УДК 349:004.49
DOI https://doi.org/10.32782/yuv.v3.2024.29

О. Скіцько,
кандидат технічних наук,
старший науковий співробітник
Національної академії Служби безпеки України

Р. Ширшов,
Національна академія Служби безпеки України

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ УКРАЇНИ: СУЧАСНИЙ СТАН

Вступ. Сьогодні забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного напряму здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1]. Сучасне століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій [2].

З 2014 року Україна змушена надавати відсіч гібридній російській збройній агресії, в тому числі у кіберпросторі. На теперішній час кіберпростір, разом з іншими фізичними просторами, визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [1].

Протягом останнього десятиліття все ширше крім більш вузького та технічного терміну «кіберзахист» почав вживатися термін «кібероборона» як частина національної системи оборони країни. Досягнення належного рівня кіберборони, здатного задовольнити інтереси держави, безпосередньо залежить від якості її законодавчого забезпечення.

Проблематику, пов'язану з правовим забезпеченням кібероборони в Україні, в своїх дослідженнях розглядали О. Бакалинський, С. Вдовенко, Р. Грищук, А. Давидюк, Ю. Даник, В. Докіль, Є. Живило, Р. Лук'янчук, Д. Пахольченко, В. Тютюнник, С. Фараон, О. Черноног, В. Шеломенцев та інші. Проте, сучасний стан нормативно-правового забезпечення кібероборони України висвітлені фрагментарно.

Метою статті є розкриття особливостей нормативно-правового забезпечення кібероборони України в умовах сьогодення.

Виклад основного матеріалу. Правову основу забезпечення кібероборони України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законодавством, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові

 © О. Скіцько, Р. Ширшов, 2024

акти, що приймаються на виконання законів України. Дефініція «кібероборона» закріплено на законодавчому рівні. Зокрема, в Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [3]. Тобто кібероборона знаходить свій вираз у системі певних заходів у кіберпросторі, спрямованих на захист національної безпеки України. Вона спрямована на забезпечення захисту суверенітету й обороноспроможності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Водночас, погодимось з науковцями, які доводять, що законодавчо визначена дефініція кібероборони потребує корегування, адже цілком зрозуміло, що політичні, економічні, соціальні, правові, організаційні заходи, які спрямовані на досягнення її мети здійснюються не в кіберпросторі. Тому цілком доцільним виявляється пропозиція визначати кібероборону як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в державі та кіберпросторі й спрямовані на забезпечення захисту її суверенітету та обороноздатності, запобігання виникненню збройного конфлікту та відсіч збройній агресії [4, с. 24].

На сучасному етапі розвитку суспільства законодавче забезпечення кібероборони відбувається як на міжнародному рівні, так і на національному. Базовим міжнародним документом у сфері кібероборони, ратифікованим Верховною Радою України, є Конвенція про кіберзлочинність [5] (далі – Конвенція). У Конвенції наголошується, що для ефективності боротьби з кіберзлочинністю надважливим є зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими правопорушеннями, зокрема, кримінальними, шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [5].

В національному законодавстві низка нормативно-правових актів створює правове підґрунтя кібероборони. Зокрема, Конституція України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про оборону України», «Про національну безпеку України», «Про ратифікацію Конвенції про кіберзлочинність», «Про інформацію», «Про державну таємницю» тощо. Окремі закони безпосередньо встановлюють правові засади кібероборони, а інші – опосередковано, лише в окремій їх частині.

Базовим законом щодо кібероборони України є Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забез-

печення кібербезпеки. Відповідно до цього Закону оборонні заходи входять до національної системи кібербезпеки, а Міністерство оборони України та Генеральний штаб Збройних сил України виконують завдання щодо підготовки держави до відбиття воєнної агресії у кіберпросторі, тобто кібероборони [3]. Також у наведеному Законі передбачена необхідність військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану, що є надзвичайно актуальним в умовах протистояння повномасштабному вторгненню рф в Україну. Таким чином, з-поміж іншого в Базовому законі розподілено повноваження між органами державної влади щодо здійснення заходів забезпечення кібербезпеки, а органом, що здійснює кібероборону відповідно до компетентності, визначено Міністерство оборони України й Генеральний штаб Збройних Сил України. При цьому в законі не встановлено момент розмежування, коли під час кібератаки необхідно переходити від заходів кіберзахисту до заходів кібероборони та якими повноваженнями наділені згадані суб'єкти для здійснення кібероборони [6, с. 140]. Цей момент врегульований відомчими актами, що містять інформацію з обмеженим доступом.

У свою чергу у Законі України «Про оборону України» [7] закріплена обов'язковість здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії, у тому числі – проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі при підготовці до захисту та захисту України в разі збройної агресії. Привертає увагу, що обов'язковість здійснення таких заходів передбачена в мирний час в ході підготовки держави до оборони, проте безпосередні кроки, які необхідно робити в напрямі кібероборони під час протистояння збройній агресії у зазначеному законі не відображені.

Систему законодавчого забезпечення кібероборони також складають підзаконні нормативно-правові акти, серед яких важливе місце посідають Укази Президента України, якими затверджено низку стратегій та концепцій, що висвітлюють практичні заходи у цьому напрямі. До таких стратегій та концепцій відносяться: Стратегія національної безпеки України, Концепція розвитку сектору безпеки і оборони України, Стратегія кібербезпеки України, Стратегія воєнної безпеки України, Стратегія інформаційної безпеки тощо.

У чинній Стратегії кібербезпеки України (далі – Стратегія) визначені пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Враховуючи зміст зазначеної Стратегії можна стверджувати, що основними викликами та загрозами, які виникають у сфері кібероборони є:

– активне використання кіберзасобів у міжнародній конкуренції;

– змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;

– мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

– вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

– упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків [1].

У нормативно-правових актах чітко окреслено, що рф залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [1] та актуалізує розроблення сучасних заходів у сфері кібероборони.

На теперішній час прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед рф, міжнародних хакерських угруповань для реалізації кібервпливу [1].

Пріоритетами у сфері кібероборони України є:

– 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.

У законодавстві передбачено, що дієва кібероборона є ціллю, що необхідно досягнути для формування потенціалу стримування, тобто спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму. Формуючи дієву кібероборону Україна має здійснити низку заходів, а саме:

– створити та забезпечити розвиток (у тому числі кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі;

– сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування;

– забезпечити ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони;

– забезпечити належне навчання та фінансове забезпечення структур, зазначених вище;

– забезпечити систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності [1].

Ефективній реалізації зазначених заходів сприятимуть певні кроки з боку держави, зокрема:

– утворення у системі Міністерства оборони України кібервійськ та

забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору;

– запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

– розроблення та виконання плану кібероборони як складової частини плану оборони України;

– проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності;

– створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею;

– забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

– запровадження у системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки [1].

Наведені вище заходи також знайшли своє закріплення у Стратегії, що надає їм ознак обов'язковості та дозволяє сподіватись на створення дієвої системи кібероборони України.

Ми погоджуємось з тим, що поряд із активним законодавчим забезпеченням кібероборони, нажаль, ні законами України, ні іншими нормативно-правовими актами не визначено перелік вичерпних заходів щодо підготовки до відбиття та безпосередньо відбиття воєнної агресії у кіберпросторі. Тому, для досягнення мети та безпосереднього виконання заходів у сфері забезпечення кібербезпеки сектору безпеки і оборони, визначених в окреслених вище нормативно-правових актах, необхідно стандартизувати та гармонізувати в нормативно-правовому полі України дефініції термінологічних систем сфери кібероборони [4, с. 25]. Більше того, система правового регулювання повинна бути всеосяжною і включати як фактичні засоби правового регулювання, які можуть чітко описувати зміст і сутність публічних правовідносин, що виникають у кібероборoні, так і методи та засоби, що дозволяють суб'єктам правовідносин у цій сфері бути захищеними від різних незаконних посягань [8, с. 269].

Висновок. Враховуючи європейський вектор руху країни необхідно прагнути вдосконалювати законодавство, зокрема, у сфері кібероборони, з врахуванням вимог міжнародних нормативно-правових актів. Варто погодитись, що впровадження досвіду та передової практики країн ЄС та стандартів НАТО має бути пріоритетом. До того ж в ході вдосконалення системи законодавства необхідно брати до уваги надзвичайно швидкі темпи розвитку технологій, що призводить до випередження правопорушниками представників держави на декілька кроків у вдосконаленні своєї діяльності. Тому лише скоординовані дії відповідних органів на всіх рівнях кібероборони гарантуватиме її ефективність та досягнення цілей, які постають перед державою у цей складний час протистояння збройній агресії рф проти України.

В статті розкрито особливості нормативно-правового забезпечення кібероборони України в умовах сьогодення. З 2014 року Україна надає відсіч гібридній російській збройній агресії. На теперішній час кіберпростір, разом з іншими фізичними просторами, визнано одним з можливих театрів воєнних дій.

Кібероборона знаходить свій вираз у системі певних заходів у кіберпросторі, спрямованих на захист національної безпеки України. Вона спрямована на забезпечення захисту суверенітету й обороноспроможності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Правову основу забезпечення кібероборони України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законодавством, Конвенція про кіберзлочинність, інші міжнародні договори, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Враховуючи європейський вектор руху країни необхідно прагнути вдосконалювати законодавство, зокрема, у сфері кібероборони, з врахуванням вимог міжнародних нормативно-правових актів. Варто погодитись, що впровадження досвіду та передової практики країн ЄС та стандартів НАТО має бути пріоритетом. До того ж в ході вдосконалення системи законодавства необхідно брати до уваги надзвичайно швидкі темпи розвитку технологій, що призводить до випередження правопорушниками представників держави на декілька кроків у вдосконаленні своєї діяльності. Тому лише скоординовані дії відповідних органів на всіх рівнях кібероборони гарантуватиме її ефективність та досягнення цілей, які постають перед державою у цей складний час протистояння збройній агресії рф проти України.

Ключові слова: кібероборона, кіберпростір, кібербезпека, кібертероризм, воєнна агресія.

Skicko O., Shirshov R. Regulatory and legal provision of cyber defense of Ukraine: current state

The article reveals the peculiarities of regulatory and legal support of cyber defense of Ukraine in today's conditions. Since 2014, Ukraine has been repelling hybrid Russian armed aggression. Currently, cyberspace, along with other physical spaces, is recognized as one of the possible theaters of war.

Cyber defense finds its expression in the system of certain measures in cyberspace aimed at protecting the national security of Ukraine. It is aimed at ensuring the protection of the sovereignty and defense capability of the state, preventing the emergence of an armed conflict and repelling armed aggression.

The legal basis for ensuring cyber defense of Ukraine is the Constitution of Ukraine, laws of Ukraine on the foundations of national security, principles of domestic and foreign policy, electronic communications, protection of state information resources and information, the requirement for protection of which is established by legislation, the Convention on Cybercrime, other international treaties, decrees of the President of Ukraine , acts of the Cabinet of Ministers of Ukraine, as well as other regulatory acts adopted to implement the laws of Ukraine.

Taking into account the European vector of the country's movement, it is necessary to strive to improve legislation, in particular, in the field of cyber defense, taking into account the requirements of international legal acts. It is worth agreeing that the implementation of experience and best practices of EU countries and NATO standards should be a priority. In addition, during the improvement of the legal system, it is necessary to take into account the extremely fast pace of technological develop-

ment, which leads to offenders being several steps ahead of state representatives in improving their activities. Therefore, only the coordinated actions of the relevant bodies at all levels of cyber defense will guarantee its effectiveness and the achievement of the goals facing the state in this difficult time of confronting the armed aggression of the Russian Federation against Ukraine.

Key words: cyber defense, cyber space, cyber security, cyber terrorism, military aggression.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 сер. 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

2. Матанська, А. О., Борисов, М.Ю. Шостий технологічний уклад в сучасній світовій економіці: зміст і початок. Добробут націй в умовах європейської інтеграції : зб. наук. праць 10-ї міжнар. наук.-практ. конф. – Одеса: Одес. нац. ун-т ім. І. І. Мечникова, 2020

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. CS&CS, Issue 1(13) 2019. p. 17-29.

5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вер. 2005 р. № 2824-IV. URL : https://zakon.rada.gov.ua/laws/show/2824-15#Text.

6. Роллер В.М. Правове регулювання здійснення кібероборони. Право і суспільство. 2018. № 5. Ч. 2. С. 137-141.

7. Про оборону України : Закон України від 06 груд. 1991 р. № 1932-XII. URL : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

8. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. Юридичний науковий журнал. 2023. № 1. С. 267-270.