правові акти державних органів), а також узгодження її положень з нормами кримінального, адміністративного і цивільного права.

Через функціональний рівень здійснюють практичні заходи із кібербезпеки, підвищення кваліфікації державних службовців, підтримка освітніх та дослідницьких ініціатив, розвиток стартапів. Цей рівень передбачає створення платформи, спрямованої на розвиток дослідницького та інноваційного потенціалу, а також залучення до цього процесу науково-дослідних центрів та інших зацікавлених сторін.

Матеріальний рівень забезпечує розширення та модернізацію відповідної інфраструктури, інвестування коштів у розвиток новітніх інформаційних технологій і сучасних засобів і систем захисту інформаційних ресурсів тощо. Програмний рівень регламентує: формування та реалізацію відповідних програм, співробітництво з іншими державами у сфері забезпечення кібернетичної безпеки; підготовку та підвищення кваліфікації кадрів, дослідження та імплементацію світового досвіду запобігання кіберінцидентам та протидії кібератакам; запровадження державно-приватної взаємодії у сфері забезпечення кібербезпеки; розвиток інфраструктури кіберзахисту; стимулювання освітньої та науково-дослідної діяльності у сфері кіберзахисту.

Нарешті, організаційний рівень має на меті: формування та реалізацію механізму публічного управління у сфері кібербезпеки; активізацію міжнародного співробітництва в боротьбі з кіберзлочинністю на державному та галузевому рівнях; залучення неурядових організацій до боротьби з кіберзлочинністю; формування механізмів реалізації проєктів державно-приватної взаємодії у сфері кібербезпеки; запровадження та реалізацію програм співробітництва з обміну інформацією у сфері кібербезпеки між державою та бізнесом.

Запропоновані аспекти, сфери та рівні кібербезпеки у комплексі здатні забезпечити: завершення створення Національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки й оборони України для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері; кіберзахист державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка перебуває під юрисдикцією України.

Отже, задля збереження та розвитку національного кіберпростору є доцільним своєчасне виявлення, запобігання й нейтралізація реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним і національним інтересам, що потребує передусім комплексного підходу.

Варто зазначити, що для формування безпечного кібернетичного простору та ефективної реалізації державної політики у сфері кібербезпеки є необхідним належне правове, організаційне, технічне, інституційне та інші види забезпечення.

Крім цього, потрібно звернути увагу, що формування та реалізація державної політики у сфері кібербезпеки здійснюється на основі 10 принципів, визначених ст. 7 Закону України "Про основні засади забезпечення кібербезпеки України". Враховуючи зазначене, варто окреслити основні напрями формування державної політики у сфері кібербезпеки (рис. 2).

Координаційно-контрольний	вироблення й оперативна адаптація державної політики у сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС та НАТО; проведення аудиту інформаційної безпеки та періодичного огляду Національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки
Нормативний	створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки; забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації
Профільно-навчальний	проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі; підготовка фахівців для задоволення потреб державного сектору економіки, а також за небюджетні кошти, зокрема для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу
Інноваційно-дослідницький	розвиток мережі команд реагування на комп'ютерні надзвичайні події; вдосконалення системи технічного і криптографічного захисту інформації; залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проєктів концептуальних документів у сфері кібербезпеки
Інформаційно-розвідувальний	здійснення заходів для розширення можливостей сектору безпеки й оборони України з використанням кіберпростору; розвиток системи контррозвідувального забезпечення кібербезпеки; проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки; здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів
Технічного забезпечення	забезпечення функціонування Національної телекомунікаційної мережі; впровадження організаційно-технічної моделі Національної системи кібербезпеки; програмно-цільове забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту
Внутрішнього розвитку	державно-приватна взаємодія у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагування на кібератаки та кіберінциденти; встановлення вимог щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами
Зовнішнього розвитку	розвиток міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, поглиблення співпраці України з ЄС та НАТО, участь у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі

Рис. 2. Основні напрями формування державної політики у сфері кібербезпеки

Враховуючи специфіку і масштабність сучасних кіберзагроз, задля вирішення актуальних питань у сфері кіберзахисту, розроблення ефективних, дієвих державних і управлінських рішень та формування адекватної державної політики в зазначеній сфері, треба наголосили, що ці напрями формування державної політики у сфері кібербезпеки потребують періодичного перегляду, уточнення та коригування.

Зазначимо, що систематизація підходів до розуміння державотворчих процесів у цій сфері дає змогу інтегрувати відповідні наукові знання та дає змогу 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 [2, с. 58, 59].

Висновки і перспективи подальших розвідок. Проведене дослідження засвідчує, що формування основних аспектів забезпечення кібербезпеки України здійснюють на основі відповідної державної політики, яка є самостійним напрямом політики цифрового розвитку.

З огляду на це наявні загрози вимагають формування та реалізації державної політики у сфері кібербезпеки, яка має бути спрямована на:

- забезпечення інформаційного суверенітету України у кіберпросторі, створення надійного захисту національного сегмента кіберпростору в умовах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації в Донецькій та Луганській областях;
- 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;
- взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Список використаної літератури

1. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки // Інформаційні технології і засоби навчання. 2016. т. 55, вип. 5. С. 187–197.

2. Островий О.В. Формування державної політики забезпечення кібернетичної безпеки в Україні: дис…. канд. наук з держ. упр. 25.00.02 / Донец. держ. універ. управ. Маріуполь, 2019. 239 с.

3. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу США, Канади та інших. URL : http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf (дата звернення: 12.11.2021).

4. Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 12.11.2021).

5. Про ратифікацію Конвенції про кіберзлочинність : Закон України. URL : https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 12.11.2021).

6. Про національну безпеку України : Закон України. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.11.2021).

7. Про основні засади забезпечення кібербезпеки України : Закон України. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.11.2021).

8. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України" : Указ Президента України № 92/2016 від 14.03.2016 р. URL : https://zakon.rada.gov.ua/laws/show/92/2016 (дата звернення: 12.11.2021).

9. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" : Указ Президента України № 392/2020 від 14.09.2020 р. URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 12.11.2021).

10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України № 447/2021 від 26.08.2021 р. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 12.11.2021).

11. Шайхет С.О. Механізми реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України: дис…. канд. наук з держ. упр. 25.00.02 / НАДУ. Київ, 2019. 252 с.

Статтю подано: 29.10.2021 Статтю схвалено: 24.12.2021

Arsenovych Leonid Antonovych

Doctor of Philosophy in Public Management and Administration, deputy head – head of division at the HR Management Department of the Administration of the State Service for Special Communication and Information Protection of Ukraine

ORCID: 0000-0001-7081-2838
e-mail: arsen-leon@ukr.net

ESSENCE OF CYBERSECURITY AS DIRECTLY THE PROCUREMENT OF THE STATE POLICY OF DIGITAL DEVELOPMENT

Problem setting. The science and technology progress has changed the modern society dramatically: today, the information technology plays probably the most important role in the development of countries and in determining people's living standards. Over the recent decades, information has become so much a powerful society development driver that it was able to have resulted in the origination of a new information structure that encourages the domestic and global integration and reintegration. These days, Ukraine is strongly underway introducing new technology.

Recent research and publications analysis. The key task of the state cybersecurity policy is ever more becoming to ensure guaranteed conditions for advocating the national interests in the cyberspace. This process is made possible by way of developing an effective system of legal regulation of the cybersecurity policy implementation. An important task in this context is also to contribute to the development of the successful, cybersmart and cybereducated cybersociety, which would be able to drive Ukraine's technological breakthrough in cybersecurity and to catalyze the state development within the landscape of permanent transformational changes and information globalization.

But despite quite a batch of scientific works, the issues of safeguarding and implementing the cybersecurity as directly the procurement of the state policy of digital development have been little-studied.

Highlighting previously unsettled parts of the general problem. Segregation of the previously unresolved parts of the overall problem. Due to no effective system of information security in Ukraine's national information space, there are a lot of negative phenomena in place that result in both real and hidden threats to information security of individuals, the society and the state. And today this issue is relevant not only for Ukraine but also for all other countries, because no effective system of protection has been developed to prevent offenses (crimes) through the virtual space or, as scientists say, the cyberspace. That is why the cyberspace has no limits or borders, and anyone may enjoy vast opportunities within its boundaries to use it in whatever way. This is what makes such a space extremely convenient for any wrongful actions.

The purpose of the article is to study the theoretical approaches to understanding the essence of cybersecurity as directly the procurement of the state policy of digital development.

Paper main body. The article analyzes various foreign approaches and summarizes the world's best practices in outlining and developing the cybersecurity strategies. The comprehensive essence of cybersecurity as directly the procurement of the state policy of digital development has been studied, which components are as follows: aspects (legal, economic, technical, financial, international, scientific), areas of safeguarding the cybersecurity (education, foreign policy, law enforcement, science and technology, information, law), and the appropriate cybersecurity levels (technological, regulatory, functional, material, program and organizational). The principal areas of the state cybersecurity policy development (coordination and control, regulation, area-specific education, innovation and research, informational intelligence, technical support, internal development, external development) have been developed, which would further allow responding to relevant cybersecurity issues, delivering effective state and management decisions, and developing the adequate state policy in the area mentioned.

Conclusions of the research and prospects for further studies. The study in question shows that the development of the main aspects of safeguarding Ukraine's cybersecurity is based on the appropriate state policy, which is an independent area of the digital development policy.

In this respect, the existing threats require that the state policy in the area of cybersecurity be developed and implemented, which should intend to:

- ensure the information sovereignty of Ukraine in the cyberspace, provide for reliable protection of the national segment of the cyberspace in the context of taking measures to safeguard the national security and defense, to support the counteraction to and deterring the armed aggression of the Russian Federation in Donetsk and Luhansk regions;
- strengthen the state's defense capacity in the cyberspace;
- fight against cybercrime and cyberterrorism;
- avoid and prevent the interference with Ukraine's internal affairs, and put an end to any encroachments on Ukraine's Internet resources by other states;
- ensure the cybersecurity cooperation between the state bodies, local self-government authorities, army units, law enforcement bodies, science and research institutions, educational institutions, non-government organizations, as well as companies, institutions and organizations regardless of their ownership, which operate in the area of electronic communications and information security and/or are the owners (managers) of the critical information infrastructure facilities.

Key words: state policy; information technology; cybersecurity; strategy; digital development.

References

1. Melnyk, S. V. (2016). Poniatiino-katehorialnyi aparat u systemi profesiinoi pidhotovky maibutnikh fakhivtsiv z kiberbezpeky. *Informatsiini tekhnolohii i zasoby navchannia*, Issue 55(5), pp. 187-197. **[**In Ukrainian**]**.

2. Ostrovyi, O. V. (2019). Formuvannia derzhavnoi polityky zabezpechennia kibernetychnoi bezpeky v Ukraini. Mariupol, 239 p. **[**In Ukrainian**]**.

3. Zakonodavstvo ta stratehii u sferi kiberbezpeky krain Yevropeiskoho soiuzu SShA, Kanady ta inshykh. URL : http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf. **[**In Ukrainian**]**.

4. Konstytutsiia Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D%80#Text. **[**In Ukrainian**]**.

5. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist. URL : https://zakon.rada.gov.ua/laws/show/2824-15#Text **[**In Ukrainian**]**.

6. Pro natsionalnu bezpeku Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text. **[**In Ukrainian**]**.

7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/2163-19. **[**In Ukrainian**]**.

8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 bereznia 2016 roku "Pro Kontseptsiiu rozvytku sektoru bezpeky i oborony Ukrainy". № 92/2016 (2016). URL : https://zakon.rada.gov.ua/laws/show/92/2016. **[**In Ukrainian**]**.

9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy". № 392/2020 (2020). URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text. **[**In Ukrainian**]**.

10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy". № 447/2021 (2021). URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text. **[**In Ukrainian**]**.

11. Shaikhet, S. O. (2019). Mekhanizmy realizatsii servisno-oriientovanoi derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy. Kyiv, 252 p. **[**In Ukrainian**]**.

Paper submitted: 29.10.2021 Paper accepted: 24.12.2021

Цитування: Арсенович Л. А. Сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку // Ефективність державного управління : зб. наук. пр. Вип. 3/4 (68/69) : у 2 ч. Ч.1 / за заг. ред. чл.-кор. НАН України В. С. Загорського, доц. А. В. Ліпенцева. Львів : НЛТУ України, 2021. С. 9–21. (DOI: https://doi.org/10.36930/506801)

Citation: Arsenovych, L. A. (2021). Essence of cybersecurity as directly the procurement of the state policy of digital development. *Efficiency of Public Administration,* Issue 3/4(68/69), pp. 9–21. (DOI: https://doi.org/10.36930/506801)