УДК 342.95
DOI https://doi.org/10.32782/klj/2021.3.22

Омельченко А. В.,
доктор юридичних наук, професор,
завідувач кафедри цивільного та трудового права
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Анотація. У статті автором відзначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Питома вага кіберзагроз зростає, і ця тенденція за ступенем розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту посилюватиметься. Зростання такого впливу на функціонування структур управління, як національних, так і транснаціональних, формує нову безпекову ситуацію.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, Конвенція про кіберзлочинність, інші міжнародні договори, нормативно-правові акти, що приймаються на виконання законів України.

Правові та організаційні основи забезпечення кібербезпеки визначають Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII та Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021.

Координація діяльності у сфері кібербезпеки як складової частини національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки. Сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури являє собою Національну систему кібербезпеки.

Ключові слова: *кібербезпека, кіберзагроза, кібератака, кіберзахист, кіберпростір, Національна система кібербезпеки, державно-приватне партнерство.*

Omelchenko A. V. Organizational and legal bases of cybersecurity of Ukraine

Abstract. In this article, the author notes that ensuring cybersecurity is one of the priorities in Ukraine's national security system. The share of cyber threats is growing and this trend will intensify with the development of information technologies and their convergence with artificial intelligence technologies. The growth of such influence on the functioning of both national and transnational governance structures creates a new security situation.

The legal basis for cybersecurity in Ukraine is the Constitution of Ukraine, laws of Ukraine on national security, principles of domestic and foreign policy, electronic communications, protection of state information resources and information, the Convention on Cybercrime, other international treaties, regulations adopted to enforce laws of Ukraine.

Legal and organizational bases of cybersecurity are determined by the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" of October 5, 2017 № 2163-VIII and Cyber Security Strategy of Ukraine, approved by the Decree of the President of Ukraine of August 26, 2021 № 447/2021.

Coordination of activities in the field of cybersecurity as a component of national security of Ukraine is carried out by the President of Ukraine through the National Security and Defense Council of Ukraine headed by him. The National Coordination Center for Cyber Security, as a working body of the National Security and Defense Council of Ukraine, coordinates and monitors the activities of entities in the security and defense sector that provide cyber security. The Cabinet of Ministers of Ukraine ensures the formation and implementation of state policy in

the field of cybersecurity. A system of subjects of cybersecurity and interrelated measures of political, scientific and technical, informational, educational nature, organizational, legal, operational and investigative, intelligence, counterintelligence, defense, engineering and technical measures, as well as measures of cryptographic and technical protection of national information resources, cyber protection of critical information infrastructure is the National Cyber Security System.

Key words: *cybersecurity, cyberthreat, cyberattack, cyberdefense, cyberspace, National Cyber Security System, public-private partnership.*

Постановка проблеми. Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Питома вага кіберзагроз зростає, і ця тенденція за ступенем розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту найближчим десятиліттям посилюватиметься. Зростання такого впливу на функціонування структур управління, як національних, так і транснаціональних, формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами визнано одним із можливих театрів воєнних дій. Зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти та механізми кібератак. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пандемія COVID-19 матиме довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів оброблення інформації, зокрема персональних даних. Це вимагає забезпечення належного рівня їх захищеності та змушує державу і бізнес впроваджувати додаткові механізми й заходи щодо належного функціонування і захисту всіх необхідних для життєдіяльності інформаційних ресурсів і систем [1].

Метою статті є висвітлення організаційно-правових засад забезпечення кібербезпеки України.

Стан дослідження. Дослідженням окремих питань організаційно-правового забезпечення кібернетичної безпеки України присвячені наукові праці Р.В. Лук'янчука, І.В. Діордіци, Д.В. Дубова, В.В. Бухарєва, Ю.Г. Даника, А.В. Тарасюка [2–9].

Виклад основного матеріалу. Правову основу забезпечення кібербезпеки 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 законом, закони України, 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 акти, що приймаються на виконання законів України.

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини й 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 забезпечення кібербезпеки визначає Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [10].

Важливим нормативно-правовим актом у сфері забезпечення кібербезпеки є Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021, яка ґрунтується на положеннях Конституції України, законів України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України», Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392, Концепції боротьби з тероризмом в Україні, затвердженої Указом Президента України від 5 березня 2019 р. № 53, інших нормативно-правових актів [1].

В Законі України «Про основні засади забезпечення кібербезпеки України» вперше

в законодавстві України наведено нормативне визначення таких нових юридичних термінів, як «кібербезпека», «кіберзагроза», «кібератака», «кіберзахист», «кіберзлочин» («комп'ютерний злочин»), «кіберзлочинність», «кібероборона», «кіберпростір». Так, кіберзагрози – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Кіберпростором є середовище (віртуальний простір), яке дає можливість здійснювати комунікації та/або реалізацію суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Таким чином, кібербезпека визначається як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці України у кіберпросторі [10].

До об'єктів кібербезпеки належать конституційні права і свободи людини й громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури. Відповідно, до об'єктів кіберзахисту належать комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [10].

Координація діяльності у сфері кібербезпеки як складової частини національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини й громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України). Суб'єктами, які безпосередньо вживають у межах своєї компетенції заходів із забезпечення кібербезпеки, є міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [10].

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції вживають заходів щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; вживають інших заходів із забезпечення розвитку та безпеки кіберпростору.

Сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури являє собою Національну систему кібербезпеки.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Відповідно до Конституції і законів України, зазначені суб'єкти виконують такі основні завдання.

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; вживає організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

2) Національна поліція України забезпечує захист прав і свобод людини й громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; вживає заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

4) Міністерство оборони України, Генеральний штаб Збройних Сил України, відповідно до компетенції, вживають заходів із підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

5) Розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз

національній безпеці України у кіберпросторі, інших подій та обставин, що стосуються сфери кібербезпеки.

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг.

Крім зазначених, до суб'єктів забезпечення кібербезпеки слід віднести Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA, завданнями якої є накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST; взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України.

Однією з форм забезпечення кібернетичної безпеки є державно-приватна взаємодія, яка застосовується з урахуванням установлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності [5; 10].

Висновок. 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 сегменту кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя. Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі [1]. У такій ситуації дослідження організаційно-правових питань забезпечення кібербезпеки є актуальним та перспективним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 6 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7.

2. Лук'янчук Р. Державне управління у сфері забезпечення кібербезпеки України : автореф. дис. … канд. наук з держ. упр. : 25.00.01 ; Інститут законодавства Верховної Ради України. Київ, 2017. 19 с.

3. Діордіца І.В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія. Запоріжжя : Гельветика, 2017. 547 с.

4. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки Україн : автореф. дис. … докт. юрид. наук : 12.00.07 ; Запорізький національний університет. Запоріжжя, 2018. 32 с.

5. Дубов Д.В. та ін. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналітична доповідь. Київ : НІСД, 2018. 81 с.

6. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України : автореф. дис. … канд. юрид. наук : 12.00.07 ; Сумський державний університет. Суми, 2018. 20 с.

7. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони : підручник. 2-ге вид., перероб. та доп. Одеса : ОНАЗ ім. О.С. Попова, 2019. 319 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. … докт. юрид. наук : 12.00.07 ; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

10. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.