УДК 342.951

ГОРУН О.Ю., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-0447-1729.

ПРІОРИТЕТНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *Розглянуто пріоритети державної політики кібербезпеки. Визначено сучасні виклики та загрозливі тенденції у сфері забезпечення кібербезпеки. Деталізовано засади формування та реалізації державної політики кібербезпеки. Проаналізовано окремі акти вітчизняного законодавства, присвячені актуальним питанням забезпечення кібербезпеки. Обґрунтовано доцільність посилення спроможностей національної системи кібербезпеки України. Окреслено пріоритетні напрями розбудови критичної інформаційної інфраструктури. Визначено завдання та шляхи удосконалення нормативно-правового регулювання державної політики кібербезпеки.*

Ключові слова: *кібербезпека, кіберзагроза, кібератака, кіберзброя, кіберзахист, національна система кібербезпеки, кіберінцидент, кіберпростір, державна політика кібербезпеки, цифровізація.*

Summary. *The priorities of the state cybersecurity policy are considered. Modern challenges and threatening trends in the sphere of cybersecurity have been identified. The main principles of formation and implementation of the state cybersecurity policy are detailed. Some acts of domestic legislation devoted to the topical issues of cybersecurity are analyzed. The expediency of strengthening the capabilities of the national cybersecurity system of Ukraine is substantiated. The priority directions of development of the critical information infrastructure are outlined. The tasks and directions of improvement regulatory framework of state cybersecurity policy have been identified.*

Keywords: *cybersecurity, cyberthreat, cyberattack, cyberweapons, cyberdefense, national cybersecurity system, cyberincident, cyberspace, state cybersecurity policy, digitalization.*

Аннотация. *Рассмотрены приоритеты государственной политики кибербезопасности. Определены современные вызовы и угрожающие тенденции в сфере обеспечения кибербезопасности. Детализированы основы формирования и реализации государственной политики кибербезопасности. Проанализированы отдельные акты отечественного законодательства, посвященные актуальным вопросам обеспечения кибербезопасности. Обоснована целесообразность усиления возможностей национальной системы кибербезопасности. Очерчены приоритетные направления развития критической информационной инфраструктуры. Определены задачи и направления усовершенствования нормативно-правового регулирования государственной политики кибербезопасности.*

Ключевые слова: *кибербезопасность, киберугроза, кибератака, кибероружие, киберзащита, национальная система кибербезопасности, киберинцидент, киберпространство, государственная политика кибербезопасности, цифровизация.*

Постановка проблеми. Кібербезпека була і залишається однією із важливих складових системи національної безпеки України. Питома вага, форми та види кіберзагроз в контексті національної безпеки постійно та динамічно зростають й трансформуються. Ця загрозлива тенденція в міру розвитку інформаційно-комп'ютерних (цифрових) технологій (далі – ІКТ) та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на

функціонування структур управління як національних, так і транснаціональних, формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів.

Реалізація зазначеного пріоритету забезпечує в епоху тотальної цифровізації повноцінну життєдіяльність політикуму держави, бізнесу та пересічених громадян і здійснюється шляхом посилення спроможностей національної системи кібербезпеки. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору. Це зумовлює нові можливості для цифровізації всіх сфер суспільного життя. Враховуючий такий стан справ, актуальним та своєчасним є уточнення та деталізація пріоритетних засад державної кібербезпекової політики.

Результати аналізу наукових публікацій. Проведення контент-аналізу та розгляд основ державної політики у сфері забезпечення кібербезпеки, пошук оптимальних шляхів її удосконалення здійснювали у своїх наукових працях такі фахівці, як: О. Бакалінська [1], Л. Веселова [2], Ю. Геращенко [3], Р. Лук'янчук [4] та ін. Адже з набуттям чинності 14 вересня 2020 року Стратегії національної безпеки України [5] пріоритетні засади державної кібербезпекової політики набувають неабиякої актуальності в епоху масштабного поширення ІКТ, суцільної світової діджіталізації та потребують уточнення на рівні науково-теоретичної проблеми.

Метою статті є визначення пріоритетних засад державної кібербезпекової політики з урахуванням загрозливих тенденцій та викликів сучасності, визначення шляхів, практична реалізація яких надасть змогу досягнути такого рівня захищеності кіберпростору, який забезпечує реалізацію національних інтересів України у кібернетичній сфері.

Виклад основного матеріалу. Основним правовим актом, положення якого визначають основні цілі, напрями та принципи державної політики у сфері кібербезпеки є Закон України "Про основні засади забезпечення кібербезпеки" від 05.10.17 р. [6]. Забезпечення кібербезпеки здійснюється відповідно до пріоритетних засад державної політики у цій сфері, яка включає формування, удосконалення та реалізацію організаційно-правових, науково-технічних, правоохоронних, економічних заходів забезпечення національної безпеки в кіберсфері. Обов'язком політичного керівництва будь-якої держави світу є забезпечення безперешкодного та надійного доступу громадян і суспільства до безпечного кібернетичного середовища шляхом упровадження та реалізації виваженої державної політики, спрямованої на мінімізацію наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, недопущення блокування спецслужбами іноземних держав або хакерськими групами діяльності стратегічно важливих інформаційно-комунікаційних мереж, електронних комунікацій, цілеспрямованих посягань на об'єкти національної критичної інформаційної інфраструктури.

Розуміючи загрозливий характер та масштаби поширення кіберзагроз у сучасному світі, і зокрема для України, у Посланні Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України в 2020 році" [7] визначено, що інформаційне протиборство з державою-агресором триває й у кіберпросторі.

Адже формування та реалізація пріоритетів державної кібербезпекової політики повинні враховувати сучасні виклики у сфері кібербезпеки, виходячи із внутрішніх та зовнішніх негативних факторів й загрозливих тенденцій, до яких можна віднести:

активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, змагальний характер розвитку засобів кібербезпеки та реалізації кіберзагроз у процесі швидких прогресуючих змін ІКТ щодо Хмарних обчислень, Великих Даних, Інтернету речей, 5G-мереж тощо; мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї, які надають можливість здійснювати приховане проведення противником кібератак та кібероперацій, віддаленого взяття під контроль систем управління, завдання шкоди та руйнування критичної інформаційної інфраструктури; зростання технологічного рівня протиправних зовнішніх посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій; вплив поширення пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинило швидку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням саме електронних сервісів та інформаційно-комунікаційних систем.

В сучасному світі передумовами динамічного поширення кіберзагроз все ще залишаються: недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування кіберзлочинів, низький рівень правової відповідальності за порушення вимог законодавства у цій сфері; відсутність у значної частини органів державної влади відповідних структурних підрозділів, фінансування робіт із кіберзахисту за залишковим принципом з технологічними помилками; відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів; незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Надзвичайно актуальною загрозою в сучасних умовах є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов’язана з проведенням спецслужбами іноземних держав, насамперед Російської Федерації, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об’єктів критичної інформаційної інфраструктури, передусім систем управління державою, об’єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій). Загальновідомо, що з 2014 року Росія активно використовує кіберпростір у форматі гібридної агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об’єкти критичної інфраструктури. Держава-агресор постійно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей та спроможностей у сфері забезпечення кібербезпеки органами сектору безпеки і оборони.

Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних

країні-агресору та іншим країнам. Збільшення кількості інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах призвело до створення глобального ринку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет. Дедалі частіше спрямовані кібератаки не здійснюються напряму на уряди та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до великої кількості їх клієнтів та завдання масштабної шкоди. Популярні веб-сайти, соціальні мережі, реєстри збирають значну кількість різноманітних персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

В Україні в останні роки відчутно зросла загроза кібертероризму, що насамперед, пов'язано з кіберможливостями держави-агресора РФ, яка веде проти України кібервійну із застосуванням кіберзброї. Дедалі частіше спостерігається тенденція використання кіберпростору з метою фінансування терористичних угруповань. Водночас недостатньою є взаємодія України з міжнародними партнерами щодо опрацювання на взаємовигідній основі механізмів протидії кібертероризму. Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до ІКТ та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору з метою вчинення інших кримінальних правопорушень (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація значно ускладнюється через низький рівень кіберграмотності населення, зокрема, пересічних користувачів електронних послуг.

Держава зацікавлена у створенні системи захисту від ризиків, викликів та загроз для державних інформаційних ресурсів та об'єктів критичної інфраструктури, тобто забезпеченні такого важливого елементу, як "кіберстабільність". Слід вказати, що в Україні до 2021 року були відсутні концептуальні засади формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян, що значно гальмувало процес забезпечення розвитку усіх сфер суспільного життя відповідно до сучасних вимог, процесів глобальної цифровізації економіки, сфер життєдіяльності суспільства, які відбуваються у більшості країн світу. З метою розв'язання окреслених проблемних питань, останнім часом, спостерігається активна та плідна нормотворчість Уряду України з метою визначення пріоритетних напрямків щодо проведення послідовної та виваженої державної політики, спрямованої на досягнення інтеграційного курсу до європейського співтовариства та євроатлантичних спільнот, визначення та реалізації заходів, спрямованих на стрімкого розвитку цифрової економіки, підвищення кіберграмотності населення України.

Так, протягом останнього часу, були схвалені: Національна економічна стратегія на період до 2030 року (Постанова Кабінету Міністрів України від 03.03.21 р. № 179) [8], та Концепція розвитку цифрових компетентностей (Розпорядження Кабінету Міністрів України від 03.03.21 р. № 167) [9]. Аналіз вказаних нормативно-правових актів дає змогу констатувати, що прискорена цифрова трансформація є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Впровадження нових

технологій, цифрових послуг та механізмів взаємодії громадян з державою, включаючи виборчий процес, створює значну кількість прихованих взаємозв'язків на рівні технологій і процесів. Проте, за відсутності системного підходу до кібербезпеки та оцінки ризиків існує ймовірність втрати довіри громадян до процесів цифрової трансформації, актуалізації поширення кіберзагроз. Адже обов'язок політичного керівництва України – це створення безпечних інформаційних систем та відкриття доступу до них задля суспільного блага.

Важливим та актуальним напрямком залишається розбудова національної системи кібербезпеки. Держава має розбудовувати національну систему кібербезпеки, ґрунтуючись на: всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей України), неухильному захисті національних інтересів України у сфері кібербезпеки; перманентності заходів з удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо її актуалізації відповідно до безпекових умов, що змінюються; орієнтованості на суспільство, що сприятиме його економічному і соціальному зростанню; використанні принципу мінімальної достатності ролі держави у процесах розвитку та забезпечення безпеки кіберпростору, встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту, повазі до основоположних цінностей, прав людини і особи на свободу вираження думки, такому самому захисті загальновизнаних основоположних прав в онлайн-середовищі, як і в офлайновому; засудженні практики перевищення встановлених меж необхідності щодо обмеження прав громадян та юридичних осіб під час використання кіберпростору та ІКТ; відкритості та створенні умов для активної участі всіх заінтересованих сторін з урахуванням їх потреб і зобов'язань в умовах, коли кібербезпека цифрового середовища набула надважливого значення для держави, суспільства і громадян; визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності, застосування стимулюючих механізмів та обміну унікальними знаннями і досвідом; ризик-орієнтованому підході в частині заходів забезпечення кібербезпеки та кіберзахисту тощо.

Узагальнюючи викладене, державними пріоритетами забезпечення кібербезпеки України виступають такі складові:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки.

З метою реалізації вказаних пріоритетів держава повинна не лише створити та розвивати ефективні (у тому числі кадрові та технологічні) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну організаційно-правову та технологічну модель їх функціонування та застосування, що неможливо уявити без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності. Україна має забезпечити проведення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів

держави, суспільства і окремих громадян. Правоохоронні та державні органи спеціального призначення з правоохоронними функціями мають посилити спроможності для мінімізації загроз кіберзлочинності, свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів. Важливим напрямком залишається створення необхідних умов задля забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору.

Держава об'єктивно зацікавлена у створенні системи захисту від ризиків, викликів та загроз у тому числі й для державних інформаційних ресурсів та об'єктів критичної інфраструктури, тобто забезпеченні такого важливого елементу, як "кіберстійкість". З цією метою актуальним завданням держави має стати посилення національної кіберготовності, що являє собою здатність суб'єктів сектору безпеки і оборони своєчасно й ефективно реагувати на кібератаки, забезпечувати штатний режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед, об'єктів критичної інформаційної інфраструктури. Актуальним при цьому, залишається забезпечення гарантій з боку держави щодо надійності та безпеки цифрових послуг.

У рамках реалізації пріоритетних напрямів державної політики у сфері забезпечення безпеки критичної інфраструктури, з метою вдосконалення правової основи захисту критичної інфраструктури та створення системи її державного управління РНБО України ухвалила Рішення "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29.12.16 р., що затверджено Указом Президента України від 16.01.17 р. № 8/2017 [10], яким, зокрема, передбачалося:

створення державної системи захисту критичної інфраструктури;

визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;

визначення функцій, повноважень та відповідальності центральних органів виконавчої влади, інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;

запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;

запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації тощо.

На підставі вказаного Постановою Кабінету Міністрів України була затверджена "Концепція створення державної системи захисту критичної інфраструктури" від 06.12.17 р. № 1009 [11]. Реалізація положень цієї Концепції мала сприяти: створенню державної системи захисту критичної інфраструктури, здатної забезпечувати належний рівень захисту такої інфраструктури від усіх видів загроз; виробленню механізмів ефективного реагування у разі виникнення кризових ситуацій та ліквідації їх наслідків, а також швидкому відновленню функціонування об'єктів критичної інфраструктури; налагодженню ефективної взаємодії між усіма суб'єктами державної системи захисту критичної інфраструктури за активної підтримки суспільства, місцевих громад, засобів масової інформації та недержавних дослідних інституцій, що вивчають проблеми безпеки та оборони; гармонізації законодавства України у сфері захисту критичної інфраструктури із законодавством ЄС; міжнародному співробітництву у сфері захисту критичної інфраструктури.

У рамках реалізації спроможностей держави у вказаному сегменті, відповідальні суб'єкти національної системи кібербезпеки мали розробити Національний перелік об'єктів критичної інфраструктури. На жаль, станом на 2021 рік, такий перелік все ще не сформульований, хоча останнім часом було схвалено декілька нормативно-правових актів, присвячених поступовому вирішенню цього стратегічного завдання держави. Зокрема, за цією тематикою було прийнято низку актів Уряду України, серед яких виділяються Постанови Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.19 р. № 518 [12] та "Деякі питання об'єктів критичної інформаційної інфраструктури" від 09.10.20 р. № 943 [13].

Також в нашій державі відсутній уніфікований законодавчий акт про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури. Не випадково в умовах технологічного відставання від світових країн-лідерів у сфері високих технологій вітчизняна ІТ-інфраструктура, в тому числі й об'єкти критичної інформаційної інфраструктури, ще й досі залежні від імпортних програмно-апаратних комплексів та відповідного програмного забезпечення.

Аналіз положень чинного законодавства надає підстави констатувати про відсутність у нашій державі системних правових актів є прямим свідченням того, що на сьогодні існують та поширюються загрозливі тенденції в кіберпросторі, які безпосередньо впливають на цілісність державної політики у сфері кібербезпеки. Очевидним фактом є також недостатня нормативна урегульованість міжвідомчої координації з питань забезпечення кібербезпеки, відсутність схваленої на державному рівні оновленої Стратегії кібербезпеки на 2021 – 2025 роки.

Таким чином, у сучасних умовах державна політика у сфері забезпечення кібербезпеки повинна бути сконцентрована на досягненні вагомих результатів з метою створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України та блокування будь-яких посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; зниження рівня вразливості об'єктів кіберзахисту; приєднання до європейської системи та дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення міжнародної кібербезпеки.

Забезпечення кібербезпеки як важлива складова державної політики залишається комплексною проблемою, яка потребує, у першу чергу, схвалення законодавчих та нормативно-правових актів, спрямованих на розв'язання проблемних питань у цій сфері. Основною метою реалізації державної політики у сфері забезпечення кібербезпеки є: створення політико-правових, фінансово-економічних, організаційних та матеріально-технічних умов для формування її сучасної моделі, орієнтованої на позитивний досвід ЄС та НАТО; підвищення ефективності використання усіх видів інформаційно-телекомунікаційних ресурсів і управління елементами інформаційно-комунікаційної інфраструктури, державної підтримки виробництва вітчизняної ІТ-продукції, забезпечення розвитку та дієвого захисту кіберпростору.

Висновки.

Пріоритетні засади державної політики України у сфері забезпечення кібербезпеки мають формуватися комплексно, виходячи із сфери національних інтересів, балансу інтересів людини, суспільства і держави. Формування державної політики забезпечення кібербезпеки передбачає реалізацію дієвих заходів організаційно-правового, технічного, фінансово-економічного, виховного і наукового спрямування та зовнішньополітичного характеру.

Серед організаційно-правових заходів, зокрема, виділяється: прискорення схвалення Стратегії кібербезпеки на 2021 – 2025 роки, затвердження Національного переліку об'єктів критичної інфраструктури, розроблення та запровадження індикаторів стану кібербезпеки на основі системного моніторингу виявлення і прогнозування кіберзагроз, що надасть змогу фіксувати досягнення або недоліки функціонування системи кібербезпеки.

Технічні заходи в рамках державної політики забезпечення кібербезпеки мають бути спрямовані на: створення технологічної складової національної системи кібербезпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; удосконалення технічного захисту інформації, забезпечення регламентації процедури підтвердження відповідності засобів технічного захисту інформації; створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення; тотальну модернізацію програмно-апаратного оснащення комплексів, що забезпечують роботу (CERT-UA); розробку та практичне впровадження галузевих індикаторів стану кібербезпеки; удосконалення системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних ІКТ (включаючи технології онлайн-доступу); розробку нових методів запобігання кібератакам, кіберінцидентам.

Фінансово-економічні заходи мають бути спрямовані на створення економічних передумов для розвитку і забезпечення безпеки критичної інформаційної інфраструктури держави та її ресурсів, активізації інвестиційної діяльності держави у сферу високих технологій та покращення інвестиційного клімату української ІТ-індустрії, збільшення державного бюджетного фінансування на потреби реалізації заходів щодо забезпечення кібербезпеки, збільшення обсягів на фінансування сектору безпеки і оборони України; створення конкурентоспроможної національної системи виробництва ІТ-продукції, розвинутої інформаційно-комунікаційної інфраструктури; сприяння розвитку конкуренції, вдосконалення антимонопольної політики в інформаційній сфері, зокрема шляхом розроблення і вжиття комплексу заходів, спрямованих на запобігання надходженню контрафактної продукції, захист вітчизняного інформаційного ринку, вітчизняного ІТ-виробника та споживачів. Обсяги бюджетного фінансування потрібно визначати щороку під час складання проектів бюджетів на відповідний рік виходячи із завдань та фінансових можливостей держави.

Заходи державної політики у сфері забезпечення кібербезпеки виховного та наукового спрямування мають передбачати: налагодження процесу підготовки кадрів у сфері кібербезпеки, забезпечення внесення змін до навчальних планів і програм середньої та вищої школи, підготовки наукових та науково-педагогічних кадрів, що спрямовані на інформування основних цільових груп про кіберзагрози та методи протидії їм; посилення державної підтримки розвитку основних напрямів науки і техніки як основи створення високих ІКТ; забезпечення створення необхідних умов для реалізації прав інтелектуальної власності в кіберпросторі України; розробку загальнодержавних програм підвищення рівня обізнаності населення щодо кіберзагроз. Потребують державної підтримки вітчизняні фундаментальні та прикладні дослідження, розробки у сфері інформатизації, телекомунікацій і зв'язку, необхідні активні загальнодержавні зусилля, спрямовані на підтримку та формування кадрового потенціалу у сфері забезпечення кібербезпеки.

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки залишається поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. Таким чином, у зовнішньополітичній сфері діяльність держави має бути зосереджена на постійному забезпеченні вільного доступу громадян до мережі Інтернет в аспекті вільного користування зарубіжними та міжнародними інформаційними ресурсами; формуванні позитивного міжнародного іміджу України на світовій арені; налагодженні тісного співробітництва з міжнародними партнерами України; забезпеченні поглиблення співпраці України з ЄС та НАТО для посилення спроможностей держави у сфері кібербезпеки; забезпеченні участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки, неухильному дотриманні взятих на себе міжнародних зобов'язань у сфері кібербезпеки; організації та проведенні науково-практичних заходів, зокрема конференцій, семінарів, форумів, симпозіумів з питань забезпечення кібербезпеки і захисту інформації в кіберпросторі на міжнародному рівні.

Таким чином, український вектор зовнішньої політики має бути сфокусований на активізацію міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримку міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, продовження комплексної взаємодії з питань кібербезпеки за участю органів державної влади і відповідних структур НАТО шляхом співпраці на двосторонній основі, впровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування (CERT) на кіберінциденти, поглиблення співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ. Світова спільнота в рамках міжнародного співробітництва також повинна спрямувати свої ініціативи щодо недопущення проведення локальних та міжнародних війн у кіберпросторі, посилити міжнародно-правову відповідальність держав за протиправну діяльність в Інтернеті та в кіберпросторі.

Ефективність заходів державної політики у сфері забезпечення кібербезпеки може бути набагато результативнішою, якщо держава обере композитну стратегію активного учасника міжнародного інформаційного ринку, що вимагає налагодження виробництва та захисту власного ІТ-продукту, створення умов для його просування на відповідні світові ринки. Державна політика у сфері забезпечення кібербезпеки сконцентрована на досягненні вагомих результатів з метою створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України та блокування будь-яких посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; зниження рівня вразливості об'єктів кіберзахисту; приєднання до міжнародної системи та дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю і кібертероризмом; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки.

Використана література

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія: "Юридичні науки"*. 2019. № 2. С. 23-28.

3. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Державне управління"*. 2019. № 1. С. 140-145.

4. Лук'янчук Р. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. № 3. С. 110-117. URL: http://nbuv.gov.ua/UJRN/Vnadu_2015_3_18 (дата звернення: 20.03.2021).

5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.03.2021).

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

7. Про внутрішнє та зовнішнє становище України у 2020 році: послання Президента України до Верховної Ради. URL: https://www.president.gov.ua/news/poslannya-prezidenta-ukrayini-volodimira-zelenskogo-do-verho-64717 (дата звернення: 20.03.2021).

8. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.21 р. № 179. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-nacionalnoyi-eko-a179 (дата звернення: 20.03.2021).

9. Концепція розвитку цифрових компетентностей: Розпорядження Кабінету Міністрів України від 03.03.21 р. № 167. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text (дата звернення: 20.03.2021).

10. 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 16.01.17 р. № 8/2017. URL: https://zakon.rada.gov.ua/laws/show/8/2017#n2 (дата звернення: 20.03.2021) .

11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 06.12.17 р. № 1009. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р#Text (дата звернення: 20.03.2021).

12. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 20.03.2021).

13. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (дата звернення: 20.03.2021).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~