СЕКЦІЯ 2
МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ

ШЛЯХИ УДОСКОНАЛЕННЯ ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ В ОСВІТНІЙ СФЕРІ

WAYS TO IMPROVE THE FUNCTIONING OF THE NATIONAL CYBERSECURITY SYSTEM IN EDUCATION

УДК 35.088.6:[004:007:351.86] (477)
DOI https://doi.org/10.32782/pma2663-5240-2023.33.6

Арсенович Л.А.
докт. філософії з публічного управління та адміністрування,
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 розвитку інформаційних технологій та питань кібербезпеки у суспільстві. 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. Українська держава будує власну національну систему ІТ-індустрії та відповідну сферу кібербезпеки.

Нині в усьому світі надзвичайно актуальною є проблема підготовки висококласних фахівців у сфері кібербезпеки. Із врахуванням тенденцій сучасного ринку праці збільшується кількість закладів вищої освіти, здатних впроваджувати освітню діяльність у напрямку підготовки таких спеціалістів. До недавнього часу підготовка таких кадрів в Україні здійснювалася в достатньо обмежених обсягах, а молодь, яка отримувала вищу освіту за даною спеціальністю, змушена була виїжджати 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 кібербезпеки.

У статті здійснено аналіз нормативно-правового підґрунтя щодо підготовки фахівців у сфері захисту критичної інфраструктури (який вказує на відсутність окремого нормативно-правового акта, який би визначав порядок проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури), узагальнено освітню практику щодо підготовки спеціалістів у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури у різних провідних державах світу (які приділяють досить важливу увагу процесу навчання та підготовці фахівців у зазначеній сфері), та запропоновано модель проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, яку розроблено для поступового самовдосконалення особистості шляхом поетапного присвоєння відповідного фахового рівня.

Ключові слова: *кібербезпека, об'єкти критичної інфраструктури, періодична атестація (переатестація), професійний розвиток, фахівці із кібербезпеки.*

The dynamic development of the Ukrainian state requires an almost annual adjustment of conceptual approaches to the advance in information technology and to cybersecurity issues in the society. The higher education system becomes a strategic area of raising professional competences in specialists to cater for the global labor market. It is getting highly relevant to adapt these issues not only in legal, regulatory and economic terms, but also in terms of dynamic restructuring of the general goal and strategic directions of reforming all education sectors to be consistent with the world standards. The Ukrainian state is building its own national system of the IT industry and the appropriate cybersecurity environment.

Currently, the training of qualified cybersecurity specialists has got an extremely relevant issue worldwide. Given today's labor market trends, the higher education institutions that train such specialists are growing in numbers. Until recently, the training of such personnel in Ukraine was fairly limited, and young people graduating in this profession had to seek employment abroad or work within Ukraine for the needs of foreign customers. This situation has been developing over the past several years and has led to an increased shortage of skilled cybersecurity specialists.

The publication analyzes the regulatory basis for the training of critical infrastructure protection specialists (which shows the absence of some specific legal instrument that would outline the procedure for mandatory periodic attestation (re-attestation) of the personnel responsible for cybersecurity of critical infrastructure facilities), summarizes the education practices for training critical infrastructure cybersecurity specialists in various leading countries of the world (which pay quite serious attention to training specialists in the above area), and proposes a model of mandatory periodic attestation (re-attestation) of the personnel responsible for the critical infrastructure cybersecurity designed for step-by-step self-improvement of individuals through being gradually assigned the appropriate professional levels.

Key words: *cybersecurity, critical infrastructure facilities, periodic attestation (re-attestation), professional development, cybersecurity specialists.*

Постановка проблеми у загальному вигляді. В умовах розвитку інформаційних технологій та розбудови цифрового світу особливого значення набувають проблеми професійної підготовки спеціалістів ІТ-сфери, і перш за все фахівців із кібербезпеки.

Внутрішні та зовнішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах протидії збройній агресії російської федерації опікуються питаннями кібербезпеки, кіберзахисту, кібероборони, у тому числі у сфері захисту критичної інфраструктури.

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

Аналіз останніх досліджень і публікацій. Наукові напрацювання вчених засвідчують, що професійна підготовка фахівців, відповідальних за забезпечення кібербезпеки об'єктів 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, відповідальних за забезпечення кібербезпеки об'єктів критичної інфраструктури, є малодослідженими. Так, науковці С. Бєлай, І. Євтушенко та В. Мацюк у своєму дослідженні аналізують теоретико-методологічне підґрунтя щодо підготовки фахівців з реагування на кризові ситуації на об'єктах критичної інфраструктури Україні, надають пропозиції щодо розвитку спеціалізації «Захист критичної інфраструктури та її стійкість» та практичні рекомендації в контексті розвитку створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури щодо розвитку державно-приватного партнерства, а також проведення міжвідомчих командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять [1]. А кандидат юридичних наук 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 (2020 – 2021 роки) дослідження вищевказаних науковців, які стосуються питань підготовки фахівців у сфері захисту критичної інфраструктури, питанням основних теоретико-методологічних засад підготовки кадрів у зазначеній сфері приділено мало уваги, що й обумовило актуальність дослідження.

Виділення невирішених раніше частин загальної проблеми. Українська ІТ-індустрія як невід'ємна частина глобальної економіки безпосередньо залежить від навичок та знань фахівців, які працюють у галузі, а подальший фінансовий успіх – від кількості та якості кадрів. Тому розвиток кадрового потенціалу в Україні – одне з головних питань для представників вітчизняного ринку кібер-послуг. На теперішній час в галузі кібербезпеки, за різними оцінками, – більш ніж 120 тис. спеціалістів з розробки програмного забезпечення, а приріст спеціалістів, за неофіційними даними, становить близько 19% щороку [3, с. 5].

Сучасне суспільство характеризується стрімкими змінами в усіх сферах життя, що особливо впливає на розвиток освітянського простору. Освітня сфера нині зазнає значних трансформаційних процесів та вимагає нових та сучасних освітніх підходів. При цьому дієвим інструментом поліпшення якості освіти визначають застосування компетентнісного підходу до неї, який на перше місце ставить не поінформованість особи, а вміння на основі знань розв'язувати проблеми, які виникають у різних ситуаціях. Тому, з метою створення ефективної системи професійного розвитку фахівців із кібербезпеки, у тому числі відповідальних за забезпечення кібербезпеки об'єктів критичної інфраструктури, потрібно змінювати технологію освітнього процесу та підходи до його організації.

Метою статті є вивчення питання щодо обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури.

Виклад основного матеріалу. Інформаційно-комунікаційні технології у всьому світі визнані провідними технологіями XXI століття та є основними двигунами технологічного прогресу у найближчі десятиріччя. Інформатизація освітнього напрямку є частиною цього глобального процесу. Світова практика розбудови інформаційно-комунікаційних технологій в освіті показує тенденцію до зміни звичних форм організації та забезпечення освітнього процесу в умовах стрімкого розвитку інформаційного суспільства. За таких умов змінюється зміст самої освіти, різноманітні методики та підходи до її організації. Перш за все це стосується кіберосвіти, яка має тенденцію до постійних змін та потребує удосконалення відповідно до вимог сучасного інформаційного суспільства.

Не дивлячись на існуючі дослідження з питань кіберосвіти, професійної підготовки фахівців із кібербезпеки, кіберзахисту, кібероборони, окремі аспекти залишаються висвітленими не повною мірою, зокрема: дослідження кваліфікаційних напрямів підготовки спеціалістів у галузі кібербезпеки; розробка професійного стандарту для фахівців з кібербезпеки; наукові підходи і принципи формування кадрового забезпечення фахівців ІТ-галузі; запровадження обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури тощо. За таких умов проблема професійної підготовки фахівців із кібербезпеки набуває особливої актуальності, а її розв'язання потребує ґрунтовних змін у системі освіти.

Рівень підготовки таких фахівців повинен відповідати не лише сучасним потребам, але й забезпечити здатність спеціалістів із кібербезпеки адаптуватися в процесі змін у різних сферах діяльності, знаходити рішення у різноманітних ситуаціях, неупереджено і творчо мислити. Зазначене потребує якісних змін, перш за все, у підготовці фахівців із кібербезпеки [4, с. 99].

У підготовці фахівців із кібербезпеки, у тому числі тих, хто опікується питаннями забезпечення кібербезпеки об'єктів критичної інфраструктури, зацікавлені як органи публічної влади, підприємства, установи та організації, так і складові сектору безпеки і оборони України. Ефективність їх підготовки потребує реформування системи вищої освіти в Україні на всіх рівнях, належної технологічної оснащеності закладів освіти та складових сектору безпеки і оборони України, а також залучення висококваліфікованих спеціалістів. Абсолютно очевидно, що задовольнити потребу в висококваліфікованих фахівцях в області забезпечення кібербезпеки об'єктів критичної інфраструктури можна тільки на основі комплексного використання всіх можливостей професійної освіти та професійного розвитку особи в контексті просування її по службі.

Сучасні підходи до забезпечення безпеки критичної інфраструктури враховують її нерозривний зв'язок з кібербезпекою, і усвідомлення цього факту знаходить своє відображення в національному законодавстві. З упевненістю можна стверджувати, що значення проблематики кібербезпеки у захисті критичної інфраструктури у подальшому буде лише збільшуватися.

Так, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [5], що був прийнятий Верховною Радою України 05 жовтня 2017 року, функціонування національної системи кібербезпеки забезпечується, у тому числі, шляхом проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури.

Крім цього, відповідно до Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 06 грудня 2017 року № 1009-р [6], одними із шляхів і способів розв'язання існуючих проблем у сфері захисту критичної інфраструктури, крім розроблення, виконання та перегляду програм забезпечення інформаційної безпеки та кібербезпеки, є створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури.

У розрізі предмета даного дослідження слід констатувати, що на сьогодні в державі відсутній окремий підзаконний нормативно-правовий акт, який би визначав порядок проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури. Зазначений факт суттєво знижує ефективність функціонування національної системи кібербезпеки в освітньому аспекті.

Необхідність підготовки спеціалістів у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури також добре усвідомлюється в багатьох провідних країнах світу. Так, наприклад у Франції питаннями пов'язаними із кібербезпекою об'єктів критичної інфраструктури опікується підрозділ з державного захисту та безпеки (англ., State Protection and Security – PSE), який діє при Генеральному секретаріаті з питань оборони та національної безпеки (фр., Secrйtariat Gйnйral de la Dйfense et de la Sйcuritй Nationale, SGDSN). Зазначений підрозділ крім планування безпекових заходів займається питаннями навчання та розробки технологій безпеки, в тому числі стосовно сфери захисту критичної інфраструктури.

А в Іспанії, враховуючи напрямки глобальної політики безпеки та ініціативу Європейського Союзу щодо захисту критичної інфраструктури, був створений Національний центр розвідки, який є важливим підрозділом для захисту критичної інфраструктури. Даний центр відповідає за забезпечення кібербезпеки інформаційно-комунікаційних систем державних адміністрацій та тих, хто обробляє, зберігає або передає секретну інформацію, проведення технологічно-криптографічних досліджень, а також навчання персоналу з питань безпеки.

Узагальнення освітніх підходів щодо забезпечення кібербезпеки об'єктів критичної інфраструктури у різних провідних державах дозволяє сформувати думку про те, що владні органи зазвичай приділяють досить важливу увагу процесу навчання та підготовці фахівців у зазначеній сфері.

Забезпечення необхідного рівня кібербезпеки об'єктів критичної інфраструктури в освітній сфері має бути засновано на створенні нормативно-правової і термінологічної бази у цій сфері, періодичному проведенні різноманітних навчань щодо реагування на можливі надзвичайні ситуації та інциденти у кіберпросторі, підвищенні інформаційної грамотності персоналу та культури безпекового поводження в кіберпросторі, піднятті комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, а також на гармонізації відомчих нормативних документів з питань проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури.

Враховуючи зазначене, з метою розвитку підготовки кадрів з питань захисту та забезпечення стійкості критичної інфраструктури, необхідним є введення відповідного механізму, що можна зробити шляхом впровадження моделі проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури (рис. 1), яка складена на основі деяких компонентів оцінювання військовослужбовців, що впроваджені в службову діяльність Державної служби спеціального зв'язку та захисту інформації України.

Розроблений механізм професійного і особистісного зростання у порядку просування по службі, який покладено в основу моделі проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, забезпечує потребу у кваліфікованому персоналі у сфері кібербезпеки та найбільш ефективно використовує його потенціал шляхом побудови службової (військової) кар'єри.

Суттю успішної кар'єри фахівця із кібербезпеки є позитивна динаміка професійного розвитку особи в контексті проходження її по службі, що пов'язано з набуттям практики, навичок, досвіду, професіоналізму в межах відповідної посади й передбачає реалізацію особистісного потенціалу та досягнення відповідного рівня знань.

Професійний розвиток в свою чергу полягає в ефективному використанні потенціалу фахівців із кібербезпеки відповідно до потреб сектору безпеки і оборони України, з одного боку, та забезпечення потреб кожної особи-

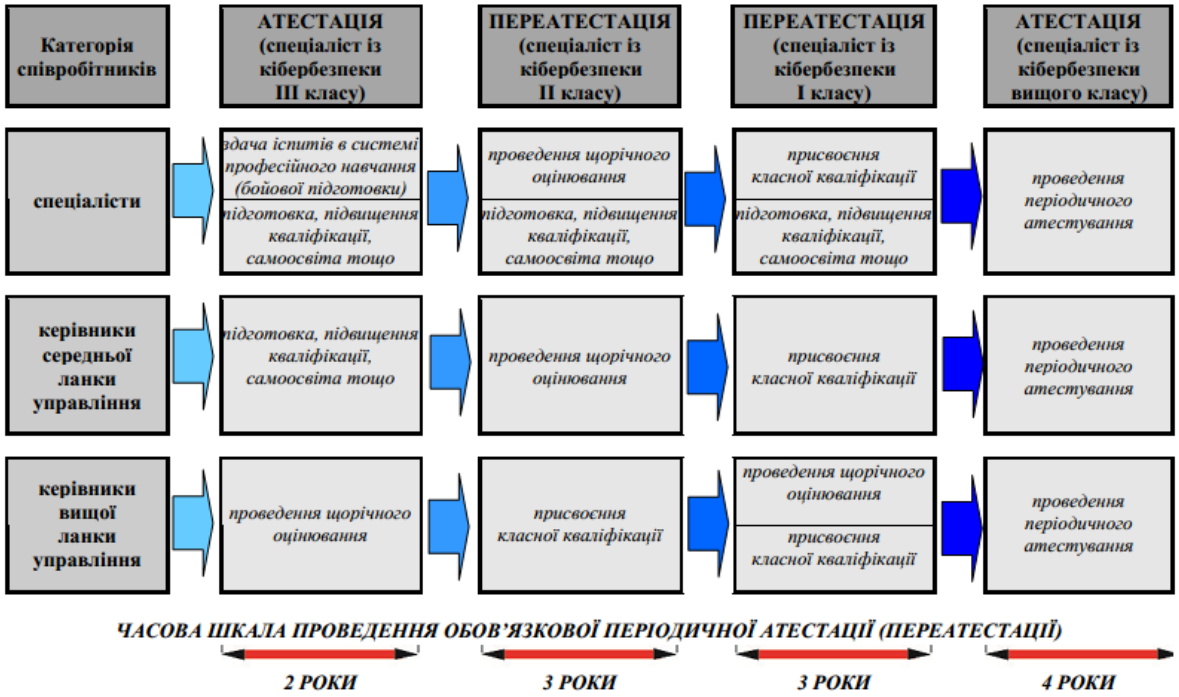

Рис. 1. Модель проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури

Розробив автор

стості, розвитку в неї мотивації до реалізації свого потенціалу, з іншого боку.

Професійний розвиток передбачає поступове самовдосконалення особистості шляхом поетапного присвоєння відповідного фахового рівня (спеціаліст із кібербезпеки III класу, спеціаліст із кібербезпеки II класу, спеціаліст із кібербезпеки I класу, спеціаліст із кібербезпеки вищого класу) через проведення обов'язкової періодичної атестації (переатестації) персоналу.

Фаховий рівень спеціаліста із кібербезпеки III класу передбачає уміння запобігати проявам несанкціонованого втручання у функціонування об'єктів критичної інфраструктури; прогнозувати та запобігати кризовим ситуаціям на об'єктах критичної інфраструктури; попереджувати кризові ситуації, що порушують безпеку критичної інфраструктури.

Фаховий рівень спеціаліста із кібербезпеки II класу присвоюється у разі набуття вмінь розробляти нормативно-правові та нормативно-технічні документи з питань забезпечення безпеки об'єктів критичної інфраструктури, державні цільові програми із захисту критичної інфраструктури, заходи з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури.

Фаховий рівень спеціаліста із кібербезпеки I класу надається після опанування питань пов'язаних із встановленням обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, у тому числі під час створення та прийняття в експлуатацію; можливістю здійснювати аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури; розробленням методології аналізу результативності державної політики у сфері захисту критичної інфраструктури.

Фаховий рівень спеціаліста із кібербезпеки вищого класу передбачає майстерність розробляти та забезпечувати виконання заходів щодо захисту і забезпечення стійкості критичної інфраструктури, протидії загрозам, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об'єктах критичної інфраструктури.

Якість теоретичної та практичної підготовленості військовослужбовців до виконання завдань за призначенням, а також поетапне присвоєння відповідного фахового рівня шляхом проведення обов'язкової періодичної атестації (переатестації) особового складу забезпечується проведенням відповідних контрольно-оцінювальних заходів. До таких заходів слід віднести:

– для спеціалістів (провідних, головних спеціалістів, інженерів, фахівців із захисту інформації тощо) – здача іспитів в системі професійного навчання (бойової підготовки), підготовка, підвищення кваліфікації, самоосвіта тощо, проведення щорічного оцінювання, присвоєння класної кваліфікації, проведення періодичного атестування;

– для керівників середньої ланки управління (начальники секторів, відділів, управлінь та їх заступники у складі окремих структурних підрозділів) – підготовка, підвищення кваліфікації, самоосвіта тощо, проведення щорічного оцінювання, присвоєння класної кваліфікації, проведення періодичного атестування;

– для керівників вищої ланки управління (начальники окремих центрів, управлінь, департаментів та їх заступники) – проведення щорічного оцінювання, присвоєння класної кваліфікації, проведення періодичного атестування.

Контрольно-оцінювальні заходи також мають свої особливості. Вони проводяться в умовах постійної службової готовності, характеризуються різко вираженою практичною направленістю та знаходяться здебільшого в безпосередній залежності від технічних можливостей того чи іншого підрозділу.

Професійне навчання (бойова підготовка) – це організований за відповідним планом щорічний процес навчання (навчально-виховних заходів), який спрямований на підтримання на належному рівні набутих знань та удосконалення практичних навичок, а також забезпечення підвищення рівня професійної підготовки особового складу для якісного та ефективного виконання службових обов'язків.

Підготовка, підвищення кваліфікації, самоосвіта тощо особового складу в свою чергу передбачає набуття нових та/або вдосконалення раніше набутих знань, практичного досвіду виконання завдань та обов'язків у службовій діяльності, оновлення, розширення і формування нових професійних знань у сфері захисту критичної інфраструктури, кібербезпеки, кіберзахисту, кібероборони тощо.

Щорічне оцінювання передбачає визначення якості виконання військовослужбовцем своїх завдань та обов'язків, визначених у посадових інструкціях, професійного рівня, особистої дисциплінованості, вимогливості до себе та підлеглих, добротності роботи щодо удосконалення знань та навичок тощо.

Класна кваліфікація відповідного класу є показником, що відповідає певному рівню майстерності та фахової підготовки військовослужбовця до виконання ним завдань за призначенням і присвоюється за результатами складання відповідних іспитів.

Атестування військовослужбовців проводиться для забезпечення правильного добору, розстановки, виховання і вдосконалення підготовки військових кадрів шляхом об'єктивного оцінювання професійного рівня, ділових та моральних якостей кожного військовослужбовця, відповідності їх посаді, визначення перспективи службового використання, створення резерву кандидатів для просування по службі [7].

Таким чином контрольно-оцінювальні заходи орієнтовані на визначення індивідуального розвитку кожного фахівця із кібербезпеки. При цьому досягнення таких фахівців поєднують характеристики, що відображають об'єктивні результати пізнавальної діяльності – знання, уміння, навички, досвід, предметні компетентності тощо. Звісно, такі подальші нововведення можливі тільки після ефективних нормативно-правових змін у відповідних актах.

Необхідно також відмітити, що для участі в обов'язковій періодичній атестації (переатестації) фахівець із кібербезпеки визначає для себе правила і стиль поведінки, які є допоміжними в його професійному розвитку. До зазначених правил і стилів належать: розуміння власних сильних і слабких сторін; постійне підвищення свого професійного рівня; відповідальність за доручену справу; вміння розставляти пріоритети і розраховувати час; відстоювання власних поглядів; сприйняття конструктивної критики та формування правильних висновків [4, с. 103].

Крім цього, проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, надасть змогу:

– спеціалістам – оволодіти системністю і аналітичним мисленням, умінням прогнозувати розвиток ситуації та мислити масштабно і реалістично одночасно, комунікативними вміннями, навичками ефективної міжособистісної взаємодії;

– керівникам середньої ланки управління – опанувати здатність до прийняття самостійних рішень, уміння розв'язувати нестандартні проблеми і виконувати складні завдання, прагнути до постійного підвищення професіоналізму, реалістичного сприйняття своїх здібностей і можливостей, самоповаги;

– керівникам вищої ланки управління – розвивати і розширювати особистісно орієнтовану спрямованість (особисті цілі та інтереси, індивідуальні потреби, цінності й мотиви), формувати необхідні якості лідера, формувати професійні компетентності у підлеглого особового складу.

Висновки. Впровадження у службову діяльність моделі проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури надасть змогу:

– створити сучасну єдину та гнучку систему професійного розвитку;

– забезпечити якість та безперервність набуття відповідного досвіду;

– створити належні умови для реалізації права на професійне зростання;

– забезпечити розвиток професійної компетентності;

– створити умови для конкуренції серед співробітників.

Таким чином, в світлі реалізації положень Закону України «Про основні засади забезпечення кібербезпеки України» та Концепції створення державної системи захисту критичної інфраструктури актуальною є необхідність впровадження моделі проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури у службову діяльність зацікавлених органів публічної влади, підприємств й організацій України, у тому числі в органах і підрозділах що входять до складу сектору безпеки і оборони України.

Завдяки своїй новизні дане дослідження має перспективу подальшої інтеграції його результатів у розвиток української професійної освіти з підготовки фахівців у галузі кібербезпеки та продовження на шляху удосконалення системи української освіти [4, с. 104].

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. Подальший розвиток системи професійного навчання фахівців із кібербезпеки в умовах розвитку цифрових технологій. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2022. Вип. 3. С. 3–13.

4. Арсенович Л. А. Модель професійного розвитку фахівця з кібербезпеки (на прикладі Державної служби спеціального зв'язку та захисту інформації України). *Вісн. НАДУ. Серія «Державне управління».* 2019. № 4 (95). С. 98–104.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жов. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.02.2023).

6. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06 груд. 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 05.02.2023).

7. Про Положення про проходження військової служби (навчання) військовослужбовцями Державної служби спеціального зв'язку та захисту інформації України : Указ Президента України від 31 лип. 2015 р. № 463/2015. URL: https://zakon.rada.gov.ua/laws/show/463/2015#Text (дата звернення: 05.02.2023).