DOI 10.20535/2411-1031.2021.9.2.249976
УДК 004.056.53::378.1

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

АНАЛІЗ КЛЮЧОВИХ ЧИННИКІВ ФОРМУВАННЯ СИСТЕМИ КОМПЕТЕНТНОСТЕЙ ФАХІВЦІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Показано, що побудова усталеної системи кібербезпеки держави в умовах глобалізації, розвитку інформаційних технологій, перенесення “гібридних війн” у кіберпростір, потребує підвищення якості підготовки фахівців, від яких залежить надійність захисту національного кіберпростору. Уточнено, що ключовим показником кваліфікації фахівців в галузі кібербезпеки є компетентності, але їх остаточне визначення і актуальне наповнення, відповідно до вимог швидкоплинного техніко-технологічного розвитку, потребує обґрунтування теоретичних засад, що становлять об’єкт дослідження. Обґрунтовано, що суттєвою складовою теоретичних основ визначення системи компетентностей є сукупність чинників, що зумовлюють її конституювання та визначають предмет і мету дослідження. Ключовими факторами, що потребують врахування у визначенні професійних компетентностей визначено такі: вимоги сучасної системи освіти; системний характер процесів, що розгортаються в глобальному кіберпросторі; концептуальні засади кібербезпеки; швидкий розвиток інформаційних технологій та перехід на квантову основу; нові загрози національної безпеці, що виникають з конвергенції інформаційних і новітніх технологій; кібератаки, спрямовані на державні установи і структури національної безпеки; спроби деструктивного психологічного впливу на особовий склад сектору безпеки і оборони; курс України на євроатлантичну інтеграцію, узгодження національної системи стандартів із стандартами НАТО в сфері забезпечення кібербезпеки; підвищення ризикогенності професійної діяльності; виклики ґендерної політики щодо досягнення ґендерної рівності у сфері безпеки і оборони України. Отже потрібно зауважити, що навчання фахівців у галузі кібербезпеки в інтересах майбутнього країни, має базуватися на методологічно обґрунтованій системі компетентностей, впровадження яких, має зумовлювати якісну підготовку до професійнійної діяльності у галузі кібербезпеки держави.

Ключові слова: кібербезпека, кіберпростір, кіберзагроза, освіта, компетентність, підготовка фахівців, євроатлантичні стандарти.

Постановка проблеми. Ефективність, сталість і захищеність державного кіберпростору є важливим чинником надійного забезпечення національної безпеки, передумовою сталого інформаційного розвитку Української держави [1]. В умовах проведення операції Об’єднаних сил, розв’язання проблеми вдосконалення національної системи кібербезпеки і забезпечення надійного захисту національного кіберпростору, постає найактуальнішим завданням теорії і практики забезпечення національної безпеки України [2]. Одним з впливових чинників розв’язання цієї проблеми є підготовка фахівців у галузі кібербезпеки, компетентності яких відповідають сучасним реаліям і потребам держави [3]. Питання надійного захисту національного кіберпростору багато в чому залежить від адекватного визначення і впровадження в освітню практику системи компетентностей в галузі кібербезпеки.

Аналіз останніх досліджень і публікацій. Питання підготовки фахівців в галузях захисту інформації та кібербезпеки було розкрито у [3] – [7]. Безпосередньо, завдання методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони вирішувалось в [3]. Питання аналізу професійних компетентностей і шляхів підвищення якості підготовки фахівців з кібербезпеки в інтересах сектору безпеки і оборони розкриті в [4], [5]. Аналіз змісту ключових компетентностей Європейської довідкової рамки та впровадження компетентнісної парадигми в освіті зроблено у працях [6], [7]. Але питання відповідності професійних компетентностей

вимогам швидкоплинного техніко-технологічного розвитку потребують більш глибокого і системного вивчення. Актуальними є розроблення і обгартування теоретичних положень побудови системи компетентностей як визначальних вимог підготовки фахівців у галузі кібербезпеки. Розв'язання поставленої проблеми, в першу чергу, потребує з'ясування принципових засад її розроблення і впровадження в практику підготовки фахівців з кібербезпеки.

Метою статті є визначення і обґрунтування ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки.

Виклад основного матеріалу дослідження. Глобалізаційний вплив на кіберпростір, що проявляється у інтернаціоналізації кіберзлочинності, кібертероризму, домінуванні зовнішньої інформаційній експансії, виникненні нових кіберзагроз, свідчить про підвищення ролі кібербезпеки у забезпеченні національної безпеки будь якої держави. Необхідність надійного захисту національного кіберпростору України, особливо в умовах прагнення до євроатлантичної інтеграції та проведення операції Об'єднаних сил, вимагає якісної підготовки фахівців в галузі кібербезпеки [3], [4]. Глобалізація інформаційного простору, розвиток комунікаційної інфраструктури та новітніх технологій значною мірою впливають на визначення компетентностей, що зумовлюють спрямованість і якість підготовки фахівців, які забезпечують захист кіберпростору держави.

Актуальність якісної підготовки фахівців в галузі кібербезпеки, в цей важкий для України час соціально-політичних і військових випробувань, є очевидною і стає одним з провідних чинників забезпечення національної безпеки [4], [5]. Проте, деякі питання відповідності змісту професійних компетентностей вимогам інформаційного і технологічного розвитку потребують більш глибокого і системного вивчення. Це пов'язано, перш за все, з всебічним розумінням і усвідомленням процесів, що розгортаються в сучасному глобальному кіберпросторі та його конкретних секторах, переходом інформаційних технологій на квантову основу, новими можливостями впливу новітніх інформаційних технологій на національну безпеку, що зумовлює необхідність формування у майбутніх фахівців відповідних компетентностей. У зв'язку з розвитком галузі кібербезпеки, розширенням відповідних функцій Державної служби спеціального зв'язку та захисту інформації України, формуванням нової нормативної бази стандартів, виявляється низка освітніх завдань, спрямованих на введення, з'ясування, розкриття, засвоєння нових знань, понять і термінів в систему підготовки фахівців для Держспецзв'язку.

Компетентнісний підхід, що використовується в сучасній системі освіти і акцентує увагу на необхідності застосування здобувачем, набутих знань, навичок і умінь на практиці, набуває свого розвитку і закріплюється в педагогічних освітніх системах, як результативно-цільова спрямованість навчання фахівця. В умовах глобалізаційних і технологічних трансформацій сьогодення компетентнісний підхід перетворився на філософію, яка формує інноваційне бачення освіти, фундаментальних принципів її розвитку [6].

Досліджуючи питання загальної компетентності людини у професійній діяльності, науковці, поряд з власно професійними компетентностями, зазначають низку таких характеристик [5]: здатність працювати самостійно без постійного керівництва; здатність брати на себе відповідальність за власною ініціативою; здатність виявляти ініціативу, не питаючи інших, чи слід це робити; готовність помічати проблеми та шукати шляхи їх вирішення; уміння аналізувати нові ситуації й застосовувати вже наявні знання для такого аналізу; здатність знаходити спільну мову з іншими; здатність засвоювати будь-які знання за власною ініціативою; уміння приймати рішення на основі здорових суджень. Високий рівень компетентності як результат професійного розвитку передбачає гармонійне поєднання інтелектуальних компетенцій (здібності до продуктивної аналітичної діяльності), соціальних компетенцій (громадянської грамотності) й особистісних (здатності до спілкування, рефлексії, готовності до самоосвіти впродовж усього життя) [7].

Провідним комплексним показником якості підготовки фахівців у галузі кібербезпеки є професійні і соціальні компетентності Відповідно до [8], компетентність розуміється як

динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність. Системо-організуючі засади професійних і соціальних компетентностей майбутніх фахівців з кібербезпеки визначаються, перш за все, призначенням Держспецзв'язку [9], що полягає в забезпеченні функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формуванні та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України.

Згідно зі стандартом вищої освіти України за спеціальністю 125 Кібербезпека, інтегральну компетентність визначено як здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. Конкретно визначено 7 загальних і 12 фахових компетентностей, яким має відповідати спрямованість підготовки бакалавра [10].

Отже, постає запитання, з одного боку, про відповідність визначених стандартів сучасним вимогам кібербезпеки з огляду на технологічні і нормативні зміни її забезпечення, з іншого, – про змістовну складову освіти фахівців, що має відповідати встановленим стандартам і відповідність спрямованості підготовки фахівців встановленим вимогам. *Методологічною умовою* розв'язання цього питання пропонується застосування методу факторного аналізу, як складової системного підходу, що розглядається як виявлення і аналіз комплексу провідних чинників, що суттєво впливають на сферу функціональної відповідальності посадових осіб в галузі кібербезпеки та успішність виконання завдань за призначенням.

Одним із найбільш впливових системних чинників, що потребують врахування при з'ясуванні фахових компетентностей в галузі кібербезпеки, є швидкий розвиток інформаційно-телекомунікаційних технологій та відповідні зміни в ставленні до галузі охоплення понять кібербезпеки. Це викликає феномен упередження технологічних змін в кіберпросторі, науковому розробленню способів його захисту. Таке упередження зумовило необхідність переосмислення обсягу поняття кібербезпеки з відповідним розширенням його змісту та змінами в галузі забезпечення [11]. Під час створення Закону "Про основні засади забезпечення кібербезпеки України" забезпечення кібербезпеки розглядалось як окрема вузька галузь інформаційної безпеки, поряд з іншими її складовими, функціонування якої обмежувалось законом певними рамками [12]. Однак, останні дослідження свідчать про тенденцію розширення змісту завдань забезпечення кібербезпеки [3], [11], аж до її ототожнення з інформаційною безпекою, що потребує відповідного розширення обсягу компетентностей для фахівців цієї галузі.

З огляду на тенденцію застосування у наукових працях і нормативних документах, зокрема, у згаданому стандарті вищої освіти [10], понять "інформаційна безпека" і "кібербезпека" як тотожних, необхідно звернути увагу на їх змістовну різницю. З погляду на сферу охоплення, поняття інформаційної безпеки не обмежується кіберпростором, але поряд з ним, розповсюджується на область функціонування засобів масової інформації і публічну інформаційну сферу. Предметна характеристика інформаційної безпеки містить більш широкий спектр питань, зокрема, щодо забезпечення позитивного іміджу держави на міжнародному рівні, інформаційних прав і свобод її громадян, інформаційного суверенітету, інформаційно-психологічного протиборства, здійснення правоохоронної та контррозвідувальної діяльності з цих питань [3]. З погляду на об'єкт захисту, інформаційна безпека, поряд із захистом інформації у телекомунікаційних системах, спрямована на захист взагалі всіх інформаційних ресурсів держави, життєво важливих інформаційних інтересів людини і суспільства, а в контексті впливу інформації та інформаційних технологій на людину, – колективну та індивідуальну свідомість. З погляду на способи забезпечення безпеки, у дослідженнях [13], поряд з криптографічними, техніко-технологічними та організаційними способами захисту інформації, зауважується на необхідності протидії

інформаційним загрозам у контексті їх негативного впливу на свідомість і пропонується розв'язання проблем захисту інформаційного простору в ідеологічному, психологічному і правовому ключі.

Тобто, у межах загального об'єкту забезпечення інформаційної безпеки – інтересів людини, суспільства і держави, в наукових працях, в одному випадку, пропонується розглядати предметом захисту інформаційні ресурси і телекомунікаційні системи держави, в іншому, – індивідуальну, суспільну, національну свідомість та інтереси громадян [13]. Теоретичне розв'язання означеного протиріччя між інформаційно-психологічним та техніко-технологічним аспектами інформаційної безпеки має важливу теоретичну і практичну значущість для сталого функціонування національної безпеки як цілісної системи і має враховуватись при визначенні компетентностей фахівців в галузі кібербезпеки. Але це завдання може бути вирішено за умов застосування системного підходу до забезпечення інформаційної безпеки України [14], [15].

На думку фахівців [16], запроваджені у 2016 році зміни у стандартах освіти, призвели до об'єднання чотирьох спеціальностей в одну, що робить неможливим та і недоцільним у межах однієї спеціальності "Кібербезпека" надати різнопланові основні знання та вміння, які необхідні фахівцям колишніх трьох спеціальностей галузі знань "Інформаційна безпека" та спеціальності "Криптологія". З огляду на зазначене, пропонується внесення відповідних змін до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Це дозволить охопити базові аспекти підготовки фахівців з інформаційної та кібербезпеки та буде відповідати сучасним викликам та потребам в сфері забезпечення кібербезпеки та інформаційної безпеки, включаючи необхідні спеціалізації з врахуванням вимог постквантового періоду. Перехід на інформаційні технології постквантового періоду потребує перегляду теоретичних і технологічних основ захисту інформації в телекомунікаційних системах і відповідного перегляду стандартів, відображення у компетентностях фахівців та змістовної складової навчання. Це також стосується перегляду способів криптографічного захисту інформації в кіберпросторі, що викликає необхідність уточнення відповідних компетентностей [16].

Важливою умовою набуття компетентностей здобувачами є практична підготовка. Зауважуючи питання значущості практичної підготовки фахівців у галузі захисту інформації та кібербезпеки, Заступник Голови Держспецзв'язку Олександр Потій наголошує на необхідності налагодження партнерських відносин між навчальними закладами та промисловістю, надання можливості студентам проходити на базі органів державної влади або приватних структур, тренінгів для підвищення своїх навичок у галузі кібербезпеки. Іншою умовою, коригуючою зміст фахових компетентностей, закріплених в освітніх програмах, на думку Олександра Потія, є розробка класифікатора професій кібербезпеки і захисту інформації. "Якщо ми проробимо і законодавчо закріпимо класифікатор професій, відповідальності фахівців, які працюють в цих галузях, тоді і закладам освіти буде простіше розробляти відповідні освітні програми, що сприятиме підготовці майбутніх спеціалістів", – резюмує він [16].

Отже, у розробленні фахових компетентностей потрібно чітко відгалужувати змістовну частину компетентностей з кібербезпеки від компетентностей в сфері інформаційної безпеки. І це відокремлення має відбуватися за принциповими відмінностями предмету захисту і способів забезпечення безпеки.

Революційним документом, з огляду на запропоновані новації з забезпечення кібербезпеки, стала Стратегія кібербезпеки України (2021–2025 роки) "Безпечний кіберпростір – запорука успішного розвитку країни", в якому, на засадах стримування, кіберстійкості та взаємодії, ґрунтовно окреслено коло умов для безпечного функціонування кіберпростору України на 2021–2025 роки [2]. У документі визначено концептуальні підходи до подальшого розвитку національної системи кібербезпеки, які базуються на аналізі цифрового середовища, глобальних трендів середовища з кібербезпеки, захисту національних інтересів України; перманентності заходів щодо вдосконалення законодавства у сфері

кібербезпеки; запровадженні механізмів державно-приватного партнерства у сфері забезпечення кібербезпеки; проактивному підході, що передбачає вжиття превентивних заходів. Врахування визначених базових засад Стратегії кібербезпеки України є однією з умов, яким мають відповідати професійні компетентності фахівців.

Актуальність розробки і формування професійних компетентностей фахівців з кібербезпеки підвищується з огляду на стратегічний курс України до членства в ЄС і НАТО, що задекларовано на офіційному сайті Альянсу в березні 2018 р., коли Україна була внесена до списку країн-партнерів. В 2020 р. Північноатлантична рада визнала Україну членом Програми розширених можливостей НАТО. Однією з умов членства в НАТО є впровадження загальних стандартів. Отже, необхідною складовою підготовки військових фахівців в галузі кібербезпеки, постає опанування нормами і стандартами діяльності із забезпечення системного захисту інформації та кібербезпеки, які застосовуються не тільки в Україні, але і в країнах – членах ЄС і НАТО, що має бути враховано при розробленні компетентностей для фахівців з кібербезпеки.

Стандарти НАТО – "Угода зі стандартизації" (від англ. Standardization Agreement; STANAG) покликані забезпечувати взаємодію між видами збройних сил різних країн для досягнення взаємосумісності. Система стандартів НАТО включає в себе союзні стандарти – власне стандарти НАТО (АР – Allied Publications, МР – Multinational Publications) та стандарти окремих держав-членів НАТО. Стандарт НАТО (АР) – це документ, що встановлює нормативні вимоги, призначені для безпосереднього застосування органами військового управління країн-учасниць Альянсу, конкретними організаціями та підрозділами. Стандарти ухвалюються консенсусом і можуть бути реалізовані повністю або частково, із зауваженнями або без. На даний час існує близько 2 тис. окремих стандартів. "Угода зі стандартизації" (англ. Standardization Agreement; STANAG) – міжнародний договір, який регламентує загальні правила, визначає спільний порядок дій, закріплює єдину термінологію і встановлює умови уніфікації технічних процесів, а також озброєння та військової техніки, іншої матеріальної частини збройних сил Альянсу та країн-партнерів. Угода зі стандартизації може охоплювати один або декілька стандартів. Поряд з Угодами про стандартизацію STANAG, останнім часом в НАТО набуває поширення практика розробки стандартизованих рекомендацій STANREC, відносною перевагою яких вважають відсутність потреби у ратифікації [17].

Стандарти НАТО об'єднані в складну і взаємопов'язану ієрархію керівних документів Альянсу, що мають утворювати певну систему. Стандарти умовно поділяються на адміністративні, оперативні, матеріально-технічні та соціальні. Адміністративні стандарти визначають процеси управління та обміну інформацією, систему адміністративних взаємовідносин і керівних компетентностей, відповідальність, порядок роботи з документацією. Оперативні стандарти спрямовані на оперативне планування застосування військ або сил. Матеріально-технічні стандарти визначають єдині вимоги до озброєння і військової техніки союзників, управління життєвим циклом, кодифікації обладнання. Соціальні стандарти призначені для регулювання норм соціальних відносин і взаємодії, гарантування захисту прав людини, розв'язання гендерних питань у військових колективах [17].

Основними вимогами національного нормативного забезпечення в галузі безпеки інформації та кібербезпеки, що потребують врахування у підготовці фахівців, є впровадження гармонізованих стандартів з проектування та оцінки безпеки систем інформаційних технологій серії ISO/IEC 15408 та стандартів системи управління інформаційною безпекою серії ISO/IEC 27к, що забезпечують надійність і стійкість захисту інформації. Поряд із зазначеними вимогами національного нормативного забезпечення в галузі кібербезпеки з гармонізації стандартів, важливим є ознайомлення із моделлю забезпечення безпеки інформації на основі серії стандартів NIST SP 800 Національного інституту стандартів та технологій США.

З метою досягнення цілей партнерства у військових структурах сил безпеки і оборони України впроваджуються і гармонізуються такі соціальні стандарти НАТО: STANAG 7196

(SERE) – підготовка з питань виживання в екстремальних умовах та полоні; STANAG 6001 – мовна підготовка особового складу; STANAG 2222 та STANAG 600 – підготовка військових капеланів; STANAG 7226 – підготовка з питань правил поводження після захоплення в полон (CAC); стандарти спеціальної психологічної підготовки особового складу для кожного роду військ [18]. Питання впровадження стандартів НАТО в сфері забезпечення кібербезпеки, організації взаємодії, проведення експертиз та акредитації потребує внесення відповідних нормативно-правових організаційних змін і, головне, потребує підготовки компетентних фахівців.

Таким чином, опанування військовими і соціальними стандартами, прийнятими в країнах – членах НАТО, починаючи з фахових вимог із забезпечення кібербезпеки і закінчуючи етичними нормами взаємовідносин і поведінки у військових колективах, стає окремою ланкою вимог військової освіти.

Ішим фактором, що потребує врахування при розробленні компетентностей фахівців в галузі кібербезпеки є принципове положення Стратегії кібербезпеки України (2021–2025 роки), про необхідність врахування шостого технологічного укладу, що характеризується тенденцією конвергенції біо-, нано-, інфо-, когнотехнологій з технологіями штучного інтелекту та характеризується ризиками, з якими стикається цивілізація внаслідок їх провадження і використання у кіберпросторі [2]. Значущість інформаційної безпеки посилюється завдяки поєднанню сучасних інформаційних і мережевих технологій з гуманітарними технологіями, спрямованими на маніпулювання колективною свідомістю [19], кіберризиками, породженими поєднанням виробничого і мережевого середовищ шляхом використання кіберфізичних виробничих систем [20].

Синергетична взаємодія нанонаук, генної інженерії, інформаційних і новітніх гуманітарних технологій все більш радикально змінює людину, трансформуючи її власно людську природу, попереджують науковці [21]. Отже, домінуючий неконтрольований вплив сучасного інформаційного середовища на свідомість фахівців, діяльність яких пов’язана із захистом кіберпростору України, може мати негативні наслідки в їх професійній справі. Сучасні можливості інформаційних технологій, що забезпечують доступність і великі обсяги інформації, з одного боку, і неусвідомлена спрямованість людини на опанування нею, з іншого, можуть сприяти формуванню поверхневого, безсистемного знання, коли втрачається зв’язок між отриманим знанням і майбутньою професійною діяльністю, загублюється цінність і значущість знання, пов’язаного із захистом інформаційного простору України.

Сучасні глобальні зміни, що супроводжуються підвищенням ризикогенності професійної діяльності, обумовлюють необхідність переосмислення значущості безпекової складової у підготовці фахівців до діяльності в ситуаціях підвищеного ризику. Потреба у впровадженні в систему підготовки фахівців з кібербезпеки, поряд із спеціальними знаннями, теоретичних знань про національну безпеку, з відповідною кореляцією світоглядних настанов зумовлена, також, посиленням проявів тероризму в світі та Україні, зростанням масштабів гуманітарних, технологічних, екологічних катастроф та відхиленнями у соціальній поведінці. У доповіді Римському клубу Лін Речел Андерсен (2020) зазначено, що для вирішення екзистенційних криз, таких як кліматичні зміни, масове вимирання видів, сервільний капіталізм, штучний інтелект, тероризм, зростаюча нерівність та фінансовий крах, пандемій, таких як COVID-19, – нам потрібна освіта [22]. Важливим завданням освіти, згідно з вимогами “Національної стратегії розвитку освіти в Україні на період до 2021 року”, є розвиток інноваційного мислення, орієнтованого на майбутнє, на комплексне вирішення проблем суспільства. У такому контексті, одним з головних завдань освіти постає формування у майбутнього фахівця не тільки фахових компетентностей, але і здатностей превентивного мислення, антикризової поведінки, відповідальності за можливі наслідки прийнятих рішень.

Згідно з окресленими компетентностями у контексті адаптації до безпекових потреб, важливим завданням підготовки фахівців є формування таких здатностей [13]: комплексна (професійна, інтелектуальна, моральна, психологічна, фізична) готовність фахівця до діяльності в умовах зростаючого ризику, воєнних, техногенних і гуманітарних загроз; прогнозування, попередження і подолання імовірних небезпек у професійній, службовій

діяльності; здійснення самостійного, адекватного і відповідального вибору у прийнятті рішення в критичних професійних ситуаціях; критична оцінка і врахування небезпечних наслідків власної професійної діяльності й прийнятих рішень; самостійного пошуку і відпрацювання наукових джерел для систематичного оновлення власних знань з безпеки і сталого людського розвитку з метою загальнотеоретичного і професійного самовдосконалення.

Отже, проблема поєднання інформаційних і новітніх гуманітарних технологій виводить на проблематику формування компетентностей із забезпечення індивідуальної і колективної безпеки, здатностей передбачення і попередження технологічних і соціальних ризиків, з'ясування моральних регулятивів службової і професійної діяльності, базисних цінностей підготовки фахівців кібербезпеки.

Іншим суттєвим чинником, що потребує врахування у системі компетентностей фахівців у галузі кібербезпеки, є виклики ґендерної політики, стосовно організації службової і професійної діяльності в секторі безпеки і оборони згідно із світовими стандартами досягнення ґендерної рівності. Рівність прав та можливостей жінок та чоловіків, зокрема, у сфері безпеки і оборони України є засадничою складовою сприйняття світу, що впливає на світогляд та утворює соціально-психологічні підстави організації службової діяльності у військових колективах. Згідно з вимогами Резолюції Ради Безпеки ООН 1325 "Жінки. Мир. Безпека" [23] та її суміжних резолюцій, в Україні відбувається встановлення світових стандартів для досягнення ґендерної рівності [24]. Відповідно до Річної національної програми під егідою Комісії Україна-НАТО, ґендерна тематика має бути включена до системи підготовки особового складу сектору безпеки і оборони України.

Виклики ґендерної політики, щодо досягнення рівності у структурах сектору безпеки і оборони України, є надзвичайно актуальним питанням. Впровадження цього підходу у секторі безпеки та оборони має зумовлювати: підвищення довіри до Держспецзв'язку, Збройних Сил, та інших структур; розширення можливостей щодо протидії негативному інформаційному впливу противника, іншим гібридним загрозам; подолання ґендерних стереотипів, від яких страждають і жінки, і чоловіки; покращення соціальної та економічної інфраструктури для забезпечення рівних прав і можливостей жінок і чоловіків; створення умов для більшої збалансованості між сімейним та професійним життям [25].

Важливою умовою реалізації освітньої складової ґендерної політики у секторі безпеки і оборони є вимоги ґендерної компетентності до керівного і викладацького складу сектору безпеки і оборони України. Збільшення чисельності жінок Держспецзв'язку, Збройних силах України, їхня активна участь у захисті України від збройної агресії, необхідність врахування прав та інтересів усіх фахівців, зумовили потребу формування ґендерної компетентності працівників сектору безпеки і оборони та впровадження сучасної політики забезпечення рівних прав та можливостей жінок і чоловіків у всіх його структурних складових. У "Методичних рекомендаціях з інтеграції ґендерних підходів в систему підготовки фахівців для сектору безпеки і оборони України", надаються поради, стосовно змісту і впровадження засад ґендерної компетентності в процес підготовки військовослужбовців сектору безпеки і оборони [25].

Саме, знання механізмів формування ґендерних ролей та стосунків в суспільстві, вміння розпізнавати ґендерну нерівність та боротися із нею, забезпечуючи зміну дискримінаційних структур, є складовими ґендерної компетентності. Поряд із зазначеним, ґендерна компетентність містить [25]: знання про ґендерну політику і ґендерні політичні стратегії; про інструменти і практики використання ґендерного підходу; навички використання ґендеру як соціальної категорії, як спонукання до дій для всіх співробітників організації або особового складу підрозділу. Ґендерна компетентність вимагає, з одного боку, вміння пов'язувати отримані ґендерно диференційовані експертні знання з професійно-орієнтованими знаннями, що розглядається як експертна компетентність, з іншого – вміння використовувати різноманітні ґендерні аналізи в своїй галузі спеціалізації – методична компетентність. Крім того, вона пов'язана із соціальною компетентністю в конструктивному формуванні ґендерних відносин в організації, проявляється у здатності відображати особисті ґендерні ролі і ґендерні образи всередині організації, а також в оцінці особистих сильних і слабких сторін [25].

Узагальнюючи викладене, доцільно окреслити коло ключових чинників, що потребують врахування у визначенні професійних компетентностей. На погляд авторів, ними є: вимоги компетентнісної парадигми освіти як система принципів і теоретичних положень про інституалізацію системи компетентностей вищої освіти України; системний характер процесів, що розгортаються в сучасному глобальному кіберпросторі, його конкретних секторах і національному рівні; концептуальні зміни у підходах до розуміння змісту кібербезпеки і розширення функцій з її забезпечення; швидкий розвиток інформаційних технологій та їх перехід на квантову основу, що потребує врахування завдань з кіберзахисту постквантового періоду; загрози, що виникають із конвергенції інформаційних технологій з новітніми технологіями; участь в операції Об'єднаних сил, і необхідність реагування на кібератаки, спрямовані на державні установи і структури національної безпеки; спроби деструктивного психологічного впливу на особовий склад сектору безпеки і оборони; курс України на євроатлантичну інтеграцію, узгодження національної системи стандартів у кібербезпеки з стандартами НАТО і формування нової нормативної бази; сучасні глобальні зміни, що супроводжуються підвищенням ризикогенності професійної діяльності, вступ людства в період підвищеного соціального, екологічного і технологічного ризиків; виклики ґендерної політики щодо досягнення ґендерної рівності у сфері безпеки і оборони України і міжнародні вимоги до гендерної політики держави, стосовно гендерного інтегрування.

Наведений перелік актуальних чинників не є остаточним і передбачає можливість подальшого обговорення і доопрацювання в наукових і педагогічних колективах. Але він зосереджує увагу на ключових моментах сьогодення, що потребують врахування при внесенні змін в систему освітніх компетентностей фахівців з кібербезпеки.

Аналіз перелічених чинників вимагає орієнтуватись у підготовці фахівців, перш за все, на формування фахових і соціальних компетентностей, що відповідають вимогам професійної діяльності в сфері забезпечення кібербезпеки в умовах швидких технологічних змін, зростаючих ризиків і небезпек, які припускають спроможність фахівця приймати ефективні, відповідальні професійні і управлінські рішення в непередбачуваних умовах зростання ризику, враховуючи їх можливі соціальні наслідки.

Висновки. Потрібно зауважити, що навчання і виховання фахівців у галузі кібербезпеки в інтересах майбутнього країни має базуватися на методологічно обґрунтованій системі освітніх, професійних, соціальних знань, навиків, здібностей і вмінь, що утворюють сферу компетентностей, впровадження яких в освітній процес, має зумовлювати якісну підготовку до майбутньої професійній діяльності.

Акцентування уваги науково-педагогічних колективів на необхідності вивчення питання підготовки фахівців у контексті відповідності вимогам сучасного інформаційного техніко-технологічного розвитку, сприятимете ефективному розв'язанню проблем захисту національного кіберпростору, особливо в умовах проведення операції об'єднаних сил.

Питання захисту національного кіберпростору в умовах прагнення України до євроатлантичної інтеграції, вимагає подальших науково-теоретичних, законодавчих і освітніх зусиль у справі його надійного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] С. О. Гахов, "Кіберпростір як основна категорія науки кібернетика", *Сучасний захист інформації. Державний університет телекомунікацій*, № 1. с. 53-57, 2017. [Електронний ресурс]. Доступно: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1412. Дата звернення: Трав. 21, 2021.

[2] Президент України. (2021, трав. 14). *Указ № 447/2021, Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/4472021-40013. Дата звернення: Трав. 21, 2021.

[3] Ю. Даник, та О. Корнейко, "Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України", *Information Technology and Security*, vol. 6, iss. 2, (11), July-December 2018, doi: https://doi.org/ 10.20535/2411-1031.2018.6.2.153495.

[4] Ю. Ф. Щиголь, та О. О. Пучков, "Шляхи підвищення якості підготовки фахівців з кібербезпеки в інтересах сектору безпеки і оборони України", на *наук.-практ. конф. "Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання",* Київ, 2020. с. 16.

[5] Г. Гапоненко, "Професійна компетентність фахівців сектору безпеки і оборони, *Вісник Національної академії Державної прикордонної служби України. Серія: Педагогіка*, вип. 2, 2017. [Електронний ресурс]. Доступно: https://nadpsu.edu.ua/wp-content/uploads/2018/10/visnik_2_2017_pdn.pdf. Дата звернення: Трав. 21, 2021.

[6] О. І. Локшина, "Європейська довідкова рамка ключових компетентностеї для навчання впродовж життя: оновлене бачення 2018 року", *Український педагогічний журнал*, № 3, с. 21-30. 2019.

[7] Ю. Д. Бойчук, та Ю. С. Таймасов, "Компетентнісна парадигма в сучасній вищій професійній освіті", *Новий Колегіум.* № 1, с. 38-44, 2015.

[8] Верховна Рада України. (2017, Вер. 5). *Закон України № 2145-VIII, Про освіту.* [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/2145-19. Дата звернення: Трав. 21, 2021.

[9] Верховна Рада України. (2006, Лют. 23). *Закон України № 3475-IV, Про Державну службу спеціального зв'язку та захисту інформації України.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/3475-15#Text. Дата звернення: Трав. 21, 2021.

[10] Міністерство освіти і науки України. (2018, Жовт. 4). *Наказ № 1074, Про затвердження стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти.* [Електронний ресурс]. Доступно: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf. Дата звернення: Трав. 21, 2021.

[11] В. В. Горлинський, та Б. В. Горлинський, "Кібербезпека як підсистема інформаційної безпеки", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 136-148, July-December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190559.

[12] Верховна Рада України. (2017, жовт. 5). *Закон № 2163-VIII. Про основні засади кібербезпеки України*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Дата звернення: Трав. 21, 2021.

[13] В. В. Горлинський, *Філософія безпеки і сталого людського розвитку: ціннісний вимір : монографія.* Київ, Україна: ПАРАПАН, 2011. [Електронний ресурс]. Доступно: https://classroom.google.com/c/MjU0NjM5Mzk5NzU4/m/MzQwMDM3NjQ4OTc5/details. Дата звернення: Трав. 21, 2021.

[14] І. Діордіца, "Система забезпечення кібербезпеки: сутність та призначення", *Підприємство, господарство і право. Інформаційне право* № 7, 2018. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Pgip_2017_7_24. Дата звернення: Трав. 21, 2021.

[15] Ю. Кожедуб, "Організаційна парадигма забезпечення інформаційної безпеки", *Information Technology and Security*, vol. 6, iss. 1 (10), January-June 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153133.

[16] О. Потій, Zoom-конференція, *"Цифрова трансформація держави: перспективи та ризики кібербезпеки"*. Верес. 25, 2020. [Електронний ресурс]. Доступно: https://galinfo.com.ua/news/dlya_posylennya_kiberbezpeky_neobhidna_spivpratsya_naukovyh_ustanov_pidpryiemstv_ta_navchalnyh_zakladiv__potiy_351916.html. Дата звернення: Трав. 21, 2021.

[17] С. Закірова, "Український шлях до запровадження військових стандартів НАТО", *Центр досліджень соціальних комунікацій НБУВ.* Доступно: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=4484:ukrajinskij-shlyakh-do-zaprovadzhennya-vijskovikh-standartiv-nato&catid=71&Itemid=382. Дата звернення: Трав. 21, 2021.

[18] Запровадження стандартів та інших керівних документів НАТО, *Офіційний вебсайт Міністерства оборони України,* [Електронний ресурс]. Доступно: https://www.mil.gov.ua/diyalnist/vprovadzhennya-standartiv-ta-inshih-kerivnih-dokumentiv-nato.html. Дата звернення: Трав. 21, 2021.

[19] В. Покровська, "Аналіз методів виявлення інформаційно-психологічного впливу в соціальних мережах", *Information Technology and Security*, vol. 8, iss. 1 (14), pp. 40-48, January-June 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218002.

[20] Ю. Кожедуб, Ю. Крамська, та В. Гирда, "Аналіз впливу людського фактору на кіберфізичну систему", *Information Technology and Security*, vol. 8, iss. 1, (14), pp. 102-115, January-June 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218013.

[21] В. С. Лукьянец, "Наука нового века. Гуманитарные трансформации", *Наука и образование: современные трансформации: монография. Ин-т философии им. Г. С. Сковороды НАН Украины*. Киев, Україна: ПАРАПАН, 2008. с. 8-36.

[22] L. R. Andersen, "Bildung: Keep Growing. Nordic Bildung", 2020. [Електронний ресурс]. Доступно: https://clubofrome.org/wp-content/uploads/2020/06/Bildung__Keep_Growing__by_Lene_Rache_Andersen__Excerpt.pdf. Дата звернення: Трав. 21, 2021.

[23] Рада Безпеки ООН. *Резолюція 1325 "Жінки. Мир. Безпека"*. [Електронний ресурс] Доступно: https://www.unwomen.org/en/what-we-do/peace-and-security/global-norms-and-standards#_WPS_resolutions. Дата звернення: Трав. 21, 2021.

[24] Кабінет Міністрів України. (2020, жовт. 28). *Розпорядження № 1544-р, Про затвердження Національного плану дій з виконання резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" на період до 2025 року.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/1544-2020-%D1%80#Text. Дата звернення: Трав. 23, 2021.

[25] Методичні рекомендації з інтеграції ґендерних підходів в систему підготовки фахівців для сектору безпеки і оборони України. [Електронний ресурс] Доступно: https://drive.google.com/drive/folders/12rBM7EBkTX-6EwhigmKLUGP3A-KQkCqp. Дата звернення: Трав. 21, 2021.

Стаття надійшла до редакції 03.07.2021.

REFERENCES

[1] S. O. Gakhov, "Cyberspace as the main category of cybernetics science", *Modern information security. State University of Telecommunications*, № 1. pp. 53-57, 2017. [Online]. Available: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1412. Accessed on: May, 21, 2021.

[2] President of Ukraine. (2021, May 14). *Decree № 447/2021, On the Decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine"*. [Online]. Available: https://www.president.gov.ua/documents/4472021-40013. Accessed on: May 21, 2021.

[3] Yu. Danyk, and O. Korneiko, "Basics of methodology of cybercompetence formation in specialists of the security and defense sector of Ukraine", *Information Technology and Security*, vol. 6, iss. 2-11, July-December 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153 495.

[4] Yu. F. Shchigol, and O. O Puchkov, "Ways to improve the quality of training of cybersecurity specialists in the interests of the security and defense sector of Ukraine", in *Proc. of the scientific-practical conference "Information and telecommunication systems and technologies and cybersecurity: new challenges, new tasks"*, Kyiv, 2020, p. 16.

[5] G. Gaponenko, "Professional competence of specialists in the security and defense sector", *Bulletin of the National Academy of the State Border Guard Service of Ukraine. Series: Pedagogy*, iss. 2, 2017. [Online]. Available: http://nbuv.gov.ua/UJRN/Vnadped_2017_2_10. Accessed on: May 21, 2021.

[6] O. I. Lokshyna, "European reference framework of key competences for Lifelong learning: an updated 2018 version", *Ukrainian pedagogical journal*, № 3, pp. 21-30, 2019. [Online] Available: http://uej.undip.org.ua/upload/iblock/c76/c7686993c393e6aed3078760b447511a.pdf. Accessed on: May 21, 2021.

[7] Yu. D. Boychuk, and Yu. S. Taimasov, "Competence paradigm in modern higher professional education", *Novyi Kolehium*, № 1, pp. 38-44, 2015.

[8] Verkhovna Rada of Ukraine. (2017, Sept. 5). *Law of Ukraine no. 2145-VIII. About education.* [Online]. Available: http://zakon.rada.gov.ua/laws/show/2145-19. Accessed on: May 21, 2021.

[9] Verkhovna Rada of Ukraine. (2006, Feb. 23). *Law of Ukraine no. 3475-IV, About the State Service for Special Communications and Information Protection of Ukraine.* [Online] Available: https://zakon.rada.gov.ua/laws/show/3475-15#Text. Accessed on: May 21, 2021.

[10] Ministry of Education and Science of Ukraine. (2018, Oct. 4). *Order no. 1074. On approval of the standard of higher education by specialty 125 "Cyber Security" for the first (Bachelor) level of higher education.* [Online]. Available: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf. Accessed on: May 21, 2021.

[11] V. V. Horlynskyi, and B. V. Horlynskyi, "Cybersecurity as a component of information security of Ukraine", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 136-148, July-December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190559.

[12] Verkhovna Rada of Ukraine. (2017, Oct. 5). *Law no. 2163-VIII. About the Basic Principles of Cyber Security of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/ 2163-19. Accessed on: May 21, 2021.

[13] V. V. Horlynskyi, *The philosophy of security and sustainable human development: a value dimension: a monograph.* Kiev, Ukraine: PARAPAN, 2011. [Online] Available: https://classroom.google.com/c/MjU0NjM5Mzk5NzU4/m/MzQwMDM3NjQ4OTc5/details. Accessed on: May 21, 2021.

[14] I. Diordica, "Cybersecurity: Essence and Purpose, Enterprise*", Business and Law. Information law*, №7, 2017. [Online]. Available: http://nbuv.gov.ua/UJRN/Pgip_2017_7_24. Accessed on: May 21, 2021.

[15] Yu. Kojedub, "Organizational paradigm for information security", *Information Technology and Security*, vol. 6, iss. 1, January-June 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153133.

[16] O. Potyi, Zoom-conference *"Digital transformation of the state: prospects and risks of cybersecurity"*, Sept. 25, 2020. [Online]. Available: https://galinfo.com.ua/news/dlya_posylennya_kiberbezpeky_neobhidna_spivpratsya_naukovyh_ustanov_pidpryiemstv_ta_navchalnyh_zakladiv__potiy_351916.html. Accessed on: May 21, 2021.

[17] S. Zakirova, "Ukraine's path to the introduction of NATO military standards", *Center for Social Communications Research NBUV*. [Online]. Available: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=4484:ukrajinskij-shlyakh-do-zaprovadzhennya-vijskovikh-standartiv-nato&catid=71&Itemid=382. Accessed on: May 21, 2021.

[18] Introduction of NATO standards and other guidelines, *Official Website of the Ministry of Defense of Ukraine.* [Online]. Available: https://www.mil.gov.ua/diyalnist/vprovadzhennya-standartiv-ta-inshih-kerivnih-dokumentiv-nato.html. Accessed on: May 21, 2021.

[19] V. Pokrovska, "Analysis of information-psychological impact detection methods in social networks", *Information Technology and Security*, vol. 8, iss. 1 (14), pp. 40-48, January-June 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218002.

[20] Yu. Kozhedub, Yu. Kramska, and V. Hyrda, "Analysis of the human factor influence on the cyber-physical system", *Information Technology and Security*, vol. 8, iss. 1 (14), pp. 102-115, January-June 2020, doi: 10.20535/2411-1031.2020.8.1.218013. [Online]. Available: http://its.iszzi.kpi.ua/issue/view/13208 Accessed on: May 21, 2021.

[21] V. S. Lukkyanets, "Science of the new century. Humanitarian transformations", *Science and education: modern transformations: monograph. Institute of Philosophy named after. G. S. Skovoroda pans of the National Academy of Sciences of Ukraine.* Kiev, Ukraine: PARAPAN, 2008. pp. 8-36.

[22] Andersen L. R., "Bildung: Keep Growing. Nordic Bildung", p. 12, 2020. [Online]. Available: https://clubofrome.org/wp-content/uploads/2020/06/Bildung__Keep_Growing__by_Lene_ Rache_ Andersen__Excerpt.pdf. Accessed on: May 21, 2021.

[23] UN Security Council. Resolution 1325 "*Women. Peace. Security*". [Online]. Available: https://www.unwomen.org/en/what-we-do/peace-and-security/global-norms-and-standards#_WPS_resolutions. Accessed on: May 21, 2021.
[24] Ministry of Education and Science of Ukraine. (2020, Oct. 28). *Order № 1544-p, National Action Plan for the Implementation of UN Security Council Resolution 1325 "Women, Peace, Security" for the period up to 2025*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1544-2020-%D1%80#Text. Accessed on: May 21, 2021.
[25] Methodical recommendations on integration of gender approaches into the system of training specialists for the security and defense sector of Ukraine. [Online]. Available: https://drive.google.com/drive/folders/12rBM7EBkTX-6EwhigmKLUGP3A-KQkCqp. Accessed on: May 21, 2021.

VICTOR HORLYNSKYI,
BORYS HORLYNSKYI

ANALYSIS OF KEY FACTORS OF FORMATION OF THE SYSTEM OF COMPETENCES OF PROFESSIONALS IN THE FIELD OF CYBERSECURITY

It is shown that the construction of an established system of cybersecurity of the state in the context of globalization, development of information technologies, transfer of "hybrid wars" to cyberspace, requires improving the quality of training, on which depends the reliability of national cyberspace. It is specified that the key indicator of qualification of specialists in the field of cybersecurity is competence, but their final definition and actual content, in accordance with the requirements of rapid technical and technological development, requires substantiation of theoretical principles that are the object of study. It is substantiated that an essential component of the theoretical basis for determining the system of competencies is a certain set of factors that determine its constitution and determine the subject and purpose of the study. The key factors that need to be taken into account in determining professional competencies are the following: the requirements of the modern education system; the systemic nature of the processes unfolding in global cyberspace; conceptual principles of cybersecurity; rapid development of information technologies and the transition to a quantum basis; new threats to national security arising from the convergence of information and high-tech technologies; cyberattacks aimed at government agencies and national security structures; attempts at destructive psychological influence on the personnel of the security and defense sector; Ukraine's course towards Euro-Atlantic integration, harmonization of the national system of standards with NATO standards in the field of cyber security; increasing the riskiness of professional activity; challenges of gender policy to achieve gender equality in the field of security and defense of Ukraine. Therefore, it should be noted that the training of specialists in the field of cybersecurity in the interests of the future of the country should be based on a certain, methodologically sound system of competencies, the implementation of which should lead to quality training in professional activities in the field of cyberspace.

Keywords: cybersecurity, cyberspace, cyber threat, education, competence, training, Euro-Atlantic standards.

Горлинський Віктор Вікторович, кандидат філософських наук, доцент, доцент кафедри теоретичних основ експлуатації засобів спеціальних телекомунікаційних систем, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-1190-5991, gvv1004@gmail.com.

Горлинський Борис Вікторович, кандидат технічних наук, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна, ORCID 0000-0002-9993-2427, vjzgoxnf@gmail.com.

Horlynskyi Viktor, candidate of philosophical sciences, associate professor, associate professor at the academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Horlynskyi Borys, candidate of technical sciences, Administration of State serves of special communication and information protection of Ukraine, Kyiv, Ukraine