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

Семенченко Андрій Іванович,
д.держ.упр., проф.,
директор Інституту вищих керівних кадрів НАДУ при Президентові України,
м. Київ
ORCID 0000-0001-6482-3872

УДК 004.056.5:343.326 (045) **doi: 10.34213/tp.20.03.05**

РОЗВИТОК ІНСТИТУЦІЙНИХ СПРОМОЖНОСТЕЙ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ УКРАЇНИ

Визначено поняття, сутність, структуру інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та системи кіберзахисту України, проведено аналіз та оцінювання їхнього стану, обґрунтовано пріоритетні напрями їхнього вдосконалення, спрямовані на підвищення ефективності та результативності публічної політики у сфері кібербезпеки та кіберзахисту України.

Уточнено сутність поняття "інституційна спроможність суб'єктів забезпечення системи кібербезпеки та кіберзахисту". Окреслено основні складники інституційної спроможності суб'єктів забезпечення системи кібербезпеки України та кіберзахисту: правовий, організаційний, кадровий та фінансовий. Організаційний складник інституційної спроможності суб'єктів забезпечення системи кібербезпеки України та кіберзахисту подано у вигляді трирівневої ієрархічної моделі (стратегічний, оперативний і тактичний рівні).

Обґрунтовано пріоритетні напрями удосконалення правового механізму інституційних спроможностей для ієрархічної моделі правового забезпечення: на законодавчому, підзаконному та нормативно-технічному (нормативно-правовому) рівнях.

Визначено проблеми кадрового складника інституційних спроможностей та сформульовано пропозиції щодо вирішення їх шляхом розроблення та упровадження формалізованих вимог до професійних компетенцій для працівників, зокрема через доопрацювання державного класифікатора професій.

На підставі проведеного аналізу запропоновано удосконалити діяльність спеціально уповноваженого центрального органу виконавчої влади з питань спеціального зв'язку та захисту інформації з уточненням його функціоналу як національного компетентного органу з безпеки інформації та інформаційно-комунікаційних систем, визначеному Директивою NIS. Визначено пріоритетність завдання розроблення нормативно-технічних та технічних документів із забезпеченням інтероперабельності їхніх вимог із міжнародними стандартами та практиками.

Ключові слова: кібербезпека, кіберзахист, система кібербезпеки, ієрархічна модель, інституційні спроможності.

Постановка проблеми. Одним із пріоритетних напрямів розвитку сфери кібербезпеки та кіберзахисту є ефективне та результативне формування та реалізація державної інституційної політики. Незважаючи на те, що в Україні в цілому створено правові та організаційні передумови в цій сфері, її якість та ефективність потребують удосконалення. Головною причиною такого становища є низька інституційна спроможність забезпечення системи кібербезпеки України та системи кіберзахисту як її складника, що сьогодні характеризується низкою недоліків законодавчого, організаційного, ресурсного, інформаційно-аналітичного та інших видів забезпечення, у т. ч. неповнотою та нечіткістю категорійно-понятійного апарату, зокрема відсутністю

поняття інституційних спроможностей суб'єктів національної системи кібербезпеки та кіберзахисту, а також відсутністю в цілому концептуальних засад розвитку цієї сфери, що в сукупності актуалізує тематику дослідження.

В Україні актуальність цієї проблеми також зумовлена необхідністю розроблення нових редакцій Стратегії національної безпеки України [1] та одного з її складників – Стратегії кібербезпеки України, незавершеністю проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, зумовлена рівнем та масштабом кіберзагроз, у т. ч. з боку Російської Федерації, динамікою цифрових трансформацій економіки та суспільства, недостатнім рівнем теоретико-методологічних розробок у цій сфері.

Аналіз досліджень. Нормативно-правові аспекти систем кібербезпеки розглядалося у працях Дж. Ліпмана, В. Мазурова, Р. Олдрича, Є. Старостиної. Вітчизняними науковцями здійснювались дослідження різних аспектів забезпечення кібербезпеки України, у т. ч.: І. Дороніним – щодо державного органу з формування єдиної політики у сфері кібербезпеки на державний орган, В. Кравцем – із питань виміру оцінки кібербезпеки на різних рівнях через глобальний, національний та галузевий індекс кібербезпеки, Р. Лук'янчуком – щодо міжнародного співробітництва за участі НАТО, Д. Дубовим – із проблем терміносистем та аналізу стану утворення національної системи кібербезпеки та стратегічних аспектів кібербезпеки, В. Петровим – щодо формування національної системи кібербезпеки України та співробітництва України з НАТО.

Мета цієї **статті** полягає у визначенні поняття, сутності, структури та інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та системи кіберзахисту України, в аналізі та оцінюванні їхнього стану, обґрунтуванні пріоритетних напрямів удосконалення, спрямованих на підвищення ефективності та результативності публічної політики у сфері кібербезпеки та кіберзахисту України.

Основна частина. Динамічний розвиток інформаційно-комунікаційних технологій, масштабне упровадження їх в усі сфери суспільного життя громадян, суспільства та держави сприяють підвищенню конкурентоспроможності економіки, якості та оперативності надання суспільних послуг, рівня демократизації суспільства та держави, однак ці ж самі процеси є одночасно і джерелом небезпек, викликів та загроз громадянам, суспільству, державі та бізнесу в кіберпросторі.

З метою зменшення негативного впливу деструктивних факторів на діяльність у кіберпросторі у світі на міжнародному, регіональному, національному та місцевому рівнях розробляється відповідна політика забезпечення кібербезпеки, одним із пріоритетних напрямів якої є розвиток інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту.

У формалізованому вигляді така політика в директивних, концептуальних, стратегічних, програмних, планових та інших документах включає, зокрема, процедури стратегічного моніторингу, аналізу, оцінювання та прогнозування.

В Україні актуальність цієї проблеми зумовлена необхідністю розроблення нових редакцій Стратегії національної безпеки України [Там само] та Стратегії кібербезпеки України [2], незавершеністю проведення огляду

стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, рівнем та масштабом кіберзагроз, у т. ч. з боку РФ, динамікою цифрових трансформацій економіки та суспільства, недостатнім рівнем теоретико-методологічних розробок у цій сфері.

Незважаючи на те, що в Україні в цілому створено правові та організаційні передумови для розвитку цієї сфери, вони потребують суттєвого удосконалення, насамперед через низьку інституційну спроможність суб'єктів забезпечення системи кібербезпеки та кіберзахисту України (ІССЗККУ), яка сьогодні характеризується:

– неповнотою, несистемністю та відсутністю кодифікації, суперечливістю, декларативністю, неактуальністю, нечіткістю та неконкретністю законодавчої та нормативно-правової бази, термінологічною невизначеністю, недостатнім рівнем її узгодженості з міжнародним законодавством, насамперед з європейським, розбіжністю між положеннями правових актів та рівнем їхнього виконання;

– несформованістю національної системи кібербезпеки та кіберзахисту, перманентними та значною мірою науково необґрунтованими її структурними та функціональними змінами, відсутністю чітких взаємозв'язків та взаємодії між її суб'єктами та об'єктами кібербезпеки та кіберзахисту, а також відсутністю національного компетентного органу з безпеки інформації та інформаційно-комунікаційних систем, визначеного Директивою NIS;

– браком кадрових ресурсів суб'єктів забезпечення системи кібербезпеки України та кіберзахисту, плинністю їх, а також недостатнім рівнем професійних компетенцій їхніх працівників;

– відсутністю необхідних фінансових ресурсів для розвитку ІССЗККУ;

– низьким рівнем інформаційно-аналітичного та організаційно-технічного забезпечення;

– швидкою зміною формальних правил;

– відсутністю або слабкістю системи санкцій та низькою якістю контролю виконання їх;

– низьким рівнем правової культури українського суспільства.

Щодо термінологічної невизначеності: на сьогодні в національному законодавстві відсутні терміни "інституалізація", "інституційна та інституалізаційна спроможності суб'єктів забезпечення системи кібербезпеки та кіберзахисту".

У національному законодавстві визначено сукупність термінів. У наказі Міністерства економіки та з питань європейської інтеграції України [3] лише для однієї специфічної сфери надається достатньо вузьке визначення "інституційного забезпечення" та його мети, а саме:

– інституційне забезпечення – утворення нових або реорганізація (удосконалення) існуючих інституцій (структур), а також дії щодо кадрової підготовки з метою організаційного забезпечення діяльності цих інституцій та процесу євроінтеграції в цілому;

– інституційне забезпечення процесу євроінтеграції має на меті утворення нових або реорганізацію (удосконалення) існуючих інституцій (структур), а також проведення роботи щодо кадрового забезпечення діяльності цих інституцій та процесу євроінтеграції в цілому, у т. ч. стажування спеціалістів за кордоном, вивчення ними мов країн – членів ЄС.

У законодавчих актах, що визначають організацію та проведення оглядів сектору безпеки та оборони згідно із Законом України "Про національну безпеку України" [4] та Указом Президента "Про рішення Ради національної безпеки і оборони України від 16 травня 2019 р. "Про організацію планування в секторі безпеки і оборони України" [5], надано такі визначення терміна "спроможність":

спроможність (оперативна, бойова, спеціальна) – це здатність органів військового управління, з'єднань, військових частин, військових навчальних закладів, установ та організацій Збройних Сил або сукупності сил і засобів сил оборони виконувати певні завдання (забезпечувати реалізацію визначених військових цілей) за певних умов, ресурсного забезпечення та відповідно до встановлених стандартів [6];

спроможність суб'єктів боротьби з тероризмом – здатність таких суб'єктів виконувати завдання із запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків відповідно до встановлених рівнів терористичних загроз [7];

спроможність оборонно-промислового комплексу – здатність підприємств, установ та організацій промисловості та науки виконувати завдання із задоволення потреб сектору безпеки і оборони в озброєнні, боєприпасах, військовій та спеціальній техніці [8].

Термінологічне визначення інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту України відсутнє в чинному законодавстві, тому потрібні окреме формулювання та формалізація шляхом як адаптації вищевказаних термінів до особливостей сфери кібербезпеки та кіберзахисту, так і узагальнення наукових загальноприйнятих підходів до визначення цих термінів.

Зокрема, науковцями та фахівцями термін "інституційна спроможність" у широкому розумінні вживається як спроможність державної структури ефективно виконувати власні найголовніші функції та контролювати виконання їх [9].

До системи інституалізаційних спроможностей влади при цьому часто включають такі складники, як стратегія, організаційна структура, процеси і шаблони, вміння та навички персоналу, а "спроможність" тлумачиться як сукупність організаційних та технічних можливостей, відносин та цінностей, що дозволяють країнам, організаціям, групам осіб та окремим громадянам на будь-якому суспільно-політичному рівні виконувати функції та досягати визначених цілей розвитку протягом певного часу [10].

Спроможність можна також визначити з огляду на загальнодержавний, секторальний, інституційний, інституціональний (організаційний), груповий, індивідуальний рівні [11]. "Інституційна (інституціональна) спроможність" є менш уживаним терміном, ніж "організаційна спроможність". Організаційна спроможність розглядається як здатність організації формувати і використовувати внутрішні можливості для виконання місії та подальшого розвитку. У ній виокремлюють такі складники, як система управління; мотиваційний механізм; організаційна культура; маркетингова діяльність; ресурсна база [12]. Підсумком інституціоналізації є створення відповідно до норм і правил чіткої статусно-рольової структури, соціально схваленої більшістю учасників цього процесу.

З урахуванням специфіки сфери дослідження та узагальнення результатів вищевказаних підходів під інституційною спроможністю суб'єктів забезпечення системи кібербезпеки та кіберзахисту пропонується розуміти: *здатність таких суб'єктів ефективно виконувати власні найголовніші завдання та функції у сфері кібербезпеки та кіберзахисту, контролювати виконання їх за певних умов ресурсного, організаційного-правового, інформаційного та науково-методичного забезпечення відповідно до встановлених стандартів.*

Ієрархія ІССЗККУ (її організаційний складник) у Законі України "Про основні засади забезпечення кібербезпеки України" (далі – Закон) [13] порівняно зі Стратегією кібербезпеки України визначено більш системно, детально і конкретно. Наприклад, у Стратегії кібербезпеки України з*агальнодержавну координувальну та контрольну управлінську ланку (стратегічний рівень)* взагалі не визначено, у той час як згідно зі ст. 5 та 15 цього Закону вона включає Верховну Раду України, Президента України через очолювану ним Раду національної безпеки і оборони України, Національний координаційний центр кібербезпеки України як робочий орган Ради національної безпеки і оборони України, Кабінет Міністрів України (КМУ) та визначає їхні агреговані завдання, але обмежуючи при цьому всупереч Конституції України роль парламенту виключно парламентським контролем за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки, захисту персональних даних та доступу до публічної інформації, розглядом звітів про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки.

Тому ця організаційна ланка ІССЗККУ має включати парламент з урахуванням його повноважень згідно зі ст. 85 Конституції України із завданнями насамперед щодо: визначання ним засад внутрішньої і зовнішньої політики, реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору; затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля та в структурі якої комітети з питань цифрових трансформацій та національної безпеки, оборони та розвідки безпосередньо розглядають законопроєкти з проблем кібербезпеки та кіберзахисту. Має бути також посилено координувальну та контрольну роль Національного координаційного центру кібербезпеки України.

Наступною ланкою ІССЗККУ (*оперативний рівень)* Закон визначає коло *суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки,* але без встановлення між ними чітких зв'язків та механізмів взаємодії: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні й контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України (ЗСУ), інші військові формування, утворені відповідно до закону; Національний банк України (НБУ); підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Серед сукупності цих суб'єктів, яку неможливо повною мірою ідентифікувати як систему, оскільки, насамперед між її елементами, законодавчо не визначено чітких взаємозв'язків та механізмів взаємодії, ст. 8 Закону [13] виокремлює перелік (ядро) *основних суб'єктів національної системи кібербезпеки України*, до яких відносяться Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України (СБУ), Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, НБУ, а також визначає їхні основні завдання.

Тактичний рівень ІССЗККУ представлено: Державним центром кіберзахисту ДССЗЗІ; мережею ситуаційних центрів кібербезпеки СБУ; мережею центрів захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах ЗСУ; урядовою та галузевими (державними та недержавними) командами реагування на комп'ютерні надзвичайні події України; підрозділами кібербезпеки та кіберзахисту (інформаційної безпеки), насамперед основних суб'єктів національної системи кібербезпеки України, об'єктів критичної інфраструктури, а також інших суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Загальний перелік вищевказаних суб'єктів забезпечення системи кібербезпеки України та системи кіберзахисту та повноваження їх у міжнародному контексті не відповідають європейській організаційній структурі системи кібербезпеки та кіберзахисту, не забезпечують якісної інтероперабельність із відповідними підрозділами НАТО та ЄС, а також ефективної реалізації механізмів державно-приватного партнерства та інших механізмів публічного управління в цій сфері.

Наприклад, усупереч європейській Директиві щодо мережевої та інформаційної безпеки (Директиви NIS [14]), якої, правда,Україна поки що не імплементувала, не створено єдиного компетентного органу у сфері безпеки мереж та інформаційних систем (Спеціального уповноваженого органу з безпеки інформації та інформаційно-комунікаційних систем), який здійснює координацію та співробітництво національних суб'єктів у цій сфері, узагальнення практик, надання методичної допомоги, консультацій та рекомендацій з організації діяльності щодо безпеки інформації та ІКС, а також транскордонне співробітництво з державами – членами ЄС та НАТО. Держспецзв'язку та Національний координаційний центр із кібербезпеки за своїм функціоналом не повною мірою відповідають вищевказаному призначенню.

На сьогодні відсутній перелік об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, не встановлено правових норм щодо створення команд реагування на комп'ютерні надзвичайні події у відповідних галузях економіки та сферах суспільного життя, не визначено їхніх завдань (Computer Emergency Response Team, CERT), а також не визначено місце команд реагування на інциденти комп'ютерної безпеки (Computer Security Incident Response teams, CSIRTs'), їхню взаємодію з іншими суб'єктами кібербезпеки та кіберзахисту. Принципова відмінність цих команд полягає в організації своєї діяльності: якщо CERT функціонує на постійній основі з відповідним штатом працівників, то CSIRT – це команда, яка об'єднує фахівців різних організацій та підприємств для вирішення конкретного завдання реагування на кіберінциденти. Крім того, не визначено вимог до таких команд, критеріїв та суб'єктів оцінювання виконання ними цих вимог, періодичності такого оцінювання тощо.

На сьогодні в Законі чітко визначено лише Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA та її повноваження. У ст. 10 "Державно-приватна взаємодія у сфері кібербезпеки" Закону [13] зазначено, що одним зі шляхів державно-приватної взаємодії у сфері кібербезпеки є здійснення партнерства та координації команд реагування на комп'ютерні надзвичайні події. Хоча саме команди, сформовані за галузевим або за іншим принципом, мають відігравати основну роль у реагуванні на кіберінциденти.

Також законодавчо не визначено розроблення такими командами рекомендацій, правовий статус таких рекомендацій, результатів їхньої роботи та обов'язковість звітування про виявлені недоліки в кіберзахисті, зокрема, об'єктів критичної інформаційної інфраструктури, а також обов'язкове опрацювання їхніми власниками виявлених недоліків у захисті та рекомендацій команд. Крім того, Законом не визначено, саме яку команду з цих двох типів необхідно створювати, враховуючи, що команду CERT-UA було утворено ще до його прийняття, вона пройшла акредитацію у Форумі команд із надзвичайних подій та безпеки (Forum of Incident Response and Security Teams, FIRST) та Службі довірених представників (Trusted Introducer Service, TI).

Вищевказане є однією з причин незавершеності формування та об'єднання в мережі галузевих (державних та недержавних) команд реагування на комп'ютерні надзвичайні події України. Зокрема, окрім CERT-UA, після прийняття Закону [13] було створено галузеві команди реагування лише в окремих галузях:

– Державне підприємство "Галузевий центр цифровізації та кібербезпеки" Міністерства інфраструктури України;

– Команда реагування на кіберінциденти в банківській системі України Центру кіберзахисту НБУ (csirt.bank.gov.ua) та Центр кібербезпеки Кредобанку (https://www.trusted-introducer.org/directory/teams/cert-kredobank.html).

У стадії формування перебуває мережа підрозділів кібербезпеки та кіберзахисту суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, між ними не забезпечено чітких вертикальних та горизонтальних зв'язків.

Іншою організаційною проблемою є відсутність конкретного переліку суб'єктів кібербезпеки, які входять до кожного з її складників. Закон [13] визначив складники сфери кібербезпеки та сутність їх, відповідальні за них державні органи з числа основних суб'єктів національної системи кібербезпеки України та їхні агреговані завдання: кіберзахист – відповідальний – Держспецзв'язку; кібероборона – відповідальні – Міноборони та Генеральний штаб ЗСУ; протидія кіберзлочинності – сукупності кіберзлочинів – Національна поліція України; кіберрозвідка – розвідувальні органи; протидія кібертероризму та кібершпигунству – СБУ.

Але при цьому не визначено суб'єкти кібербезпеки, які входять до кожного із зазначених складників, у т. ч. до такого, як кіберзахист. Хоча організаційну структуру суб'єктів забезпечення кіберзахисту законодавство чітко не визначило, її модель також повинна мати ієрархічну структуру і включати ті ж самі суб'єкти забезпечення кібербезпеки України, що відносяться до її стратегічної управлінської ланки.

Оперативна й тактична ланки організаційної структури державного складника системи кіберзахисту, виходячи з Закону, включають: Державну службу спеціального зв'язку та захисту інформації України, підпорядковані їй Державний центр кіберзахисту та Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA. Цю ланку має бути доповнено галузевими CERT/CSIRT, а також пунктом міжнародного контакту, повноважного отримувати/надсилати офіційні повідомлення про інциденти транскордонного характеру від аналогічних пунктів контакту інших країн.

Правовий складник інституційних спроможностей суб'єктів забезпечення системи кібербезпеки України та системи кіберзахисту також можна подати у вигляді ієрархічної структури, що включає законодавчий, підзаконний та нормативно-правовий (нормативно-технічний) рівні.

Слід зазначити, що в Україні законодавчу базу з питань кібербезпеки та кіберзахисту в цілому створено, і вона перебуває в перманентному динамічному розвитку, намагаючися відповідати сучасним світовим тенденціям, новим викликам та загрозам у цій сфері, потребам та вимогам громадян, суспільства та держави, міжнародним зобов'язанням України щодо надійного захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Особливо значних зрушень вона набула за останні п'ять років і станом на 2020 р. включає низку таких важливих актів національного законодавства, як Конституція України, закони України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про національну безпеку України", "Про основні засади забезпечення кібербезпеки України", "Про електронні довірчі послуги", "Про захист персональних даних" тощо, а також підзаконні акти, затверджені Президентом України та Урядом.

Серед них до законодавчого рівня сьогодні, окрім Конституції України та зазначених вище законів України, також відносяться й міжнародні акти в цій сфері, до яких приєдналась Україна, а саме: Конвенція ООН проти транснаціональної організованої злочинності (2000), Статут Міжнародного союзу електрозв'язку 1992 р., Будапештська конвенція про кіберзлочинність Ради Європи 2005 р. та ін.

В основу національної системи законодавства щодо створення систем захисту інформації було покладено найкращі світові практики – Критерії оцінки захисту комп'ютерної системи (англ. Trusted Computer System Evaluation Criteria, TCSEC, т. зв. "Оранжева книга") – стандарт Міністерства оборони США, що встановлює базові вимоги щодо контролю комп'ютерної безпеки, вбудованої в обчислювальну систему (рисунок).

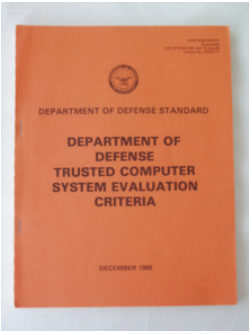

Рисунок. Видання (uk.wikipedia.org)

Саме цей стандарт у подальшому став стандартом ISO/IEC 15 408 "Загальні критерії оцінки безпеки інформаційних *TCSEC* технологій" (Common Criteria for Information Technology Security Evaluation), який було перевидано у 2015 р. та який активно застосовується в світі.

Основними національними чинниками впливу на розвиток законодавства в Україні у сфері забезпечення кібербезпеки та кіберзахисту є: адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного Договору, Закон України "Про електронні довірчі послуги" та набуття змінами до Закону України "Про технічні регламенти та оцінку відповідності" чинності; ведення гібридної війни проти України; сучасні тенденції розвитку інформаційно-комунікаційних технологій, поява нових загроз конфіденційності, цілісності, доступності, авторства та спостережності інформації, безпечної взаємодії систем (мереж) та їхніх елементів тощо.

Тому, незважаючи на значний перелік вищевказаних законодавчих актів, кібербезпекове законодавство *потребує суттєвого вдосконалення*:

має бути розроблено та прийнято низку нових взаємозв'язаних законопроєктів, частину з яких вже надано до парламенту: "Про об'єкти критичної інфраструктури та їх захист", "Про електронні комунікації", "Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про безпеку інформації та інформаційно-комунікаційних систем", "Про хмарні послуги", "Про публічні електронні реєстри" тощо;

потребують суттєвого коригування з метою приведення у відповідність до європейського законодавства Закон [13] та Закон України "Про електронні довірчі послуги".

Підзаконний рівень подано довгостроковими концептуальними та стратегічними документами: Концепцією розвитку сектору безпеки і оборони України (2016), Стратегією національної безпеки України (2015) та Стратегією кібербезпеки України (2016), затвердженими відповідними рішеннями Президента України та Уряду, термін дії яких завершується у 2020 р., а також середньостроковими та короткостроковими плановими та програмними документами, які визначають розвиток сфери кібербезпеки, конкретизують та деталізують вищевказані стратегічні документи, насамперед Плани заходів з реалізації Стратегії кібербезпеки України. Сукупність підзаконних актів має також включати низку рішень Президента та Уряду України, що конкретизують та деталізують рамковий Закон [Там само], зокрема (в інтересах формування та контролю виконання вищевказаних стратегічних документів) Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Згідно зі ст. 25 Закону України "Про національну безпеку України" [4], по-перше, Концепцію розвитку сектору безпеки і оборони, як і Воєнну доктрину та Доктрину інформаційної безпеки, виключено з переліку обов'язкових довгострокових планових документів у сфері національної безпеки і оборони, по-друге, Стратегію [2] включено до системи довгострокових стратегічних документів у цій сфері з визначенням у ст. 31 зазначеного Закону її міста в системі планових документів, структури та загального механізму ініціації, розроблення та схвалення.

Зокрема, Стратегія [Там само] є документом довгострокового планування, у якому визначаються пріоритети національних інтересів України у сфері

кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору тощо.

Структура та зміст Стратегії [2] в цілому відповідає вимогам Закону України "Про національну безпеку України" за виключенням відсутності в ній обґрунтованих кількісно-якісних показників щодо кінцевих результатів її виконання, потреб бюджетного фінансування, строків виконання, прозорих механізмів контролю та коригування, що перетворило її разом із планами заходів з її реалізації на суто декларативний та популістській документ.

У 2019 р. рішеннями Уряду були розроблені та затверджені уніфіковані порядки проведення оглядів сектору безпеки та оборони та його окремих складників, за якими було оцінено стан готовності складників сектору безпеки та оборони у відповідних сферах. Винятком є огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Результати зазначених оглядів є основою для формування сукупності взаємозв'язаних довгострокових документів, визначених Законом України "Про національну безпеку України" [4].

Водночас у вищеназваному Законі запроваджено дискусійний підхід щодо повного відокремлення сфери кібербезпеки від сфери інформаційної безпеки без визначення чітких критеріїв такого відокремлення та їхнього взаємозв'язку. Відсутня чіткість у цьому питанні також і в Законі [13], у якому кібербезпеку обмежено кіберпростором ("середовищем (віртуальним простором), 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"), а також низкою вкрай дискусійних інших обмежень щодо непоширення його дії: на відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші вебресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

По-перше, критерій відокремлення інформаційної безпеки від кібербезпеки через поняття "кіберпростір" із появою засобів масових комунікацій (ЗМК), які передбачають використання кіберпростору, зокрема Інтернету, втрачає актуальність. По-друге, такі складники кібербезпеки, як кіберрозвідка, кібероборона, протидія кібертероризму, кіберзлочинності, кібершпигунству, базуються саме на аналізі та оцінці відповідної інформації в кіберпросторі. Не можна також погодитися з іншими законодавчими обмеженнями, у т. ч. щодо діяльності, пов'язаної із захистом інформації, що становить державну таємницю, комунікаційними та технологічними системами, призначеними для її оброблення.

На нашу думку, більш обґрунтованим є підхід, згідно з яким вважається, що кібербезпека є одним із складників інформаційної безпеки, специфіка якої зумовлена особливостями суспільних відносин у кіберпросторі порівняно з простором ЗМК (ЗМІ). Тоді ієрархію стратегій у сфері кібербезпеки та кіберзахисту і послідовність їхнього розроблення можна було б подати таким рядом: Стратегія національної безпеки України – Стратегія інформаційної безпеки України – Стратегія кібербезпеки України – Стратегія кіберзахисту України.

Але така модель взаємозв'язку зазначених стратегій також не є загальноприйнятою навіть у національному законодавстві. Наприклад, згідно з пріоритетами та напрямами забезпечення кібербезпеки України, що визначені Стратегією кібербезпеки України, кібербезпека та кіберзахист розглядаються як споріднені, але різні сфери, насамперед щодо: проведення огляду національної системи кібербезпеки та розроблення галузевих індикаторів стану кібербезпеки; створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту ЗСУ на стратегічному, оперативному й тактичному рівнях; розвитку підрозділів кібербезпеки та кіберзахисту ЗСУ, Державної служби спеціального зв'язку та захисту інформації України, СБУ, Національної поліції України, розвідувальних органів, досягнення сумісності з відповідними підрозділами кібербезпеки та кіберзахисту держав – членів НАТО; проведення наукових досліджень у галузі кібербезпеки та кіберзахисту.

Водночас, відповідно до Закону [13], кіберзахист розглядається як невід'ємний "техніко-технологічний" складник кібербезпеки поряд зі "змістовними складовими" – кібероборoною, протидією кібершпигунству, кібертероризму, кіберзлочинності тощо.

У розвиток Закону [Там само], Стратегії [2] та Концепції створення державної системи захисту критичної інфраструктури Держспецзв'язку було розроблено та затверджене Урядом лише Постанову КМУ від 19 червня 2019 р. № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [15], якою визначено організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які, відповідно до законодавства, віднесено до об'єктів критичної інфраструктури.

Законодавчого впорядкування потребують відносини щодо забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час запобігання кібератакам і кіберінцидентам, виявлення, припинення їх, а також під час усунення їхніх наслідків.

Нормативно-технічний та нормативно-правовий рівень. Європейський та північно-атлантичний вектор зовнішньої політики України, визначений Конституцією України, у низці законодавчих актів концептуального та стратегічного рівня, у т. ч. в Законі [13], у міжнародних договорах, з одного боку, а з іншого боку суттєві недоліки, що притаманні сьогодні стандартизації в нашій країні у сфері кібербезпеки та кіберзахисту, стримують успішну безпекову діяльність у світовому кіберпросторі, розбудову цифрової економіки та суспільства, у сукупності зумовлюють необхідність вивчення та узагальнення міжнародного та національного досвіду в цій сфері з метою його узагальнення та подальшого використання під час формування та реалізації державної політики кібербезпеки та кіберзахисту.

Зокрема, незважаючи, на прийняті закони [4] та [13], украй актуальною залишається проблема подальшого розроблення та прийняття низки підзаконних актів, особливо нормативних та нормативно-правових документів (стандартів, кодексів усталеної практики, технічних регламентів тощо).

Найбільш *перспективним при цьому є підхід,* що орієнтований на розроблення національних стандартів на базі міжнародних та регіональних стандартів; стандартів держав, що є членами відповідних міжнародних чи регіональних організацій стандартизації. Такий підхід дозволяє економити фінансові та часові ресурси, забезпечувати транскордонну інтероперабельність та є основним для розвитку національної системи стандартизації.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі.

1. Аналіз та оцінювання інституційних спроможностей суб'єктів забезпечення системи кібербезпеки України та системи кіберзахисту, як і їхніх складників, показав, що, незважаючи на відповідні успіхи останніх років у сфері інституціональних спроможностей забезпечення кібербезпеки та кіберзахисту, їм притаманна низка суттєвих недоліків.

2. У зв'язку з відсутністю в національному законодавстві терміна "інституційна спроможність суб'єктів забезпечення системи кібербезпеки України та системи кіберзахисту" запропоновано авторське його визначення.

3. Окреслено основні складники інституційної спроможності суб'єктів забезпечення системи кібербезпеки України та кіберзахисту, а саме: правовий, організаційний, кадровий та фінансовий.

4. Організаційний складник інституційної спроможності суб'єктів забезпечення системи кібербезпеки України та кіберзахисту подано у вигляді трирівневої ієрархічної моделі, що включає стратегічну, оперативну (з основних суб'єктів національної системи кібербезпеки) та тактичну ланки з уточненням їхнього складу та функціоналу елементів, шляхом урахування конституційних повноважень парламенту в стратегічній ланці, конкретизації переліку суб'єктів тактичної ланки, які безпосередньо здійснюють заходи із забезпечення кібербезпеки та кіберзахисту, у т. ч. щодо включення до неї додатково підрозділів CSIRT із визначенням їхніх завдань та функцій.

5. Охарактеризовано правовий механізм інституційних спроможностей суб'єктів забезпечення системи кібербезпеки України та системи кіберзахисту та обґрунтовано конкретні напрями його вдосконалення для всіх рівнів ієрархічної моделі правового забезпечення: на законодавчому; підзаконному та нормативно-технічному(нормативно-правовому) рівнях.

6. Визначено основні проблеми кадрового складника інституційних спроможностей та обґрунтовано напрями розв'язання їх.

Напрямами подальших наукових досліджень можуть бути механізми публічного управління та адміністрування проведенням огляду у сфері кібербезпеки та кіберзахисту.

Список використаних джерел*

1. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 р. № 287/2015. *Офіційний вісн. України*. 2015. № 43. С. 14, ст. 1353.

2. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. *Офіційний вісн. України*. 2016. № 23. С. 69, ст. 899.

3. Методика визначення критеріїв євроінтеграційної складової державних цільових програм : наказ Міністерства економіки та з питань європейської інтеграції України від 13.04.2005 р. № 62. *Офіційний вісн. України*. 2005. № 17. С. 163, ст. 926.

4. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Офіційний вісн. України*. 2018. № 55. С. 51, ст. 1903.

5. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України" : Указ Президента України від 16.05.2019 р. № 225/2019. *Офіційний вісн. України*. 2019. № 41. С. 69, ст. 1429.

6. Порядок проведення оборонного огляду Міністерством оборони України : Постанова КМУ від 31.10.2018 р. № 941. *Офіційний вісн. України*. 2018. № 92. С. 56, ст. 3049.

7. Порядок проведення огляду загальнодержавної системи боротьби з тероризмом : Указ Президента України від 09.07.2019 р. № 506/2019. *Офіційний вісн. України*. 2019. № 55. С. 8, ст. 1907.

8. Порядок проведення огляду оборонно-промислового комплексу : Постанова КМУ від 22.05.2019 р. № 490. *Офіційний вісн. України*. 2019. № 49. С. 7, ст. 1653.

9. Колісніченко Н. М., Войновський М. М. Інституційна та інституціональна спроможність місцевого самоврядування: сутність понять та особливості визначення. *Теоретичні та прикладні питання державотворення : електрон. наук. фах. вид*. Одеса : ОРІДУ НАДУ, 2015. Вип. 16. С. 296–309.

10. Чемерис О. Інституалізація спроможності влади до взаємодії з громадськістю у контексті формування і реалізації державної політики. *Демократичне врядування : наук. вісн. : електрон. фах. вид*. Львів : ЛРІДУ НАДУ, 2015. Вип. 15. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Chemerys.pdf/.

11. Павлова А. В. К вопросу об институциональных проблемах управления изменениями в социально-экомических системах макро-, мезо- и микроэкономики. *Региональная экономика: теория и практика*. 2012. № 28 (259). С. 30–39. URL: https://cyberleninka.ru/article/n/k-voprosu-ob-institutsionalnyh-problemah-upravleniya-izmeneniyami-v-sotsialno-ekonomicheskih-sistemah-makro-mezo-i-mikroekonomiki.

12. Гбур З. В. Інституційне забезпечення економічної безпеки України. *Інвестиції: практика та досвід.* 2018. № 3. С. 98–102. URL: http://www.investplan.com.ua/?op=1&z=5924&i=19/.

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Офіційний вісн. України*. 2017. № 91. С. 31, ст. 2765.

14. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016) 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.

15. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19.06.2019 р. № 518. *Офіційний вісн. України*. 2019. № 50. С. 53, ст. 1697.

** Список побудовано в порядку посилань.*

References

1. Strategiya nacionalnoyi bezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 26.05.2015 r. No. 287/2015 (2015). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 43, p. 14, art. 1353* [in Ukrainian].

2. Strategiya kiberbezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 15.03.2016 r. No. 96/2016 (2016). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 23, p. 69, art. 899* [in Ukrainian].

3. Metodyka vyznachennya kryteriyiv yevrointegracijnoyi skladovoyi derzhavnyx cilovyx program: nakaz Ministerstva ekonomiky ta z pytan yevropejskoyi integraciyi Ukrayiny No. 62 vid 13.04.2005 r. (2005).*Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 17, p. 163, art. 926* [in Ukrainian].

4. Pro nacionalnu bezpeku Ukrayiny: Zakon Ukrayiny vid 21.06.2018 r. No. 2469-VIII (2018). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine*, *No. 55, p. 51, art. 1903* [in Ukrainian].

5. Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 16 travnya 2019 roku "Pro organizaciyu planuvannya v sektori bezpeky i oborony Ukrayiny: Ukaz Prezydenta Ukrayiny vid 16.05.2019 r. No. 225/2019 (2019). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 41, p. 69, art. 1429* [in Ukrainian].

6. Poryadok provedennya oboronnogo oglyadu Ministerstvom oborony Ukrayiny: postanova Kabinetu Ministriv Ukrayiny vid 31.10.2018 r. No. 941 (2018). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 92, p. 56, art. 3049* [in Ukrainian].

7. Poryadok provedennya oglyadu zagal noderzhavnoyi systemy borotby z teroryzmom: Ukaz Prezydenta Ukrayiny vid 19.07.2019 r. No. 506/2019 (2019). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 55, p. 8, art. 1907* [in Ukrainian].

8. Poriadok provedennia ohliadu oboronno-promyslovoho kompleksu: Postanova KMU vid 22.05.2019 r. No. 490. *Ofitsiinyi visn. Ukrainy – Official Bulletin of Ukraine, No. 49. p. 7, art. 1653* [in Ukrainian].

9. Kolisnichenko, N.M., Vojnovskyj, M.M. (2015). Instytucijna ta instytucionalna spromozhnist miscevogo samovryaduvannya: sutnist ponyat` ta osoblyvosti vyznachennya. *Teoretychni ta prykladni pytannya derzhavotvorennya – Theoretical and applied issues of state formation, issue 16, 296–309*. URL: http://nbuv.gov.ua/UJRN/tppd_2015_16_22 [in Ukrainian].

10. Chemerys, O. (2015). Instytualizaciya spromozhnosti vlady do vzayemodiyi z gromadskistyu u konteksti formuvannya i realizaciyi derzhavnoyi polityky. *Demokratychne vryaduvannya – Democratic Governance: naukovyj visnyk, issue 15* URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Chemerys.pdf/ [in Ukrainian].

11. Pavlova, A.V. (2012). K voprosu ob institutsionalnyih problemah upravleniya izmeneniyami v sotsialno-ekomicheskih sistemah makro-, mezo- i mikroekonomiki. *Regionalnaya ekonomika: teoriya i praktika, No. 28 (259), 30–39.* URL: https://cyberleninka.ru/article/n/k-voprosu-ob-institutsionalnyh-problemah-upravleniya-izmeneniyami-v-sotsialno-ekonomicheskih-sistemah-makro-mezo-i-mikroekonomiki [in Russian].

12. Gbur, Z.V. (2018). Instytucijne zabezpechennya ekonomichnoyi bezpeky Ukrayiny. *Investyciyi: praktyka ta dosvid – Investments: Practice and Experience, No.* 3, *98–102.* URL: http://www.investplan.com.ua/?op=1&z=5924&i=19 [in Ukrainian].

13. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 05.10.2017 r. No. 2163-VIII. (2017). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 91, p. 31, art. 2765* [in Ukrainian].

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

15. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19.06.2019 р. № 518. *Офіційний вісн. України. 2019. № 50. С. 53, ст. 1697.*

15. Zagalni vymogy do kiberzaxystu obyektiv krytychnoyi infrastruktury: postanova Kabinetu Ministriv Ukrayiny vid 19.06.2019 r. No. 518 (2019). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine, No. 50, p. 53, art. 1697.*

Myalkovsky D. V.,
Candidate of Institute of Personnel Training of the State Employment Service of Ukraine, Kyiv
ORCID 0000-0002-8246-8437;
Semenchenko A. I.,
Doctor of Public Administration, Full Professor, Chief of the Institute for Senior Executives, NAPA, Kyiv
ORCID 0000-0001-6482-3872

DEVELOPMENT OF INSTITUTIONAL CAPACITIES OF THE SUBJECTS OF PROVIDING THE CYBER SECURITY AND CYBER DEFENSE SYSTEM OF UKRAINE

The article defines the concept, essence, structure of institutional capacities of the cyber security and cyber defense systems of Ukraine, analyzes and evaluates their condition, substantiates the priority areas for their improvement, aimed at improving the efficiency and effectiveness of public policy in cyber security and cyber defense of Ukraine.

The essence of the concept of "institutional capacity of the subjects of cyber security and cyber defense" is proposed, which today has a number of significant shortcomings. The paper outlines the main components of the institutional capacity of the subjects of the cyber security system of Ukraine and cyber defense: legal, organizational, personnel and financial.

The organizational component of the institutional capacity of the subjects of the cybersecurity system of Ukraine and cyber defense is presented in the form of a three-level hierarchical model.

The concrete directions of improvement of the legal mechanism of institutional capacities for all levels of hierarchical model of legal maintenance are substantiated: on legislative; by-laws and normative-technical (normative-legal) levels.

The problems of the personnel component of institutional capacities are identified and proposals for their solution are formulated by developing and implementing formalized requirements for professional competencies for employees, in particular through the revision of the state classifier of professions.

Based on the analysis, it is proposed to improve the activities of the specially authorized central executive body for special communications and information protection, clarifying its functionality as a national competent network and information security authority, as defined by the NIS Directive.

The priority of the task of developing normative-technical and technical documents with ensuring the interoperability of their requirements with international standards and practices is determined.

Keywords: cybersecurity, cyber protection, cybersecurity system, hierarchical model, institutional capacities.

Надійшла до редколегії 13.07.2020 р.