НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

REGULATORY SUPPORT OF PROFESSIONAL TRAINING FOR SPECIALISTS OF THE NATIONAL SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION

УДК 35.088.6:[004:007:351.86] (477)
DOI https://doi.org/10.32782/pma2663-5240-2024.40.5

Арсенович Л.А.
д. філос. з публіч. упр. та адміністр.,
заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрація Держспецзв'язку

Динамічний розвиток української держави потребує практично щорічної корекції концептуальних підходів до формування державної політики у сфері захисту критичної інфраструктури, у тому числі і в освітній складовій. Система вищої освіти стає стратегічною сферою формування професійних компетентностей фахівців відповідно до потреб світового ринку праці. Виникає гостра потреба в адаптації даних питань не тільки на законодавчому, нормативно-правовому, економічному рівні, але і в динамічній перебудові загальної мети та стратегічних напрямів реформування всіх ланок освіти згідно зі світовими стандартами. На сьогодні Українська держава будує власну національну систему захисту критичної інфраструктури.

Нині в усьому світі надзвичайно актуальною є проблема підготовки висококласних фахівців у сфері захисту критичної інфраструктури. У зв'язку із повномасштабним вторгненням російської федерації на територію України та відсутністю відповідної галузі знань, підготовка таких кадрів в Україні здійснюється в достатньо обмежених обсягах, а молодь, яка отримала вищу освіту за певним напрямом, змушена вийджати працювати за кордон або ж працювати всередині країни на потреби зарубіжних замовників. Дана ситуація складалася упродовж декількох останніх років і зумовила підсилення кадрового голоду щодо спеціалістів у сфері захисту критичної інфраструктури.

У статті здійснено аналіз нормативно-правового підґрунтя щодо підготовки фахівців у сфері захисту критичної інфраструктури, який вказує на неузгодженість нормативно-правового регулювання щодо професійної підготовки фахівців національної системи захисту критичної інфраструктури, відсутність єдиної загальноосвітньої системи захисту критичної інфраструктури, невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури, що призводить до глобальних проблем у забезпеченні безпеки громадян і держави у сфері захисту критичної інфраструктури.

Ключові слова: *кібербезпека, національна система захисту критичної інфраструктури, підвищення кваліфікації, підготовка фахівців, сфера захисту критичної інфраструктури.*

Strong development of the Ukrainian state requires almost annual correction of conceptual approaches to developing the state policy related to critical infrastructure protection, including in the educational component. The system of higher education is becoming a strategic area for developing professional competencies of specialists in accordance with the needs of the global labor market. There is an urgent need not only to adapt these issues at the legislative, regulatory and economic level, but also to dynamically restructure the overall goal and strategic directions of reforming all levels of education in accordance with international standards. Today, the Ukrainian state is building its own national system of critical infrastructure protection.

These days, the problem of training highly qualified critical infrastructure protection specialists is extremely relevant worldwide. Due to the full-scale invasion of Ukraine by the Russian Federation and the lack of relevant knowledge, the training of such specialists in Ukraine is rather limited, and young people with higher education in a particular area have to leave their home country looking for employment abroad, or work domestically for foreign customers. This situation has been developing over the past few years and has led to an increased shortage of critical infrastructure protection specialists.

The article analyzes the regulatory framework for training critical infrastructure protection specialists showing the inconsistencies in the regulatory support of professional training for specialists of the national system of critical infrastructure protection, the lack of a unified general education system for critical infrastructure protection, uncertainty of powers, tasks and responsibilities of central executive authorities and other state bodies in the area of critical infrastructure protection, as well as the rights, duties and responsibilities of owners (managers) of critical infrastructure facilities, which leads to global problems in ensuring the security of citizens and the state in the area of critical infrastructure protection.

Key words: *cybersecurity, national system of critical infrastructure protection, advanced professional training, training of specialists, critical infrastructure protection.*

Постановка проблеми у загальному вигляді. В умовах відсутності єдиної загальнодержавної системи захисту критичної інфраструктури, недостатності та неузгодженості нормативно-правового регулювання з питань захисту систем і об'єктів критичної інфраструктури та нерозвиненості державно-приватного партнерства в освітній сфері особливого значення набувають проблеми професійної підготовки фахівців національної системи захисту критичної інфраструктури.

Зовнішні та внутрішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах повномасштабного вторгнення російської федерації на тери-

торію України опікуються питаннями у сфері захисту критичної інфраструктури.

У контексті проведення освітніх реформ у всіх сферах діяльності українського суспільства, питання професійної підготовки фахівців, які відповідають за забезпечення безпеки та стійкості критичної інфраструктури, набуває особливої актуальності та потребує окремої уваги.

Аналіз останніх досліджень і публікацій. Нещодавні наукові напрацювання вчених засвідчують, що професійна підготовка фахівців у сфері захисту критичної інфраструктури є одним із напрямів державної політики у сферах національної безпеки і оборони, без якого є неможливими створення та функціонування національної системи захисту критичної інфраструктури.

Як свідчать останні публікації та дослідження, проблеми професійного розвитку фахівців національної системи захисту критичної інфраструктури є малодослідженими. Так, С. Бєлай разом з І. Євтушенко та В. Мацюком у своїй науковій роботі аналізують теоретико-методологічне підґрунтя щодо підготовки фахівців з реагування на кризові ситуації на об'єктах критичної інфраструктури Україні, надають пропозиції щодо проведення міжвідомчих командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять, розвитку спеціалізації «Захист критичної інфраструктури та її стійкість», а також практичні рекомендації в контексті розвитку створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури [1]. А інший науковець, С. Теленик, у своїй статті встановлює перелік суміжних спеціальностей, які можуть бути затребувані в галузі захисту критичної інфраструктури та аналізує причини, що перешкоджають високій ефективності навчання та підвищення кваліфікації персоналу [2].

Незважаючи на нещодавні дослідження вищевказаних науковців, які стосуються питань підготовки фахівців у сфері захисту критичної інфраструктури, питанням нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури приділено мало уваги, що й обумовило актуальність дослідження.

Виділення невирішених раніше частин загальної проблеми. Відсутність єдиної загальноосвітньої системи у сфері захисту критичної інфраструктури, незлагодженість нормативно-правового регулювання з питань підготовки, перепідготовки та підвищення кваліфікації у зазначеній сфері, невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів щодо навчання особового складу з питань захисту критичної інфраструктури, а також відсутність механізму визначення потреби на підвищення кваліфікації фахівців національної системи захисту критичної інфраструктури зумовлюють актуалізацію питання щодо нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання зазначених проблем на загальнодержавному рівні створення нормативно-правового підґрунтя професійної підготовки фахівців національної системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Мета статті. Метою статті є необхідність аналізу нормативно-правової бази підготовки фахівців у сфері захисту критичної інфраструктури, яка на сьогодні є критично важливою для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

Виклад основного матеріалу. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як об'єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями [3, с. 48].

Посилення загроз техногенного і природного характеру, підвищення складності та збільшення кількості кібератак, активізація терористичної злочинності, а також пошкодження об'єктів інфраструктури на всій території України внаслідок повномасштабного вторгнення російської федерації засвідчують нагальність розгляду питання щодо забезпечення національної безпеки, соціально-економічного розвитку держави та захисту об'єктів і ресурсів, які є критично важливими для функціонування суспільства.

На необхідності та першочерговості захисту об'єктів критичної інфраструктури у своєму щорічному Посланні до Верховної Ради України «Про внутрішнє та зовнішнє становище в Україні» ще у 2017 році наголосив Президент України. Проте, наявного у держави законодавчого та інституційного інструментарію недостатньо щоб оперативно та якісно реагувати на проблеми, пов'язані із забезпеченням інформаційної безпеки об'єктів критичної інфра-

структури. Наразі виникла ситуація, коли жоден орган державної влади комплексно не опікується цією проблематикою. Єдина державна система захисту критичної інфраструктури фактично відсутня. Відсутній і єдиний закон, який визначав би термінологію професійної підготовки фахівців національної системи захисту критичної інфраструктури. Очевидно, що сектор безпеки та оборони України в частині захисту об'єктів критичної інфраструктури потребує реформування, в першу чергу шляхом прийняття відповідного закону та удосконалення діючих нормативно-правових актів в частині, що стосується [4, с. 23].

Забезпечення безпеки та безперебійного функціонування об'єктів критичної інфраструктури значною мірою залежить від так званого «людського фактору». Саме рівень підготовленості фахівців, їхні компетенції, розуміння специфіки діяльності об'єктів та механізмів здійснення взаємодії багато в чому зумовлюють успіх справи в цілому. Разом із тим, слід розуміти, що подібні якості не з'являються самі по собі. Сподівання лише на життєвий досвід, який набувається роками роботи в галузі, також занадто дорого може обійтися державі [2, с. 91].

Первинна систематизація наукових праць та їх огляд за обраною темою надає можливість встановити, що попри значний інтерес науковців до підготовки фахівців із захисту критичної інфраструктури поза увагою вчених залишаються деякі аспекти даної проблеми. Перш за все, йдеться про те, що сфера захисту критичної інфраструктури не може вичерпуватися лише категорією ІТ-спеціалістів. Освітній процес щодо кадрового забезпечення об'єктів критичної інфраструктури на всіх рівнях, включаючи управлінський персонал, насамперед, має здійснюватися на підставі чітко сформульованого наукового обґрунтування та нормативно-правового забезпечення.

Виклики національній безпеці вимагають побудови в Україні системи захисту критичної інфраструктури, невід'ємним складником якої є розроблення якісної нормативно-правової бази. Належний стан захисту об'єктів критичної інфраструктури від загроз природного й техногенного характеру значно залежить від нормативно-правового регулювання діяльності сфери та потребує якісного й детального наукового дослідження [5, с. 59].

На теперішній час в Україні ведуться роботи зі створення нормативно-правової бази й організаційної-структури системи захисту критичної інфраструктури. Хоча деяка частина законодавства вже прийнята, водночас основоположні акти, у тому числі у сфері професійної підготовки фахівців національної системи захисту критичної інфраструктури, перебувають у процесі розроблення.

З метою надання раціональних пропозицій у частині вдосконалення чинного законодавства щодо професійної підготовки фахівців у сфері захисту критичної інфраструктури існує реальна потреба в дослідженні чинних норм нормативно-правових актів, їх критичному аналізі, а також розробленні шляхів підвищення ефективності нормативно-правової діяльності й подальшому практичному впровадженні наукових напрацювань.

На законодавчому рівні питання підготовки фахівців національної системи захисту критичної інфраструктури врегульовано Законом України від 16 листопада 2021 року № 1882-IX «Про критичну інфраструктуру» [6], який регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час, визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Слід зазначити, що особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій (надзвичайного та воєнного стану, особливого періоду) регулюються законами України «Про правовий режим надзвичайного стану» [7], «Про функціонування єдиної транспортної системи України в особливий період» [8] та «Про оборону України» [9]. Окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.

Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури [6]. При цьому, до завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури, крім іншого, належить підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури.

Так, відповідно до Закону, державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури, здійснюють, у тому числі, організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури, а місцеві

органи виконавчої влади (військово-цивільні адміністрації – у разі утворення) у сфері захисту критичної інфраструктури забезпечують розроблення, затвердження та погодження із заінтересованими органами програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Крім цього Закон врегульовує завдання, права та обов'язки операторів критичної інфраструктури. Так, одним із основних завдань операторів критичної інфраструктури є розроблення, затвердження у встановленому законодавством порядку та проведення навчань і тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури.

На секторальному (галузевому) та регіональному рівнях планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури відбувається органами державної влади шляхом розроблення і затвердження галузевих, регіональних планів та програм з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань. При цьому організація взаємодії між суб'єктами національної системи захисту критичної інфраструктури здійснюється шляхом проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об'єктів критичної інформаційної інфраструктури.

Разом з тим, Закон встановив, що Україна відповідно до міжнародних договорів може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» [10] та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України» [11].

Крім цього, зазначений Закон встановив, що уповноважений орган у сфері захисту критичної інфраструктури України, функції якого в умовах воєнного стану виконує Держспецзв'язку, бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури.

Серед актів Президента України слід виділити Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України, затверджену Указом Президента України від 22 жовтня 2021 року № 544/2021 [12], метою якої є реформування та розвиток Держспецзв'язку як суб'єкта сектору безпеки і оборони із запровадженням уніфікованої системи планування та управління ресурсами на основі сучасних європейських та євроатлантичних підходів, що дасть змогу підвищити інституційну спроможність, а також оптимізувати організаційну структуру Держспецзв'язку. Так, поміж пріоритетів та напрямів реформування Держспецзв'язку слід виділити оновлення технологічної бази кіберполігону (тренінгової кіберплатформи) та проведення кібернавчань в інтересах суб'єктів забезпечення кібербезпеки державного сектору та критичної інфраструктури.

«Першопрохідником» серед нормативно-правових актів Кабінету Міністрів України щодо нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури є Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [13], яка визначає основні напрями, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту критичної інфраструктури. Так, Концепція передбачає протягом 2017–2027 років реалізувати та забезпечити на загальнодержавному рівні створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури та встановлення вимог до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань (тренувань).

Передбачається, що реалізація Концепції сприятиме створенню державної системи захисту критичної інфраструктури, виробленню механізмів ефективного реагування у разі виникнення кризових ситуацій, налагодженню ефективної взаємодії між усіма суб'єктами державної системи захисту критичної інфраструктури, гармонізації законодавства України у сфері захисту критичної інфраструктури із законодавством ЄС та міжнародному співробітництву у сфері захисту критичної інфраструктури.

«Другим нагадуванням» про зазначену проблему стали Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затвер-

джені постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [14], які визначають 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 віднесені до об'єктів критичної інфраструктури. Так, Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, затверджений зазначеною постановою, передбачає, що власник/керівник об'єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності.

Розроблення та впровадження зазначених програм підвищення обізнаності/навчання працівників з питань інформаційної безпеки надасть змогу:

– запобігати кіберінцидентам, порушенням конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– запобігати порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– запобігати порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– забезпечити спостережність за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонування засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Наступним кроком на шляху нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури став затверджений на засіданні Уряду Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (постанова Кабінету Міністрів України від 11 листопада 2020 року № 1176 [15]), який проводиться з метою ефективного і оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак і кіберінцидентів, ліквідації їх наслідків, відновлення функціонування об'єктів критичної інформаційної інфраструктури. Зазначений Порядок встановив, що під час основного (виконавчого) етапу огляду робоча група, склад якої затверджується Адміністрацією Держспецзв'язку, готує пропозиції щодо шляхів і напрямів вдосконалення системи підготовки кадрів та науково-технічної підтримки розвитку національної системи кібербезпеки, а також пропозиції стосовно вжиття заходів, спрямованих на досягнення кіберстійкості критичної інформаційної інфраструктури.

За результатами огляду визначаються напрями вдосконалення і розвитку національної системи кібербезпеки в частині:

– проведення аналізу кіберстійкості критичної інформаційної інфраструктури, стану кіберзахисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

– формування пропозицій щодо вдосконалення законодавства у сфері кібербезпеки та кіберзахисту та визначення напрямів розвитку національної системи кібербезпеки в частині кіберзахисту;

– формування пропозицій щодо вдосконалення суб'єктами критичної інформаційної інфраструктури та уповноваженими органами заходів з кіберзахисту;

– планування заходів щодо забезпечення кіберстійкості критичної інформаційної інфраструктури.

Наступним дієвим кроком у розбудові нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури стало утворення центрального органу виконавчої влади із спеціальним статусом, який забезпечує реалізацію державної політики у сфері захисту критичної інфраструктури та формування національної системи стійкості (постанова Кабінету Міністрів України від 12 липня 2022 року № 787 [16]). Мова йде про Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України, діяльність якої спрямовується і координується Кабінетом Міністрів України, і одними із основних завдань якої є:

– участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури;

– забезпечення підготовки, перепідготовки, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури.

Передбачається, що створення такої Служби запустить процес виконання Закону України «Про критичну інфраструктуру», буде

сприяти впровадженню єдиного державного підходу до захисту критичної інфраструктури, що є актуальним завданням як під час війни, так і в мирний час, а також забезпечить координацію у питаннях критичної інфраструктури між усіма залученими органами державної влади.

Подальше нормативно-правове забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури знайшло відображення у постанові Кабінету Міністрів України від 14 жовтня 2022 року № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [17], яку розроблено відповідно до частини другої статті 19 та пункту 4 частини четвертої статті 21 Закону України «Про критичну інфраструктуру» та яка затвердила форму річного звіту про виконання секторальним органом повноважень, визначених Законом України «Про критичну інфраструктуру», а також форму річного звіту про виконання оператором критичної інфраструктури повноважень, визначених Законом України «Про критичну інфраструктуру».

Зазначеною постановою Кабінету Міністрів України установлено, що секторальні органи у сфері захисту критичної інфраструктури щороку до 30 січня подають уповноваженому органу у сфері захисту критичної інфраструктури України (в умовах воєнного стану – Держспецзв'язку) звіт про виконання повноважень, визначених Законом України «Про критичну інфраструктуру», за минулий рік, який серед іншого передбачає надання інформації щодо:

– розроблення та затвердження галузевих (регіональних) планів і програм з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань;

– організації системи підготовки персоналу, навчань та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури (кількість: підготовлених здобувачів вищої освіти (у тому числі на курсах підвищення кваліфікації); залучених секторальним органом осіб до проведення спільних командно-штабних навчань, тактико-спеціальних навчань, спільних тренувань, занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об'єктів критичної інфраструктури; залучених операторами критичної інфраструктури осіб до навчань, тренінгів, практичних занять, перевірок персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури).

Разом з тим, оператори критичної інфраструктури щороку до 15 січня подають секторальним органам у сфері захисту критичної інфраструктури звіт про виконання повноважень, визначених Законом України «Про критичну інфраструктуру», за минулий рік, який серед іншого передбачає надання інформації щодо організації підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту структурних підрозділів (відповідальних осіб) критичної інфраструктури, а саме:

– кількості підготовлених здобувачів вищої освіти (у тому числі на курсах підвищення кваліфікації);

– кількості проведених навчань, тренінгів, практичних занять, перевіреного персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури.

– Надання секторальними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури такої інформації надасть змогу здійснити аналіз щодо:

– фактичного стану захищеності об'єкта критичної інфраструктури, дотримання вимог законодавства у сфері критичної інфраструктури;

– здійснення контролю за ризиками безпеки та удосконалення заходів, які здійснюються для забезпечення безпеки та стійкості об'єкта критичної інфраструктури;

– визначення перспектив подальшого функціонування і розвитку національної системи захисту критичної інфраструктури, а також про удосконалення системи захисту об'єктів критичної інфраструктури.

На окрему увагу заслуговують нормативно-правові акти, які було прийнято Урядом у 2023 – 2024 роках та розроблено за активної участі Адміністрації Держспецзв'язку, яка під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, забезпечує здійснення повноважень уповноваженого органу у сфері захисту критичної інфраструктури.

І першим актом, який передбачав, у тому числі, питання щодо вдосконалення освітньої складової сфери захисту критичної інфраструктури стало розпорядження Кабінету Міністрів України від 24 березня 2023 року № 243-р «Про затвердження плану заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2023 рік» [18], яке затвердило заходи із вдосконалення інформаційно-комунікаційної інфраструктури системи управління державою в умовах мирного часу, державних інформаційних ресурсів, протидії технічним розвідкам та рівня матеріально-технічного оснащення Держспецзв'язку.

Так, відповідно до вищезазначеного розпорядження Адміністрації Держспецзв'язку протягом IV кварталу 2023 року необхідно було забезпечити модернізацію кіберполігону (тренінгової кіберплатформи) шляхом оновлення його технологічної бази для проведення кібернавчань в інтересах суб'єктів забезпечення кібербезпеки державних органів, підприємств, установ та організацій державної форми власності, об'єктів критичної інфраструктури. Індикатором виконання зазначеного завдання стало придбання та впровадження спеціального обладнання для нарощування спроможностей кіберполігону (тренінгової кіберплатформи).

Справжнім «проривом» у питаннях підготовки персоналу сфери захисту критичної інфраструктури стало розпорядження Кабінету Міністрів України від 19 вересня 2023 року № 825-р «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» [19], яке передбачає протягом 2023–2024 років виконання заходів щодо подальшого розвитку правової регламентації діяльності суб'єктів національної системи захисту критичної інфраструктури, створення системи координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури, запровадження управління ризиками критичної інфраструктури, посилення стійкості національної системи захисту критичної інфраструктури та налагодження міжнародної співпраці. Так, серед п'ятнадцяти завдань, які затверджено Національним планом, необхідно виділити такі завдання та заходи що передбачають:

– запровадження планів взаємодії суб'єктів національної системи захисту критичної інфраструктури щодо забезпечення стійкості надання життєво важливих функцій та/або послуг шляхом розроблення та затвердження протягом II кварталу 2024 року секторальними органами у сфері захисту критичної інфраструктури, обласними держадміністраціями (обласними військовими адміністраціями), функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури галузевих, регіональних планів та програм з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань;

– розвиток спроможності суб'єктів національної системи захисту критичної інфраструктури та реагування на загрози критичній інфраструктурі шляхом:

– затвердження протягом IV кварталу 2024 року секторальними органами у сфері захисту критичної інфраструктури секторальних програм підготовки персоналу щодо забезпечення стійкості та захисту критичної інфраструктури;

– проведення на постійній основі суб'єктами національної системи захисту критичної інфраструктури спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак;

– запровадження системи постійного підвищення рівня кваліфікації персоналу операторів критичної інфраструктури шляхом проведення на постійній основі операторами критичної інфраструктури навчань та тренінгів, підготовки та перевірки персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

– розвиток спроможностей територіальних громад підтримувати власними силами мінімальний рівень життєво важливих функцій та/або послуг шляхом затвердження протягом IV кварталу 2024 року обласними держадміністраціями (обласними військовими адміністраціями), операторами критичної інфраструктури, секторальними органами у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та Адміністрацією Держспецзв'язку програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Виконання Національного плану, який розроблено за сприяння проєкту USAID «Кібербезпека критично важливої інфраструктури України» та розрахований на три роки, сприятиме безперебійній роботі об'єктів критичної інфраструктури різних категорій, забезпечить захист від загроз та безперебійне надання життєво важливих послуг населенню.

Наступним не менш важливим нормативно-правовим актом щодо професійної підготовки фахівців у сфері захисту критичної інфраструктури стало розпорядження Кабінету Міністрів України від 10 листопада 2023 року № 1025-р «Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» [20], яке направлене на збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації.

План містить заходи щодо запровадження єдиної та цілісної системи пріоритезації, ідентифікації, запобігання та ефективного реагу-

вання на загрози та ризики будь-якого характеру. Документ направлений на посилення спроможності органів влади та місцевого самоврядування у сфері національної системи стійкості, у тому числі підвищенню компетенцій їх представників. Також план спрямований на розвиток навичок та алгоритмів поведінки громадян під час загрози і виникнення кризових ситуацій, у тому числі щодо підтримки сил безпеки і оборони цивільним населенням. Документ містить заходи з моніторингу та аналізу ефективності функціонування національної системи стійкості [21].

Так, в рамках проведення аналізу загроз та ризиків для найбільш важливих сфер життєдіяльності суспільства і держави секторальним органам у сфері захисту критичної інфраструктури, Адміністрації Держспецзв'язку, Мінекономіки, Міносвіти, Нацдержслужбі, Національному агентству кваліфікацій та функціональним органам у сфері захисту критичної інфраструктури протягом II кварталу 2024 року передбачено забезпечити розроблення переліку посад та кваліфікаційних характеристик для фахівців, відповідальних за забезпечення захисту об'єктів критичної інфраструктури.

Крім цього, з метою посилення спроможності державних органів проводити ідентифікацію загроз, виявляти вразливості та оцінювати ризики національній безпеці Нацдержслужбі, Міноборони та Адміністрації Держспецзв'язку на постійній основі передбачено забезпечити розроблення та впровадження програм підвищення кваліфікації державних службовців, працівників державних органів, що входять до складу сектору безпеки та оборони, посадових осіб органів управління та органів місцевого самоврядування з питань кібербезпеки та захисту критичної інфраструктури.

«Запровадження національної системи стійкості розвиватиме необхідну спроможність держави і суспільства запобігати широкому спектру загроз та ризиків будь-якого характеру, а у разі їх настання – реагувати та відновлюватись швидко, якісно та ефективно. Розроблений підхід до стійкості синхронізований із основними вимогами НАТО і враховує український контекст повномасштабного вторгнення росії. Національна система стійкості багаторівнева: вона охоплюватиме національний, регіональний і місцевий рівні», – зазначила Віце-прем'єр-міністр України з питань європейської та євроатлантичної інтеграції України Ольга Стефанішина [21].

Крім цього слід зазначити, що з метою нормативно-правового забезпечення діяльності у сферах кібербезпеки, кіберзахисту та кібероборони, розвитку технологічної складової національної системи кібербезпеки та налагодження більш тісного співробітництва з міжнародними партнерами Урядом у грудні 2023 року було прийнято план заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України, затверджений розпорядженням Кабінету Міністрів України від 19 грудня 2023 року № 1163-р [22]. Так, пунктом 53 плану передбачено забезпечення протягом 2023 – 2024 років участі щонайменше п'яти представників основних суб'єктів національної системи кібербезпеки та об'єктів критичної інфраструктури (МЗС України, Апарат РНБО України, Адміністрація Держспецзв'язку, Мінфін, Мінекономіки, Нацполіція, СБ України, Міноборони, ГШ ЗС України, СЗР України, Адміністрація Держприкордонслужби та Нацбанк) у навчаннях та підвищенні кваліфікації за міжнародними програмами. Виконання зазначеного заходу дасть змогу забезпечити подальший розвиток організаційно-технічної моделі кіберзахисту, організацію наукових досліджень у сфері кібербезпеки, посилення кіберзахисту об'єктів критичної інформаційної інфраструктури, а також налагодження процесу підготовки кадрів у сферах кібербезпеки та захисту критичної інфраструктури.

При великій кількості кібератак, кіберінцидентів та кіберзагроз, від яких потерпає Україна майже щодня, питання нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури є важливим управлінським та урядовим завданням. Виходячи з того, що забезпечення захисту критичної інформаційної інфраструктури має проводитись як на державному, так і на місцевому рівнях, Україні необхідно розробити дієву та ефективну нормативно-правову базу для врегулювання освітньої складової.

Висновки. Підсумовуючи зазначене, можемо виділити дві відносно самостійні групи джерел нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури в Україні. Перша група – це нормативно-правові акти, якими врегульовані суспільні відносини у сфері захисту критичної інфраструктури. Друга група – це нормативно-правові акти, які регулюють деякі освітні питання щодо професійної підготовки фахівців сфери захисту критичної інфраструктури в Україні в практичній площині.

Головним недоліком нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури на сьогодні є відсутність відповідних нормативно-правових та організаційно-розпорядчих актів, які б унормову-

вали питання підготовки та підвищення кваліфікації громадян України, фахівців із захисту критичної інфраструктури силового напряму, працівників міністерств та інших ЦОВВ у всіх її аспектах. Відсутність трактування такої дефініції як фахівець національної системи захисту критичної інфраструктури, а також не сформованість (у нормативному відношенні) системи підготовки кадрів для сфери захисту критичної інфраструктури зумовлюють послаблення методологічних засад діяльності суб'єктів державної системи захисту критичної інфраструктури, деградацію інформаційного суспільства України та цифрового комунікативного середовища, зменшення кількості підготовлених фахівців для сфери захисту критичної інфраструктури, необхідних для задоволення потреб державного сектора економіки, а також призводять до зниження компетентності громадян України та фахівців різних сфер діяльності з питань захисту критичної інфраструктури.

Відсутність єдиної загальнодержавної системи захисту критичної інфраструктури, недостатність та неузгодженість нормативно-правового регулювання щодо професійної підготовки фахівців національної системи захисту критичної інфраструктури, невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури призводять до глобальних проблем у забезпеченні безпеки громадян і держави у сфері захисту критичної інфраструктури. На теперішній час сфера захисту критичної інфраструктури в Україні розвивається швидкими темпами, а нормативно-правове врегулювання цієї сфери не встигає за цим активним розвитком, що породжує низький рівень стійкості критичної інфраструктури.

Враховуючи зазначене, шляхами удосконалення нормативно-правового забезпечення професійної підготовки фахівців національної системи захисту критичної інфраструктури слід вважати:

– внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266 (у редакції постанови Кабінету Міністрів України від 07 липня 2021 року № 762) [23], у частині доповнення галуззю знань «Забезпечення стійкості та захисту критичної інфраструктури»;

– розроблення Адміністрацією Держспецзв'язку:

– проєкту розпорядження Кабінету Міністрів України «Про схвалення Концепції системи підготовки кадрів для сфери захисту критичної інфраструктури»;

– міжвідомчого наказу стосовно запровадження механізму визначення потреби на підвищення кваліфікації фахівців національної системи захисту критичної інфраструктури з числа військовослужбовців та осіб начальницького складу;

– розроблення Адміністрацією Держспецзв'язку проєктів нормативно-правових (організаційно-розпорядчих) актів щодо:

– організації та впровадження проведення обов'язкової перевірки персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

– організації та проведення тренувань працівників національної системи захисту критичної інфраструктури;

– організації та впровадження проведення навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Сьогодні в державі тільки починається процес розбудови сфери захисту критичної інфраструктури. Однак без здійснення відповідної оцінки та вирішення проблемних питань щодо стану реалізації Закону України «Про критичну інфраструктуру» та Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури така робота лише засвідчить поверхневий та формальний підхід до питань захисту критичної інфраструктури. З огляду на це проблематика організації професійної підготовки фахівців національної системи захисту критичної інфраструктури стає особливо актуальною та порушує питання про подальший її розвиток як для потреб секторальних органів у сфері захисту критичної інфраструктури, так і держави в цілому.

ЛІТЕРАТУРА:

1. Бєлай С. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. *Вісник Національного університету цивільного захисту України. Серія : Державне управління.* 2021. Вип. 2. С. 342–350.

2. Теленик С. С. Напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури. *Правові новели.* 2020. № 10/2020. Т. 2. С. 91–99.

3. Арсенович Л. А. Понятійно-категоріальний апарат у сфері підготовки фахівців із кібербезпеки органів державної влади України. *Наукові перспективи: журнал.* 2022. № 2(20). С. 33–53.

4. Жевелєва І. С. Правові засади забезпечення інформаційної безпеки об'єктів критичної інфраструк-

тури. *Міжнародний науковий журнал «Інтернаука». Серія : Юридичні науки.* 2020. № 5. С. 22–28.

5. Єрменчук О. П. Правове регулювання захисту об'єктів критичної інфраструктури від загроз національній безпеці природного й техногенного характеру. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція.* 2019. Вип. 37. С. 59–62.

6. Про критичну інфраструктуру : Закон України від 16 лист. 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.06.2024).

7. Про правовий режим надзвичайного стану : Закон України від 16 бер. 2020 р. № 1550-III. URL: https://zakon.rada.gov.ua/laws/show/1550-14#top (дата звернення: 01.06.2024).

8. Про функціонування єдиної транспортної системи України в особливий період : Закон України від 20 жов. 1998 р. № 194-XIV. URL: https://zakon.rada.gov.ua/laws/show/194-14#Text (дата звернення: 01.06.2024).

9. Про оборону України : Закон України від 06 груд. 1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#top (дата звернення: 01.06.2024).

10. Про порядок направлення підрозділів Збройних Сил України до інших держав : Закон України від 02 бер. 2000 р. № 1518-III. URL: https://zakon.rada.gov.ua/laws/show/1518-14#top (дата звернення: 01.06.2024).

11. Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України : Закон України від 22 лют. 2000 р. № 1479-III. URL: https://zakon.rada.gov.ua/laws/show/1479-14#top (дата звернення: 01.06.2024).

12. Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» : Указ Президента України від 22 жов. 2021 р. № 544/2021. URL: https://zakon.rada.gov.ua/laws/show/544/2021#Text (дата звернення: 01.06.2024).

13. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 01.06.2024).

14. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19 чер. 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 01.06.2024).

15. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : постанова Кабінету Міністрів України від 11 лист. 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (дата звернення: 01.06.2024).

16. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : постанова Кабінету Міністрів України від 12 лип. 2022 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 01.06.2024).

17. Деякі питання подання інформації у сфері захисту критичної інфраструктури : постанова Кабінету Міністрів України від 14 жов. 2022 р. № 1175. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#Text (дата звернення: 01.06.2024).

18. Про затвердження плану заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2023 рік : розпорядження Кабінету Міністрів України від 24 бер. 2023 р. № 243-р. URL: https://zakon.rada.gov.ua/laws/show/243-2023-%D1%80#Text (дата звернення: 01.06.2024).

19. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19 вер. 2023 р. № 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 01.06.2024).

20. Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року : розпорядження Кабінету Міністрів України від 10 лист. 2023 р. № 1025-р. URL: https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text (дата звернення: 01.06.2024).

21. Уряд затвердив план реалізації Концепції забезпечення національної системи стійкості до 2025 року. Урядовий портал. URL: https://www.kmu.gov.ua/news/uriad-zatverdyv-plan-realizatsii-kontseptsii-zabezpechennia-natsionalnoi-systemy-stiikosti-do-2025-roku (дата звернення: 01.06.2024).

22. Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 19 груд. 2023 р. № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (дата звернення: 01.06.2024).

23. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : постанова Кабінету Міністрів України від 29 квіт. 2015 р. № 266. URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF (дата звернення: 01.06.2024).