Мялковський Данило Владиславович,
здобувач,
Інститут підготовки кадрів Державної служби зайнятості України,
м. Київ
ORCID 0000-0002-8246-8437

УДК 35.316 **doi: 10.34213/tp.19.03.26**

ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ МІЖНАРОДНИМ СПІВРОБІТНИЦТВОМ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

В статті проаналізовано організаційно-правові механізми державного управління міжнародним співробітництвом України у сфері кібербезпеки. Також розроблено на його основі пропозиції органам державної влади та пріоритетні напрямами, спрямовані на удосконалення чинних організаційно-правових механізмів державного управління міжнародним співробітництвом України на загальнодержавному рівні.
Ключові слова: кібербезпека, міжнародне співробітництво, кіберінцидент, безпека інформації.

Постановка проблеми. Зростання кількості, масштабів, інтенсивності, складності кіберінцидентів та кіберзагроз у світовому кіберпросторі, ефективно протидіяти яким окремо неспроможна будь-яка з держав, є одним із головних факторів, що зумовлює необхідність їхньої міжнародної співпраці у сфері кібербезпеки та кіберзахисту, об'єднання їхніх сил та засобів для зменшення рівня кіберзагроз для громадян, суспільства та держави. Незважаючи на те, що законодавство України передбачає виконання заходів з міжнародної взаємодії у сфері кібербезпеки, аналізу його, що би дав змогу об'єктивно оцінити відповідність запроваджених організаційно-правових механізмів державного управління міжнародним співробітництвом до сучасних вимог, як і обґрунтування підходів та визначення пріоритетних напрямів щодо їх удосконалення, не проводилося.

Аналіз останніх досліджень і публікацій. Проблемі вдосконалення міжнародного співробітництва в галузі кібербезпеки та кіберзахисту присвячено достатньо наукових робіт іноземних та вітчизняних науковців та практиків [1–7]. Автори здебільшого констатують необхідність міжнародного співробітництва у сфері кібербезпеки у форматах: Україна – ЄС, Україна – НАТО, Україна – регіональні об'єднання країн, двостороннє міжнародне співробітництво, удосконалення дійових та розроблення нових механізмів такого співробітництва, але при цьому однією з основних проблем залишається проблема координованості дій суб'єктів міжнародного співробітництва в цій сфері.

Метою статті є аналіз організаційно-правових механізмів державного управління міжнародним співробітництвом України у сфері кібербезпеки та розроблення на його основі пропозицій органам державної влади щодо їхнього вдосконалення.

Виклад основного матеріалу. Актуальність проблеми міжнародного співробітництва для України у сфері кібербезпеки насамперед зумовлено: зростанням кількості, масштабів, інтенсивності, складності кіберінцидентів та кіберзагроз у світовому кіберпросторі, ефективно протидіяти яким окремо не спроможна жодна держава; веденням проти нашої країни гібридної війни

з боку РФ, складником якої є кібервійна, що особливо загострилася у зв'язку з виборчими кампаніями в нашій країні; європейським та євроатлантичним вектором нашої зовнішньої політики. Тому одним з пріоритетних напрямів державної політики забезпечення національної безпеки, невід'ємним складником кібербезпеки, європейської та євроатлантичної інтеграції є міжнародне співробітництво, що має органічно доповнювати інші напрями політик.

В Україні міжнародним співробітництвом у сфері кібербезпеки, зокрема проблемою упровадження міжнародних стандартів у цій сфері, займаються декілька державних органів, громадських та професійних об'єднань і організацій, бізнес-структур, а також галузевих регуляторів, що об'єктивно потребує їхньої відповідної координації.

На загальнодержавному рівні, відповідно до Закону України "Про основні засади кібербезпеки України" (далі – Закон) [8], взаємодія суб'єктів забезпечення кібербезпеки в цілому та зокрема у сфері міжнародного співробітництва здійснюється Верховною Радою України, Президентом України (безпосередньо та через Раду національної безпеки і оборони України (РНБОУ) та її робочий орган – Національний координаційний центр кібербезпеки (НКЦК)), Кабінетом Міністрів України (КМУ) та іншими основними суб'єктами національної системи кібербезпеки (рисунок).

Рисунок. Суб'єкти міжнародної взаємодії у сфері кібербезпеки

Оскільки в міжнародному співробітництві беруть участь майже всі суб'єкти забезпечення кібербезпеки, що визначені законодавством, то координованість їхніх дій повинна забезпечуватися насамперед відповідними правовими та організаційними механізмами публічного управління та адміністрування. При цьому необхідно враховувати, що кожний із таких суб'єктів, є суб'єктом міжнародного співробітництва в рамках конкретних міжнародних договорів з отримання міжнародної допомоги у сфері кібербезпеки у своїй галузі. Водночас реалізація стратегічного курсу держави на

набуття повноправного членства України в Європейському Союзі (ЄС) та в Організації Північно-Атлантичного договору (НАТО), зокрема, передбачає [9]:

– забезпечити поглиблення співробітництва з ЄС у питаннях інформаційної безпеки та кібербезпеки, забезпечення стійкості критичної інфраструктури;

– опрацювати з ЄС можливості розширення співпраці у сферах протидії дезінформації, у т. ч. шляхом співпраці з East StratCom Task Force, зміцнення інституційних спроможностей у боротьбі з кіберзагрозами.

Їхнє виконання доручено КМУ, який серед органів виконавчої влади здійснює загальну координацію процесу формування та реалізації державної політики у сфері кібербезпеки.

У складі Секретаріату КМУ як самостійний структурний підрозділ функціонує Урядовий офіс координації європейської та євроатлантичної інтеграції, який згідно з Положенням про цей орган [10; 11] та ст. 21 Закону України "Про Кабінет Міністрів України" має, зокрема, компетенції щодо планування, моніторингу та оцінювання результативності виконання завдань та координації діяльності органів виконавчої влади з розроблення та здійснення заходів, спрямованих на виконання:

– Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [12] (далі – Угода про асоціацію), інших міжнародних договорів України з питань європейської інтеграції і домовленостей між Україною та ЄС;

– річних національних програм в рамках Комісії Україна – НАТО, рішень цієї Комісії в рамках Хартії про особливе партнерство між Україною та Організацією Північно-Атлантичного договору та Декларації про її доповнення, інших міжнародних договорів між Україною та НАТО та уповноваженими органами НАТО;

– удосконалення системи та механізму координації діяльності органів виконавчої влади у сферах європейської та євроатлантичної інтеграції.

З метою підвищення ефективності, оперативності та обґрунтованості прийняття урядових рішень за відповідною тематикою в структурі КМУ створено Урядовий комітет з питань європейської, євроатлантичної інтеграції, міжнародного співробітництва та регіонального розвитку, до складу якого включено керівників профільних міністерств та Національного банку України.

Головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері зовнішніх зносин є Міністерство закордонних справ (МЗС) України [13], на яке покладається завдання щодо координації діяльності державних органів стосовно реалізації єдиного зовнішньополітичного курсу України, зокрема й у сфері кібербезпеки та кіберзахисту.

Питання загальної координації міжнародного співробітництва України з ЄС належить Міністерству економічного розвитку та торгівлі України (Мінекономрозвитку), на яке згідно із законодавством [14] покладено і завдання: щодо державної політики з питань економічного співробітництва України з ЄС, залучення міжнародної технічної допомоги (далі – МТД) у сфері технічного регулювання, стандартизації, відповідно до яких воно забезпечує і координує виконання Українською Стороною зобов'язань за міжнародними

договорами України з ЄС; координацію міжвідомчої роботи з питань імплементації положень Угоди про асоціацію, забезпечує формування стратегічних і щорічних програм залучення МТД та координує діяльність, пов'язану із її залученням; проводить державну реєстрацію/перереєстрацію проектів (програм) МТД в Україні; координує здійснення заходів із розроблення проектів (програм) МТД, проводить моніторинг їхнього виконання тощо. Програму технічного співробітництва 2018 ENI/2018/041-188, згідно з Угодою про фінансування Програми технічного співробітництва 2018 [15], підписантом якої є Мінекономрозвитку, спрямовано на підтримку України в реалізації Угоди про асоціацію. Ця Програма забезпечуватиме консультації в галузі політики та щодо процесу наближення нормативної бази України до вимог ЄС та формування потенціалу за пріоритетними напрямами, охопленими Угодою про асоціацію. Зокрема, допомога надаватиметься в галузях стандартизації, електронного зв'язку та кібербезпеки. Основними результатами заходу щодо кібербезпеки має бути підтримка реалізації ключових напрямів та заходів, визначених у Стратегії кібербезпеки України для забезпечення кібербезпеки, консолідація законодавчої бази у сфері кібербезпеки відповідно до вимог ЄС та формування потенціалу в рамках національної системи кібербезпеки в Україні для забезпечення кращого захисту критично важливої інфраструктури та підвищення стійкості та реакції на кіберзагрози.

Водночас, згідно з інформацією офіційного веб-порталу координації МТД ProAID [16], жодної програми технічної допомоги у сфері кібербезпеки не було розроблено, зареєстровано або перереєстровано.

У частині участі у формуванні та реалізації державної політики щодо захисту в кіберпросторі інформаційних ресурсів держави та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури основну роль покладено на Державну службу спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ), яка, згідно із законодавством [17], координує діяльність інших суб'єктів забезпечення кібербезпеки та є головним суб'єктом серед центральних органів виконавчої влади в питаннях міжнародного співробітництва у сфері кібербезпеки та кіберзахисту. ДССЗЗІ забезпечує функціонування Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, яка здійснює взаємодію з іншими державами та міжнародними організаціями з питань насамперед оперативного реагування на кіберінциденти, зокрема в межах участі у Форумі команд реагування на інциденти безпеки FIRST.

На загальнодержавному рівні міжнародне співробітництво у сфері кібербезпеки Україною здійснюється як шляхом двосторонньої взаємодії з окремими державами, так і шляхом співробітництва з міжнародними організаціями, насамперед ЄС та НАТО.

Взаємодія в рамках співробітництва з ОБСЄ здійснюється, зокрема, за напрямом боротьби з кіберзлочинністю. Суб'єктом міжнародної взаємодії згідно із Законом України "Про ратифікацію Конвенції про кіберзлочинність" [18] є Міністерство внутрішніх справ (МВС) України, яке визначено органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних із комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі.

Нормативно-правовими актами, які безпосередньо не визначають організацію взаємодії щодо кіберінцидентів, але можуть бути використаними, є Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах [19] та розроблений на її виконання Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [20].

Проект Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час запобігання появі, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків [21] передбачає конкретні заходи на різних фазах (стадіях, від 0 до 3) життєвого циклу кіберінциденту.

У межах запобігання кіберінцидентам та кібератакам ДССЗЗІ взаємодіє з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в межах участі у Форумі команд реагування на інциденти безпеки FIRST. Міністерство оборони України (далі – Міноборони) та Генеральний штаб Збройних Сил України (далі – Генштаб) здійснюють військову співпрацю з НАТО, у т. ч. з військовими CERT країн – членів НАТО.

При виявленні спроб та/або фактів вчинення кібератак та кіберінцидентів, стримування кібератак Міноборони та Генштаб інформують ДССЗЗІ, CERT-UA, Службу безпеки України (СБУ) про об'єкт та про джерело кібератаки на об'єкти воєнної сфери або сфери оборони держави.

Під час припинення та усунення наслідків кібератак та кіберінцидентів, відновлення сталого функціонування об'єктів критичної інформаційної інфраструктури ДССЗЗІ разом із суб'єктами кіберзахисту здійснюють взаємодію з суб'єктами кіберзахисту, а також міжнародну взаємодію з командами реагування (CERT, CSIRT) інших країн щодо припинення (блокування) кібератак (кіберінцидентів) та усунення їхніх наслідків. Міноборони та Генштаб забезпечують безпосередню взаємодію з військовими CERT країн – членів НАТО.

Під час аналізу виявлених кібератак та кіберінцидентів, проведених заходів, надання рекомендацій щодо запобігання реалізації кіберзагроз ДССЗЗІ та суб'єкти кіберзахисту здійснюють взаємний обмін інформацією з командами реагування (CERT, CSIRT) інших країн щодо виявлених кібератак та кіберінцидентів та проведених заходів із запобігання реалізації кіберзагроз. Міноборони та Генштаб забезпечують взаємодію з військовими CERT країн – членів НАТО та з виконавчими підрозділами суб'єктів забезпечення кібербезпеки з питань захисту інформації, кіберзахисту, кібербезпеки та кібероборони.

Зведений порядок взаємодії та міжнародну активність під час його виконання наведено в таблиці.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Було проаналізовано нормативно-правові акти, норми яких зіставлено з чинними вимогами до спроможностей України у здійсненні міжнародного співробітництва у сфері кібербезпеки. Доведено, що однією з головних проблем залишається проблема координованості дій національних суб'єктів кібербезпеки як між собою, так і з відповідними міжнародними організаціями та інституціями, яка є основною причиною недостатньої ефективності державної політики в цій сфері.

Міжнародна взаємодія суб'єктів кібербезпеки
на етапах життєвого циклу кіберінциденту

Фаза	Запобігання	Виявлення	Припинення	Аналіз
Суб'єкт кібербезпеки	Іноземна організація, з якою здійснюється взаємодія			
ДССЗЗІ	Іноземні та міжнародні організації з питань реагування на кіберінциденти, у т. ч. FIRST	–	CERT, NCSIRT	CERT, NCSIRT
Міноборони та Генштаб	NCSIRC, nation's CERT (Mil-CERT)	–	NCSIRC, CERT інших країн (Mil-Cert)	NCIRC, CERT інших країн (Mil-Cert)
Суб'єкти кіберзахисту	–	–	CERT, CSIRT, MCSIRT інших країн	CERT, CSIRT, Mil-CERT інших країн

Зазначено, що нині проблемою кібербезпеки з міжнародними інституціями та організаціями на загальнодержавному рівні займається ціла низка державних органів, але визначено в конкретних виконавчих міжнародних договорах щодо кібербезпеки або отримали міжнародну технічну допомогу в цій сфері лише Апарат Верховної Ради України, МВС України, Мінекономрозвитку, Міністерство енергетики та вугільної промисловості України, ДССЗЗІ, СБУ, Центральна виборча комісія. При цьому здійснення оцінки відповідності цієї допомоги до реальних потреб із забезпечення кібербезпеки, як і визначення способу її застосування при можливих спільних з іншими суб'єктами забезпечення кібербезпеки заходах залишається в зоні відповідальності цих органів.

При цьому загальний стан національної системи кібербезпеки не повною мірою відповідає сучасним вимогам щодо забезпечення надійного, оперативного, ефективного, результативного та випереджального реагування на кіберзагрози, у т. ч. внаслідок обмежених ресурсів, що виділяються на розвиток цієї сфери, і підкреслює відсутність дієвої державної політики в організації отримання та використання міжнародної технічної допомоги та здійсненні міжнародної взаємодії в цій сфері.

Вибудувана на основі Закону [8] національна система кібербезпеки не забезпечує належним чином виконання завдань з забезпечення, зокрема, міжнародної співпраці у сфері кібербезпеки. Її основні елементи, які безпосередньо виконують завдання із забезпечення кібербезпеки на рівні інституціональної взаємодії, мають пройти глибоку трансформацію (не обмежуючись наведеним нижче).

Зокрема, *Національний координаційний центр кібербезпеки*, який згідно із законодавством є робочим органом РНБОУ і має забезпечувати координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України [22], підвищувати ефективність системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки, просто не має достатнього ресурсу для виконання цієї місії. Він повинен отримати нову парадигму своєї діяльності, статус, реальні повноваження в координації діяльності у сфері кібербезпеки основних суб'єктів національної системи кібербезпеки, відбудові сучасної, ефективної, гнучкої, відповідальної, клієнт-орієнтованої системи забезпечення кібербез-

пеки, зокрема щодо питань міжнародного співробітництва, належного представництва у міжнародних дорадчих органах у сфері кібербезпеки, імплементації найкращого міжнародного досвіду у сфері кібербезпеки, співпраці з міжнародними організаціями та інститутами щодо питань кібербезпеки, залучення на взаємно зрозумілих засадах представників фахового середовища та врахування, після взаємної згоди, його пропозицій.

ДССЗЗІ, маючи широке коло завдань із забезпечення кіберзахисту, має зосередитися на приведенні у відповідність функціонування національної системи кібербезпеки до конкретних регламентів, стандартів та протоколів ЄС та НАТО, а саме NIS Directive [23]:

– виконувати функцію пункту міжнародного контакту щодо кіберінцидентів;

– розробити та упровадити дієві протоколи оброблення кіберінцидентів відповідно до життєвого циклу таких інцидентів, запровадити єдину систему ведення технологічних карток кіберінцидентів;

– запровадити обов'язкове звітування про опрацювання іншими суб'єктами національної системи кібербезпеки наданих їм рекомендацій у сфері кіберзахисту, а також про результати оброблення кіберінцидентів та вказаних вище їхніх технологічних карток;

– розробляти для інших суб'єктів забезпечення кібербезпеки політику щодо МТД, реалізуючи принципи її доцільності та відповідності до реальних потреб, власних спроможностей отримувачів у її використанні, зокрема щодо ліцензійної підтримки, визначення її безпечності та застосовності;

– розробити та упровадити організаційно-правові механізми розвитку національної нормативно-правової бази у сфері криптографічного та технічного захисту інформації, які б забезпечили найшвидший еволюційний перехід до ризик-орієнтованого підходу до організації та забезпечення безпеки інформації з упровадженням цих нових норм (передусім на об'єктах критичної та критичної інформаційної інфраструктури), систем для публічного адміністрування та надання адміністративних послуг, оброблення персональних даних, сприяти відстеженню та упровадженню міжнародних стандартів у сфері безпеки систем, продукції та послуг інформаційно-телекомунікаційних технологій;

– вжити заходів із підготовки та укладання міжнародних договорів щодо взаємодії у сфері кібербезпеки, першочергово з країнами, які законодавчо визначили свою співпрацю з Україною (США, ЄС (в особі ENISA)), а також хоча б з однією країною – членом ЄС та НАТО.

– *МЗС України* повинне мати можливість виступати ініціатором відносин із новими міжнародними партнерами з чітким для них розумінням щодо потреб України та її спроможностей у сфері кібербезпеки;

– *Міноборони та Генштаб,* розбудовуючи свою інфраструктуру відповідно до стандартів НАТО та ЄС та упроваджуючи AJP-6 (Союзницька спільна доктрина з питань зв'язку та інформаційних систем) [24], повинні ретельно опрацьовувати положення інших взаємно пов'язаних документів, зокрема Політики НАТО щодо кібероборони (NATO Policy on Cyber Defence (C-M(2011)0042)), як підмножини системи вимог, викладених у Політиці безпеки НАТО (C-M(2002)49) [25], та Первинної директиви з безпеки комунікаційно-інформаційних систем (Primary Directive on CIS Security, AC/35-D/2004-REV3) [26].

– *Мінекономрозвитку* повинне запроваджувати механізми відповідальності за вчасну реєстрацію програм МТД, організовуючи їхню консультативну

підтримку щодо змісту заходів, засобів та забезпечення застосування в подальшому МТД суб'єктами її отримання. Крім того, зусилля мають зосереджуватися на підготовці міжнародних договорів щодо визнання відповідності продукції інформаційно-телекомунікаційних технологій до вимог кібербезпеки.

Пріоритетними напрямами з удосконалення чинних організаційно-правових механізмів державного управління міжнародним співробітництвом України на загальнодержавному рівні також є:

– визначення вимог та механізмів публічного управління та адміністрування міжнародним співробітництвом у сфері кібербезпеки в умовах повсякденної діяльності та розвитку, а також надзвичайного та воєнного стану, надзвичайних ситуацій, особливого періоду;

– розроблення терміносистеми з питань кібербезпеки на основі узагальнення та систематизації вітчизняного законодавства та його гармонізації з міжнародним законодавством;

– перегляд змісту завдань щодо кібербезпеки органів, що існують, та утворення координаційного ЦОВВ з покладанням на нього одним із головних завдань координацію органів виконавчої влади з питань міжнародного співробітництва у сфері кібербезпеки;

– забезпечення взаємодії Національного центру оперативно-технічного управління мережами телекомунікацій з аналогічними центрами НАТО та ЄС, а також можливе його перепідпорядкування Міноборони з метою підвищення ефективності функціонування національної системи забезпечення кібербезпеки, особливо в умовах надзвичайних ситуацій, надзвичайного стану, воєнного стану, особливого періоду;

– створення системи моніторингу та оцінювання якості державного управління міжнародним співробітництвом України.

Подальші дослідження передбачатимуть проведення аналізу інституційного забезпечення кібербезпекових новацій ЄС та США задля визначення напрямів подальшого вдосконалення організаційно-правових та інших механізмів публічного управління у сфері кібербезпеки.

Список використаних джерел

1. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник НАДУ.* 2015. № 4. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnadu_2015_4_10.

2. Шемчук В. В. Основні напрямки міжнародного співробітництва у сфері кібербезпеки. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Юрид. науки. Кримінальне право та кримінологія; кримінально-виконавче право.* 2018. Т. 29 (68), № 2. С. 125–129.

3. Дешко Л. М., Бонарєва К. Д. Кібербезпека в Україні: Національна стратегія та міжнародне співробітництво. *Порівняльно-аналітичне право.* 2018. № 2. URL: http://pap.in.ua/2_2018/112.pdf.

4. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки, URL: journals.iir.kiev.ua/index.php/pol_n/article/download/3389/3066.

5. Доронін І. М. Організація звітування суб'єктів кібербезпеки. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf. С. 211–213.

6. Забара І. М. Кібернетична безпека держави в умовах розвитку штучного інтелекту: до питання визначення напрямків міжнародно-правового регулювання. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf. С. 213–215.

7. Кравець В. М. Порівняльний аналіз міжнародних індексів кібербезпеки. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf. С. 230–234.

8. Про основні засади кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *ВВР України*. 2017. № 45. Ст. 403.

9. Питання європейської та євроатлантичної інтеграції : Указ Президента України від 20 квіт. 2019 р. № 155/2019. *Урядовий кур'єр.* 2019. № 78.

10. Про Урядовий офіс координації європейської та євроатлантичної інтеграції : Постанова КМУ від 4 жовт. 2017 р. № 759. *Урядовий кур'єр*. 2017. № 199.

11. Деякі питання Секретаріату Кабінету Міністрів України : Постанова КМУ від 24 лип. 2019 р. № 665. *Урядовий кур'єр.* 2019. № 141.

12. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011.

13. Про затвердження Положення про Міністерство закордонних справ України: Постанова Кабінету Міністрів України від 30 березн. 2016 р. № 281. *Урядовий кур'єр.* 2016. № 86.

14. Питання Міністерства економічного розвитку і торгівлі: Постанова Кабінету Міністрів України від 20 серп. 2014 р. № 459. *Урядовий кур'єр.* 2014. № 175.

15. Угода про фінансування Програми технічного співробітництва 2018. URL: https://zakon.rada.gov.ua/laws/show/984_004-18.

16. Веб-портал координації міжнародної технічної допомоги ProAID жодної програми технічної допомоги. URL: http://proaid.gov.ua/uk/projects.

17. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова КМУ від 3 верес. 2014 р. № 411. *Урядовий кур'єр*. 2014. № 166.

18. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. *Урядовий кур'єр.* 2005. № 185.

19. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова Кабінету Міністрів України від 16 листоп. 2002 р. № 1772. *Урядовий кур'єр.* 2002. № 221.

20. Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : наказ Адміністрації Держспецзв'язку від 10 черв. 2008 р. № 94. *Офіц. вісн. України*. 2008. № 52. Ст. 1753.

21. Проект Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=308016&cat_id=38837&ctime=1559743156921.

22. Стратегія кібербезпеки України : Указ Президента України від 15 берез. 2016 р. № 96/2016. *Урядовий кур'єр.* 2016. №52.

23. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

24. Союзницька спільна доктрина з питань зв'язку та інформаційних систем (AJP-6). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602827/doctrine_nato_cis_ajp_6.pdf.

25. Політика безпеки НАТО (C-M(2002)49). URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf.

26. Первинна директива з безпеки комунікаційно-інформаційних систем (Primary Directive on CIS Security, AC/35-D/2004-REV3. URL: http://www.dksi.bg/NR/rdonlyres/6DC49C44-5C52-47A2-8773-6BF11C59E53C/0/Primary_CIS_SecurityAC35D2004REV3.pdf.

References

1. Lukianchuk, R.V. (2015). Mizhnarodne spivrobitnytstvo u sferi zabezpechennia kibernetychnoi bezpeky: derzhavni priorytety, *Visnyk NADU*. *№ 4.* URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnadu_2015_4_10) [in Ukrainian].

2. Shemchuk, V.V. (2018). Osnovni napriamky mizhnarodnoho spivrobitnytstva u sferi kiberbezpeky. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: yurydychni nauky. Kryminalne pravo ta kryminolohiia; kryminalno-vykonavche pravo, vol. 29 (68), No. 2, 125–129* [in Ukrainian].

3. Deshko, L.M., Bonarieva, K.D. (2018). Kiberbezpeka v Ukraini: Natsionalna stratehiia ta mizhnarodne spivrobitnytstvo. *Poriaivnialno-analitychne pravo, 2.* URL: http://pap.in.ua/2_2018/112.pdf [in Ukrainian].

4. Piskorska, H.A., Yakovenko, N.L. Suchasni vyklyky i zahrozy v kiberprostori: formuvannia mekhanizmu mizhnarodnoi informatsiinoi bezpeky. URL: journals.iir.kiev.ua/index.php/pol_n/article/download/3389/3066 [in Ukrainian].

5. Doronin, I.M. (2019). Orhanizatsiia zvituvannia subiektiv kiberbezpeky. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf, p. 211-213 [in Ukrainian].

6. Zabara, I.M. Kibernetychna bezpeka derzhavy v umovakh rozvytku shtuchnoho intelektu: do pytannia vyznachennia napriamkiv mizhnarodno-pravovoho rehuliuvannia. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf, p. 213-215 [in Ukrainian].

7. Kravets V. M. Porivnialnyi analiz mizhnarodnykh indeksiv kiberbezpeky, URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf [in Ukrainian].

8. Pro osnovni zasady kiberbezpeky Ukrainy: Zakon Ukrainy vid 5.10.2017 No. 2163-VIII. (2017). *Vidomosti Verkhovnoi Rady*, *45, art. 403*.

9. Pytannia yevropeiskoi ta yevroatlantychnoi intehratsii: Ukaz President of Ukraine. Decree No. 155/2019. (2019). *Uriadovyi kurier, No. 78*.

10. Pro Uriadovyi ofis koordynatsii yevropeiskoi ta yevroatlantychnoi intehratsii: Postanova Kabinetu Ministriv Ukrainy vid 04.10.2017 №759. (2017). *Uriadovyi kurier, No 199.*

11. Deiaki pytannia Kabinetu Ministriv Ukrainy: Postanova Kabinetu Ministriv Ukrainy vid 24.07.2019 No. 665. (2019). *Uriadovyi kurier. No. 141*.

12. Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony. URL: https://zakon.rada.gov.ua/laws/show/984_011.

13. Pro zatverdzhennia Polozhennia pro Ministerstvo zakordonnykh sprav Ukrainy: Postanova Cabinetu Ministriv Ukrainy vid 30.03.2016 No. 281. (2016). *Uriadovyi kurier. No. 86*.

14. Pytannia Ministerstva ekonomichnoho rozvytku i torhivli: Postanova Kabinetu Ministriv Ukrainy vid 20.08.2014 No. 459. (2014). *Uriadovyi kurier.* No. 175.

15. Uhodoiu pro finansuvannia Prohramy tekhnichnoho spivrobitnytstva Prohramu tekhnichnoho spivrobitnytstva. (2018). URL: https://zakon.rada.gov.ua/laws/show/984_004-18.

16. Veb-portal koordynatsii mizhnarodnoi tekhnichnoi dopomohy ProAID. URL: http://proaid.gov.ua/uk/projects.

17. Pro zatverdzhennia Polozhennia pro Administratsiiu Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy: Postanova Kabinetu Ministriv Ukrainy vid 03.09.2014 No. 411. (2014). *Uriadovyi kurier. No. 166.*

18. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist: Zakon Ukrainy vid 07.09.2005 No. 2824-IV. (2005). *Uriadovyi kurier. No. 185*.

19. Poriadok vzaiemodii orhaniv vykonavchoi vlady z pytan zakhystu derzhavnykh informatsiinykh resursiv v informatsiinykh ta telekomunikatsiinykh systemakh: Postanova Kabinetu Ministriv Ukrainy 16.11.2002 No. 1772. (2002). *Uriadovyi kurier. No. 221*.

20. Poriadok koordynatsii diialnosti orhaniv derzhavnoi vlady, orhaniv mistsevoho samovriaduvannia, viiskovykh formuvan, pidpryiemstv, ustanov i orhanizatsii nezalezhno vid form vlasnosti z pytan zapobihannia, vyiavlennia ta usunennia naslidkiv nesanktsionovanykh dii shchodo derzhavnykh informatsiinykh resursiv v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh : nakaz Administratsii Derzhspetszviazku vid 10.06.2008 No. 94. (2008). *Ofitsiinyi visnyk Ukrainy*. *No. 52. Art. 1753*.

21. Proekt Protokolu spilnykh dii osnovnykh subiektiv zabezpechennia kiberbezpeky, subiektiv kiberzakhystu ta vlasnykiv (rozporiadnykiv) obiektiv krytychnoi informatsiinoi infrastruktury ta pid chas poperedzhennia, vyiavlennia, prypynennia kiberatak ta kiberintsydentiv, a takozh pry usunenni yikhnikh naslidkiv. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=308016&cat_id=38837&ctime=1559743156921.

23. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

24. Allied Joint Doctrine for Communication and Information Systems. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602827/doctrine_nato_cis_ajp_6.pdf.

25. Security Within the North Atlantic Trean Organisation (NATO) (C-M(2002)49). URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf.

26. Primary Directive on CIS Security, AC/35-D/2004-REV3. URL: http://www.dksi.bg/NR/rdonlyres/6DC49C44-5C52-47A2-8773-6BF11C59E53C/0/Primary_CIS_SecurityAC35D2004REV3.pdf.

Mialkovskyi D. V., *Postgraduate Student, Institute of Staff Training of the State Employment Service of Ukraine, Kyiv*
ORCID 0000-0002-8246-8437

ORGANIZATIONAL AND LEGAL MECHANISMS OF PUBLIC ADMINISTRATION OF UKRAINE'S INTERNATIONAL COOPERATION IN CYBERSECURITY

No state is capable of effectively alone counteracting the growth, number, scale, intensity, complexity of cyber incidents and cyber threats. This necessitates international cooperation in cybersecurity and cyber defense, joining forces and means to reduce the level of cyber threats to citizens, society and the state.

The purpose of the article is to analyze the experience of Ukraine on the organizational and legal mechanisms of international cooperation in the field of cybersecurity in order to improve the relevant national mechanisms of public administration.

One of the priorities of the national policy of national security, its integral component of cybersecurity, European and Euro-Atlantic integration is international cooperation, which should organically complement other areas of this policy.

Adoption, implementation and application of international standards, in particular those of the European Union and NATO, are among the main ways of ensuring the effective functioning of the national cybersecurity system.

In Ukraine, several state authorities, public and professional associations and organizations, business structures, and industry regulators are engaged in international cooperation in the field of cybersecurity. This requires their proper coordination.

In order to increase the efficiency, effectiveness and validity of governmental decision-making, a Governmental Committee on European, Euro-Atlantic Integration, International Cooperation and Regional Development has been established within the Cabinet of Ministers of Ukraine, and designated ministrys' coordinators.

But only six ministries cooperate within the framework of concluded agreements or international executive agreements of Ukraine within the framework of the Association Agreement with the European Union or within the framework of the 1997 Charter on a Distinctive Partnership.

Cooperation with the EU is being carried out more and more through the ENISA. Cooperation with the NATO is being carried out through implementation the AJP-6, C-M(2002)49 and AC/35-D/2004-REV3.

Despite the adoption of the Law of Ukraine "On the Main Principles of sustainment of Cybersecurity of Ukraine ", Ukraine's capabilities do not meet the modern requirements sufficiently and need improvement:

– organization of the national cybersecurity system;

– receipt of international technical assistance by cyber-security entities, their proper coordination, applicability, appropriateness and adequacy of modern requirements, responsibility for their receipt and usability;

– enhancement of professional skills not only of cybersecurity professionals but also of other employees of state bodies, enterprises and organizations;

– protocols of interaction and information on cyber incidents both in Ukraine and foreign partners.

Key words: cybersecurity, international cooperation, cyberincident, information security.

Надійшла до редколегії 10.09.2019 р.