УДК 351.86:004](477+100)

Тарас Станіславський
здобувач Інституту підготовки кадрів Державної служби зайнятості України

РОЗВИТОК МІЖНАРОДНОГО СПІВРОБІТНИЦТВА УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

Організація міжнародного співробітництва задля поліпшення кібербезпекових спроможностей України в сучасних умовах набуває особливої актуальності, обумовленої проблемами зростання кількості та рівням кіберзагроз та кіберінцендентів в кіберпросторі, масштабним та динамічним впровадженням ІКТ в усі сфери суспільного життя, а для України - веденням проти неї РФ гібридної війни, а також неможливістю ні однієї з країн самостійно розвязати ці проблеми. В статті проведено аналіз досвіду провідних країн світу та їх об'єднань щодо організаційно-правових та фінансових механізмів міжнародного співробітництва у сфері кібербезпеки. На його основі запропоновано підходи та напрямки удосконалення відповідних національних механізмів державного управління та обґрунтовані рекомендації державним органам.

***Ключові слова**: кібербезпека; національна система кібербезпеки; критична інфраструктура; кіберінцидент; протокол взаємодії; стратегія; обмін інформацією про кіберінциденти; міжнародне співробітництво.*

Taras Stanislavskyi
PhD student, the Institute o Staff Training of the State Employment Service of Ukraine

DEVELOPMENT OF UKRAINE'S INTERNATIONAL COOPERATION IN THE CYBER SECURITY

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 EU's Eastern European Partnership initiative and is constantly evolving.

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; national cybersecurity system; critical infrastructure; cyber incident; interaction protocol; strategy; exchange of information on cyber incidents; international cooperation.*

Постановка проблеми

Зростання кількості, масштабів, інтенсивності, складності кіберінцидентів та кіберзагроз в світовому кіберпросторі ефективно протидіяти яким окремо не спроможна ні одна держава, є одним з головних факторів, що обумовлює необхідність їх міжнародної співпраці в сфері кібербезпеки та кіберзахисту, об'єднання їх сил та засобів для зменшення рівня кіберзагроз для громадян, суспільства та держави.

Аналіз останніх досліджень і публікацій

Проблемі удосконалення міжнародного співробітництва в галузі кібербезпеки та кіберзахисту присвяче-

но достатньо наукових робіт іноземних та вітчизняних науковців та практиків. Так, наприклад, Р. В. Лук'янчук [1] наголошує, що Український вектор зовнішньої політики насамперед має бути спрямований на активізацію міжнародного співробітництва у сфері забезпечення кібернетичної безпеки, продовження взаємодії з питань кібербезпеки за участі органів державної влади України і відповідних органів НАТО шляхом співпраці на двосторонній основі, упровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування (CERT) на кіберінциденти, в цілому інтеграції Національної системи кібербезпеки до відповідних систем ЄС та НАТО, затвердження офіційної акредитації з боку НАТО Національного центру кіберзахисту та протидії кіберзагрозам. Шемчук В.В. [2], розвиваючи цю ідею, доходить висновку, що кібербезпека є пріоритетом у діяльності не тільки різних держав, а й їх регіональних об'єднань і навіть всієї світової спільноти, а міжнародне співробітництво має мати системний і послідовний характер, супроводжуватися грунтовними дослідженнями. Дешко Л.М. та Бонарєва К.Д. у [3] визначають важливість міжнародного співробітництва та стверджують, що особливістю міжнародного співробітництва України є те, що начебто створений нормативно-правовий (імплентація Будапештської конвенції про кіберзлочинність, Угода про реалізацію Трастового фонду Україна – НАТО тощо) та організаційно-правовий механізми співпраці (Україна – ЄС та Україна – НАТО та інші). Піскорською Г.А. та Яковенко Н.Л. [4] зазначається про широкий спектр напрямків міжнародної взаємодії у кіберпросторі та наголошується про необхідність, вдосконалення міжнародних механізмів і загальну міжнародну політику по розробці і здійсненню дієвих та ефективних інструментів. Доронін І.М. [5], аналізуючи норми законодавства у сфері кібербезпеки доходить висновків щодо недосконалості термінологічної бази та необхідності законодавчого встановлення вимог до порядку звітування суб'єктів кібербезпеки так само як у цілому в сфері національної безпеки і оборони. Забара І.М. у своїх тезах [6], зокрема, вважає, що актуальним напрямками міжнародно-правового регулювання постануть укладення двосторонніх, регіональних і універсальних міжнародних угод з інформаційної і кібербезпеки. Кравець В.М. [7] виокремлює важливі характеристики та вимір оцінки успішності діяльності у сфері кібербезпеки на різних рівнях такі, як Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI), Національний індекс кібербезпеки (National Cyber Security Index, NCSI) та галузевий індекс кібербезпеки (Index of Cyber Security, ICS).

Нікітіна Є.О. [8] наводить опис основних інструментів проактивного аналізу кіберзагроз щодо пошуку та розслідування кіберзагроз як ефективних механізмів забезпечення безпеки інформації. Ожеван М.А. [9] розглядає політичні та технологічні наслідки міжнародної політики щодо автономізації РФ в Інтренеті та необхідність розроблення Україною адекватних заходів забезпечення кібербезпеки для об'єктів критичної інфраструктури. Вищевказаними авторами здебільше констатується необхідність міжнародного співробітництва у сфері кібербезпеки у форматах Україна-ЄС, Україна-НАТО, Україна-регіональні об'єднання країн, двостороннє міжнародне співробітництво, удосконалення існуючих та розроблення нових механізмів такого співробітництва, у тому числі порядку інформаційного обміну про стан та інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки в Україні, вимірювання рівнів кібербезпеки, але при цьому одною з основних проблем залишається проблема координованості дій суб'єктів міжнародного співробітництва в цій сфері.

Мета

Метою статті є аналіз досвіду України, провідних країн світу та міжнародних організацій щодо організаційно-правових механізмів міжнародного співробітництва у сфері кібербезпеки та на його основі удосконалення відповідних національних механізмів державного управління і формування рекомендацій державним органам.

Виклад основного матеріалу

Актуальність проблеми міжнародного співробітництва обумовлена проблемами зростання кількості, видів та рівнів кіберзагроз та кіберінцидентів в кіберпросторі, масштабним та динамічним впровадженням ІКТ в усі сфери суспільного життя, розбудовою цифрового суспільства та держави, неможливістю ні однієї з країн самостійно розв'язати ці проблеми, а для України додатково- веденням проти неї РФ гібридної війни.

Цей напрям як пріоритетний формально визначено в цілій низці законодавчих актів України, що стосуються розвитку національної безпеки, інформаційного (цифрового) суспільства, цифрової економіки, європейської та євроатлантичної інтеграції України, тощо. Так, наприклад, метою Стратегії кібербезпеки України (Стратегія) [10] є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, для досягнення якої, поряд з іншим, необхідними є поглиблення міжнародного співробітництва у цій сфері. В щорічних планах заходів з її реалізації передбачено заходи з виконання завдання [11-13] щодо розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у цій сфері та співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі.

Один з базових принципів забезпечення кібербезпеки визначено ст.7 Закону України «Про основні засади забезпечення кібербезпеки України» [14] та сформульовано як: «міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях».

Двостороння міжнародна взаємодія з кібербезпеки: США. Незважаючи на досить високій рівень двосторонньої взаємодії України з багатьма країнами-членами НАТО та ЄС у сфері кібербезпеки, формалізація такої взаємодії оформлена лише з США. Так, наприклад, у Звіті про Другий американсько-український діалог з кібербезпеки [15] зазначено, що Сполучені Штати Америки зобов'язалися фінансувати програми допомоги в галузі кібербезпеки для України, спрямовані на: по-

силення кібербезпеки виборчих систем та критичної інфраструктури, сприяння впровадженню національної кібер-стратегії України, посилення реагування на кіберзахист та реагування на інциденти, підвищення обізнаності про кібербезпеку та проведення тренінгів з підготовки фахівців у галузі кібербезпеки та цифрової криміналістики.

У подальшому для унормування цієї допомоги Палатою представників США в лютому 2018 року схвалений та переданий у серпні 2018 року до Конгресу США Ukraine Cybersecurity Cooperation Act of 2017 (Акт) [16], який спрямований на просування активної взаємодії між Україною та США в сфері кібербезпеки, насамперед, у забезпеченні відкритості, сумісності, надійності і безпечності Інтернету, зокрема з питань розширення можливостей у сфері кібербезпеки, покращенні здатності України реагувати на підтримувану РФ дезінформацію та пропаганду в кіберпросторі, в тому числі через соціальні медіа та інші способи. Він включає такі пріоритетні напрямки як:

- убезпечення урядових мереж від зловмисних кібер-вторгнень, зокрема таких мереж, які захищають критичну інфраструктуру України;
- зменшення залежності від російських інформаційно-комунікаційних технологій;
- розбудова власного потенціалу, розширення обміну інформацією про кібербезпеку та співпраця з міжнародними зусиллями у сфері кіберпростору.

В рамках цього напрямку США анонсували $5 мільйонну підтримку у кіберсфері задля посилення здатності України запобігати, пом'якшувати і реагувати на кібератаки.

Механізм реалізації Акту передбачає підготовку Державним секретарем США Звіту про Співробітництво США з Україною з проблем кібербезпеки, якій включає інформацію, щодо:

- зусиль Сполучених Штатів щодо зміцнення спроможності України у запобіганні, пом'якшенні та реагуванні на кібер-інциденти, включаючи навчання, освіту, технічну допомогу, розбудову спроможностей та стратегії управління ризиками кібербезпеки;
- потенціалу для нових сфер співпраці та взаємодопомоги між Сполученими Штатами та Україною у спільному вирішенні кіберзлочинів, включаючи кіберзлочинність, захист критичної інфраструктури та стійкість до ботнетів та інших автоматизованих розподілених загроз;
- зусиль НАТО щодо надання Україні допомоги у розробці технічних можливостей для протидії кіберзагрозам.

Реалізація цього Акту буде здійснюватися США в контексті Національної кіберстратегії США [17], в якій зокрема зазначається, що США:

- сприяють посиленню механізмів міжнародної координації та обміну інформацією;
- продовжуватимуть виявляти прогалини та розвивати потенційні механізми притягнення до суду кіберзлочинців з іноземним базуванням;
- будуть «підштовхувати» інші країни до прискорення їхньої допомоги в розслідуванні та дотримання будь-яких двосторонніх або багатосторонніх угод або зобов'язань;
- повинні надавати допомогу країнам-партнерам у розбудові їхньої спроможності вирішувати кримінальну кібер-діяльність;
- продовжувати будувати потенціал боротьби з кіберзлочинністю, що сприяє посиленню міжнародного співробітництва в галузі правоохоронних заходів щодо кіберзлочинності;
- будуть прагнути поліпшення міжнародного співробітництва в розслідуванні злочинної кібер-активності, включаючи розробку рішень потенційних бар'єрів для збирання та обміну доказами;
- будуть керуватися розробкою взаємно сумісних та взаємовигідних систем для заохочення ефективного транскордонного обміну інформацією для цілей правоохоронних органів та зменшення бар'єрів у координації;
- будуть наполягати на ефективному використанні існуючих міжнародних інструментів, таких як Конвенція ООН проти транснаціональної організованої злочинності;
- працюватимуть над розширенням міжнародного консенсусу на користь Конвенції про кіберзлочинність Ради Європи (Будапештська конвенція), включаючи підтримку більшого прийняття Конвенції.

За звітом Агентства США з міжнародного розвитку за 2018 рік [18] зазначено, що напередодні президентських і парламентських виборів 2019 року USAID сприяло підвищенню рівня спроможності Центральної виборчої комісії протидіяти кіберзагрозам виборчій системі України.

На жаль, такий рівень формалізації двосторонньої взаємодії з питань кібербезпеки Україна на сьогодні має лише з США.

Співробітництво з міжнародними організаціями у сфері кібербезпеки: НАТО. Найвищим органом, який ухвалює рішення стосовно розвитку відносин Україна – НАТО та спрямовує заходи в плані практичного співробітництва, є Комісія Україна – НАТО (КУН) [19]. Це співробітництво охоплює операції з підтримання миру, реформування структур безпеки і оборони, безпосереднє військове співробітництво, оборонні технології, розвиток оперативної сумісності, оборонну промисловість і готовність цивільного суспільства, а також науку і довкілля й громадську дипломатію. У складі КУН представлені усі країни Альянсу та Україна.

Відповідно до положень Хартії про особливе партнерство між Україною та НАТО [20], КУН передбачено ієрархічну систему проведення зустрічей: по мірі необхідності - на рівні глав держав та урядів, періодичні зустрічі — на рівні міністрів закордонних справ та оборони, послів та військових представників. Заяви Комісії Україна – НАТО на рівні міністрів закордонних справ [21-22], свідчать про постійну підтримку Альянсом України у сфері кіберзахисту: у 2015 році розвиток Цільових фондів з питань, у тому числі кіберзахисту; у 2017 році НАТО започаткували роботу Платформи Україна – НАТО з протидії гібридній війні, в тому числі в реалізації другого етапу Трастового фонду з кіберзахисту [23]; у 2018 році зазначено, що НАТО і її держави–члени залишаються відданими подальшому наданню допомоги Україні щодо реалізації порядку денного реформування національних структур безпеки і оборони, зокрема, у рамках Комплексної програми допомоги (КПД) з таких напрямів, як кіберзахист [24].

Координація учасників КУН, системність та взаємну узгодженість їх дій організаційно повинна забезпечуватись національною системою координації євроатлантичної інтеграції України (до якої входять центральні органи виконавчої влади, інші державні органи, діяльність яких пов'язана з виконанням завдань у сфері євроатлантичної інтеграції України і співробітництва з НАТО) та новоутвореною Комісією з питань координації євроатлантичної інтеграції України як допоміжний орган при Президентові України [25].

Цим документом затверджено перелік національних координаторів у визначених сферах, затверджено персональний склад комісії (увійшли представники основних суб'єктів забезпечення національної системи забезпечення кібербезпеки) визначено, що основною організаційною формою роботи Комісії є засідання, які проводяться в міру потреби, але не рідше одного разу на три місяці, а рішення Комісії в разі необхідності реалізуються шляхом видання в установленому порядку актів Президента України.

Реформування структур безпеки і оборони є одним з пріоритетних напрямків діяльності КУН здійснюється під егідою Спільної робочої групи з оборонної реформи, у рамках Процесу планування і огляду сил, Програм НАТО із сприяння доброчесності і розвитку військової освіти, діяльності Спільної робочої групи з оборонно-технічного співробітництва, а також Дорадчої місії при Представництві НАТО у Києві.

Участь України у Процесі планування і огляду сил (ППОС) є важливим механізмом для визначення досяжних цілей реформування і вдосконалення функціональних спроможностей національних структур безпеки і оборони взаємодіяти із силами Альянсу. Щодо Цілей партнерства то 26 з них стосуються Міністерства оборони і Збройних сил; 15 – Міністерства внутрішніх справ і підпорядкованих йому підрозділів безпеки; і лише одна ціль – кіберзахисту, в якій НАТО надає сприяння з питань розбудови потенціалу у цій галузі. Зокрема, зазначено про започаткування експертних зустрічей з представниками безпекових установ.

Оборонно-технічне співробітництво здійснюється Спільною робочою групою і спрямоване на підвищення оперативної сумісності українських підрозділів, визначених для участі у міжнародних операціях, із збройними силами країн НАТО.

Участь України у проектах ініціативи Розумної оборони НАТО, у рамках якої у 2017 році вона долучилася до трьох із них, у тому числі: «Платформа обміну інформацією про шкідливі комп'ютерні програми», «Багатонаціональна система освіти і підготовки НАТО з питань кіберзахисту».

Програма НАТО «Наука заради миру і безпеки» (НМБ). Поточні проекти у рамках НМБ передбачають широке коло новітніх викликів у галузі безпеки, таких як боротьба з тероризмом, передові технології, кіберзахист, енергетична безпека і захист від хімічних, біологічних, радіоактивних та ядерних (ХБРЯ) речовин.

В сфері співробітництва України з НАТО щодо проблем кібербезпеки важливе значення має Угода про реалізацію Трастового фонду Україна - НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації (Угода) [25], яка передбачає основним суб'єктом її реалізації з української сторони Службу безпеки України і яка є отримувачем допомоги як для власних потреб, так і для потреб інших державних органів.

Предметом Угоди є формування та реалізація Трастового фонду Україна (ТФ) - НАТО з кібербезпеки і надання Україні необхідної підтримки виключно для розвитку оборонних технічних можливостей (таких, як CSIRT-1), у тому числі лабораторій для розслідування інцидентів у кіберсфері.

Розвиток оборонного технічного потенціалу України у сфері кібербезпеки реалізується через:

- впровадження на об'єктах критичної інфраструктури України передових технічних рішень та систем кібербезпеки, які забезпечуватимуть належний рівень кібербезпеки;
- створення центральної та мережевої лабораторії комп'ютерно-технічних експертиз з фіксованими та мобільними компонентами;
- тренінги та консультації для персоналу з експлуатації, ремонту і управління створеними системами.

Такий підхід надає можливість досягти конкретних відповідних результатів у короткостроковій перспективі, залишаючись гнучким залежно від наявності ресурсної бази та з урахуванням доцільності адаптації позитивного досвіду реалізації ТФ.

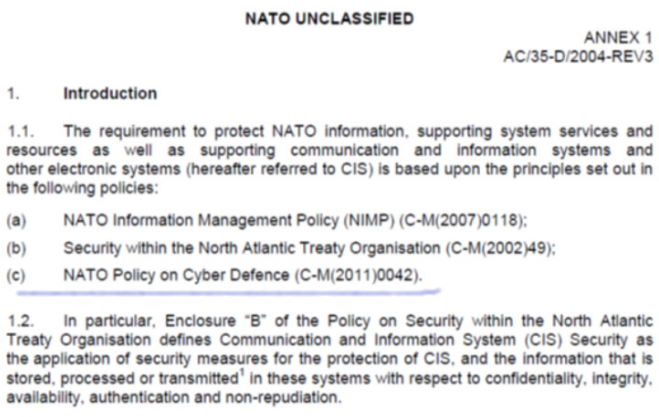
Іншим напрямком взаємодії з НАТО є імплементація Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між Урядом України та організацією Північно-Атлантичного договору [26], які враховують національне законодавство України у сфері охорони та поводження з інформацією з обмеженим доступом, так і мінімальні стандарти безпеки, затверджені у документі "Політика безпеки НАТО" (C-M(2002)49), а також її підтримуючих директивах (зі змінами).

Так, відповідно до пункту 11 статті 7 Адміністративних домовленостей, усі комунікаційно-інформаційні системи (КІС), де обробляється інформація НАТО з обмеженим доступом, підлягають акредитації (підтвердження відповідності) з питань безпеки з метою встановлення достатнього рівня захисту з урахуванням умов конфіденційності, цілісності, доступності, ідентифікації та безвідмовності. Акредитація з питань безпеки національних КІС, де обробляється інформація НАТО з обмеженим доступом, відноситься до національних зобов'язань та її організація проводиться національним Безпековим акредитаційним органом (БАО), яким в Україні є Державна служба спеціального зв'язку та захисту інформації України. БАО, що здійснює організацію акредитації КІС, у яких обробляється інформація НАТО з обмеженим доступом, має бути тим самим органом, що здійснює організацію акредитації всіх національних КІС, у яких обробляється національна інформація з обмеженим доступом.

Іншими директивами та керівними документами, які не зазначені в Адміністративних домовленостях, але підтримують Політику безпеки НАТО (С М(2002)49) та безпосередньо стосуються діяльності БАО є Первинна директива з безпеки комунікаційно-інформаційних систем (Primary Directive on CIS Security, AC/35-D/2004-REV3) [27].

Ця директива визначає, що вимога захисту інформації НАТО, підтримка системних сервісів та ресурсів, що підтримують ґрунтуються на принципах, викладених у таких політиках:

- управління інформацією НАТО (NIMP) (C-M (2007) 0118);
- безпеки в Організації Північноатлантичного договору (C-M (2002) 49);
- щодо кібероборони (C-M (2011) 0042) (Рис. 1).



NATO UNCLASSIFIED

ANNEX 1
AC/35-D/2004-REV3

1. **Introduction**

1.1. The requirement to protect NATO information, supporting system services and resources as well as supporting communication and information systems and other electronic systems (hereafter referred to CIS) is based upon the principles set out in the following policies:

(a) NATO Information Management Policy (NIMP) (C-M(2007)0118);

(b) Security within the North Atlantic Treaty Organisation (C-M(2002)49);

(c) NATO Policy on Cyber Defence (C-M(2011)0042).

1.2. In particular, Enclosure "B" of the Policy on Security within the North Atlantic Treaty Organisation defines Communication and Information System (CIS) Security as the application of security measures for the protection of CIS, and the information that is stored, processed or transmitted[1] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

Рис. 1. Фрагмент первинної Директиви НАТО з безпеки інформаційно-комунікаційних систем

При цьому виконання, поряд з іншими, політики НАТО щодо кібероборони обов'язково наводиться в підсумковому звіті із зазначенням відповідного підрозділу в загальній інфраструктурі функціонування КІС.

Однією з форм координації інтеграційних процесів щодо вступу до НАТО є організація та виконання Річної національної програми під егідою Комісії Україна – НАТО на відповідний рік (РНП). Оновлене Положення про розроблення річних національних програм під егідою Комісії Україна - НАТО та оцінювання результатів їх виконання [28] значно удосконалило алгоритм їх підготовки. Так, Урядовий офіс координації європейської та євроатлантичної інтеграції Секретаріату Кабінету Міністрів України виконує основну роботу з підготовки напередодні планового року проекту РНП, її попереднього узгодження, в тому числі з Міжнародним секретаріатом НАТО, та після доопрацювання надає його МЗС для проведення офіційного погодження із заінтересованими органами в Україні та схвалення Урядом для подальшого розгляду Президентом України. Важливою новацією стало уведення в формування РНП методології стратегічного планування S.M.A.R.T. (з англ.: specific, measurable, attainable, relevant, time-bound — конкретна, вимірювана, досяжна, доцільна, обмежена в часі) можливо окреслити такі рівні планування та шляхи їх досягнення: стратегічна мета; цілі, які необхідно досягнути для її досягнення; конкретні заходи для досягнення цілей; обмеженість у часі виконання заходів; оцінювання їх ефективності та корегування. Ця методологія вперше запроваджена в РНП-2019.

Водночас, основним недоліком, який залишився в РНП, є її декларативність, відсутність реального фінансового забезпечення, надмірна забюракратизованість, і як наслідок, значна затримка в часі затвердження РНП, яка передбачає її погодження не тільки на національному рівні але й з НАТО.

З метою запровадження принципів стратегічного планування для реалізації завдань акредитації до проекту Річної національної програми під егідою Комісії Україна – НАТО на 2019 рік [29] включено нову ціль 4.12, якою у 2019-2021 роках передбачається нарощування спроможностей Держспецзв'язку в цьому напрямку, а в 2019 році – розроблення проекту нормативного акта з організації акредитації таких КІС.

Щодо цілей РНП-2019 у сфері кібербезпеки слід відмітити, що шість державних органів (МЗС, НГУ, Національна поліція, Держспецзв'язку, СБУ, РНБО) ставлять завдання щодо підвищення та розвитку до кінця 2020 року своїх кібербезпекових спроможностей. Водночас, у рамках визначеної стратегічної мети «4.3 Удосконалення національної системи кібербезпеки» наведено низку цілей, спрямованих на розвиток її системоутворюючих елементів (Ситуаційного центру СБУ, Державного центру кіберзахисту Держспецзв'язку, Національного контактного центру Національної поліції) та поліпшення якості їх роботи і взаємодії як між суб'єктами забезпечення кібербезпеки (включаючи об'єкти критичної інфраструктури), так і з уповноваженими органами інших держав.

Співробітництво з міжнародними організаціями у сфері кібербезпеки: Європейський Союз. Взаємодія з ЄС здійснюється в рамках Угоди про асоціацію, співробітництва з Організацією безпеки та співробітництва в Європі (ОБСЄ) та в рамках ініціативи ЄС «Східноєвропейське партнерство».

Відповідно до Угоди про асоціацію, координатором робіт з боку ЄС є Рада асоціації, яка утворюється згідно з статтею 461 Угоди про асоціацію/ПВЗВТ. Вона здійснює контроль і моніторинг застосування і виконання цієї Угоди та періодично переглядає функціонування цієї Угоди у світлі її цілей. Також засновується Комітет асоціації. Він надає допомогу Раді асоціації під час виконання нею своїх обов'язків. Комітету асоціації надають допомогу підкомітети, створені відповідно до цієї Угоди.

Рада асоціації може прийняти рішення про створення будь-якого спеціального комітету чи органу у конкретних сферах, які необхідні для виконання цієї Угоди, і визначає склад, обов'язки та порядок функціонування таких органів. Крім того, такі спеціальні комітети і органи можуть обговорювати будь-яке питання, яке вони вважають доцільним.

Статтею 469 Угоди про асоціацію створюється Платформа громадянського суспільства, яка може надавати рекомендації Раді асоціації. 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.

Комітет асоціації та Парламентський комітет асоціації повинні здійснювати регулярні контакти з представниками Платформи громадянського суспільства з метою отримання їхньої думки щодо досягнення цілей цієї Угоди.

Згідно Звіту про виконання Угоди про асоціацію між Україною та Європейським Союзом у 2018 році [30] за чотирма пріоритетними напрямками інтеграції до ЄС (Рис. 2) в рамках п'ятого засідання Ради асоціації підписано п'ять міжнародних договорів про фінансування нових програм міжнародної допомоги із загальним бю-

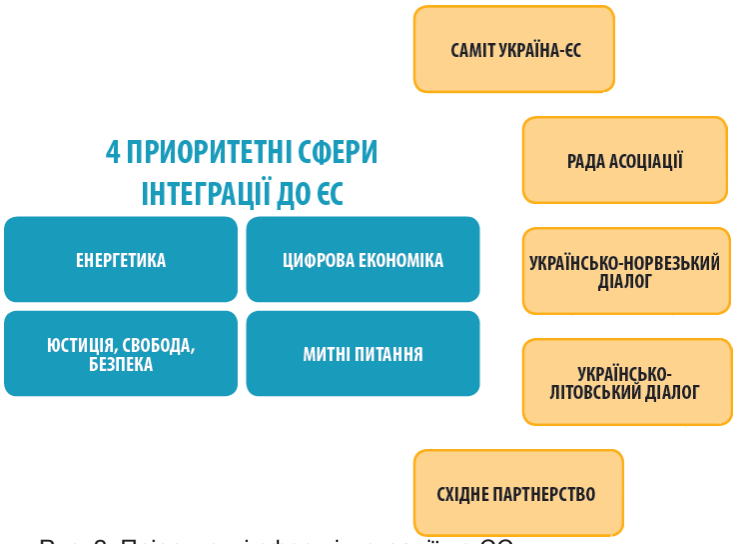


Рис. 2. Пріоритетні сфери інтеграції до ЄС

джетом 222,5 млн. євро. (табл.1). Предметом зазначених договорів визначено реформування, у тому числі, стандартизації, електронного зв'язку, кібербезпеки та розширення контактів України та країн-членів ЄС з метою професійного обміну.

У напрямку 4.2 «Юстиція, Свобода, Безпека та права людини» окреслено такі результати: Україна приєдналась до ряду ініціатив ЄС, які посилюють її спроможність протидіяти кіберзагрозам: залучення до роботи Агентства з питань мережевої та інформаційної безпеки Європейського Союзу (ENISA), а також Європейського центру досліджень та компетенцій з кібербезпеки; проведення тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки; розробка законопроекту щодо внесення змін до Закону України «Про захист персональних даних»; набуття чинності Закону України «Про електронні довірчі послуги».

Україна приєдналась до ряду ініціатив ЄС, які посилюють її спроможність протидіяти кіберзагрозам:

- залучення до роботи Агентства з питань мережевої та інформаційної безпеки Європейського Союзу (ENISA) та Європейського центру досліджень та компетенцій з кібербезпеки;

Таблиця 1

Програма міжнародної технічної допомоги з боку ЄС 20152018 рр.

ПРОТЯГОМ ПЕРІОДУ ДОПОМОГА НАДАВАЛАСЬ В РАМКАХ СПЕЦІАЛЬНИХ ЗАХОДІВ			ПРОГРАМНИЙ ПІДХІД
2015	2016	2017	2018
EU SURE 55 + 40 млн. ЄВРО	**Антикорупційна ініціатива ЄС в Україні** 15 млн. ЄВРО	**Підтримка ЄС для Сходу України** Support for the East 50 млн. ЄВРО	**фінансування Фонду енергоефективності Energy Efficiency** 50 млн. ЄВРО
U-LEAD з Європою 90 млн. ЄВРО	**Підтримка комплексного реформування державного управління** Public Administration Reform 104 млн. ЄВРО	**Програма технічного співробітництва** Technical Cooperation Facility 37 млн. ЄВРО	**Управління державними фінансами** Public Finance Management 55.5 млн. ЄВРО
Програма технічного співробітництва Technical Cooperation Facility 15 млн. ЄВРО	**Підтримка реформ з розвитку верховенства права в Україні PRAV0** 52.5 млн. 6ВРО	**NIF - Local Current Lending** 13 млн. ЄВРО	**Підтримка енергоефективності в Україні EE4U-II** 54 млн. ЄВРО
	Technical Cooperation Facility 28.5 млн. ЄВРО		**Програма технічного співробітництва** Technical Cooperation Facility 37 млн. ЄВРО
			Програма ЄС для навичок: кращі навички для сучасної України **EU4Skills:** Better Skills for Modern Ukraine 58 млн. ЄВРО
			Програми сприяння міжлюдським контактам: Будинок Європи» **People to People Contacts Programme:** House of Europe 18 млн. ЄВРО
200 млн. ЄВРО	**200 млн. ЄВРО**	**100 млн. ЄВРО**	**272,5 млн. ЄВРО**

- тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки.

У 2019 році за Мін'юстом як координатором напрямку 4.2 «Юстиція. Свобода. Безпека» внесено пропозиції української сторони щодо оновлення Плану дій Україна – ЄС у цій сфері [31], а саме: виокремити в розділі «Співробітництво у сфері забезпечення кібербезпеки та захисту інформації», в якому передбачити такі основні подальші цілі:

- посилити співпрацю між ЄС та органами влади України стосовно заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем, а також обміну найкращими практиками між кібер-організаціями ЄС та України;
- створити Регіональний центр кібербезпеки Східного партнерства в Україні;
- розпочати переговори щодо підписання Угоди про співробітництво з ENISA між Україною та ЄС;
- розпочати співробітництво з ENISA з питань скоординованого розкриття вразливостей за досвідом країн-членів ЄС;
- отримати статус спостерігача та залучення України до роботи з ENISA;
- подальше розширення дорадчої та технічної підтримки ЄС в сфері кібербезпеки та захисту інформації;
- підвищення підтримки ЄС щодо підготовки кадрів у профільних установах України з кібербезпеки, а також сприяння розвитку співпраці у сфері досліджень та інновацій в галузі кібербезпеки та захисту інформації;
- залучити правоохоронні органи України до ініціатив ЄС у сфері посилення кібербезпеки з урахуванням прийняття пакету ЄС з кібербезпеки;
- залучення України до діяльності Європейського дослідницького центру з кібербезпеки та до тренінгів (семінарів, круглих столів) ЄС стосовно координації механізмів спільного реагування держав-членів ЄС на масштабні кібератаки та кіберінциденти, а також вивчення досвіду країн-членів ЄС з питань запобігання, виявлення, припинення та розслідування кібератак та кіберінцидентів;
- створення, під егідою Комітету з кіберзлочинності Ради Європи національних робочих груп експертів з числа постійних членів проектів ЄС, представників заінтересованих державних органів та досвідчених фахівців у сфері нормотворчості, представників наукових та бізнес-кіл, які опрацьовуватимуть та розроблятимуть пропозиції щодо вдосконалення чинного законодавства для повної імплементації положень Конвенції;
- здійснення фахової експертизи на рівні експертів ЄС проектів нормативно-правових актів, запропонованих за результатом роботи даних груп.

В 2019 році на основі принципів визнання важливості Стратегії кібербезпеки Європейського Союзу та NIS Директиви передбачається реалізація заходів з підтримки прийняття стандартів, що встановлюватимуть базис для обміну інформацією про загрози та захисні заходи, а також з розроблення та впровадження рекомендацій та практик з безпеки інформації в рамках новостворюваної робочої групи з кібербезпеки визначити вимоги з кібербезпеки, пов'язані із забезпеченням захисту персональних даних у відповідності з європейськими регламентами із захисту персональних даних (GDPR) [32] та електронної ідентифікації та електронних довірчих послуг (eIDAS) [33], визначити загальні схеми інформаційного обміну та кооперації, взаємного визнання сертифікатів з кібербезпеки між країнами-членами ЄС та Східного партнерства, а також навчальних візитів до центрів з забезпечення безпеки (Security Operational Centre, SOC) в країні-члені ЄС.

Висновки

В Україні на законодавчому рівні визначено необхідність та пріоритетність здійснення міжнародного співробітництва в кібербезпековій сфері, яке вона здійснює як на двосторонній основі з окремими державами, насамперед з США, так і з їх об'єднаннями (НАТО та ЄС). В статті проаналізовано їх досвід щодо організаційно-правових та фінансових механізмів міжнародного співробітництва у сфері кібербезпеки з Україною, які зіставлено з існуючими спроможностями України в цій сфері. Аналіз показав, що двостороння міжнародна взаємодія України в сфері кібербезпеки на сьогодні формалізована або знаходиться в стадії завершення формалізації лише з США.

Щодо міжнародної взаємодії України в цій сфері з НАТО та ЄС то, незважаючи на цілу низку розроблених та імплементованих організаційно-правових механізмів державного управління міжнародним співробітництвом, однією з головних проблем залишається проблема координованості дій суб'єктів кібербезпеки, і яка є основною причиною недостатньої ефективності державної політики в цій сфері.

Доведено, що ефективність та результативність міжнародної співпраці в сфері кібербезпеки залежить від багатьох факторів, але основними з них є взаємоузгодженість та координованість дій як основних суб'єктів забезпечення кібербезпеки в Україні, так і відповідних міжнародних акторів. Зазначається, що значно складніша ситуація з координацією діяльності міжнародних акторів, які діють, як правило, не системно для України та незалежно один від одного, виходячи, насамперед, з своїх власних інтересів (інтересів міжнародних донорів), які не завжди в повній мірі відповідають національним пріоритетам України, та, іноді, навіть конкурують між собою в тій чи інший сфері (галузі), стаючи джерелом безсистемних, неупорядкованих, неузгоджених дій, створюючи, у тому числі, загрозу для інтероперабельності організаційно-технічних систем і, як наслідок, суттєво знижують показники ефективності та результативності міжнародної співпраці. Неодноразові спроби з боку держави розв'язати цю проблему в Україні не мали успіху, оскільки кожний міжнародний донор самостійно, виходячи зі своїх особистих інтересів, спроможностей та розуміння наших національних інтересів обирає сферу (галузь, регіон, тощо) та критерії відбору потенційних виконавців (бенефіціарів, реципієнтів). Механізми самоорганізації та саморегулювання серед міжнародних донорів хоча й мають місце, але в силу вищевказаної специфіки тех-

нічної допомоги є фрагментарними, неформалізованими, недостатньо мотивованими для донорів і тому, як правило, неефективними та недієвими.

Сьогоднішній стан міжнародного співробітництва у сфері кібербезпеки характеризує:

- відсутність дієвої державної політики в організації міжнародної взаємодії у сфері забезпеченні кібербезпеки;
- неефективне, некоординоване, неконтрольоване та не обліковане використання отриманих в рамках міжнародної, в тому числі, технічної допомоги в програмного та апаратного забезпечення для підвищення рівня їх кіберзахисту ;
- недостатньо відповідальне ставлення з боку бенефіціарів до отриманих у рамках технічної допомоги програмних та апаратних засобів кіберзахисту, негативно впливає на її міжнародний імідж та інвестиційну привабливості, а також втрати спроможностей України у динамічному впровадженні цифрових технологій.

Зазначається, що вибудувана на основі Закону [14] національна система кібербезпеки не забезпечує належним чином виконання завдань з забезпечення, зокрема, міжнародної співпраці у сфері кібербезпки. Її основні елементи мають пройти глибоку трансформацію. Так, наприклад, Національний координаційний центр кібербезпеки має отримати новий статус, реальні повноваження у відбудові сучасної, ефективної, гнучкої, відповідальної, клієнт-орієнтованої системи забезпечення кібербезпеки. До оновленого органу мають належати повноваження, зокрема:

- впровадження організаційного механізму стратегічного планування заходів з реалізації Стратегії кібербезпеки з визначеними відповідно до цілей Стратегії завданнями та заходами, об'єднаними єдиним задумом, вимірюваними результатами та постійним переглядом ефективності заходів для досягнення визначених цілей, передбачаючи конкретні заходи з міжнародного співробітництва;
- забезпечення належного представництва у міжнародних дорадчих органах у сфері кібербезпеки;
- організації обліку, оцінки захисних якостей, використання та модернізації (заміни) засобів і систем, які застосовуються для забезпечення кібербезпеки об'єктів критичної інфраструктури, критичної інформаційної інфраструктури;
- організації та забезпечення участі українських команд в кібертренуваннях та кібернавчаннях, аналіз отриманого досвіду та поширення кращих отриманих практик;
- організація підготовки та підписання міжнародних договорів з США, ЄС та її країнами-членами, НАТО про співпрацю у сфері кібербезпеки;
- постійний моніторинг, оцінка та імплементація передових норм законодавства у сфері кібербезпеки провідних країн світу та їх об'єднань, міжнародних, в тому числі, європейських стандартів та рекомендацій.

Напрямками подальших досліджень є визначення стану справ щодо спроможностей України у здійснені міжнародного співробітництва на підставі відповідних нормативно-правових актів, конкретних суб'єктів такого співробітництва. Крім того, слід окремо зазначити, що кібербезпекові питання в ЄС чітко регламентовані в декількох документах, а саме: Регламент eIDAS, Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року «Про підвищення загального рівня безпеки мереж та інформаційних систем по всьому Союзу» [34], Закон про кібербезпеку [35], проект Програми цифрової Європи (DIGITAL EUROPE PROGRAMME) [36]. Ці акти будуть розглянуті в наступній розвідці.

Література.

1. Р. В. Лук'янчук. 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: юридичні науки. Кримінальне право та кримінологія; кримінально-виконавче право*. 2018. № 2. Том 29(68). С. 125–129.

3. Дешко Л. М. та Бонарєва К. Д., «Кібербезпека в Україні: Національна стратегія та міжнародне співробітництво», Поряівняльно-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.

6. Забара І. М. Кібернетична безпека держави в умовах розвитку штучного інтелекту: до питання визначення напрямків міжнародно-правового регулювання. С. 213–215

7. Кравець В. М. Порівняльний аналіз міжнародних індексів кібербезпеки». С. 230–2348.

8. Нікітіна Є. О. НТУ «Дніпровська політехніка» Тимофєєв Д.С. НТУ «Дніпровська політехніка» стор. 252-254

9. Ожеван М. А. «Наступальні операції у кіберпросторі та проблема «паралельного інтернет», стор.254-257

10. Стратегія кібербезпеки України, затверджена Указом Президента України Від 15 березня 2016 року № 96/2016 (https://www.president.gov.ua/documents/962016-19836).

11. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 24.06..2016 р. № 440-р. *Урядовий кур'єр* від 05.07.2016. № 123.

12. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.2017 р. № 155 р. *Урядовий кур'єр* від 22.03.2017. № 54.

13. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 11.07.2018 р. № 481-р.

14. Про основні засади кібербезпеки України: Закон України 08.07.2018 р. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19).

15. Другий американсько-український діалог з кібербезпеки. URL: https://ua.usembassy.gov/uk/cybersecurity-bilat/?_ga=2.152620025.114990530.1561925031-954771303.1561925031.

16. Ukraine Cybersecurity Cooperation Act of 2017. URL: https://www.congress.gov/bill/115th-congress/house-bill/1997/text.

17. Національна кіберстратегія США. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

18. Звіт Агентства США з міжнародного розвитку за 2018 рік, USAID. URL: https://www.usaid.gov/sites/default/files/documents/1863/report_ukr.pdf.

19. Офіційний портал НАТО. URL: https://www.nato.int/cps/uk/natohq/topics_37750.htm.

20. Хартія про особливе партнерство між Україною та НАТО. URL: https://zakon4.rada.gov.ua/laws/show/994_002.

21. Спільні заяви Комісії Україна – НАТО. URL: https://www.nato.int/cps/uk/natohq/topics_50319.htm та URL: https://www.nato.int/cps/en/natohq/official_texts_119425.htm?selectedLocale=uk.

22. Спільна заява Комісії Україна – НАТО з нагоди 20-ї річниці Хартії про особливе партнерство між Україною та НАТО. URL: https://mfa.gov.ua/ua/press-center/news/58521-spilyna-zajava-komisiji-ukrajina--nato-z-nagodi-20-ji-richnici-khartiji-pro-osoblive-partnerstvo-mizh-ukrajinoju-ta-nato

23. Угода про реалізацію Трастового фонду Україна - НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації. URL: https://zakon.rada.gov.ua/laws/show/642_063.

24. Заява Головуючого про відносини Україна – НАТО за підсумками засідання Північноатлантичної ради з Грузією та Україною. URL: https://www.nato.int/cps/en/natohq/official_texts_156623.htm?selectedLocale=uk.

25. Питання координації євроатлантичної інтеграції України: Указ Президента України від 08.07.2016 р. № 296/2016. Питання координації євроатлантичної інтеграції Українихttps://zakon.rada.gov.ua/laws/show/296/2016.

26. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та організацією Північно-Атлантичного договору URL:https://zakon.rada.gov.ua/laws/show/950_035-16.

27. 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.

28. Про річні національні програми під егідою Комісії Україна – НАТО: Указ Президента України від 02.10.2018 р. № 298/2018. URL: https://www.president.gov.ua/documents/2982018-25074.

29. Про Річну національну програму під егідою Комісії Україна – НАТО на 2019 рік: Указ Президента України від 10.04.2019 р. №117/2019. URL: https://www.president.gov.ua/documents/1172019-26450.

30. Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом У 2018 році. URL: https://eu-ua.org/sites/default/files/inline/files/association-agreement-implementation-report-2018.pdf.

31. План дій Україна – ЄС у сфері «Юстиція. Свобода. Безпека». URL: https://minjust.gov.ua/m/plan-diy-ukraina-es-u-sferi-yustitsii-svobodi-ta-bezpeki-1224.

32. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad-/.

33. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf.

34. Про підвищення загального рівня безпеки мереж та інформаційних систем по всьому Союзу: директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 06.07.2016 р. 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.

35. Закон ЄС про кібербезпеку. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

36. Програма цифрової Європи. URL: https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027.

References:

1. R. V. Lukianchuk. Mizhnarodne spivrobitnytstvo u sferi zabezpechennia kibernetychnoi bezpeky: derzhavni priorytety, Visnyk NADU, 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. Shemchuk V. V., «Osnovni napriamky mizhnarodnoho spivrobitnytstva u sferi kiberbezpeky». Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: yurydychni nauky. Kryminalne pravo ta kryminolohiia; kryminalno-vykonavche pravo. 2018. № 2. Tom 29(68). S. 125–129.

3. Deshko L. M. ta Bonarieva K. D., «Kiberbezpeka v Ukraini: Natsionalna stratehiia ta mizhnarodne spivrobitnytstvo», Poriaivnialno-analitychne pravo. 2018. № 2. URL: http://pap.in.ua/2_2018/112.pdf.

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.

5. Doronin I. M., Orhanizatsiia zvituvannia subiektiv kiberbezpeky. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

6. Zabara I. M. Kibernetychna bezpeka derzhavy v umovakh rozvytku shtuchnoho intelektu: do pytannia vyznachennia napriamkiv mizhnarodno-pravovoho rehuliuvannia. S. 213–215

7. Kravets V. M. Porivnialnyi analiz mizhnarodnykh indeksiv kiberbezpeky». S. 230–2348.

8. Nikitina Ye. O. NTU «Dniprovska politekhnika» Tymofieiev D.S. NTU «Dniprovska politekhnika» stor. 252-254

9. Ozhevan M. A. «Nastupalni operatsii u kiberprostori ta problema «paralelnoho internet», stor.254-257

10. Stratehiia kiberbezpeky Ukrainy, zatverdzhena Ukazom Prezydenta Ukrainy Vid 15 bereznia 2016 roku № 96/2016 (https://www.president.gov.ua/documents/962016-19836).

11. Pro zatverdzhennia planu zakhodiv na 2016 rik z realizatsii Stratehii kiberbezpeky Ukrainy:

Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 24.06..2016 r. № 440-r. Uriadovyi kurier vid 05.07.2016. № 123.

12. Pro zatverdzhennia planu zakhodiv na 2017 rik z realizatsii Stratehii kiberbezpeky Ukrainy: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 10.03.2017 r. № 155 r. Uriadovyi kurier vid 22.03.2017. № 54.

13. Pro zatverdzhennia planu zakhodiv na 2018 rik z realizatsii Stratehii kiberbezpeky Ukrainy: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 11.07.2018 r. № 481-r.

14. Pro osnovni zasady kiberbezpeky Ukrainy: Zakon Ukrainy 08.07.2018 r. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19).

15. Druhyi amerykansko-ukrainskyi dialoh z kiberbezpeky. URL: https://ua.usembassy.gov/uk/cybersecurity-bilat/?_ga=2.152620025.114990530.1561925031-954771303.1561925031.

16. Ukraine Cybersecurity Cooperation Act of 2017. URL: https://www.congress.gov/bill/115th-congress/house-bill/1997/text.

17. Natsionalna kiberstratehiia SShA. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

18. Zvit Ahentstva SShA z mizhnarodnoho rozvytku za 2018 rik, USAID. URL: https://www.usaid.gov/sites/default/files/documents/1863/report_ukr.pdf.

19. Ofitsiinyi portal NATO. URL: https://www.nato.int/cps/uk/natohq/topics_37750.htm.

20. Khartiia pro osoblyve partnerstvo mizh Ukrainoiu ta NATO. URL: https://zakon4.rada.gov.ua/laws/show/994_002.

21. Spilni zaiavy Komisii Ukraina – NATO. URL: https://www.nato.int/cps/uk/natohq/topics_50319.htm ta URL: https://www.nato.int/cps/en/natohq/official_texts_119425.htm?selectedLocale=uk.

22. Spilna zaiava Komisii Ukraina – NATO z nahody 20-yi richnytsi Khartii pro osoblyve partnerstvo mizh Ukrainoiu ta NATO. URL: https://mfa.gov.ua/ua/press-center/news/58521-spilyna-zajava-komisiji-ukrajina--nato-z-nagodi-20-ji-richnici-khartiji-pro-osoblive-partnerstvo-mizh-ukrajinoju-ta-nato

23. Uhoda pro realizatsiiu Trastovoho fondu Ukraina - NATO z pytan kiberbezpeky mizh Sluzhboiu bezpeky Ukrainy ta Rumunskoiu sluzhboiu informatsii. URL: https://zakon.rada.gov.ua/laws/show/642_063.

24. Zaiava Holovuiuchoho pro vidnosyny Ukraina – NATO za pidsumkamy zasidannia Pivnichnoatlantychnoi rady z Hruziieiu ta Ukrainoiu. URL: https://www.nato.int/cps/en/natohq/official_texts_156623.htm?selectedLocale=uk.

25. Pytannia koordynatsii yevroatlantychnoi intehratsii Ukrainy: Ukaz Prezydenta Ukrainy vid 08.07.2016 r. № 296/2016. Pytannia koordynatsii yevroatlantychnoi intehratsii Ukrainyhttps://zakon.rada.gov.ua/laws/show/296/2016.

26. Administratyvni domovlenosti shchodo okhorony informatsii z obmezhenym dostupom mizh Uriadom Ukrainy ta orhanizatsiieiu Pivnichno-Atlantychnoho dohovoru URL:https://zakon.rada.gov.ua/laws/show/950_035-16.

27. 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.

28. Pro richni natsionalni prohramy pid ehidoiu Komisii Ukraina – NATO: Ukaz Prezydenta Ukrainy vid 02.10. 2018 r. № 298/2018. URL: https://www.president.gov.ua/documents/2982018-25074.

29. Pro Richnu natsionalnu prohramu pid ehidoiu Komisii Ukraina – NATO na 2019 rik: Ukaz Prezydenta Ukrainy vid 10.04.2019 r. №117/2019. URL: https://www.president.gov.ua/documents/1172019-26450.

30. Zvit pro vykonannia Uhody pro asotsiatsiiu mizh Ukrainoiu ta Yevropeiskym Soiuzom U 2018 rotsi. URL: https://eu-ua.org/sites/default/files/inline/files/association-agreement-implementation-report-2018.pdf.

31. Plan dii Ukraina – YeS u sferi «Iustytsiia. Svoboda. Bezpeka». URL: https://minjust.gov.ua/m/plan-diy-ukraina-es-u-sferi-yustitsii-svobodi-ta-bezpeki-1224.

32. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad-/.

33. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf.

34. Pro pidvyshchennia zahalnoho rivnia bezpeky merezh ta informatsiinykh system po vsomu Soiuzu: dyrektyva (IeS) 2016/1148 Yevropeiskoho Parlamentu ta Rady vid 06.07.2016 r. 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.

35. Zakon YeS pro kiberbezpeku. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

36. Prohrama tsyfrovoi Yevropy. URL: https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027.