УДК 35.316

Дубов Дмитро,
ORCID iD 0000-0001-9728-369X
Олексюк Лілія,
ORCID iD 0000-0002-9006-2592
Потій Олександр
Семенченко Андрій,
ORCID iD 0000-0001-6482-3872
E-mail: Andrii.semenchenko@gmail.com

ФУНКЦІОНУВАННЯ ЕКСПЕРТНОЇ РАДИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ЯК ДЕМОКРАТИЧНИЙ ІННОВАЦІЙНИЙ ІНСТРУМЕНТ ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ

https://doi.org/10.32689/2618-0065-2021-2(8)-92-110

Анотація. Актуальність проблеми дослідження обумовлена низкою факторів, основними з яких є вимоги законодавства щодо посилення ефективності та результативності державно-приватного партнерства в сфері кібербезпеки та кіберзахисту, незадовільний стан державно-приватної взаємодії суб'єктів кібербезпеки в Україні, масштабне та динамічне зростання кіберзагроз та кіберінцидентів, ліквідація та нейтралізація яких самостійно лише силами та засобами державних органів не можлива, недієвість існуючих інструментів державно-приватної взаємодії. Незважаючи на широкий спектр досліджень як в цілому з проблематики кібербезпеки та кіберзахисту, так і щодо державно-приватної взаємодії в цій сфері суб'єктів кібербезпеки залишились по за увагою інноваційні підходи та інструменти державно-приватної взаємодії, що базуються на нових концептуальних засадах, кращому національному та міжнародному досвіді, та їх впровадження в практику шляхом організації функціонування Експертної ради інформаційної та кібербезпеки. Метою статті є узагальнення національного та міжнародного досвіду застосування інструментів державно-приватної взаємодії суб'єктів кібербезпеки та кіберзахисту, визначення ролі, концептуальних засад та моделі функціонування Експертної ради інформаційної та кібербезпеки як демократичного інноваційного інструменту державно-приватної взаємодії основних суб'єктів кібербезпеки та кіберзахисту, її місця в перспективній організаційно-технічній моделі кіберзахисту. Охарактеризовано основні інструменти державно-приватної взаємодії та партнерства у суміжних з кібербезпекою сферах; узагальнено досвід діяльності рад з кібербезпеки Нідерландів, Литви й Естонії та оцінена можливість його застосування в Україні; вперше визначено концептуальні засади та модель діяльності Ради

інформаційної та кібербезпеки, що містять базові принципи, стратегічні цілі та завдання, структуру, механізм її формування та функціонування; розкрито особливості та доведена унікальність Ради як демократичного інноваційного та перспективного інструменту державно-приватної взаємодії у сфері кібербезпеки, а також її місце в організаційно-технічній моделі кіберзахисту; сформульовано напрями подальшого розвитку Ради та обґрунтовано основні ризики для його позитивного тренду.

Ключові слова: рада інформаційної та кібербезпеки, державно-приватна взаємодія, концептуальні засади, основні суб'єкти кібербезпеки, організаційно-технічна модель кіберзахисту

Постановка проблеми. Розвиток інформаційно-комунікаційних технологій, їх масштабне та динамічне впровадження в усі сфери суспільних відносин орієнтовано на підвищення конкурентоспроможні держав, рівня життєдіяльності їх громадян, демократизації управління, формування інформаційного суспільства, цифрової економіки тощо. Але одночасно це є джерелом загроз для громадян, суспільства й держави особливо в умовах хаотичного впровадження та безконтрольного застосування цих технологій, ведення гібридної війни з боку Російської федерації.

Збільшення кількості, складності, інтенсивності кіберзагроз, їх комплексного застосування; зростання масштабів негативних наслідків для громадян, суспільства й держави від їх реалізації; принципова неможливість виключно своїми силами та засобами ефективно реагувати на кіберінциденти й кібератаки зумовлюють необхідність заміни традиційних підходів і актуалізують пошук нових. Ці нові підходи базуються на застосуванні інноваційних способів, принципів, методів і механізмів для протидії кіберзагрозам; об'єднанні зусиль та засобів суб'єктів кібербезпеки на глобальному, регіональному, національному та місцевому рівнях; ефективному формуванні та виконанні публічної політики й адмініструванні у сфері інформаційної безпеки та кібербезпеки, у тому числі шляхом запровадження сучасних вмотивованих інструментів державно-приватної взаємодії.

Вкрай актуальною проблемою є формування і реалізація науково обґрунтованої публічної політики у сфері інформаційної безпеки та кібербезпеки, яка б синергетично

об'єднала інтереси й ресурси органів влади, громадськості, бізнесу, міжнародної технічної допомоги та експертів.

У законах України «Про національну безпеку України» [1], «Про основні засади забезпечення кібербезпеки України» [2], Стратегії національної безпеки України [3] наголошується на пріоритетності застосування інструментів в державно-приватного співробітництва у сфері національної безпеки, зокрема, у сфері інформаційної безпеки та кібербезпеки.

Але попри те, що в ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» [2] визначено низку конкретних шляхів державно-приватної взаємодії у сфері кібербезпеки, залишається проблема щодо їх реального впроваджування. Більшість з указаних шляхів наразі є простою декларацією, яка не має під собою чітких механізмів імплементації, ресурсного, організаційного, мотиваційного та законодавчого забезпечення.

Основними причинами такого стану є, насамперед, відсутність достатньої мотивації для такої взаємодії з боку громадян, громадських організацій і бізнесу; розбіжності в поглядах на таку взаємодію, високий рівень їхньої недовіри до влади [4,5], а також, недостатня активність самої влади в розв'язанні цих питань, декларативність і недієвість більшості із запропонованих шляхів та механізмів державно-приватної взаємодії.

Для української сфери кібербезпеки ці проблеми додатково загострюються відсутністю традицій справді багатостороннього розв'язання складних управлінських питань на довготривалій основі. Моделі, які напрацьовані в інших сферах, наразі банківській, енергетичній чи медійній, майже не мають випадків екстраполяції на кібербезпекову сферу. Хоча формально законодавство загалом відмічає важливість багатьох суб'єктів кібербезпеки в державі (зокрема кожної людини як такого суб'єкта), але самим законом нівелює це, не визначивши ані реальних зон відповідальності, ані повноважень, ані механізмів впливу, крім вузького кола основних суб'єктів національної системи кібербезпеки, які повністю складаються з органів сектору безпеки й оборони. Будь-які спроби демократизувати цю сферу, посилити участь громадськості в

процесі ухвалення рішень, забезпечити інструменти демократичного контролю чи навіть зробити прозорішим процес творення кібербезпекової політики, залишалися невдалими. Громадські ради при окремих основних суб'єктах національної системи кібербезпеки (НСК) часто формуються непрозоро, рівень їхнього впливу на ухвалення рішень лишається незначним; а випадків, коли такі ради самі виступали не споживачами запропонованих рішень, а їх ініціаторами (щодо сфери кібербезпеки), майже невідомо. Слід визнати, що в українській кібербезпековій сфері є помітні проблеми впровадження класичного публічного управління в частині його прозорості та передбачуваності. Це логічний наслідок природи більшості основних суб'єктів НСК, які є міліарними структурами з жорсткими ієрархічними моделями управління та браком культури внутрішніх дискусій. Академічна спільнота якщо й залучається до процесу формування кібербезпекової політики, то частіше у формі окремих наукових досліджень, що стосуються вузькоприкладних тематик. Приватний сектор ще рідше впливає на формування політик, принаймні в частині її відкритого публічного складника, а не неформальних практик.

Це становить очевидні ризики для розвитку національної системи кібербезпеки, адже зменшує гнучкість моделі управління перед усе новими викликами. Серед причин – неготовність відомств відмовлятися від вузьковідомчого підходу в розумінні проблем і небажання шукати нові компромісні підходи, що більшою мірою відповідають сучасним викликам. Це дає право стверджувати, що на сьогодні моделлю української системи кібербезпеки є фрагментарна ієрархічна моделі, у якій відсутній елемент пошуку балансу інтересів різних суб'єктів кібербезпеки. Наразі можна стверджувати, що вона не має навіть первинних ознак екосистеми. А що ще гірше, що такі суб'єкти як академічна спільнота, громадянське суспільство, приватний сектор, власники об'єктів критичної інфраструктури не мають навіть чітких і зрозумілих майданчиків для діалогу з представниками державного сектору. А якщо такий діалог і відбувався, то не з позицій пошуку спільного, а позицій «ми і вони», закріплюючи розрив у пошуку діалогу.

Ця дилема характерна не лише для України : більшість держав світу стикаються з проблемами ефективного діалогу з питань кібербезпеки, коли постає питання узгодження інтересів у такій чутливій сфері.

Для розв'язання цієї проблеми, створення демократичного інструмента державно-приватного партнерства в сфері забезпечення кібербезпеки наприкінці 2020 року започатковано функціонування Ради інформаційної та кібербезпеки. Концептуальні засади формування та функціонування якої, на основі аналізу досвіду функціонування аналогічних рад з кібербезпеки деяких європейських країн, інституцій державно-приватного партнерства інших галузей України, розкрито в статті.

Аналіз останніх досліджень і публікацій. Проблемі державно-приватного партнерства у сфері кібербезпеки приділено достатньо уваги в роботах українських та зарубіжних вчених (В. Бурячок, В. Варнавського, І. Горбенко, М. Джеррард, В. Петрова, О. Полякова, Р. Прав, В. Пучкова, В. Якуніна та ін. [6-13]).Основний акцент досліджень в них зроблено саме на механізмах взаємодії окремих державних органів та бізнесу. Залишається невирішеною проблема розробки ефективного механізму державно-приватної взаємодії основних суб'єктів кібербезпеки державного та недержавного сектору в цілому з урахуванням кращого міжнародного та національного досвіду та його впровадження в практику публічного управління національною системою кібербезпеки.

Мета статті. На основі узагальнення національного та міжнародного досвіду функціонування інституцій державно-приватного партнерства визначити роль, концептуальні засади та модель функціонування Експертної ради інформаційної та кібербезпеки (далі – РІКБ) як демократичного інноваційного інструменту державно-приватної взаємодії основних суб'єктів кібербезпеки та кіберзахисту.

Методи дослідження. При розв'язанні завдань дослідження застосовувався метод аналізу – для вивчення досвіду організації приватно-державницького партнерства та функціонування його інституцій, концептуалізації – для

визначення концептуальних засад функціонування РІКБ як інструменту державно-приватної взаємодії .

Виклад основного матеріалу. Пошук дієвих інструментів державно-приватної взаємодії корелюють із проблематикою всеосяжної європейської інтеграції України до ЄС. Ст. 469 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода) [14] передбачене створення майданчика взаємодії – Платформи громадянського суспільства. Вона складається з представників громадянського суспільства України, з однієї сторони, і членів Європейського економічного і соціального комітету (ЄЕСК), з іншої сторони, як форум для проведення ними засідань та обміну думками. При цьому, передбачений також механізм обов'язкових консультацій між Платформою громадянського суспільства, Комітетом асоціації та Парламентським комітетом асоціації з метою отримання їхньої думки щодо досягнення цілей цієї Угоди. Ця Платформа складається за паритетним принципом із представників учасників соціального діалогу – роботодавців і профспілок, а також громадських організацій, метою діяльності яких є сприяння досягнення євроінтеграційних намірів Україною. Функціонування зазначеної платформи визначається авторами як одна із можливих моделей створення та функціонування РІКБ – майданчика приватно-державної взаємодії в зазначеній сфері.

Ще один майданчик консолідації думок в рамках реалізації євроінтеграційних процесів, як можлива модель РІКБ – Дорадча група з питань сталого розвитку. Сторони визначають та скликають Дорадчі групи кожної із Сторін Угоди, з метою надання рекомендацій щодо імплементації Угоди для підтримки діалогу, що охоплює аспекти сталого розвитку торговельних відносин між Сторонами.

Що стосується України, то в ній існують інституції державно-приватної взаємодії, що створені для досягнення складних завдань в різних сферах суспільних відносин. Слід виокремити декілька – це Національна рада України з питань розвитку науки і технологій, яка створена і функціонує

відповідно до ст. 20 Закону України «Про наукову і науково-технічну діяльність» [15]. Це постійно діючий консультативно-дорадчий орган, що утворюється при Кабінетові Міністрів України з метою забезпечення ефективної взаємодії представників наукової громадськості, органів виконавчої влади та реального сектору економіки у формуванні та реалізації єдиної державної політики у сфері наукової і науково-технічної діяльності. Потенціал цього органу є набагато більшим, оскільки на відміну від попередніх, що існують на громадських засадах чи за підтримки донорів. Організаційне, матеріально-технічне, інформаційне та інше забезпечення діяльності Національної ради України з питань розвитку науки і технологій здійснює Секретаріат Кабінету Міністрів України.

Ще одна Інституція державно-приватного партнерства – Національна рада реформ – спеціальний консультативно-дорадчий орган при Президентові України з питань стратегічного планування, узгодження позицій щодо впровадження в Україні єдиної державної політики реформ та їх реалізації.

«Метою діяльності Національної ради реформ є забезпечення впровадження єдиної, узгодженої державної політики реформ в Україні, налагодження ефективного механізму взаємодії державних органів та інститутів громадянського суспільства в процесі здійснення реформ із залученням до співпраці з цих питань міжнародної спільноти, впровадження системного підходу до стратегічного планування, узгодження позицій та моніторингу реалізації реформ щодо забезпечення сталого розвитку України як передумови зростання добробуту її населення, досягнення європейських стандартів забезпечення та захисту прав і свобод людини і громадянина.» [16].

Для підтримки рішень Національної ради реформ було створено Офіс простих рішень та результатів (ОПРР) – неприбуткова організація, яка проводить свою діяльність виключно коштом добровільних внесків фізичних осіб та організацій. Місячний бюджет організації становить близько одного мільйона гривень. Серед донорів ОПРР – бізнес-асоціації, благодійні фонди, небайдужі громадяни.

Засновниками організації є члени Національної ради реформ від громадського сектору.

Що стосується розв'язання проблематики організації державно-приватного партнерства в сфері інформаційної та кібербезпеки вкрай важливим є дослідження міжнародного досвіду, насамперед, щодо визначення місця та завдань в ній Ради інформаційної та кібербезпеки.

У Нідерландах Рада з питань кібербезпеки (CSR) — національний, незалежний дорадчий орган уряду та ділової спільноти, що складається з високопоставлених представників громадських і приватних організацій та наукової спільноти. CSR докладає зусиль на стратегічному рівні для посилення кібербезпеки в Нідерландах [17].

Унікальний склад ради дає можливість стратегічно підходити до пріоритетів, вузьких місць та інцидентів і розробляти інтегроване бачення можливостей та загроз. CSR прагне співпраці з відповідними радами в інших країнах і заохочує її створення в країнах, які ще не мають таких рад.

Організаційно CSR складається із вісімнадцять членів (7-7-4): сім членів з приватного сектору, сім членів з державного сектору та чотири члени з науки. У CSR є два співголови: співголова Пітер-Яап Ольберсберг від імені державного сектору та співголова Ганс де Йонг від імені приватного сектору (VNO-NCW).

CSR має такі завдання:

надавати на запит і окремо поради державним та приватним сторонам;

консультувати щодо реалізації національної стратегії кібербезпеки;

здійснювати внесок у Національну програму досліджень кібербезпеки;

консультувати щодо кризової організації в Нідерландах під час масштабних кіберінцидентів.

Крім цього, члени CSR проводять публічні дискусії, щоб привернути увагу до кібербезпеки на стратегічному рівні. Це не лише тема для IT-відділу, кібербезпека також вимагає стратегічного спрямування в контексті безперервності бізнесу. Рада з питань кібербезпеки здійснює планування; визначає, що

очікується в Нідерландах, та надає поради перед черговим циклом політики щодо нових технологічних розроблень і наслідків кібербезпеки.

Саме CSR здійснює оцінювання кібербезпеки Нідерландів та оцінювання прогресу; аналізує різні категорії, що стосуються кіберзахисту, включно із заходами, учасниками, загрозами, методами, що використовуються, та факторами вразливості (технічними, людськими та організаційними). Оцінку кібербезпеки Міністр безпеки та юстиції представляє Кабінету Міністрів, Раді з питань кібербезпеки та нижній палаті парламенту; публічна версія надається всім зацікавленим сторонам та публікується на вебсайті NCSC [17].

У Литві створення Ради з питань кібербезпеки передбачено законом [18]. Рада з питань кібербезпеки є постійним колегіальним незалежним дорадчим органом. Він аналізує ситуацію забезпечення кібербезпеки в Литовській Республіці та вносить пропозиції до установ, що розробляють і впроваджують політику кібербезпеки, суб'єктів кібербезпеки, науково-дослідних і освітніх установ та суб'єктів господарювання, які беруть участь у діяльності в галузі інформаційних технологій (далі — «Актори кібербезпеки») щодо покращення ситуації із забезпечення кібербезпеки.

Раду з кібербезпеки очолює представник Міністерства національної оборони. Забезпечення Ради кібербезпеки покладене на Міністерство національної оборони або уповноважену ним установу.

Основними завданнями Ради з питань кібербезпеки є: подання пропозицій суб'єктам кібербезпеки щодо пріоритетів кібербезпеки, напрямів розвитку, цільових результатів і способів досягнення цілей; подання пропозицій суб'єктам кібербезпеки щодо можливостей співпраці між державним сектором, бізнесом і дослідженнями у сфері забезпечення кібербезпеки; аналіз тенденції вдосконалення забезпечення кібербезпеки, надання висновків та пропозицій щодо управління кіберінцидентами Акторам кібербезпеки; надання рекомендацій суб'єктам кібербезпеки щодо підвищення рівня кібербезпеки [18].

У 2009 році при Комітеті з безпеки уряду Естонії була

створена Рада з питань кібербезпеки [19]. Завдання Ради – сприяти безперебійній співпраці між різними установами та здійснювати нагляд за виконанням цілей Стратегії кібербезпеки. Головує в Раді Генеральний секретар Міністерства економіки та зв'язку.

Крім того, на Раду покладається контрольна функція щодо виконання стратегії шляхом подання щорічного звіту про хід її виконання урядом, у якому окреслюється поточна реалізація поставлених цілей у планах імплементації.

Міжнародний та національний досвід функціонування зазначених вище інституцій державно-приватного партнерства, наразі і в сфері інформаційної та кібербезпеки враховано при обґрунтуванні концептуальних засад формування і функціонування РІКБ. Організаційно-правові засади діяльності РІКБ закріплені в її Тимчасовому положенні.

Створення РІКБ наприкінці 2020 року стало результатом домовленостей основних суб'єктів національної системи кібербезпеки України (Національним координаційним центром кібербезпеки України, Мінцифри та Держспецзв'язку), а також за підтримки з боку Агентства США з міжнародного розвитку (United States Agency for International Development, USAID) в Україні. Ці домовленості формалізовані в Меморандумі про взаємодію та співробітництво у сфері інформаційної та кібербезпеки (Меморандум), стали одним з небагатьох позитивних прикладів створення реального інструменту державно-приватної взаємодії у сфері кібербезпеки.

Згідно з Концепцією організаційно-технічної моделі кіберзахисту України (ОТМ) [20], функціонування РІКБ є одним з механізмів реалізації взаємодії та координації (механізмом державно-приватної взаємодії) організаційно-керувальної інфраструктури кіберзахисту, а також важливим елементом національної системи кіберзахисту. Завдяки специфіці свого складу, що формується зі збереженням відповідних пропорцій з представників як державних органів (не більше за 40 відсотків від загального складу РІКБ), так і з недержавного сектору (у рівній кількості представників від громадських організацій, бізнесу, сфери освіти та науки з різних регіонів України), забезпечується баланс інтересів влади й

суспільства, а також їхній вплив на ухвалення рішень, ефективність взаємодії та можливість стратегічно підходити до пріоритетів, вузьких місць і інцидентів, розглядаючи їх з різних точок зору, та розробляти інтегроване бачення можливостей і загроз, підвищити довіру до органів влади в цій сфері.

Принципами Функціонування РІКБ як інструмента державно-приватної взаємодії є:

незалежність, компетентність і об'єктивність членів РІКБ у своїй діяльності;

колегіальність, публічність, прозорість і відкритість діяльності РІКБ;

добровільність, самоврядність, мінімальна необхідність регулювання діяльності РІКБ;

мультистейхолдерізм.

Принцип «мультистейхолдерізму» передбачає можливість приєднання до Меморандуму та подальшу участь у діяльності РІКБ представників інших основних суб'єктів національної системи кібербезпеки України та секторальних і функціональних державних органів у сфері захисту критичної інфраструктури, а також розширення кола іноземних організацій, що надають міжнародну технічну допомогу Україні в цій сфері.

При цьому вкрай важливим є дотримання центристської загальнодержавної позиції, забезпечення максимально можливої незалежності в діяльності РІКБ від суто корпоративного впливу якогось одного зі стейкхолдерів, домінування інтересів відповідних міжнародних організацій над національними інтересами України.

Враховуючи зазначене та з метою реалізації принципу незалежності РІКБ не інституалізувалася як звичайна громадська організація в жодному з органів державної влади. Органи влади самі зацікавлені в забезпеченні незалежності РІКБ її рівновіддаленості від кожного з них. Причинами такого їх ставлення є як наявність вже раніше створених при них згідно з Законом України «Про громадські об'єднання» відповідних громадських рад, їх бажання унеможливити надмірний вплив на діяльність РІКБ з боку будь-якого одного з них, збереження особливості функціонування РІКБ поза

межами вищезазначеного Закону.

Водночас, відсутність повноцінної інституалізації РІКБ як «традиційної» громадської організації ускладнює та обмежує її можливості щодо фінансового, матеріально-технічного, інформаційного й комунікативного забезпечення та є своєрідною платою за її незалежність і самоврядування, безпосередню участь у її складі та діяльності представників органів державної влади на рівні керівників.

Однією з особливостей РІКБ є її склад, який сформовано в рівних пропорціях з представників державних органів, науковців, освітян, експертів, приватних підприємців, а також громадських організацій, що здійснюють свою професійну діяльність у сферах інформаційної безпеки та кібербезпеки.

Пріоритетні завдання РІКБ, навколо яких було сформовано профільні комітети з-поміж членів РІКБ, за своїм досвідом професійної діяльності в найбільшій мірі відповідають нижче зазначеним напрямам:

розвиток організаційної системи забезпечення кібербезпеки;

удосконалення системи законодавства;

технологічна інфраструктура кібербезпеки;

удосконалення системи підготовки кадрів.

Перелік цих завдань (напрямів) не є сталим і може змінюватися в процесі діяльності РІКБ, та зміни її пріоритетів. Одночасно в РІКБ, запроваджено й проектний підхід, згідно з яким створюються тимчасові робочі групи для формування та виконання конкретних проектів за участю і власною ініціативою з-поміж членів Ради, що належать різним комітетам. Тобто в РІКБ, відпрацьовуються та інтегруються різні механізми внутрішніх і зовнішніх комунікацій.

З метою підвищення ефективності зовнішніх комунікацій РІКБ, вже встановила дієві комунікації з організаціями-підписантами Меморандуму; передбачено можливість додаткового введення до її складу на добровільних засадах представників від інших основних суб'єктів національної системи кібербезпеки України та секторальних і функціональних державних органів у сфері захисту критичної інфраструктури, розширення кола іноземних організацій, що

надають міжнародну технічну допомогу Україні в цій сфері, а також встановлення відповідних комунікацій з аналогічними Радами інших країн.

Перевагою та одночасно особливістю функціонування РІКБ, є не тільки її можливість спільного формування громадськістю, бізнесом та експертами креативних ідей та проектів, спрямованих на удосконалення сфери кібербезпеки, але й оперативного їх доведення до відповідних державних органів через представників цих органів, членів РІКБ,, попереднього узгодження позицій цих органів як між собою, так і з усьома іншими членами Ради, а також отримання інформаційної, ресурсної, комунікаційної підтримки в рамках міжнародної технічної допомоги.

Створення і започаткування функціонування РІКБ це невеликий внесок в розв'язання проблем розвитку державно-приватного партнерства в Україні. Подальший аналіз і вивчення практики її функціонування можуть бути розповсюджені не тільки на сферу кібербезпеки, а й інші сфери суспільних відносин. Процес її становлення поки що не завершився: уточняються цілі, пріоритети, завдання, підходи, механізми взаємодії, склад РІКБ; розширюється коло стейкхолдерів тощо. Але попри невеликий термін її функціонування, РІКБ вже отримала перший позитивний досвід щодо участі в експертизі проекту Закону України «Про критичну інфраструктуру»; її члени активно працюють у Робочих групах Комітету Верховної Ради України з питань цифрових трансформацій, пройшли підготовку в рамках Стратегічної сесії, організованої USAID, узяли участь в організації та проведенні круглого столу «Стратегічне бачення кібербезпеки: виклики, уроки та можливості для України» та вперше підготували проект з розроблення «Білої книги у сфері кібербезпеки», як щорічного аналітичного документа з оцінювання стану сфери та визначення основних трендів її розвитку на короткострокову перспективу.

Водночас, подальший розвиток функціонування РІКБ, посилення її впливу на процеси у сфері кібербезпеки залежатимуть від того, наскільки їй вдасться зберегти свою унікальність і незалежність, не перетворитися на звичайну

громадську раду при одному з державних органів та не стати інструментом легалізації вже винесених ним рішень або звичайним «грантоїдом» міжнародної технічної допомоги; залишитися на центристських позиціях стосовно всіх суб'єктів кібербезпеки членів РІКБ; стати ефективним майданчиком формування та реалізації публічної політики у сфері кібербезпеки, а не полем для з'ясування стосунків суб'єктів кібербезпеки; залишитися незабюрократизованою, гнучкою та адаптованою до змін, де моральні стимули домінували б над матеріальними.

Висновки та напрями подальших досліджень. Проаналізовано функціонування деяких інституцій державно-приватної взаємодії та партнерства у суміжних з кібербезпекою сферах на загальнодержавному рівні.

Узагальнено досвід функціонування рад з кібербезпеки Нідерландів, Литви й Естонії та оцінена можливість його застосування в Україні.

Визначено концептуальні засади та модель функціонування РІКБ, що містять базові принципи, стратегічні цілі та завдання, структуру, механізм її формування та функціонування. Необхідно відмітити, що на концептуальному рівні модель Ради значною мірою збігається як з вищевказаними моделями функціонування європейських країн, так і з реалізованими в Україні Платформою громадянського суспільства, Національною радою України з питань розвитку науки і технологій, Національною радою реформ тощо. В той же час, її відрізняє від зазначених рад конкретні способи її діяльності (на громадських засадах), склад учасників, рівень інституалізації та незалежності від стейкхолдерів, організація взаємодії з органами влади, перелік завдань та інструментарій їх вирішення, її місце в загальні організаційно-технічний моделі кіберзахисту, тощо. Це в сукупності позитивно виокремлює її від аналогічних рад.

Розкрито особливості РІКБ як демократичного інноваційного та перспективного інструменту державно-приватної взаємодії у сфері кібербезпеки.

Сформульовано напрями подальшого розвитку РІКБ та визначено основні ризики для його позитивного тренду.

Напрямом подальшого дослідження є наукове обґрунтування підвищення ефективності та результативності функціонування РІКБ; розроблення Програм її діяльності на короткострокову та середньострокову перспективу (сукупності взаємопов'язаних завдань і проектів з чітко обґрунтованими термінами, виконавцями, ресурсами, кількісними кінцевими очікуваними результатами тощо); моніторингу та оцінки ефективності функціонування РІКБ.

Список використаних джерел

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-19 // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення : 31.03.2021).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19 // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення : 31.03.2021).
3. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» :Указ Президента України від 14.09.2020. № 392/2020 // Президент України. Офіційне Інтернет представництво / Адміністрація Президента України. URL : https://www.president.gov.ua/documents/3922020-35037 (дата звернення 31.03.2021).
4. Комунікаційна стратегія Верховної Ради України на 2017-2021 рр: Розпорядження Голови Верховної Ради України «Про додаткові заходи з реалізації Декларації відкритості парламенту» від 21.11.2017 № 486 // Інтернет-портал ВР України / ВР України. URL : https://iportal.rada.gov.ua/uploads/documents/44841.pdf (дата звернення 31.03.2021).
5. Економічний аудит країни та Вектори економічного розвитку 2030 // Урядовий портал. Єдиний веб-портал органів виконавчої влади України / Кабінет Міністрів України. URL : https://cutt.ly/CcwMuEJ (дата звернення 31.03.2021).
6. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Львів: «Магнолія 2006», 2018. 320 с.
7. Варнавский В. Г. Государственно-частное партнерство: теория и практика / В. Г. Варнавский и др. М. : Изд. дом Гос. ун-та. Высш. шк. экон., 2010. 287 с.

8. Gerrard M. B.: Whatarepublic-privatepartnerships, andhowdotheydifferfromprivatizations? *Finance&Development*. 2010. Vol. 38. № 3. Pp. 26 – 31.
9. Полякова О. М. Державно-приватне партнерство в Україні: проблеми становлення. *Коммунальное хозяйство городов : науч.-техн. сб.* К. : Техніка, 2009. № 87. С. 317 – 322.
10. Прав Р. Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. Інвестиції: практика та досвід. 2019. № 21. С. 143–150. DOI : 10.32702/2306-6814.2019.21.143.
11. Пучков В. В. Государственно-частное партнерство как форма взаимодействия власти и бизнеса. *Ползуновский альманах. 2009. № 1.* С. 289 – 293.
12. Хєда С. Державно-приватне партнерство: світовий досвід і перспективи розвитку в Україні. *Юридична Газета.* 2014. № 31 – 32 (425 – 426). С. 18 – 22.
13. Якунин В. И. Партнерство в механизме государственного управления. *Социологические исследования.* 2007. № 2. С. 13 – 14.
14. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення 31.03.2021).
15. Про наукову і науково-технічну діяльність : Закон України від 26.11.2015 №848-19 // База даних «Законодавство України» / ВР України URL : https://zakon.rada.gov.ua/laws/show/848-19#Text (дата звернення : 31.03.2021).
16. Національна рада реформ // Президент України. Офіційне Інтернет представництво / Адміністрація Президента України. URL : https://www.president.gov.ua/administration/nacionalna-rada-reform (дата звернення 31.03.2021).
17. Cyber Security Raad // Webportal / Cyber Security Raad NL. URL: https://www.cybersecurityraad.nl/ (дата звернення 31.03.2021).
18. Lietuvos respublikos kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr. XII-1428 / E-seimas. URL : https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee (дата звернення 31.03.2021).
19. Cyber security / Republik of Estonia. Ministry of economic affairs and Communications. URL : https://www.mkm.ee/en/objectives-activities/cyber-security (дата звернення 31.03.2021).
20. Організаційно-технічна модель кіберзахисту України. *Діджиталізація і безпека* : мат-ли міжнар. наук.-практ. конф., м. Харків (19 листоп. 2020 р.) / за ред. А. П. Гетьмана і Б. М. Головкіна. Харків : Право, 2020. 402 с.

References

1. Pro natsionalnu bezpeku Ukrainy [The Law of Ukraine «On the national security of Ukraine»] : Zakon Ukrainy vid 21.06.2018 № 2469-19 // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukr.].
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [The Law of Ukraine «On the basic principles of cybersecurity in Ukraine»] : Zakon Ukrainy vid 05.10.2017 № 2163-19 // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukr.].
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» [Decree of the President of Ukraine «On the decision of the National Security and Defense Council of Ukraine of September 14, 2020»] :Ukaz Prezydenta Ukrainy vid 14.09.2020. № 392/2020 // Prezydent Ukrainy. Ofitsiine Internet predstavnytstvo / Administratsiia Prezydenta Ukrainy. Retrieved from https://www.president.gov.ua/documents/3922020-35037 [in Ukr.].
4. Komunikatsiina stratehiia Verkhovnoi Rady Ukrainy na 2017-2021 rr [Order of the Chairman of The Verkhovna Rada of Ukraine «On Additional Measures to Implement the Declaration of Openness of the Parliament»] : Rozporiadzhennia Holovy Verkhovnoi Rady Ukrainy «Pro dodatkovi zakhody z realizatsii Deklaratsii vidkrytosti parlamentu» vid 21.11.2017 № 486 // Internet-portal VR Ukrainy / VR Ukrainy. Retrieved from https://iportal.rada.gov.ua/uploads/documents/44841.pdf [in Ukr.]
5. Ekonomichnyi audyt krainy ta Vektory ekonomichnoho rozvytku 2030 [Economic audit of the country and Vectors of economic development 2030] // Uriadovyi portal. Yedynyi veb-portal orhaniv vykonavchoi vlady Ukrainy / Kabinet Ministriv Ukrainy. Retrieved from https://cutt.ly/CcwMuEJ [in Ukr.].
6. Buriachok V. L., Tolubko V. B., Khoroshko V. O., Toliupa S. V. (2018) Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : pidruchnyk. Lviv: «Mahnoliia 2006», 320 s. [in Ukr.]
7. Varnavskyi V. H. (2010) Hosudarstvenno-chastnoe partnerstvo: teoryia y praktyka / V. H. Varnavskyi y dr. M. : Yzd. dom Hos. un-ta. Vыssh. shk. эkon.. 287 s. [in Rus.].
8. Gerrard M. B. (2010) Whatarepublic-privatepartnerships, andhowdotheydifferfromprivatizations? *Finance&Development.* Vol. 38. № 3. Pp. 26 – 31.
9. Poliakova O. M. (2009) Derzhavno-pryvatne partnerstvo v Ukraini: problemy stanovlennia. Kommunalnoe khoziaistvo horodov : nauch.-tekhn. sb. K. : Tekhnika. № 87. S. 317 – 322.
10. Prav R. Yu. (2019) Rol mekhanizmu derzhavno-pryvatnoho partnerstva u rozvytku kiberbezpeky Ukrainy na suchasnomu etapi. *Investytsii: praktyka ta dosvid.* № 21. S. 143–150. DOI : 10.32702/2306-6814.2019.21.143 [in Ukr.]

11. Puchkov V. V. (2009) Hosudarstvenno-chastnoe partnerstvo kak forma vzaymodeistvyia vlasty y byznesa. Polzunovskyi almanakh. № 1. S. 289 – 293 [in Ukr.].
12. Khieda S. (2014) Derzhavno-pryvatne partnerstvo: svitovyi dosvid i perspektyvy rozvytku v Ukraini. *Yurydychna Hazeta*. № 31 – 32 (425 – 426). S. 18 – 22 [in Ukr.].
13. Yakunyn V. Y. (2007) Partnerstvo v mekhanyzme hosudarstvennoho upravlenyia. Sotsyolohycheskye yssledovanyia. № 2. S. 13 – 14 [in Ukr.].
14. Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony [The Law of Ukraine «Association agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part»] // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/984_011#Text [in Ukr.]
15. Pro naukovu i naukovo-tekhnichnu diialnist [The Law of Ukraine «On Scientific and Scientific-Technical Activity»]: Zakon Ukrainy vid 26.11.2015 №848-19 // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy Retrieved from https://zakon.rada.gov.ua/laws/show/848-19#Text [in Ukr.].
16. Natsionalna rada reform [National Reform Council] // Prezydent Ukrainy. Ofitsiine Internet predstavnytstvo / Administratsiia Prezydenta Ukrainy. Retrieved from https://www.president.gov.ua/administration/nacionalna-rada-reform [in Ukr.].
17. Cyber Security Raad // Webportal / Cyber Security Raad NL. URL : https://www.cybersecurityraad.nl/ [in Eng.].
18. Lietuvos respublikos kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr. XII-1428 / E-seimas. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee [in Lith.].
19. Cyber security / Republik of Estonia. Ministry of economic affairs and Communications. Retrieved from https://www.mkm.ee/en/objectives-activities/cyber-security [in Eng.].
20. Orhanizatsiino-tekhnichna model kiberzakhystu Ukrainy (2020). *Didzhytalizatsiia i bezpeka :* mat-ly mizhnar. nauk.-prakt. konf., m. Kharkiv (19 lystop. 2020 r.). Nats. yuryd. un-t im. Yaroslava Mudroho ; za red. A. P. Hetmana i B. M. Holovkina. Kharkiv : Pravo. 402 s. [in Ukr.]

EXPERT COUNCIL OF INFORMATION AND CYBER SECURITY AS A DEMOCRATIC INNOVATIVE TOOL OF PUBLIC-PRIVATE INTERACTION

Dubov Dmytro, Oleksiuk Liliia, Potyi Olexsandr, Semenchenko Andrii

Abstract. The urgency of the study is due to the requirements of legislation to strengthen the effectiveness and efficiency of public-private partnerships in cyber security and cyber protection, the unsatisfactory state of public-private cooperation of cyber security in Ukraine, large-scale and dynamic growth of cyber threats and cyber incidents, elimination and neutralization by means of state bodies is not possible, the ineffectiveness of existing instruments of public-private interaction. Despite the wide range of research on cyber security and cyber protection in general, as well as on public-private interaction in this area of cyber security actors, innovative approaches and tools of public-private interaction based on new conceptual frameworks, better national and international experience, and their implementation in the practice of daily activities on the basis of the Expert Council for Information and Cyber Security. Therefore, the aim of the article is to summarize national and international experience in the application of public-private partnership of cyber security and cyber protection actors, define the role, conceptual framework and model of the Information and Cybersecurity Council as a democratic innovative instrument for public-private partnership between major cybersecurity actor. As well as Information and Cyber Security Council place in the organizational and technical model of cyber defense, the directions of further development of the Council are formulated and the main risks for its positive trend are substantiated. The article describes: the main mechanisms of public-private interaction and partnership in areas related to cyber security; the experience of the cyber security councils of the Netherlands, Lithuania and Estonia is summarized and the possibility of its application in Ukraine is assessed; for the first time the conceptual bases and model of activity of the Council of information and cyber security are defined, containing basic principles, strategic purposes and tasks, structure, the mechanism of its formation and functioning; the peculiarities and uniqueness of the Council as a democratic innovative and promising instrument of public-private cooperation in the field of cyber security, as well as its place in the organizational and technical model of cyber defense are revealed; the directions of further development of the Council are formulated and the main risks for its positive trend are substantiated.

Keywords: Information and Cyber Security Council, public-private interaction, conceptual principles, main subjects of cyber security, organizational and technical model of cyber security.