УДК. 35.316

Потій Олександр,
ORCID ID 0000-0002-2366-0541
E-mail: potav1971@gmail.com

Семенченко Андрій,
ORCID ID 0000-0001-6482-3872
E-mail: Andrii.semenchenko@gmail.com

Бакалинський Олександр,
ORCID ID 0000-0001-9712-2036 E-mail:
baov@meta.ua

Мялковський Данило,
ORCID ID 0000-0002-8246-8437
E-mail: daniilvm71@gmail.com

ПУБЛІЧНЕ УПРАВЛІННЯ ІНСТИТУЦІОНАЛЬНИМ РОЗВИТКОМ У СФЕРІ КІБЕРЗАХИСТУ

[https://doi.org/10.32689/2618-0065-2021-3\(9\)-136-162](https://doi.org/10.32689/2618-0065-2021-3(9)-136-162)

Анотація. Внаслідок зростання складності, інтенсивності різноманітності кіберзагроз, способів та інструментів їх застосування, мілітаризації кіберпростору й перетворення його в одну зі сфер ведення бойових дій тощо актуалізується проблема його кіберзахисту, що зумовлює необхідність врахування цих факторів при формуванні та реалізації публічної політики і публічного управління у сфері національної безпеки, розвитку сектору безпеки та оборони, важливою складовою якої є національна система кібербезпеки. У статті проаналізовано механізм інституціонального розвитку основних суб'єктів національної системи кіберзахисту в Україні, насамперед Держспецзв'язку, формування науково обґрунтованих підходів та пропозицій щодо його удосконалення з урахуванням трансформаційних змін сектору безпеки і оборони України. Визначено роль і місце підсистеми кіберзахисту в загальній системі кібербезпеки України, а також її головного елемента – Держспецзв'язку. Запропоновано науково обґрунтований ризик-орієнтований підхід до формування моделі взаємодії суб'єктів забезпечення кіберзахисту, що надає можливість враховувати особливості й спроможності суб'єктів кібербезпеки та уникати дублювання їх функцій та завдань, зменшувати рівень конкуренції між собою за вплив на сферу. Охарактеризовано основні проблеми організаційно-правового забезпечення розвитку системи кіберзахисту в Україні та шляхи їх розв'язання. Розроблено модель взаємодії суб'єктів забезпечення кіберзахисту, яка ґрунтується як на чинному законодавстві, так і на перспективних напрямках його удосконалення. Обґрунтовано конкретні шляхи удосконалення чинного законодавства з метою усунення дублювальних функцій та завдань суб'єктів забезпечення кіберзахисту.

Ключові слова: публічне управління, інституціональний розвиток, кіберзахист, кібербезпека, національна система кібербезпеки, сектор безпеки і оборони.

Постановка проблеми. Обов'язковою умовою успішного розвитку цифрової держави й суспільства, цифрової економіки та демократії, здійснення цифрових трансформацій є наявність надійного, захищеного, всеосяжного кіберпростору. Саме у кіберпросторі громадянин здійснює свою цифрову діяльність через використання різноманітних інформаційних та телекомунікаційних технологій. Крім того, формується та розвивається цифрова економіка та суспільство, посилюються процеси глобалізації. Але внаслідок зростання складності, інтенсивності, різноманітності кіберзагроз і способів та інструментів їх застосування, мілітаризації кіберпростору й перетворення його в одну зі сфер ведення бойових дій тощо актуалізується проблема його кіберзахисту. Це зумовлює необхідність врахування зазначених факторів під час формування та реалізації публічної політики й публічного управління у сфері національної безпеки, розвитку сектору безпеки і оборони, важливою складовою якої є національна система кібербезпеки. Водночас ця система не повністю відповідає вимогам щодо своєї надійності, оперативності, адекватності й гнучкості реагування на потенційні та реальні загрози у сфері кібербезпеки й потребує суттєвого удосконалення насамперед своєї структури, правових засад функціонування і взаємодії її суб'єктів та державного органу, що її координує, – Держспецзв'язку.

Аналіз останніх досліджень і публікацій. Проблеми щодо розвитку національної системи кібербезпеки взагалі і кіберзахисту зокрема розглядалися вітчизняними та іноземними науковцями. Так, В. Шемчук [1] доходить висновку, що кібербезпека є пріоритетом у діяльності не тільки різних держав, а і їх регіональних об'єднань та навіть всієї світової спільноти. Л. Дешко та К. Бонарева наголошують на важливості міжнародного співробітництва [2]. Г. Піскорська та Н. Яковенко зазначають про широкий спектр напрямів міжнародної взаємодії у кіберпросторі [3]. І. Доронін, аналізуючи норми законодавства у сфері кібербезпеки, доходить висновків [4] щодо недоскопалості термінологічної бази та необхідності законодавчого встановлення вимог до порядку звітування суб'єктів кібербезпеки так само, як загалом

у сфері національної безпеки і оборони. І. Забара [5] вважає, що актуальними напрямками міжнародно-правового регулювання постануть укладення двосторонніх, регіональних і універсальних міжнародних угод з інформаційної та кібербезпеки. В. Кравець виокремлює важливі характеристики та вимір оцінки успішності діяльності у сфері кібербезпеки на різних рівнях [6]. Є. Нікітіна наводить опис [7] основних інструментів проактивного аналізу кіберзагроз щодо пошуку та розслідування кіберзагроз як ефективних механізмів забезпечення безпеки інформації. С. Вдовенко, Ю. Даник та О. Пермяков інституційний розвиток кібербезпеки розглядають [8] в контексті аналізу міжнародного досвіду та завдань для України щодо розвитку сфери кібероборони.

Водночас слід зазначити, що комплексного дослідження сфери кібербезпеки, визначення її невід'ємних складових підсистем, їх інституціонального складу та зв'язків між ними, шляхів розвитку сфери кіберзахисту в сучасних умовах змін не проводилося.

Методи дослідження. Під час проведення дослідження були використані загальнонаукові і спеціальні методи пізнання, а для з'ясування місця і ролі Держспецзв'язку в системі кіберзахисту – метод структурно-функціонального аналізу. Метод критичного аналізу використано для встановлення прогалин в нормативно-правових актах, що регламентують діяльність в зазначеній сфері. Застосування методів аналізу та синтезу сприяло ефективному розробленню рекомендацій щодо організації взаємодії Держспецзв'язку із суб'єктами національної системи кібербезпеки.

Мета статті полягає у визначенні місця і ролі Держспецзв'язку серед суб'єктів національної системи кіберзахисту в Україні, формуванні науково обґрунтованих пропозицій щодо удосконалення її інституційного розвитку з урахуванням трансформаційних змін сектору безпеки і оборони України.

Виклад основного матеріалу. Кіберпростір є середовищем, яке принципово відрізняється від звичайного фізичного світу. Проте він є надзвичайно фізичним

середовищем : створений фізичними мережами й системами, що поєднані між собою, та підпорядковуються певним правилам, що проявляються через програмне забезпечення й комунікативні протоколи. Крім того, основа роботи кіберпростору – це суто фізичні закони електромагнетизму та світла. Вони створюють його основну особливість – можливість глобальних комунікацій та передачі масштабних обсягів даних, які здійснюються майже миттєво і передаються на великі відстані, незважаючи на географічні кордони. Саме швидкість і незалежність від фізичних перешкод дає найважливішу перевагу і одночасно створює проблему, оскільки можливості кіберпростору можуть бути використані будь-ким та з будь-якою метою.

Визнаючи кіберпростір одним із середовищ застосування геостратегій та «п'ятим плацдармом» проведення бойових дій, разом із суходолом, морем, повітрям і космосом, дедалі більше уваги приділяється розвитку й захисту інформаційних ресурсів, а також можливостям впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави.

У Законі України «Про основні засади забезпечення кібербезпеки України» [9] *кібербезпека* визначається, як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а *кіберпростір* – «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». Ці визначення є результатом відповідного компромісу суб'єктів забезпечення кібербезпеки та не відповідають повною мірою визначенням, які запропоновані в міжнародній практиці [10]. Очікуються, що в нову редакцію Закону будуть внесені

уточнення і врахується як отриманий національний, так і міжнародний досвід.

Кібербезпеку забезпечують суб'єкти кібербезпеки, які здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних, маніпулятивних та інших протиправних і злочинних цілях, виявляють і реагують на кіберінциденти та кібератаки, усунення їх наслідків, провадять інформаційний обмін щодо реалізованих та потенційних кіберзагроз, розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту, забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління, здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору. Схематично модель взаємодії підсистеми кіберзахисту у складі системи забезпечення кібербезпеки та іншими її складовими представлена на рис. 1.

Рисунок 1 – Місце та роль кіберзахисту у забезпеченні кібербезпеки

Складено авторами

Видами діяльності у сфері кібербезпеки є: кібероборона, кіберзахист, протидія кібертероризму, кібершпигунству та кіберзлочинності, кіберрозвідка та кібердипломатія, а також координація діяльності за цими видами. Така діяльність спрямована на нейтралізацію різних видів джерел загроз і на захист людини, суспільства, держави, процесів та інформаційних технологій.

Ці види діяльності розподілені між складовими національної системи кібербезпеки, насамперед її ядра, яке утворюють основні суб'єкти національної системи кібербезпеки.

У законодавстві внаслідок його динамічного розвитку, перманентних структурних і функціональних змін сектору безпеки та оборони чітко не визначено інституалізаційну підсистему кіберзахисту системи кібербезпеки, її елементи, завдання та функції, порядки взаємодії. Винятком є Держспецзв'язку, підпорядкований йому Державний центр кіберзахисту та Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Але ці суб'єкти теж потребують суттєвого коригування своєї структури, повноважень, цілей та пріоритетів діяльності з метою максимального наближення до інституційних вимог ЄС та НАТО, підвищення рівня ефективності та результативності публічної політики й управління у цій сфері.

Відповідно до Закону України [9] Держспецзв'язку забезпечує:

формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та

усунення їх наслідків;

інформує про кіберзагрози та відповідні методи захисту від них;

забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Графічне представлення ролі і місця Держспецзв'язку в загальній системі кібербезпеки представлено на рис. 2.

Рисунок 2 – Роль і місце Держспецзв'язку в системі кібербезпеки

Складено авторами

У Законі визначено 25 основних напрямів (шляхів) розвитку та функціонування національної системи кібербезпеки, у 14-ти з яких Держспецзв'язку виступає як основний державний орган, який забезпечує їх реалізацію. Водночас шість напрямів із них Держспецзв'язку реалізовує (організовує їх реалізацію), виконуючи роль головного державного органу, на який покладено формування державної політики, координація діяльності інших суб'єктів кіберзахисту (рис. 3).

Рисунок 3 – Функції Держспецзв'язку як органу із забезпечення формування та реалізації державної політики

Складено авторами

Протягом декількох років з часу набуття чинності Законом, а перед ним – Стратегії кібербезпеки України в Адміністрації Держспецзв’язку для інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО, розробили нормативно-правове підґрунтя і засади розвитку сфери кіберзахисту об’єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена у Законі, що надало можливість :

- створити основу термінологічної бази сфери кіберзахисту;
- розпочати оновлення та гармонізацію нормативних документів у сфері захисту інформації та забезпечити їх сумісність з відповідними стандартами Європейського Союзу та НАТО;

- упровадити Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури;

- сформувані критерії та визначити порядок віднесення до критичної інфраструктури тих об’єктів, які є важливими для економіки і національної безпеки та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;

- визначитись з першочерговістю (пріоритетністю) захисту від кібератак, включених до Переліку об’єктів критичної інформаційної інфраструктури, у тому числі й шляхом забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об’єкти та безпечність їх функціонування;

- визначити мету, завдання і порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

- нормативно забезпечити розгортання та функціонування Національної телекомунікаційної мережі [11]. У рамках виконання завдань щодо створення та забезпечення функціонування Національної телекомунікаційної мережі проводяться заходи щодо побудови її транспортної платформи, системи оперативно-технічного управління та автоматизації

процесів надання послуг;

започаткувати процес створення системи аудиту інформаційної безпеки, у тому числі й об'єктів критичної інформаційної інфраструктури;

розпочати роботи з розгортання в Україні системи резервування державних інформаційних ресурсів;

запровадити експериментальний проєкт з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (ІТС), в яких обробляються державні інформаційні ресурси [12], а також розгорнути систему виявлення вразливостей і реагування на кіберінциденти та кібератаки [13].

Водночас спостерігається низька ефективність в ідентифікації інформаційно-технологічних систем (далі – ІТС), безпечне функціонування яких критично впливає на функціонування публічних органів влади. Ініційовані Урядом України заходи щодо ідентифікації об'єктів критичної інфраструктури, а в них – об'єктів критичної інформаційної інфраструктури не були повністю впроваджені державними органами насамперед щодо ідентифікації власних критично важливих для свого функціонування ІТС та внесення їх до переліку об'єктів критичної інформаційної інфраструктури (далі – ОКІІ). Наслідком цього є неналежне впровадження механізмів кіберзахисту та непідтверджений рівень захищеності таких систем.

Разом із тим з метою розгортання національної системи кіберстійкості на сьогодні Держспецзв'язку вживаються заходи щодо розвитку організаційно-технічної моделі кіберзахисту (ОТМК) як сукупності систем, комплексів і заходів, призначених для забезпечення кібербезпеки об'єктів критичної інфраструктури та кіберзахисту державних електронних інформаційних ресурсів [14], а також її телекомунікаційної платформи – Національної телекомунікаційної мережі. Ключовим елементом ОТМК є Центр реагування на кіберзагрози Держспецзв'язку (Cyber Threat Response Centre, CRC), який у режимі 24/7 забезпечує раннє виявлення аномальної активності та потенційно небезпечних подій у системах і мережах, підключених до Інтернету, та являє собою

технічну платформу взаємодії основних суб'єктів національної системи забезпечення кібербезпеки та приватного сектору, в інтересах яких розгорнуто єдину інтерактивну базу даних про кіберінциденти на підґрунті програмного забезпечення з відкритим вихідним кодом TheHive.

У межах упровадження цієї платформи забезпечується моніторинг інформації, яка надходить від сенсорів кібермоніторингу телеметрії в ІТС державних органів.

Важливим структурним елементом інституційної системи кіберзахисту є *Урядова команда реагування CERT-UA*, яка проводить аналіз даних про кіберінциденти, надає власникам об'єктів кіберзахисту практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів, готує й розміщує на своєму офіційному вебсайті рекомендації щодо протидії сучасним видам кібератак і кіберзагроз, інформує про кіберзагрози та відповідні методи захисту від них, взаємодіє з правоохоронними органами, іноземними й міжнародними організаціями з питань реагування на кіберінциденти.

Із 2009 року CERT-UA акредитована у FIRST (Forum for Incident Response and Security Teams – Форумі команд реагування на інциденти інформаційної безпеки). Членство у FIRST, в рамках протидії кіберзагрозам на міжнародному рівні, надає можливість оперативно взаємодіяти з 308 командами реагування на комп'ютерні інциденти (CERT) з 67 країн світу. Командою CERT-UA постійно вживаються заходи щодо взаємодії із зарубіжними командами CERT з питань подолання наслідків кібератак на критичну інформаційну інфраструктуру і встановлення причин та обставин кіберінцидентів.

Варто зауважити, що членство у FIRST надає Україні можливість отримувати найповнішу та найактуальнішу інформацію про кіберінциденти й кібератаки. Ці так звані індикатори компрометацій надають можливість наповнювати зазначену вище єдину інтерактивну базу даних про кіберінциденти та поширювати інформацію про них на відповідних платформах обміну інформацією. На сьогодні, окрім зазначеної платформи Держспецзв'язку, існують схожі з нею, але з меншою глибиною аналізу інформації про кіберінциденти платформи MISP-UA (Ситуаційний центр

забезпечення кібербезпеки Служби безпеки України) та MISIP Національного координаційного центру з кібербезпеки при РНБОУ. Питання ефективності організації взаємного відповідального обміну інформацією про кіберінциденти та кіберзагрози між цими трьома платформами потребують окремого дослідження, але зазначимо, що сам факт збільшення кількості таких платформ вказує на потенційне збільшення охопленої аудиторії державних та недержавних структур, які дбають про свою кібербезпеку.

У рамках державно-приватної взаємодії та співробітництва, зокрема міжнародного, з метою зміцнення взаємної довіри у сфері кібербезпеки й вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль усіх суб'єктів для забезпечення кіберзахисту укладаються меморандуми про організацію взаємодії у сфері кібербезпеки та кіберзахисту з державними органами, громадськими організаціями, державними підприємствами. Позитивним прикладом у цьому напрямі стало підписання Меморандуму між Мінцифри, Держспецзв'язку, Національним координаційним центром кібербезпеки та створення на його основі в кінці 2020 року Ради інформаційної та кібербезпеки, яка об'єднала зусилля державних органів, приватних і громадських організацій, науковців та освітян, можливості міжнародної технічної допомоги. У цій раді коло представництва постійно розширюється, що сприяє розвитку діалогу між її учасниками.

Ефективність та результативність забезпечення кіберзахисту й кібербезпеки значною мірою залежить від коректного розподілу функцій і завдань між основними суб'єктами національної системи кібербезпеки і їх ефективної взаємодії. Хоча за Законом [9] дублювання їх функцій не убачається, але на практиці спостерігаються певні перетинання щодо кіберзахисту, а також залишаються незабезпеченими вкрай важливі напрями кібероборони.

Аналіз чинного законодавства надав можливість сформулювати його основні недоліки:

1. У пункті 2 статті 3 Положення про Національний координаційний центр кібербезпеки (далі – НКЦК), затвердженого Указом Президента України від 7 червня 2016

року № 242/2016, визначено, що НКЦК «здійснює аналіз: стану кіберзахисту критично важливих об'єктів інфраструктури; огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; ... стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури». Зважаючи на те, що проведення аналізу і оцінювання потребує проведення однакових заходів, а саме: збору інформації, її обробки і аналізу, підготовки висновків і пропозицій, вважаємо, що це завдання НКЦК кореспондується з покладеним постановою Кабінету Міністрів України від 11 листопада 2020 р. № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» на Держспецзв'язку завданням щодо організації заходів з «оцінювання стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».

2. У пункті 14 статті 3 Положення про НКЦК визначено завдання НКЦК, як: «участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки, розроблення відповідних методичних документів і рекомендацій». На нашу думку, розробка методичних документів і рекомендацій у контексті організації та проведенні навчань має бути функцією державних органів, які уповноважені на їх проведення.

Водночас вважається за необхідне саме НКЦК при РНБО в процесі координації діяльності суб'єктів розмежовувати напрями відповідальності, у тому числі в частині впливу (вжиття заходів) за фактами кіберзлочинної діяльності у кіберпросторі, а саме: використання ботнет для здійснення кібератак на національну інформаційну інфраструктуру, використання хостів для здійснення фішингових атак, використання командно-управляючих серверів не на території

України для розсилки шкідливого програмного забезпечення тощо.

3. У пункті 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» зазначено, що на СБУ покладено завдання щодо «розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки.».

Слід зазначити, що на сьогодні СБУ, крім розслідування кіберінцидентів та кібератак, спрямованих на державну безпеку України, у рамках чого здійснюється збір даних щодо кібератак та кіберінцидентів, а також застосовується спеціальне програмне забезпечення або технічні пристрої для отримання, збирання та накопичення інформації стосовно обставин кіберінцидента чи кібератаки, вирішує завдання щодо виявлення та нейтралізації кібератак на комунікаційні системи державних органів і системи керування об'єктів критичної інфраструктури (завдання Ситуаційного центру забезпечення кібербезпеки СБУ), позиціонуючи себе як такий, що провадить діяльність щодо захисту об'єктів критичної інфраструктури та інформаційних ресурсів держави від кіберзагроз. Хоча ця діяльність відповідно до [9] є завданням та повноваженням Держспецзв'язку, а такий підхід суттєво ускладнює їх виконання, тому що вносить непорозуміння у діяльність посадових осіб, відповідальних за забезпечення кібербезпеки ОКИ, з яким саме органом треба взаємодіяти з питань забезпечення кіберзахисту.

Крім того, СБУ на майбутнє як пріоритетний напрям своєї діяльності у рамках формування Стратегії кібербезпеки України на 2021–2026 визначає завдання щодо «створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності», що знаходиться поза межами повноважень СБУ. Слід зазначити, що відповідальним за

функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки є Державний центр кіберзахисту Держспецзв'язку [12].

Зважаючи на повноваження Держспецзв'язку щодо проведення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, завдань щодо координації, організації та проведення моніторингу стану захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість, заходів, що проводяться у рамках розслідувань кіберінцидентів як частини системи управління кіберінцидентами, вважаємо, що проактивна позиція СБУ у питаннях кіберзахисту з акцентом на виявлення кібератак та моніторинг стану захищеності об'єктів кіберзахисту поза процедурою їх розслідування призводить до дублювання завдань і функцій Держспецзв'язку, ускладнення процесів інформаційного обміну щодо кіберінцидентів, унеможливлення розбудови державного управління кібербезпекою, зайвого витрачання державних коштів.

Крім того, СБУ позиціонує себе на міжнародній арені як орган, який «ефективно співпрацює з ЄС і НАТО для підвищення захищеності державних і фінансових структур до кіберзагроз», не маючи таких повноважень априорі та не відповідаючи за формування політик у цій сфері діяльності.

4. Слід зазначити, що у пункті 4 статті 6 Закону України [9] визначено, що відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури. Водночас у підпункті 4 пункту 2 статті 8 цього ж Закону зазначено, що Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції «впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану», що призводить до певної колізії повноважень та відповідальності суб'єктів забезпечення кібербезпеки та непорозумінь щодо передачі функцій і повноважень при

виконанні заходів із кіберзахисту у різних правових режимах функціонування держави. Тим більше, що на сьогодні в українському законодавстві відсутнє чітке визначення моменту початку війни саме у кіберпросторі, який може настати, на наш погляд, раніше ніж у країні буде введено воєнний стан. Саме тому підрозділи, які забезпечують кіберзахист України, мають бути підрозділами постійної готовності, а алгоритми, за якими Міністерство оборони України, Генеральний штаб Збройних Сил України починає виконання своїх завдань у кіберпросторі, в тому числі щодо забезпечення кіберзахисту критичної інформаційної інфраструктури, мають бути розроблені, опрацьовані на всіх рівнях ОТМ та бути постійно актуальними.

З огляду на зазначене вище пріоритетними напрямками взаємодії для Держспецзв'язку, НБУ, ЗСУ має бути кіберзахист та кібероборона, що включають:

- формування вимог до систем кіберзахисту;
- розроблення та впровадження нових технологій кіберзахисту;
- впровадження проактивних засобів кіберзахисту;
- моніторинг, аналіз та оцінку стану кіберзахисту галузей / об'єктів критичної інфраструктури.

Основним фокусом спільної діяльності СБУ, МВС, розвідок та МЗС є робота з джерелами загроз та кіберзагроз, а саме:

- аналіз технічних та технологічних можливостей джерел загроз;
- вивчення та визначення сценаріїв проведення кібератак;
- забезпечення відповідальної поведінки держав у кіберпросторі.

Інші суб'єкти системи кібербезпеки концентрують свою діяльність на забезпеченні швидкого відновлення після кібератак та зниження масштабів збитків.

Головним завданням НКЦК при РНБО має бути розробка та координація впровадження системи управління ризиками кібербезпеки у повсякденну діяльність суб'єктів забезпечення кібербезпеки, аналіз і оцінювання рівня кіберризиків секторів економіки і сфер діяльності, формування рекомендацій щодо варіантів їх оброблення, контроль та координація діяльності суб'єктів системи кібербезпеки.

Упровадження такого підходу надасть можливість усунути (зменшити) існуючі, а також уникнути у майбутньому конфліктів інтересів основних суб'єктів національної системи забезпечення кібербезпеки, спрямувати їх діяльність на основний результат – зниження ризиків для кібербезпеки.

У табл. 1 представлено інституційну модель взаємодії Держспецзв'язку із суб'єктами забезпечення кібербезпеки, в основу якої покладені положення як чинного законодавства, так і перспективні, на думку авторів, напрями його удосконалення, насамперед щодо конкретизації, деталізації, усунення дублювання завдань та функцій суб'єктів кіберзахисту, максимального використання їх спроможностей і врахування особливостей, впровадження кращого міжнародного досвіду.

Таблиця 1 – Взаємодія Держспецзв'язку із суб'єктами національної системи кібербезпеки

Назва органу	Держспецзв'язку		
	надає	отримує	потребує
Президент України	звітування як суб'єкта сектору безпеки і оборони		
Верховна Рада України	пропозиції щодо вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО; пропозиції щодо створення нормативно-правової та термінологічної бази у сфері кіберзахисту, інформаційно-аналітичні матеріали та пропозиції до проекту рекомендацій парламентських або комітетських слухань	завдання згідно з рекомендаціями відповідних слухань	сприяння якомога скорішому розробленню під своєю егідою та прийняттю Верховною Радою України вкрай актуальних законодавчих ініціатив, оскільки стандартні процедури актуальність законодавчої ініціативи не забезпечують
Кабінет Міністрів України	пропозиції щодо удосконалення та розвитку нормативно-правової бази у сфері кіберзахисту; результати первинного аналізу з питань кіберзахисту об'єктів критичної інформаційної інфраструктури	доручення і розпорядження щодо виконання завдань основними суб'єктами забезпечення кібербезпеки	визначення органу технічного регулювання у сфері кіберзахисту; визначення

Назва органу	Держспецзв'язку		
	надас	отримус	потребус
Апарат РНБО України (НКЦК)	звіт за результатами проведення огляду стану кіберзахисту КП, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом узагальнений звіт щодо актуальних кіберзагроз	оперативну інформацію щодо стану кібербезпеки	Методику управління кіберризиками національного масштабу; результати оцінки рівня кіберризиків загалом для секторів/ підсекторів економіки; аналітична інформація щодо актуальних та потенційних кіберризиків; реальна координація діяльності основних суб'єктів забезпечення кібербезпеки
Генеральний Штаб Збройних Сил України (Командування військ зв'язку та кібербезпеки)	Директиви щодо участі Держспецзв'язку в кіберопераціях ЗСУ; спроможності та їх урахування у Плані протидії кіберзагрозам та кібератакам під час оборони держави; пропозиції до Плану кібероборони України;	накази Голови Держспецзв'язку про участь у кіберопераціях, планувальні документи	інформацію про виявлені можливості противника при проведенні кібероперацій; інформацію про сили кібероборони та їх завдання і функції, передбачені плануванням
Служба безпеки України	Інформацію : про інциденти кібербезпеки; підготовку / перепідготовку фахівців у сфері кібербезпеки та кіберзахисту; проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;	інформацію про інциденти кібербезпеки	інформацію про джерела кібератак, їх технічні можливості, ступінь компетенції та фінансові можливості; інформацію про можливі сценарії кібератак; інформацію про характерні інструменти кібератак; інформацію про об'єкти, на які можуть здійснюватися

Назва органу	Держспецзв'язку		
	надає	отримує	потребує
			кібератаки
Розвідувальні органи	оцінку розвідувальних матеріалів з питань кіберзахисту сприяє вирішенню питань кіберзахисту та протидії кіберзагрозам;	розвідувальні матеріали з питань кіберзахисту за окремими спільним рішеннями (доступ обмежено)	розвідувальні матеріали з питань кіберзахисту за окремими спільним рішеннями (доступ обмежено)
Національна поліція України	інформацію про інциденти кібербезпеки; забезпечує підготовку / перепідготовку фахівців у сфері кібербезпеки та кіберзахисту; організовує проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі	інформацію про інциденти кібербезпеки	інформацію про кіберзлочинців, кіберугруповання, а також методи та засоби, які вони використовують
Національний банк України	інформацію про інциденти кібербезпеки	інформацію про інциденти кібербезпеки	депозитарій шкідливого коду, отриманого в результаті діяльності центр кіберзахисту Національного банку України
МЗС	пропозиції щодо розвитку міжнародного співробітництва у сфері кіберзахисту; позиційні матеріали для проведення переговорів на вищому рівні та рівні профільних державних органів та їх підрозділів	підтримку у проведенні кіберконсультаций, кібердіалогів та кібернавчань з іншими країнами	інформацію про участь України (її уповноважених органів) у розробці правил і норм міжнародних відносин та відповідальної поведінки у кіберпросторі; позицію України у скорегованій з союзниками та зовнішніми партнерами санкційній політиці; інформацію щодо створення або участі в існуючих міжнародних кібербезпекових структурах; консультування фахівців щодо особливостей формування державної політики в сфері кіберзахисту

Назва органу	Держспецзв'язку		
	надає	отримує	потребує
Органи державної влади (уповноважені органи) - суб'єкти забезпечення кібербезпеки	<p>рекомендації щодо кіберзахисту в інформаційно-телекомунікаційних системах координує діяльність щодо кіберзахисту;</p> <p>інформує про кіберзагрози та відповідні методи захисту від них;</p> <p>формує і веде перелік ОКІ та реєстр ОКІ;</p> <p>координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем ОКІ на вразливість;</p> <p>забезпечує впровадження аудиту інформаційної безпеки на ОКІ;</p> <p>забезпечує обмін інформацією про інциденти кібербезпеки;</p> <p>здійснює державний контроль;</p> <p>забезпечує підготовку / перепідготовку фахівців у сфері кібербезпеки та кіберзахисту;</p> <p>здійснює заходи з розвитку мережі CERT;</p> <p>організовує проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;</p> <p>надає послуги із захисту інформації та кіберзахисту;</p> <p>встановлює вимоги інформаційної безпеки об'єктів критичної інформаційної інфраструктури;</p> <p>встановлює вимоги (правила, настанови) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;</p> <p>надає власникам об'єктів кіберзахисту практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;</p> <p>організовує та проводить практичні семінари з питань</p>	<p>відомості про об'єкти критичної інфраструктури та об'єктів критичної інформаційної інфраструктури;</p> <p>інформацію щодо створення мереж команд реагування на комп'ютерні надзвичайні події;</p> <p>інформацію про ініціативи стосовно організації співпраці з міжнародними організаціями та відповідними органами інших держав;</p> <p>інформацію та бере участь у проведенні навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;</p> <p>інформацію щодо участі у практичних семінарах з питань кіберзахисту;</p> <p>проекти державних стандартів вищої освіти за рівнями підготовки «бакалавр», «магістр» та «PhD» зі спеціальності 125 «Кібербезпека»;</p> <p>інформацію про підключення до НТМ;</p> <p>інформацію про участь у заходах з упровадження ОТМ національної системи кібербезпеки;</p>	<p>Інформацію про ідентифіковані власні ОКІ та вжиті заходи з кіберзахисту</p>

Науковий вісник: Державне управління № 3(9) 2021

Назва органу	Держспецзв'язку		
	надає	отримує	потребує
	<p>кіберзахисту для суб'єктів національної системи кібербезпеки;</p> <p>розміщує на своєму офіційному вебсайті рекомендації щодо протидії сучасним видам кібератак та кіберзагроз;</p> <p>взаємодіє з українськими командами реагування на комп'ютерні надзвичайні події;</p> <p>сприяє у вирішенні питань кіберзахисту та протидії кіберзагрозам;</p> <p>організовує заходи з упровадження організаційно-технічної моделі національної системи кібербезпеки;</p> <p>створює та забезпечує функціонування НТМ;</p> <p>надає пропозиції щодо міжнародного співробітництва, у тому числі з НАТО;</p> <p>бере участь у розробці та погоджує проекти державних стандартів вищої освіти за рівнями підготовки «бакалавр», «магістр» та «PhD» зі спеціальності 125 «Кібербезпека»;</p> <p>проводить кібернавчання та тренінги</p>		
Власники/розпорядники ОКІ	<p>рекомендацій щодо кіберзахисту ОКІ;</p> <p>інформування про кіберзагрози та відповідні методи захисту від них;</p> <p>вимоги з кібер- та інформаційної безпеки ОКІІ;</p> <p>інформацію щодо впровадження аудиту інформаційної безпеки на ОКІ;</p> <p>інформацію про інциденти кібербезпеки;</p> <p>забезпечує підготовку / перепідготовку фахівців у сфері кібербезпеки та кіберзахисту;</p> <p>інформацію щодо проведення кібернавчань;</p> <p>практичну допомогу з питань запобігання, виявлення та усунення наслідків</p>	інформацію про попередню самооцінку зрілості щодо кіберзахисту ОКІІ	інформацію про впроваджені заходи кіберзахисту відповідно до категорії критичності об'єкта критичної інфраструктури; <p>інформацію про технічне обладнання та програмне забезпечення, що використовується під час надання основних послуг</p>

Назва органу	Держспецзв'язку		
	надас	отримус	потребус
	кіберінцидентів та кібератак на ОКИ; практичні семінари з питань кіберзахисту для власників об'єктів кіберзахисту; рекомендації щодо протидії сучасним видам кібератак та кіберзагроз; інформацію для підприємств, установ та організацій незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; інформація щодо вирішення питань кіберзахисту та протидії кіберзагрозам		
Громадські організації	можливість участі у формуванні та реалізації публічної політики у сфері кіберзахисту; можливість проведення експертної оцінки законопроектів з питань кіберзахисту; можливість участі у популяризації публічної політики кіберзахисту та заходів з її реалізації; можливість періодично проходити навчання на кіберполігоні; можливість брати участь у роботі CERT-UA та інших командах реагування на інциденти комп'ютерної безпеки шляхом надсилання повідомлень щодо виявлених інцидентів інформаційної безпеки;	експертні оцінки фактичного стану кіберзахисту, ефективності реалізації публічної політики кіберзахисту, пропозиції та зауваження щодо законопроектів	результати власноруч проведеної оцінки захищеності ДІР в кіберпросторі та рівня захищеності ОКІП насамперед державних органів; брати участь у кіберрозслідуваннях інцидентів та кібератак; сприяння у підвищенні рівня кіберзахисту; поширення кібергігієни в навчальних закладах, державному секторі, підготовка настанов та рекомендацій; упровадження курсів підготовки / підвищення кваліфікації державних службовців тощо

Розроблено авторами

Висновки та напрями подальших досліджень. На основі аналізу стану інституціонального забезпечення системи кіберзахисту в Україні виявлено недостатню ефективність запроваджених Урядом рішень щодо ідентифікації ОКІІ та ІТС, які критично впливають на функціонування державних органів.

На підставі визначення місця і ролі Держспецзв'язку в загальній системі забезпечення кібербезпеки України виявлено необхідність розмежування сфер відповідальності у практичній діяльності НКЦК при РНБОУ, Держспецзв'язку та СБУ.

Визначено конкретні недоліки чинного законодавства щодо визначення інституційної структури підсистеми кіберзахисту, розмежування повноважень її суб'єктів.

Запропоновано інституційну модель взаємодії суб'єктів забезпечення кіберзахисту, у формуванні якої враховано особливості, спроможності та потреби суб'єктів кібербезпеки, що сприяє уникненню дублювання їх функцій та завдань і зменшенню рівня конкуренції між собою за вплив на сферу забезпечення кібербезпеки. Це також надасть можливість більш раціонально витратити фінансові ресурси державного бюджету щодо забезпечення захисту прав та свобод громадян у кіберпросторі, спрямовуючи їх тільки на визначені у Законі повноваження основних суб'єктів національної системи забезпечення кібербезпеки.

Напрямом подальших досліджень є обґрунтування конкретних шляхів удосконалення чинного законодавства та організаційної структури національної системи забезпечення кіберзахисту.

Список використаних джерел

1. Шемчук В. В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки. Серія : Юридичні науки. Кримінальне право та кримінологія ; кримінально-виконавче право*. 2018. Т. 29(68) № 2. С. 125–129.
2. Дешко Л. М., Бонарева К. Д. Кібербезпека в Україні і Національна стратегія та міжнародне співробітництво. *Порівняльно-аналітичне право*. 2018. № 2. URL : http://pap.in.ua/2_2018/112.pdf (дата звернення : 15.05.2021).
3. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі : формування механізму міжнародної інформаційної

- безпеки. International relations, part «Political science». No 18–19(2). URL : <https://cutt.ly/GQCBYfV> (дата звернення : 16.05.2021).
4. Доронін І. М. Організація звітування суб'єктів кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : <https://cutt.ly/5QCBPIq> (дата звернення : 16.05.2021).
 5. Забара І. М. Кібернетична безпека держави в умовах розвитку штучного інтелекту : до питання визначення напрямків міжнародно-правового регулювання. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення : 16.05.2021).
 6. Кравець В. М. Порівняльний аналіз міжнародних індексів кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення : 16.05.2021).
 7. Нікітіна Є. О., Тимофеев Д. С. Інструменти проактивного аналізу кіберзагроз. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення : 16.05.2021).
 8. Вдовенко С. Г., Даник Ю. Г., Пермяков О. Ю. Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. *Modern Information Technologies in the Sphere of Security and Defence*. 2019. № 3(36) URL : <http://sit.nuou.org.ua/article/view/202623/202526> (дата звернення : 17.05.2021).
 9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163. URL : <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення : 16.05.2021).
 10. Мохор В. В., Богданов А. М., Килевої А. С. Наставлення по кибербезопасности. Киев : Три-К, 2013. 63 с.
 11. Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси : постанова Кабінету Міністрів України від 23.12.2020 р. № 1363. URL : <https://zakon.rada.gov.ua/laws/show/1363-2020-%D0%BF#Text> (дата звернення : 17.05.2021).
 12. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. URL : <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text> (дата звернення : 17.05.2021).
 13. Деякі питання функціонування Національної телекомунікаційної мережі : постанова Кабінету Міністрів України від 16.12.2020 р. № 135. URL : <https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text> (дата звернення : 17.05.2021).
 14. Потій О. В., Семенченко А. І., Дубов Д. В., Бакалинський О. О., Мьялковський Д. В. Концептуальні засади впровадження організаційно-

технічної моделі кіберзахисту України. *Захист інформації, Північна Америка*, 23 квіт. 2021 р. URL : <http://jrn1.nau.edu.ua/index.php/ZI/article/view/15434> (дата звернення : 16.05.2021).

References

1. Shemchuk, V.V. (2018). Osnovni naprjamky mizhnarodnogho spivrobitnyctva u sferi kiberbezpeky [The main directions of international cooperation in the field of cybersecurity]. *Vcheni zapysky. – Serija: jurydychni nauky. – Kryminaljne pravo ta kryminologhija; kryminaljno-vykonavche pravo – Scientific notes. Series: legal sciences. Criminal law and criminology; criminal executive law*, 2, 125-129 [in Ukrainian].
2. Deshko, L.M., Bonarjeva, K.D. (2018). Kiberbezpeka v Ukrajinі: Nacionaljna strateghija ta mizhnarodne spivrobitnyctvo [Cybersecurity in Ukraine: National Strategy and International Cooperation]. *Porivnjajlno-analitychne pravo – Comparative and analytical law*, 2. Retrieved from http://pap.in.ua/2_2018/112.pdf [in Ukrainian].
3. Piskorsjka, Gh.A., Jakovenko, N.L. (2018) Suchasni vyklyky i zagrozy v kiberprostorі: formuvannja mekhanizmu mizhnarodnoji informacijnоji bezpeky [Modern challenges and threats in cyberspace: the formation of a mechanism for international information security]. *International relations, part "Political sciences"*, 18-19 (2). Retrieved from <https://cutt.ly/GQCBYfV> [in Ukrainian].
4. Doronin, I.M. (2019) Orghanizacija zvituvannja sub'ektiv kiberbezpeky [Organization of cybersecurity reporting] Abstracts of Papers X Scientific and Practical Conference: *Aktualjni problemy upravlinnja informacijnoju bezpekoju derzhavy - Actual problems of information security management of the state*. Retrieved from <https://cutt.ly/5QCBPIq> [in Ukrainian].
5. Zabara, I.M. (2019) Kibernetychna bezpeka derzhavy v umovakh rozvytku shtuchnogho intelektu: do pytannja vyznachennja naprjamkiv mizhnarodno-pravovogho rehuljuvannja [Cyber security of the state in the conditions of development of artificial intelligence: to a question of definition of directions of the international legal regulation]. Abstracts of Papers X Scientific and Practical Conference: *Aktualjni problemy upravlinnja informacijnoju bezpekoju derzhavy - Actual problems of information security management of the state*. Retrieved from http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf [in Ukrainian].
6. Kravecj V.M., (2019) Porivnjajlnyj analiz mizhnarodnykh indeksiv kiberbezpeky [Comparative analysis of international cybersecurity indices] Abstracts of Papers X Scientific and Practical Conference: *Aktualjni problemy upravlinnja informacijnoju bezpekoju derzhavy - Actual problems of information security management of the state*. Retrieved from http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf [in Ukrainian].
7. Nikitina, Je.O., Tymofjejev, D.S. (2019) Instrumenty proaktyvnogho analizu kiberzagroz [Proactive cyber threat analysis tools] Abstracts of Papers X Scientific and Practical Conference: *Aktualjni problemy upravlinnja informacijnoju bezpekoju derzhavy - Actual problems of information security management of the state*. Retrieved from http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf [in Ukrainian].

8. Vdovenko, S.Gh., Danyk, Ju.Gh., Permjakov, O.Ju. (2019) Dosvid rozvytku system kiberbezpeky ta kiberoborony providnykh krajin svitu [Experience in the development of cybersecurity and cyber defense systems of the world's leading countries]. *Modern Information Technologies in the Sphere of Security and Defence*, 3(36). Retrieved from <http://sit.nuou.org.ua/article/view/202623/202526> [in Ukrainian].
9. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrainy: Zakon Ukrainy pryinyatiy 5 Oct. 2017 roku № 2163 [On the basic principles of cybersecurity in Ukraine: the Law of Ukraine] from 5 Oct. 2017 № 2163 Bulletin of Verkhovna Rada of Ukraine. Kyiv: Parlam. vyd-vo Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19>. [in Ukrainian].
10. Mokhor, V.V., Boghdanov, A.M., Kylevoj, A.S. (2013) Nastavlenja po kyberbezopasnosti [Cybersecurity guidelines]. Kyev: Try-K. [in Ukrainian].
11. Pro realizaciju eksperymentaljnogho proektu shhodo zaprovadzhennja kompleksu orhанизacijno-tekhnichnykh zakhodiv z vyjavlennja vrazlyvostej i nedolikov u nalashtuvanni informacijnykh, telekomunikacijnykh ta informacijno-telekomunikacijnykh system, v jakykh obroblyajutjsja derzhavni informacijni resursy: postanova Kabinetu Ministriv Ukrainy vid 23 ghrudnja 2020 r. № 1363 [On the implementation of a pilot project to implement a set of organizational and technical measures to identify vulnerabilities and shortcomings in the configuration of information, telecommunications and information and telecommunications systems in which state information resources are processed: Resolution of the Cabinet of Ministers of Ukraine from December 23, 2020 № 1363]. <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/1363-2020-%D0%BF#Text> [in Ukrainian].
12. Dejaki pytannja zabezpechennja funkcionuvannja systemy vyjavlennja vrazlyvostej i reaghuvannja na kiberincydeny ta kiberatomy: postanova Kabinetu Ministriv Ukrainy vid 23 ghrudnja 2020 r. № 1295 [Some issues of ensuring the functioning of the system of vulnerability detection and response to cyber incidents and cyberattacks: Resolution of the Cabinet of Ministers of Ukraine from December 23, 2020 № 1295]. <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text> [in Ukrainian].
13. Dejaki pytannja funkcionuvannja Nacionaljnoji telekomunikacijnoji merezhi: postanova Kabinetu Ministriv Ukrainy vid 16 ghrudnja 2020 r. № 1358 [Some issues of functioning of the National Telecommunication Network: Resolution of the Cabinet of Ministers of Ukraine from December 16, 2020 № 1358]. <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text> [in Ukrainian].
14. Potii, O.V., Semenchenko, A.I., Dubov, D.V., Bakalynskiy, O.O., Myalkovsky, D.V. (2021) Konceptualjni zasady vprovadzhennja orhанизacijno-tekhnichnoji modeli kiberzakhystu Ukrainy [Conceptual principles of implementation of organizational and technical model of cyber defense of Ukraine]. *Zakhyst informaciji, Pivnichna Ameryka - Information security, North America*, Retrieved from <http://jrnل.nau.edu.ua/index.php/ZI/article/view/15434>. [in Ukrainian].

**PUBLIC ADMINISTRATION OF INSTITUTIONAL DEVELOPMENT IN
THE FIELD OF CYBER PROTECTION**

Potii Oleksandr, Semenchenko Andrii, Bakalynskyi Oleksandr, Myalkovsky Danylo

Abstract. The increasing complexity, intensity and breadth of cyber threats and their means and tools, the militarization of cyberspace and its transformation into a battlefield, etc. make cyber-defence an urgent issue. This requires that these factors be taken into account in the formulation and implementation of public policy and public administration in the area of national security, the development of the security and defense sectors, of which the national cybersecurity system is an important component. The article analyzes the mechanism of institutional development of the main actors of the national cyber defense system in Ukraine, primarily the State Service for Special Communications and Information Protection of Ukraine, the formation of scientifically sound approaches and proposals for its improvement taking into account transformational changes in Ukraine's security and defense sector. The role and place of the cybersecurity subsystem in the general cybersecurity system of Ukraine, as well as its main element of the State Service for Special Communications and Information Protection of Ukraine, are determined. A scientifically based risk-oriented approach to the formation of a model of interaction of cybersecurity actors is proposed, which takes into account the characteristics and capabilities of cybersecurity actors and avoids duplication of their functions and tasks, and reduces competition for influence on the sphere. The main problems of organizational and legal support for the development of the cyber defense system in Ukraine and ways to solve them are described. A model of interaction between cybersecurity actors has been developed, which is based on both the current legislation and promising areas for its improvement. Specific directions of improvement of the existing legislation for the purpose of elimination of duplicating functions and tasks of subjects of maintenance of cybersecurity are substantiated.

Keywords: public administration, institutional development, cyber defense, cybersecurity, national cybersecurity system, security and defense sector.