DOI 10.20535/2411-1031.2024.12.2.315746
УДК 004.056.53::378.1

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

ОСВІТНІ ПРІОРИТЕТИ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ В ДЕРЖАВІ

Забезпечення кібербезпеки держави в умовах повномасштабного вторгнення російської федерації, поширення бойових дій на національний кіберпростір, вимагають перегляду і уточнення освітніх пріоритетів у підготовці фахівців у сфері кібербезпеки як передумови надійного захисту кіберпростору України. На підставі факторів впливу на професійну і службову діяльність фахівців у сфері кібербезпеки, визначено освітні пріоритети підготовки здобувачів, що відповідають сучасним вимогам захисту кіберпростору в умовах воєнного стану держави, а саме: спрямованість підготовки здобувачів на опанування ціннісними пріоритетами, визнаними українським суспільством, які утворюють ментальні й національно-патріотичні передумови належного виконання професійного і військового обов'язку, особистої відповідальності за забезпечення інформаційної безпеки держави та захищеності її кіберпростору; зорієнтованість навчання на превентивну підготовку фахівців, здатних активно діяти і виконувати професійне завдання в небезпечних обставинах воєнного стану, надзвичайних ситуацій і підвищеного ризику, компетентно попереджувати і протидіяти загрозам і небезпекам, зберігати морально-психологічну стійкість у небезпечних умовах воєнного часу; спрямованість підготовки на опанування фахівцями з кібербезпеки спеціальними знаннями та управлінськими здатностями, викликаних розвитком комунікаційних і квантових технологій, штучного інтелекту, новими методами кіберзахисту; націленість навчання на оволодіння здобувачами спеціальними, військовими й безпековими нормами, узгодженими із стандартами, прийнятими в країнах – членах ЄС і НАТО; відповідність навчання державній політиці цифровізації України, спрямування підготовки здобувачів на всебічний розвиток цифрових навичок взаємодії у цифровому просторі та підтримання власної кібербезпеки, опанування цифровими інструментами, зокрема, штучного інтелекту в інтересах навчальної, наукової, професійної та управлінської діяльності у сфері забезпечення кібербезпеки. На ґрунті окреслених освітніх пріоритетів, запропоновано перелік безпекових й професійних здібностей, на формування яких доцільно спрямувати підготовку фахівців у сфері кібербезпеки.

Ключові слова: здатність, здібність, кібербезпека, кіберпростір, кіберзагрози, компетентність, освіта, підготовка фахівців, штучний інтелект.

Постановка проблеми. Вдосконалення системи кібербезпеки, забезпечення надійного захисту кіберпростору в умовах озброєного вторгнення в Україну російської федерації залишається одним з актуальніших питань теорії і практики забезпечення національної безпеки України [1]–[3]. Умовою вирішення цього завдання є підготовка фахівців в галузі кібербезпеки, компетентності яких, мають відповідати сучасним реаліям воєнного часу і потребам держави [4]–[7]. Від науково обґрунтованого, адекватного визначення і впровадження в практику підготовки фахівців необхідних професійних, військових і соціальних якостей, як пріоритетної змістовної основи фахових і загальних компетентностей, багато в чому залежатиме надійність захисту кіберпростору України в умовах режиму воєнного стану. Розв'язання означеного питання потребує уточнення освітніх пріоритетів підготовки фахівців з кібербезпеки, які мають відповідати сучасним факторам і обумовлювати здібності, що утворюють змістовну основу фахових і загальних компетентностей фахівців з

здібності, що утворюють змістовну основу фахових і загальних компетентностей фахівців з кібербезпеки. Отже, розробка теоретичних засад визначення здібностей, що відповідають сучасним потребам забезпечення кібербезпеки в обставинах озброєного захисту держави, постає актуальним завданням військової та кіберосвіти.

Аналіз останніх досліджень і публікацій. Різноманітні аспекти навчання фахівців в галузях захисту інформації та кібербезпеки відображено у працях [4]–[7], [13], [14], [20], [25], [26]. Безпосередньо, аналіз методології формування кіберкомпетеностей у фахівців сектору безпеки і оборони здійснено в працях [4], [5], [7]. Вимоги і напрямки підготовки фахівців з кібербезпеки в інтересах сектору безпеки і оборони розглянуті в роботах [5]–[7], [13], [14], [20]. Проте питання відповідності професійних і загальних компетентностей фахівців в сфері кібербезпеки вимогам воєнного стану і сучасному інформаційно-технологічному розвитку, з'ясування їх змістовного наповнення відповідними здібностями, потребують додаткових досліджень.

Метою статті є обґрунтування освітніх пріоритетів підготовки здобувачів з кібербезпеки в умовах воєнного стану держави, зростання кіберзагроз національній безпеці та уточнення відповідних особистих професійних, безпекових і цифрових здібностей як змістовної основи компетентностей фахівців у сфері кібербезпеки.

Виклад основного матеріалу дослідження. Вплив на інформаційний і кіберпростір повномасштабного озброєного вторгнення в Україну російської федерації, що проявляється у зростанні кіберзлочинності, кібертероризму, інформаційної експансії, виникненні нових кіберзагроз, свідчить про підвищення ролі інформаційної та кібербезпеки у забезпеченні національної безпеки держави. Необхідність надійного захисту національного кіберпростору, особливо в умовах режиму воєнного стану, прагнення України до євроатлантичної інтеграції, актуалізує значущість якісної та адекватної освіченості фахівців в галузі кібербезпеки, вимагає переосмислення та уточнення освітніх пріоритетів їх підготовки [5]–[7], [13], [14], [20]. На визначення компетентностей та їх змістовного боку – здібностей, обумовлюючих спрямованість підготовки фахівців, також впливають поширення бойових дій на національний кіберпростір та комунікаційну інфраструктуру, вплив новітніх інформаційних технологій і штучного інтелекту на кібербезпеку. Отже, актуальність врахування спрямованості підготовки фахівців в галузі кібербезпеки в період воєнних, енергетичних, економічних і соціально-політичних випробувань Української держави є безумовною і постає одним з факторів забезпечення її національної безпеки.

Поряд із зазначеним, деякі питання відповідності змісту професійних здібностей потребам воєнного стану у державі, вимогам підвищеного захисту інформаційно-комунікаційних систем в умовах війни, вимагають додаткових теоретичних досліджень. Це викликано, як розвитком галузі кібербезпеки, так і системним характером процесів, що відбуваються в глобальному та національному кіберпросторі в умовах озброєного вторгнення російської федерації, переносом бойових дій безпосередньо у кіберпростір, перезавантаженням інформаційних технологій на квантову основу, впливом новітніх інформаційних, нейро-мережевих і технологій штучного інтелекту на кібербезпеку, а також, вимогами адаптації національної нормативної бази у сфері інформаційної та кібербезпеки до стандартів Північноатлантичного Альянсу. Як бачимо, виявляється низка пріоритетних освітніх завдань, спрямованих на з'ясування, адаптацію і впровадження нових знань, вмінь і здібностей в систему навчання фахівців в галузі кібербезпеки.

Дослідницьким підходом, що містить принципові вимоги і методологічний інструментарій дослідження якостей військового фахівця є компетентнісний підхід, що застосовується в освіті. Він зосереджує увагу на результативно-цільовій спрямованості підготовки здобувачів та визначається як комплекс методологічних, парадигмальних структурних компонентів, спрямований на формування компетентностей, заснованих на оптимальному співвідношенні теоретичних знань, умінь, здібностей, професійно значущих та особистісних якостей, що забезпечують ефективну підготовку фахівця. [4], [5], [7]. Згідно з компетентнісним підходом, провідним узагальнюючим комплексним показником якості підготовки фахівців у галузі кібербезпеки є фахові та загальні компетентності. Відповідно до

Закону України «Про вищу освіту», компетентність визначається як здатність особи успішно соціалізуватися, навчатися, провадити професійну діяльність, яка виникає на основі динамічної комбінації знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей [8]. Загальні системні засади визначення компетентностей фахівців з кібербезпеки обумовлюються призначенням Держспецзв'язку та Законом Про основні засади кібербезпеки України [9], [10]. Документами, що визначають компетентності фахівців за спеціальністю 125 Кібербезпека є стандарт вищої освіти України [11] та Освітньо-професійна програма першого (бакалаврського) рівня вищої освіти "Безпека державних інформаційних ресурсів" за спеціальністю 125 Кібербезпека та захист інформації [12]. В Освітньо-професійній програмі, розробленій в 2023 році в НТУУ КПІ ім. Ігоря Сікорського, додатково до освітнього стандарту, визначено 5 фахових компетентностей, вже з врахуванням необхідності впровадження професійних безпекових здатностей в сфері спеціального зв'язку [12]. Але, ознайомлення з документом дозволяє зазначити, що перелічені компетентності не охоплюють здібностей, необхідних для управління військовим колективом в умовах воєнного стану та надзвичайних ситуацій, змістовною частиною яких, е правові, соціально-психологічні, педагогічні й безпекові навички та якісні характеристики свідомості, що визначають приналежність фахівців до військового етосу [5], [6].

Таким чином, постає запитання про рівень відповідності результативно-цільової складової навчання, що обумовлює спрямованість підготовки військових фахівців з кібербезпеки, – сучасним вимогам воєнного стану держави як визначальному комплексному пріоритету військової освіти. Відповідь на запитання розкривається на підставі обґрунтування сучасних пріоритетів підготовки військових фахівців з кібербезпеки та уточнення відповідних особистісних здібностей як змістовної складової компетентностей та показника якості підготовки фахівців у сфері кібербезпеки.

Важливою складовою компетентностей фахівця, поряд із знаннями, навичками і вміннями, є здібності, що характеризують змістовну частину фахових і загальних компетентностей та утворюють підґрунтя здатностей особистості [6]. Якщо компетентності з кібербезпеки характеризуються сукупністю відповідних здатностей, то власно здатності утворюються внаслідок опанування фахівцем конкретними здібностями [13]. Здібності, на відміну від компетентностей та здатностей, належать до найсуттєвіших рис людини і розглядаються як індивідуально-психологічні особливості, що виявляються в діяльності, є умовами її успішного виконання і спричиняють відмінності в динаміці оволодіння необхідними для людини знаннями, навичками і вміннями. Теоретичною підставою типологізації здібностей слугують певні ознаки, що відображають їх функції і сферу застосування, взаємозв'язок з видом діяльності, певні схильності особистості [13]. Отже, здібності слугують психологічним підґрунтям для опанування особистістю здатностями та компетентностями.

Методологічною основою обґрунтування здібностей фахівців у сфері кібербезпеки є певна сукупність визначальних факторів, що мають зумовлювати пріоритетні напрями підготовки і суттєво впливають на сферу функціональної відповідальності посадових осіб в галузі кібербезпеки та успішність виконання завдань за призначенням в умовах воєнного стану держави. Визначальні фактори розглядаються як прояв функціонування зав'язків детермінації, що спричиняють обумовленість або причинність процесів і явищ у сфері професійної діяльності та основні властивості системи забезпечення кібербезпеки.

У сфері відповідальності фахівців з кібербезпеки відбуваються багато видів детермінації процесів, але в контексті обраної теми, нас більш цікавить інформаційно-технологічний, комунікаційний, безпековий, організаційно-технологічний, структурно-функціональний, соціально-психологічний та соціокультурний види детермінації. Специфічними детермінантами формування регулятивів діяльності у структурах сектору безпеки і оборони України виступають – цільові: забезпечення національної безпеки, підтримка постійної бойової готовності, військової дисципліни, виконання бойових і учбово-бойових задач, професійне навчання і виховання; структурні: централізація, єдиноначальність, субординація, координація; функціональні: виконання завдань за призначенням, участь у бойових,

миротворчих і гуманітарних операціях, оборона України, захист її суверенітету і територіальної цілісності, забезпечення стримування збройної агресії проти України [14].

Соціокультурними факторами, що визначають загальну спрямованість підготовки фахівців у сфері кібербезпеки та мають відбиватися в певних здібностях, є ціннісні пріоритети, визнані українським суспільством, проголошені у Конституції та інших правових актах України. Історично складені, ментально укорінені, вистраждані народом цінності виконують функцію зміцнення нації, згуртування військових колективів, визначають сенс і мету військової служби і професійній діяльності, спрямованість розвитку військового колективу. Відображаючись у свідомості особистості у вигляді вищих мотивів, орієнтацій, інтересів, настанов, переконань та цілей, цінності набувають регулятивної функції та виступають як соціокультурні коди поведінки, нормативні підстави професійної і соціальної діяльності. Являючись критерієм ставлення до виконання громадянського і військового обов'язку, виконуючи мотивуючу, регулятивну і орієнтуючу функцію, цінності постають внутрішньо особистісним фактором соціальної активності фахівця.

Ціннісні орієнтації особистості військовослужбовця утворюють стрижень свідомості військової людини, який забезпечує психологічну стійкість як феномен воїнського етосу, що є найбільш дієвим чинником в небезпечних умовах військової діяльності [6]. Розвинуті ціннісні орієнтації – це ознака зрілості особистості військовослужбовця, міри професіоналізму і соціальності. Мотиваційний вплив ціннісних орієнтацій на індивідуальну і групову поведінку і професійну діяльність, відповідність громадянським, національним ідеалам захисника батьківщини, стійкість, незалежність від кризових умов діяльності, складають методологічну підставу обґрунтування особистих якостей представника сектору безпеки і оборони та їх включення у систему підготовки фахівців [14].

Серед цінностей, що мають важливе значення в сучасних умовах озброєного відстоювання незалежності України, аналітики відзначають національно-патріотичні цінності, які є ядром духовного потенціалу українського суспільства, забезпечують його духовну стійкість, утворюють стержень національного духу особистості, є найважливішою умовою забезпечення національної безпеки держави. Програмним документом, що орієнтує на впровадження в українському суспільстві системи національно-патріотичних цінностей є Стратегія національно-патріотичного виховання [15]. Серед складових національно-патріотичного виховання Стратегія відзначає формування національно-культурної громадянської ідентичності, національно-патріотичного світогляду, збереження та розвиток суспільно-державницьких та духовно-моральних цінностей Українського народу; готовність громадянина до виконання обов'язку із захисту незалежності та територіальної цілісності України [15].

Поряд з національно-патріотичними, дослідники відокремлюють військові етичні цінності, що виявляються у моральних чеснотах, а саме: мужність, самовідданість, хоробрість, честь, гідність, шляхетність, відвага, звитяга, відповідальність, відданість українському народові і військової присязі. Професійні вимоги до представників структур сектору безпеки і оборони вимагають також належного ставлення до службово-професійних цінностей, що реалізуються у діяльності як здібності, а саме: професійна компетентність і службова дисциплінованість, військове лідерство, швидка навчаємість, аналітичне і системне мислення, вміння зберігати конфіденційну інформацію, корпоративність службових комунікацій, організованість, самоконтроль, неприпустимість корупції, морально-психологічна стійкість, професійне самовдосконалення тощо [5], [6], [16]. Ціннісні орієнтації військовослужбовця, виконуючи функцію певного соціокультурного коду професійної та соціальної поведінки, мають зумовлювати формування стійкості психіки, забезпечувати адекватне мислення, поведінку, способи превентивної діяльності й управління військовими колективами, необхідні для виконання військового і професійного обов'язку в умовах військових дій, надзвичайних ситуацій та екстремальних умовах діяльності, утворюють підстави формування і підтримання належного морально-психологічного стану військовослужбовців [16].

Отже, ціннісна свідомість військових фахівців з кібербезпеки – представників Держспецзв'язку має ґрунтуватися на моральних цінностях відданості українському народові,

патріотизмі, свідомому ставленні до службового обов'язку, виконання вимог Конституції та законів України, особистої відповідальності за безпеку держави і захист національного кіберпростору. Визначені цінності складають ментальну цільову основу утворення професійної та службової мотивації, сприяють формуванню відповідних здібностей у свідомості військових фахівців [17].

В умовах режиму воєнного стану в Україні, що супроводжується підвищенням ризикогенності професійної діяльності, поряд з професійними компетентностями в сфері захисту інформації та кіберпростору, набувають життєвої значущості власно *безпекові* пріоритети професійної діяльності [18]. З огляду на воєнну агресію російської федерації, посилення кібератак і озброєних нападів на об'єкти критичної інфраструктури держави і необхідності забезпечення захисту кіберпростору України в умовах постійних загроз життю і здоров'ю, постає питання щодо адаптації підготовки фахівців з кібербезпеки до професійної діяльності в умовах воєнного стану і підвищеного ризику. У Стратегії розвитку вищої освіти в Україні на 2022-2032 роки наголошується, що вища освіта стає необхідним стратегічним елементом безпеки суспільства, є фактором не лише економічної, але і політичної, соціальної, когнітивно-емоційної безпеки людини [19]. *Тому, одним з провідних безпекових пріоритетів військової освіти в умовах воєнного стану держави, є спрямованість на превентивну підготовку фахівців, здатних активно діяти і виконувати професійне завдання в умовах воєнного стану, небезпек і підвищеного ризику, компетентно попереджувати і протистояти загрозам, небезпекам і ризикам.* Безпекові пріоритети підготовки мають бути спрямовані на формування соціальних, професійних і управлінських здібностей до організації діяльності в кризових умовах воєнних небезпек і надзвичайних ситуацій, виконувати функцію формування антикризової поведінки військової людини, службова діяльність якої, пов'язана з підвищеним ризиком і необхідністю підтримання високого морально-психологічного стану військового підрозділу в умовах воєнного часу.

Згідно з окресленими пріоритетами адаптації навчання до безпекових потреб держави, підготовка фахівців в сфері кібербезпеки до діяльності в умовах воєнного стану і підвищеного ризику, поряд з власно професійними здатностями із забезпечення системного захисту інформації та кібербезпеки, має бути спрямована на формування у здобувачів безпекових здібностей, а саме: всебічної готовності до діяльності в умовах зростаючого ризику, воєнних, техногенних, гуманітарних і екологічних загроз; опанування правилами поведінки і діяльності в умовах застосування підрозділу за призначенням, виживання в екстремальних умовах та полоні; використання соціально-психологічних методів підтримання і відновлення морально-психологічного стану у військовому підрозділі, всебічної готовності до виконання завдань за призначенням, володіння методами емоційно-вольової саморегуляції та психологічної адаптації до діяльності в екстремальних умовах і надзвичайних ситуаціях; стійкості до стресу та здатності швидко відновлювати психологічний стан; вміння аналізувати небезпечну ситуацію, адекватно реагувати на загрози і приймати професійні рішення у небезпечних для життя умовах; самодисциплінованість, навички працювати під тиском критичних обставин, мужнього ставлення до труднощів військової життєдіяльності в умовах війни; дотримання норм особистої і колективної безпеки, збереження конфіденційних даних; ставлення до власної поведінки і діяльності на підставі норм права воєнного стану; прогнозування, попередження і подолання імовірних загроз в соціальній і професійній діяльності на підставі систематичного оновлення власних знань про можливі небезпеки, ризики та засоби їх попередження, подолання і захисту; критичного переосмислення і перебудови власної ієрархії ціннісних орієнтацій і життєвих смислів відповідно до умов воєнного стану у державі [7], [17], [18], [19].

Провідним фактором, що пов'язаний з попереднім й спричиняє необхідність уточнення пріоритетів підготовки фахівців і потребує врахування при з'ясуванні загальних і фахових здібностей в сфері кібербезпеки, є розв'язування збоку російської федерації кібервійни з перенесенням «бойових дій» у національний кіберпростір України [1], [2], [5], [10], [20]. Відзначений фактор має системний характер та потребує уточнення якостей фахівця з кібербезпеки як мінімум по двом пріоритетним напрямкам підготовки. Він вимагає, з одного

боку, загальної кіберосвіченості, конкретизації суто професійних якостей фахівця з кібербезпеки, зумовлених розвитком інформаційних технологій, методів кібербезпеки та захисту інформації [5], з іншого боку, викликає необхідність протидії інформаційним загрозам у контексті їх негативного впливу на свідомість фахівця, що потребує опанування відповідними соціально-психологічними якостями [13], [17]. Тобто для фахівця з кібербезпеки, компетентності в сфері захисту інформаційних ресурсів та інформаційно-комунікаційних систем держави, мають бути доповнені правовими, соціально-психологічними знаннями і здібностями, що дозволяють застосовувати методи і методики захисту власної свідомості від негативного інформаційно-психологічного впливу через засоби комунікації, управляти процесами соціально-психологічного захисту військового колективу.

Загальними умовами, яким мають відповідати професійні компетентності фахівців та їх змістовна складова – здібності, слугують засади розвитку національної системи кібербезпеки, визначені в Стратегії кібербезпеки України [1], які базуються на аналізі цифрового середовища, глобальних трендів середовища з кібербезпеки, захисту національних інтересів України; проактивному підході, що передбачає вжиття превентивних заходів тощо [1]. Принциповим положенням Стратегії кібербезпеки України, що потребує врахування при розробленні здібностей фахівців з кібербезпеки, є вимога 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 [1].

Отже, швидкий розвиток інформаційних технологій та технологій штучного інтелекту, їх перехід на квантову та нейронну мережеву основу, зміни уявлень про кіберпростір, зростання кіберзагроз та зміни методів кіберзахисту є визначальним фактором, що вимагає постійного уточнення відповідних здібностей фахівців з кібербезпеки та утворюють один з пріоритетних напрямків підготовки фахівців [1], [2], [9], [20]. Відзначені обставини потребують уточнення і конкретизації криптографічних, інформаційно-технологічних та організаційних здібностей фахівців з кібербезпеки. Так, розвиток квантової технології та створення квантового комп'ютера, спричиняють технологічний перехід на комунікації постквантового періоду і передбачають суттєві зміни теоретичних і технологічних основ захисту інформації в інформаційно-комунікаційних системах, уточнення стандартів, їх відбиття у професійних компетентностях і здібностях фахівців, перегляду змістовної складової навчання, перегляду способів криптографічного захисту інформації в кіберпросторі та уточнення відповідних компетентностей фахівців з кібербезпеки [21], [22].

Поряд із зазначеним, провідною ознакою і трендом сучасних інформаційних технологій є стрімкий розвиток та впровадження технологій штучного інтелекту у всі сфери суспільного життя, зокрема у кібербезпеку. Інформаційні технології штучного інтелекту (скорочено – ШІ, англ. "artificial intelligence", скорочено AI) науковці відносять до унікальних інструментів аналізу і узагальнення великих масивів даних за відносно короткий час, що недосяжно для інших технологічних засобів. У березні 2024 року Генеральна Асамблея ООН ухвалила першу знакову резолюцію щодо регулювання діяльності в сфері застосування ШІ [23].

Євроатлантична спрямованість стратегічного курсу України, передбачає врахування у підготовці військових фахівців, базових положень оновленої Стратегії НАТО щодо ШІ, ухваленої на Вашингтонському саміті (липень 2024). У рамках Стратегії щодо штучного інтелекту, члени Альянсу ухвалили Принци відповідального використання ШІ для цілей оборони і безпеки Альянсу, а саме: законність, відповідальність і підзвітність, зрозумілість і простежуваність, надійність, керованість і пом'якшення упередженості. Серед пріоритетів альянсу щодо ШІ у Стратегії визначено такі: просування імплементації принципів відповідального використання ШІ в НАТО; підвищення оперативної сумісності між системами штучного інтелекту в Альянсі; захист і контролювання технологій ШІ, управління пов'язаними з ними ризиками, захист від загроз зловмисного використання ШІ; формування норм, стандартів, шаблонів оцінювання, процесів перевірки та інших інструментів відповідального використання ШІ в обороні та безпеці; заходи щодо конвергенції між штучним інтелектом та іншими новими проривними технологіями (англ. Emerging Disruptive

Technologies). Стратегія також визначає дезінформацію, використання гендерних наративів як зброї, технологічне гендерно зумовлене насильство та інформаційні операції за допомогою ШІ як питання, що викликають занепокоєння щодо безпеки в Альянсі. Для сприяння готовності НАТО до ШІ, Стратегія зауважує необхідність стратегічного передбачення, зокрема широке коло проактивних заходів, від випереджувального керування до планування альтернативних сценаріїв, що ґрунтуються на спільних і відповідальних підходах [24].

Застосування технологій генеративного ШІ в інтересах забезпечення кібербезпеки значно підвищує ефективність функціонування системи та надає багато переваг, від автоматизації повторюваних завдань до використання прогнозної аналітики у виявленні кіберзагроз, автоматизації реагування на інциденти безпеки [25], [26]. У Концепції розвитку штучного інтелекту в Україні, серед низки завдань, спрямованих на комплексне розв'язання проблем кібербезпеки із ШІ, відзначено необхідність розроблення інноваційних систем кібербезпеки, які широко застосуватимуть технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії, їх стримування і запобігання, розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту з урахуванням європейських та міжнародних стандартів, зокрема ISO 27001, ISO/IEC 27032 [27]. Одним з прикладів застосування штучного інтелекту в інтересах безпеки є реалізація Корпорацією Microsoft інноваційної моделі штучного інтелекту на базі GPT-4, призначеної для аналітичної роботи в інтересах американських спецслужб. Відмінною особливістю цієї моделі є її здатність до автономної роботи без підключення до Всесвітньої мережі [28].

Але поряд з перевагами штучного інтелекту, його можливостями застосування в інтересах забезпечення кібербезпеки, експерти і фахівці з кібербезпеки вбачають небезпеки та ризики. Так, у міжнародному науковому звіті про безпеку ШІ, проведеному групою експертів зі ШІ з 30 країн, очолюваної професором Йошуа Бенджіо, визначено три основні категорії ризиків, пов'язаних зі ШІ, а саме: зловмисне використання, ризики збоїв і системні ризики. У доповіді йдеться про те, що зловмисне використання може охоплювати великомасштабне шахрайство, діпфейки, дезінформацію, допомогу в кібератаках або розробці біологічної зброї. Серед потенційних ризиків, пов'язаних зі збоями в роботі ШІ, містили побоювання з приводу втрати контролю над системами ШІ. Серед потенційних системних ризиків були побоювання з приводу ризиків, які ШІ представляє для конфіденційності [29]. Доречи, розробки у сфері штучного інтелекту Стратегія національної безпеки України відносить до прогнозованих загроз національній безпеці [2]. Серед ризиків, викликаних застосуванням штучного інтелекту, експерти, поряд із зазначеними, зауважують ризики втрати контролю над системами ШІ, прихованої зміни цілей програми, ігнорування закладених у програму етичних принципів тощо [30]. Саме тому, основним завданням у сфері кібербезпеки Концепція розвитку штучного інтелекту в Україні, визначає "захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій" [27].

Проте, потреба у ефективному застосуванні інструментів ШІ в інтересах захисту національного кіберпростору в умовах обмеженого часу на прийняття рішення, вимагає формування у фахівців з кібербезпеки відповідних професійних і загальних здібностей. *Передбачається, що перелік професійних здібностей, має містить*: знання, відомості про основи функціонування систем ШІ; розуміння принципів машинного навчання, функціонування нейронних мереж і базових алгоритмів ШІ; розуміння методів аналізу, обробки та інтерпретації візуальної інформації за допомогою комп'ютерних систем; навички роботи з великими даними та інструментами обробки та аналізу даних; здатність ефективно спілкуватися з системами ШІ з метою розв'язання складних теоретичних і практичних проблем професійної діяльності. До переліку соціальних якостей фахівців пропонується включити: здібності до аналітичного і критичного осмислення можливостей використання інструментів ШІ у професійній діяльності, аналізу проблем у сфері застосування ШІ в інтересах кібербезпеки та вироблення ефективних рішень; творчі здібності, здатність до нестандартного мислення, застосовування інноваційних рішень, що потребують використання технологій ШІ; безперервне професійне навчання і самостійний пошук нової інформації стосовно можливостей застосування ШІ в інтересах кібербезпеки; адаптація до нових

технологій, методів, інструментів, стандартів та етичних вимог застосування ШІ в інтересах захисту національного кіберпростору, що застосовуються в країнах – членах Північноатлантичного альянсу [24]. Здобувачі протягом навчання, мають отримувати знання про можливості впровадження і використання інструментів штучного інтелекту у сфері забезпечення кібербезпеки та управлінні, набувати практичних навичок управління устаткуванням, в якому застосовується штучний інтелект, мати уявлення про переваги та ризики застосування ШІ, бути ознайомленими з принципами відповідального використання ШІ [24], ризиками та обмеженнями використання штучного інтелекту у професійній діяльності, зокрема, необхідністю дотримання вимог інформаційної безпеки, конфіденційності даних, авторського права та академічної доброчесності [31].

Отже, необхідно зауважити, що вплив технологій штучного інтелекту є одним з глобальних трендів середовища кібербезпеки і передбачає опанування фахівцями основами застосування технологій штучного інтелекту в інтересах забезпечення кібербезпеки. Неосяжні можливості штучного інтелекту, вимагають суттєвих змін у методах криптографічного захисту інформації з метою підвищення її стійкості. Це потребує відповідних змін у навчальних програмах, уточнення змістовної частини кіберкомпетенцій, спрямованих на формування фахових здібностей фахівця.

Іншім фактором, що актуалізує один з напрямів підготовки фахівців з кібербезпеки, пов'язаним з процесами шостого технологічного укладу, є цифровізація освіти, суспільного життя, управлінської і професійній діяльності. Цифровізація (або диджиталізація, англ. digitization) переведення інформації в цифрову форму або оцифрування і розуміється як процес використання цифрових технологій у багатьох формах життєдіяльності суспільства в інтересах людини. Її головною метою є тотальне оцифрування інформації з метою її збереження, застосування і використання у всіх її формах – текстовій, звуковій, графічній тощо [32], [33].

В Україні відбуваються процеси цифровізації як головна вимога і умова становлення і розвитку цифрового суспільства. Але з початком війни з російською федерацію, за об'єктивних обставин ці процеси набули надзвичайно високої актуальності. Державна політика цифровізації передбачає опанування фахівцями необхідними цифровими компетенціями у всіх сферах професійній, науковій і соціальній діяльності. Реалізація державної політики цифрового розвитку ґрунтується на принципах: відкритості; прозорості; багаторазовості використання; технологічної нейтральності і портативності даних; орієнтованості на громадян; інклюзивності та доступності; безпечності та конфіденційності; багатомовності; підтримки прийняття рішень; адміністративного спрощення; збереження інформації; оцінювання ефективності та результативності [34].

Формування та реалізація державної політики цифровізації в Україні в умовах воєнного стану держави потребує докорінних змін у підготовці фахівців, які повинні володіти цифровими компетенціями та користуватися технологічними можливостями сучасного диджитального інструментарію. Дані обставини вимагають вдосконалювати навчання згідно з потребами і вимогами сьогодення, спрямовуючи його на формування у здобувачів здібностей та цифрових навичок у власній діяльності [35]. В цьому контексті, цифровізація освітнього простору та організація дистанційного навчання, викликаного війною та світовою пандемією, постає невід'ємною складовою цифрового розвитку в Україні та потребує відповідного спрямування підготовки здобувачів на опанування digital-інструментами в інтересах навчальної, наукової, професійної і управлінської діяльності. Digital-інструменти дозволяють зосередитися на практичному застосуванні знань та навичок, допомагають робити навчання ефективнішим завдяки використанню різноманітних мультимедійних матеріалів, інтерактивних завдань, більш індивідуалізованого підходу до навчання, можливостям доступу учасників освітнього процесу до великої кількості інформації з різних джерел. Це потребує розвитку відповідних цифрових навичок і відповідальності учасників педагогічного процесу, зокрема у здобувачів. Диджиталізація освіти стає пріоритетним трендом сучасного світу, а нові інформаційні технології – невід'ємною частиною нашого життя [36].

Загальними і етичними здатностями фахівців у сферах спецзв'язку, кібербезпеки та захисту інформації, на які необхідно спрямовувати професійне навчання, з погляду на процеси цифровізації освіти, професійної і управлінської діяльності та суспільного життя, мають бути: професійна, службова і правова компетентність користувача у сфері комунікацій; розвиток цифрових навичок використання інформаційно-комунікаційних і мультимедійних інтерактивних інструментів у навчанні, професійній, науковій діяльності та управлінні, підвищенні професійної кваліфікації; здатність забезпечення особистої кібербезпеки і конфіденційної інформації; постійний пошук і опанування новими знаннями із застосуванням інформаційних технологій та інструментів штучного інтелекту, готовність до їх грамотного використання; соціальна комунікабельність, творча активність, цифрова дисциплінованість, правова обізнаність і конфіденційність у використанні комунікацій; варіативність мислення, передбачення наслідків власної професійної, соціальної та комунікативної діяльності; етичність у використанні інформації у засобах комунікацій та застосуванні інструментів ШІ; відповідальність, самоконтроль, моральна складова особистості, її ціннісні орієнтації, що базуються на національно-патріотичних, державницьких та європейських гуманістичних цінностях, толерантного ставлення до гендерних відмінностей у службовій та професійної діяльності, морально-психологічна стійкість та інформаційна обізнаність в умовах деструктивного інформаційно-психологічного впливу.

Узагальнюючи аналіз наукових джерел, доцільно окреслити визначені освітні пріоритети, спрямовані на з'ясування, адаптацію і впровадження професійних здібностей в систему навчання фахівців в галузі кібербезпеки, що відповідають сучасним вимогам захисту кіберпростору в умовах воєнного стану держави, а *саме:* спрямованість підготовки здобувачів на опанування ціннісними пріоритетами, визнаними українським суспільством, проголошеними у Конституції України, які утворюють ментальні й національно-патріотичні передумови належного виконання професійного і військового обов'язку особистої відповідальності за забезпечення інформаційної безпеки держави та захищеності її кіберпростору; зорієнтованість навчання на всебічну превентивну підготовку фахівців, здатних активно діяти і виконувати професійне завдання в небезпечних умовах воєнного стану, надзвичайних ситуацій і підвищеного ризику, компетентно попереджувати і протидіяти загрозам і небезпекам, зберігати морально-психологічну стійкість у небезпечних умовах воєнного часу; спрямованість підготовки на опанування фахівцями з кібербезпеки спеціальними криптографічними, інформаційно-технологічними та організаційними здатностями, зумовленими розвитком комунікаційних і квантових технологій, штучного інтелекту, новими методами кіберзахисту; націленість навчання на оволодіння здобувачами спеціальними, військовими й безпековими нормами, узгодженими із стандартами, прийнятими для підрозділів сектору безпеки і оборони в країнах – членах ЄС і НАТО; відповідність навчання державній політиці цифровізації України, спрямування підготовки здобувачів на всебічний розвиток цифрових навичок взаємодії у цифровому просторі та підтримання власної кібербезпеки, опанування digital-інструментами, зокрема, штучного інтелекту в інтересах навчальної, наукової, професійної та управлінської діяльності у сфері забезпечення кібербезпеки.

Висновки. Підготовка фахівців з кібербезпеки в умовах зростаючих ризиків і небезпек, викликаних повномасштабним озброєним вторгненням російської федерації в Україну, має базуватися на методологічно обґрунтованій системі професійних, військових і безпекових цінностей, знань, навичок, вмінь і здібностей, що мають забезпечувати професійну здатність і всебічну готовність до виконання завдань за призначенням, відповідають вимогам професійної діяльності в умовах воєнного стану, припускають спроможність фахівця приймати оптимальні, професійні і управлінські рішення у непередбачуваних, небезпечних і надзвичайних ситуаціях.

Застосування результатів теоретичного аналізу пріоритетів підготовки фахівців з кібербезпеки для діяльності в умовах режиму воєнного стану та впровадження в практику підготовки фахівців відповідних здібностей, сприятимете компетентному розв'язанню проблем захисту національного кіберпростору в умовах повномасштабного озброєного

вторгнення російської федерації в Україну та потребує подальших науково-теоретичних і освітніх зусиль науково-педагогічної спільноти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] 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: Черв. 24, 2024.

[2] Президент України. (2020, Вер. 14). *Указ № 392/2020. Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України"* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/392/2020#Text. Дата звернення: Черв. 24, 2024.

[3] Президент України. (2021, Вер. 27). *Указ № 479/2021, Про рішення Ради національної безпеки і оборони України "Про запровадження національної системи стійкості".* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/479/2021#Text. Дата звернення: Черв. 24, 2024.

[4] Y. Danyk, and O. Korneiko, "Fundamentals methodology of formation cyber competences at security sector experts and Ukraine defense", *Information Technology and Security,* vol. 6, iss. 2, pp. 105-123, 2018. doi: https://doi.org/10.20535/2411-1031.2018.6.2.153495.

[5] O. Puchkov, and O. Uvarkina, "Sustainable development of the system of formal cyber education: reflection of modern concepts", *Information Technology and Security*, vol. 11, iss. 1, pp. 60-68, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.1.283635.

[6] О. Пучков, та О. Уваркіна, "Феномен воїнського етосу: соціально-філософська рефлексія", *Вісник Львівського університету. Серія філософські науки*, вип. 29, с. 158-164, 2022. doi: https://doi.org/10.30970/PHS.2022.29.

[7] V. Horlynskyi, and B. Horlynskyi, "*Analysis of key factors of formation of the system of competences of professionals in the field of cybersecurity*", *Information Technology and Security*, vol. 9, iss. 2, pp. 219-231. 2021. doi: https://doi.org/10.20535/2411-1031.2021.9.2.249976.

[8] Верховна Рада України. (2014, Трав. 21). *Закон України № 1556-VII, Про вищу освіту*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/1556-18#Text. Дата звернення: Черв. 24, 2024.

[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: Черв. 24, 2024.

[10] 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: Черв. 24, 2024.

[11] 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: Черв. 24, 2024.

[12] НТУУ КПІ ім. Ігоря Сікорського. (2023, Трав. 17). *Наказ № НОН/165/2023. Безпека державних інформаційних ресурсів. Освітньо-професійна програма першого (бакалаврського) рівня вищої освіти за спеціальністю 125* "*Кібербезпека та захист інформації*". [Електронний ресурс] Доступно: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppb_bdir_2023.pdf. Дата звернення: Черв. 24, 2024.

[13] В. Горлинський, та Б. Горлинський, "Визначальні чинники формування здібностей фахівців для Держспецзв'язку в сучасних умовах", на *І Міжнародної науково-*

практичної конференції "Кібербезпека державних інституцій та подолання кризових станів". Київ, , 2022, с. 164-165.

[14] В. О. Ананьїн, В. В. Горлинський, Л. О. Євдоченко, та О. О. Пучков. "Інформаційні виклики і ціннісні пріоритети суспільства" у *Безпека України: актуальні проблеми та критерії оцінки: монографія*. Київ, Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018.

[15] Президент України. (2019, Трав. 18). *Указ № 286/2019, Про Стратегію національно-патріотичного виховання*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/286/2019/print. Дата звернення: Черв. 24, 2024.

[16] В. Горлинський, *"*Ціннісний вимір національного освітнього простору в умовах війни*"*, на *Всеукраїнському науково-педагогічному підвищенню кваліфікації Різновиди інтелекту та їх роль в освітньому процесі XXI століття*, Львів, 2024, с. 29-32. [Електронний ресурс]. Доступно: https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanc_training_PSAU.pdf#page=29. Дата звернення: Черв. 24, 2024.

[17] В. Ананьїн, та В. Горлинський, "Ментальні структури свідомості як передумова сталого розвитку і безпеки суспільства", *Мультиверсум Філософський альманах,* вип. 2, т. 1, с. 3-18, 2021. doi: https://doi.org/10.35423/2078-8142.2021.2.1.01.

[18] Президент України. (2021, Серп. 20). *Указ №479/2021. Про рішення Ради національної безпеки і оборони України "Про запровадження національної системи стійкості"*. [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/4472021-40013. Дата звернення: Черв. 24, 2024.

[19] Кабінет Міністрів України. (2022, Лют. 23). *Розпорядження № 286-р. Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 роки.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text. Дата звернення: Черв. 24, 2024.

[20] V. Horlynskyi, and B. Horlynskyi, "Constitution of national cyber space and its educational significance for cyber security professionals", *Information Technology and Security*, vol. 11, iss. 1, pp. 69-83, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.1.283710.

[21] Basics of Post-Quantum Cryptography, *Archon.* [Online]. Available: https://www.archonsecure.com/post-quantum-cryptography-guide#chapter-2. Accessed on: Jun. 24, 2024.

[22] І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, та В.А. Пономар, "Проблема стандартизації криптографічних перетворень в перехідний та постквантовий періоди та стан її вирішення", на *Першому міжнародному науково-практичному форумі (Global Cyber Security Forum),* Харків, 2019, с. 6-13, [Електронний ресурс]. Доступно: https://openarchive.nure.ua/server/api/core/bitstreams/c1977b5f-9ed3-4fba-90d3-67bf1e87ed47/content. Дата звернення: Черв. 24, 2024.

[23] United Nations (2024, Mar. 21). *General Assembly adopts landmark resolution on artificial intelligence*. [Online]. Available: https://news.un.org/en/story/2024/03/1147831. Accessed on: Jun. 24, 2024.

[24] NATO (2024, Jul. 10). *Summary of NATO's revised Artificial Intelligence (AI) strategy*. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_227237.htm. Accessed on: Jul. 16, 2024.

[25] Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. [Електронний ресурс]. Доступно: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam. Дата звернення: Черв. 24, 2024.

[26] O. Puchkov, D. Lande, I. Subach, and O. Rybak, "Integration of Information Search Technologies and Artificial Intelligence in the Field of Cybersecurity", *Information Technology and Security*, vol. 11, iss. 2, pp. 206-215, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.2.293789.

[27] Кабінет Міністрів України. (2020, Груд. 02). *Розпорядження № 1556-р. "Про схвалення Концепції розвитку штучного інтелекту в Україні".* [Електронний ресурс]. Доступно:

https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80/print. Дата звернення: Черв. 24, 2024.

[28] B. Edwards, "Microsoft launches AI chatbot for spies", *Ars Technica*, 2024, [Online]. Available: https://arstechnica.com/information-technology/2024/05/microsoft-launches-ai-chatbot-for-spies/. Accessed on: Jun. 24, 2024.

[29] M. Landi. "AI experts 'uncertain' on technology's future, report says", *Independent: UK Edition*, 2024. [Online]. Available: https://www.independent.co.uk/business/ai-experts-uncertain-on-technology-s-future-report-says-b2546861.html. Accessed on: Jun. 24, 2024.

[30] By. Anubhav, "This Study Claims that AI has Learned How to Deceive Humans", *Gizmo China. News*, 2024. [Online]. Available: https://www.gizmochina.com/2024/05/13/ai-deceive-humans-study/. Accessed on: Jun. 24, 2024.

[31] НТУУ КПІ ім. Ігоря Сікорського. (2023, Груд. 29). *Наказ № НОН/393/2023. Політика використання штучного інтелекту для академічної діяльності в КПІ ім. Ігоря Сікорського*. [Електронний ресурс]. Доступно: https://osvita.kpi.ua/node/1225. Дата звернення: Черв. 24, 2024.

[32] М. Зацерківна, "Цифровізація освіти та маркетинг освітніх послуг в умовах збройної агресії російської федерації проти України", *Цифрова платформа: інформаційні технології в соціокультурній сфері,* т. 6, № 1, с. 43-52, 2023, doi: https://doi.org/10.31866/2617-796X.6.1.2023.283941.

[33] Г. Кузан, "Диджиталізація освітнього процесу і дистанційне навчання в Україні: виклики, проблеми, перспективи", *Молодь і ринок*, № 9-10, с. 107-111, 2022. doi: https://doi.org/10.24919/2308-4634.2022.271161.

[34] Кабінет Міністрів України. (2019, Січ. 30). *Постанова № 56. "Деякі питання цифрового розвитку"*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text. Дата звернення: Черв. 24, 2024.

[35] О. Карпенко, та О. Пучков, "Сучасні особливості реалізації державної політики цифрового розвитку в Україні", на *Наук.-практ. конференції "Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання"*, Київ, 2019, с.81-85.

[36] О. Котуха, та Ю. Коцан-Олинець, "Цифровізація сучасної вищої освіти: виклики та завдання", *Юридичний науковий електронний журнал,* № 11, с. 444-447, 2022. doi: https://doi.org/10.32782/2524-0374/2022-11/107. Дата звернення: Черв. 24, 2024.

Стаття надійшла до редакції 23.08.2024.

REFERENCES

[1] 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: Jun. 24, 2024.

[2] President of Ukraine. (2020, Sep. 14). *Decree № 392/2020. Decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine"* [Online]. Available: https://zakon.rada.gov.ua/laws/show/392/2020#Text. Accessed on: Jun. 24, 2024.

[3] President of Ukraine. (2021, Sep. 27). *Decree № 479/2021, Decision of the National Security and Defense Council of Ukraine "On the introduction of the national sustainability system".* [Online]. Available: https://zakon.rada.gov.ua/laws/show/479/2021#Text. Accessed on: Jun. 24, 2024.

[4] Y. Danyk, and O. Korneiko, "Fundamentals methodology of formation cyber competences at security sector experts and Ukraine defense", *Information Technology and Security,* vol. 6, iss. 2, pp. 105-123, 2018. doi: https://doi.org/10.20535/2411-1031.2018.6.2.153495.

[5] O. Puchkov, and O. Uvarkina, "Sustainable development of the system of formal cyber education: reflection of modern concepts", *Information Technology and Security*, vol. 11, iss. 1, pp. 60-68, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.1.283635.

[6] O. Puchkov, and O. Uvarkina, "The Phenomenon of the Warrior Ethos: Socio-philosophical reflection", *Visnuk of the Lviv University. Series philosophical science*, iss. 29, pp. 150-156, 2022. doi: https://doi.org/10.30970/PHS.2022.29.16.

[7] V. Horlynskyi, and B. Horlynskyi, "*Analysis of key factors of formation of the system of competences of professionals in the field of cybersecurity*", *Information Technology and Security*, vol. 9, iss. 2, pp. 219-231. 2021. doi: https://doi.org/10.20535/2411-1031.2021.9.2.249976.

[8] Verkhovna Rada of Ukraine. (2014, May 21). *Law no. 1556-VII, About Higher Education*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1556-18#Text. Accessed on: Jun. 24, 2024.

[9] Verkhovna Rada of Ukraine. (2006, Fab. 23*). Law 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: Jun. 24, 2024.

[10] Verkhovna Rada of Ukraine. (2017, Oct. 5). *Law no. 2163-VIII. About the Basic Principles of Cyber Security of Ukraine*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Accessed on: Jun. 24, 2024.

[11] 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: Jun. 24, 2024.

[12] NTUU KPI Igor Sikorsky. (2023, May 17). Order No. NON/165/2023. Security of state information resources. *Educational and professional program of the first (bachelor) level of higher education in specialty 125* "*Cyber security and information protection*". [Online]. Ava ilable: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppb_bdir_2023.pdf. Accessed on: Jun. 24, 2024.

[13] V. Horlynskyi, and B. Horlynskyi, "Determining factors in the formation of the abilities of specialists for the State Special Service in modern conditions", in *Proc. 1st International Scientific and Practical Conference "Cyber security of state institutions and overcoming crisis situations"*, Kiev, Ukraine, 2022, pp. 164-165.

[14] V. Ananin, V. Horlynskyi, L. Evdochenko, and O. Puchkov, "Information challenges and value priorities of society" in *Safety of Ukraine: Actual problems and evaluation criteria: Monograph*. Kiev, Ukraine: ISCIP Ihor Sikorskyi KPI, 2018.

[15] President of Ukraine. (2019, May 18). *Decree № 286/2019, About the Strategy of National Patriotic Education*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/286/2019/print. Accessed on: Jun. 24, 2024.

[16] V. Horlynskyi, "The value dimension of the national educational space in the conditions of war", in *Proc. All-Ukrainian Scientific and Pedagogical Advanced Training Varieties of Intelligence and Their Role in the Educational Process of the 21-st Century*, Lviv, Ukraine, 2024, pp. 29-32. [Online]. Available: https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanc_training_PSAU.pdf#page=29. Accessed on: Jun. 24, 2024.

[17] V. Ananin, V. Horlynskyi, "Mental structures of consciousness as a prerequisite for sustainable development and security of society", *Multiversum. Philosophical almanac,* iss. 2. vol. 1, pp. 3-18, 2021. doi: https://doi.org/10.35423/2078-8142.2021.2.1.01.

[18] President of Ukraine. (2021, Aug. 20). *Decree № 479/2021. Decision of the National Security and Defense Council of Ukraine "On the introduction of the national sustainability system"*. [Online]. Available: https://www.president.gov.ua/documents/4472021-40013. Accessed on: Jun. 24, 2024.

[19] Cabinet of Ministers of Ukraine. (2022, Fab. 23). *Order no. 286-p. About the praise of the*

Strategy for the development of higher education in Ukraine for 2022-2032. [Online]. Available: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text. Accessed on: Jun. 24, 2024.

[20] V. Horlynskyi, and B. Horlynskyi, "Constitution of national cyber space and its educational significance for cyber security professionals", *Information Technology and Security,* vol. 11, iss. 1, pp. 69-83, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.1.283710.

[21] Basics of Post-Quantum Cryptography, *Archon.* [Online]. Available: https://www.archonsecure.com/post-quantum-cryptography-guide#chapter-2. Accessed on: Jun. 24, 2024.

[22] I. D. Gorbenko, O. G. Kachko, Yu. I. Gorbenko, M. V. Yesina, and V. A. Ponomar, "The problem of standardization of cryptographic transformations in transition and post-quantum periods and the state of its solution", in *Proc. Global Cyber Security Forum, at the First International Scientific and Practical Forum*, Kharkiv, Ukraine, 2019, c. 6–13, [Online]. Available: https://openarchive.nure.ua/server/api/core/bitstreams/c1977b5f-9ed3-4fba-90d3-67bf1e87ed47/content. Accessed on: Jun. 24, 2024.

[23] United Nations (2024, Mar. 21). *General Assembly adopts landmark resolution on artificial intelligence*. [Online]. Available: https://news.un.org/en/story/2024/03/1147831. Accessed on: Jun. 24, 2024.

[24] NATO (2024, Jul. 10). *Summary of NATO's revised Artificial Intelligence (AI) strategy*. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_227237.htm. Accessed on: Jul. 16, 2024.

[25] The role of artificial intelligence in cyber security: predicting and preventing attacks. *Cyber security*.[Online]. Available: https://www.bdodigital.com/insights/cybersecurity/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks#:~:text=AI%20plays%20a%20crucial%20role,help%20predict%20future%20attack%20vectors. Accessed on: Jun. 24, 2024.

[26] O. Puchkov, D. Lande, I. Subach, and O. Rybak, "Integration of Information Search Technologies and Artificial Intelligence in the Field of Cybersecurity", *Information Technology and Security*, vol. 11, iss. 2, pp. 206-215, 2023. doi: https://doi.org/10.20535/2411-1031.2023.11.2.293789.

[27] Cabinet of Ministers of Ukraine. (2020, Dec. 02). *The resolution no. 1556-p. "On the approval of the Concept of the development of artificial intelligence in Ukraine".* [Online]. Available: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80/print. Accessed on: Jun. 24, 2024.

[28] B. Edwards, "Microsoft launches AI chatbot for spies", *Ars Technica*, 2024, [Online]. Available: https://arstechnica.com/information-technology/2024/05/microsoft-launches-ai-chatbot-for-spies/. Accessed on: Jun. 24, 2024.

[29] M. Landi. "AI experts 'uncertain' on technology's future, report says", *Independent: UK Edition*, 2024. [Online]. Available: https://www.independent.co.uk/business/ai-experts-uncertain-on-technology-s-future-report-says-b2546861.html. Accessed on: Jun. 24, 2024.

[30] By. Anubhav, "This Study Claims that AI has Learned How to Deceive Humans", *Gizmo China. News*, 2024. [Online]. Available: https://www.gizmochina.com/2024/05/13/ai-deceive-humans-study/. Accessed on: Jun. 24, 2024.

[31] NTUU KPI Igor Sikorsky. (2023, Dec. 29). *Order No. NON/393/2023. The Policy of Using Artificial Intelligence for Academic Activities at KPI nam. Igor Sikorsky*. [Online]. Available: https://osvita.kpi.ua/node/1225. Accessed on: Jun. 24, 2024.

[32] M. Zatserkivna, "Digitalization of Education and Marketing of Educational Services in the Conditions of the Armed Aggression of the russian federation Against Ukraine", *Digital Platform: Information Technologies in Sociocultural Sphere,* vol. 6, iss. 1, pp. 43-52, 2023. doi: https://doi.org/10.31866/2617-796X.6.1.2023.283941.

[33] H. Kuzan, "Digitization of the Educational Process and Distance Learning in Ukraine: Challenges, Problems, Prospects", *Youth & market*, no. 9, pp. 107-111, 2022. doi: https://doi.org/10.24919/2308-4634.2022.271161.

[34] Cabinet of Ministers of Ukraine. (2019, Jan. 30). *Order no. 56. "Some issues of digital*

development". [Online]. Available: https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text. Accessed on: Jun. 24, 2024.

[35] O. Karpenko, and O. Puchkov, "Modern features of the implementation of the state policy of digital development in Ukraine", in *Proc. Scientific and practical conference "Information and telecommunication systems and technologies and cyber security: new challenges, new tasks"*, Kyiv, Ukraine, 2019, pp. 81-85.

[36] O. Kotuha, and Yu. Kotsan-Olynets, "Digitalization of modern higher education: challenges and tasks", *Legal scientific electronic journal*, no. 11, pp. 444-447, 2022. doi: https://doi.org/10.32782/2524-0374/2022-11/107 Accessed on: Jun. 24, 2024.

VICTOR HORLYNSKYI,
BORIS HORLYNSKYI

EDUCATIONAL PRIORITIES OF TRAINING OF CYBER SECURITY SPECIALISTS UNDER THE CONDITIONS OF THE STATE OF MARTIAL STATE IN THE STATE

Ensuring the cyber security of the state in the conditions of a full-scale invasion of the Russian Federation, the spread of hostilities in the national cyberspace, require a review and clarification of educational priorities in the training of specialists in the field of cyber security. These are the priorities: the focus of training on mastering the values that form the mental national-patriotic prerequisites for the proper performance of professional and military duty, personal responsibility for ensuring cyber security; orientation towards the preventive training of specialists who are able to actively act and perform professional tasks in dangerous conditions of martial law and increased risk, to competently warn and counteract dangers, to maintain moral and psychological stability in dangerous conditions of wartime; targeting the mastering of special, military and security norms by the acquirers, consistent with the standards adopted in the EU and NATO member countries; focus on the assimilation of special, military and security norms by the purchasers, which correspond to the standards adopted in the EU and NATO member states; direction to the comprehensive development of digital skills of interaction in the digital space and maintaining one's own cyber security, mastering digital tools for the organization of activities, in particular, artificial intelligence in the interests of educational, scientific, professional and managerial activities in the field of ensuring cyber security. On the basis of the outlined educational priorities, a list of security and professional abilities is proposed, on the formation of which it is advisable to direct the training of specialists in the field of cyber security.

Keywords: capability, ability, cyber security, cyberspace, cyber threats, competence, education, training of specialists, artificial intelligence.

Горлинський Віктор Вікторович, кандидат філософських наук, доцент, провідний науковий співробітник Науково-дослідного центру, 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, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Київ, Україна, ORCID 0000-0002-9993-2427, vjzgoxnf@gmail.com.

Horlynskyi Viktor, candidate of philosophical sciences (Ph.D), associate professor, a leading researcher of the Scientific Research Center, Institute of special communications and information protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Horlynskyi Borys, candidate of technical sciences, deputy head of the State scientific and research institute of cybersecurity technologies and information protection, Kyiv, Ukraine.