

**НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ ПЕДАГОГІЧНОЇ ОСВІТИ І ОСВІТИ ДОРΟΣЛИХ**

БИСТРОВА БОГДАНА ВАСИЛІВНА

УДК 378.046-021.64:004.492.2(73)

**ПРОФЕСІЙНА ПІДГОТОВКА БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ
У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ США**

13.00.04 – теорія і методика професійної освіти



Автореферат

дисертації на здобуття наукового ступеня
кандидата педагогічних наук

Київ – 2018

Дисертацією є рукопис.

Роботу виконано в Інституті педагогічної освіти і освіти дорослих Національної академії педагогічних наук України (м. Київ).

Науковий керівник – доктор педагогічних наук, доцент
Пазюра Наталія Валентинівна,
Національний авіаційний університет,
завідувач кафедри авіаційної англійської мови
(м. Київ).

Офіційні опоненти: доктор технічних наук, професор,
дійсний член НАПН України
Биков Валерій Юхимович,
Інститут інформаційних технологій і
засобів навчання НАПН України,
директор (м. Київ);

доктор педагогічних наук, професор
Бідюк Наталя Михайлівна,
Хмельницький національний університет,
завідувач кафедри практики іноземної мови та
методики викладання (м. Хмельницький).

Захист відбудеться 4 липня 2018 р. об 11.00 на засіданні спеціалізованої вченої ради Д 26.451.01 в Інституті педагогічної освіти і освіти дорослих НАПН України за адресою: 04060, м. Київ, вул. М. Берлінського, 9, 5-й поверх, зал засідань.

З дисертацією можна ознайомитися на сайті www.ipood.com.ua та у бібліотеці Інституту педагогічної освіти і освіти дорослих НАПН України за адресою: 04060, м. Київ, вул. М. Берлінського, 9.

Автореферат розіслано 1 червня 2018 р.

Учений секретар
спеціалізованої вченої ради



Г.І. Сотська

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження зумовлена стрімким поширенням інформаційних технологій в усіх сферах сучасного суспільства, що потребує якісної підготовки фахівців-професіоналів, які формують нову генерацію представників високотехнологічного соціуму, здатну передавати, зберігати та обробляти інформацію у кіберпросторі, протистояти несанкціонованому втручанням в інформаційне середовище. Важливість збереження конфіденційності інформації, гострий дефіцит у кадровому забезпеченні ІТ-галузі України, а також запровадження нової спеціальності «Кібербезпека» (Постанова Кабінету Міністрів України від 29.04.2015 р.) актуалізують необхідність вивчення зарубіжного досвіду професійної підготовки бакалаврів з кібербезпеки.

Концептуальні засади розвитку ІТ-освіти та професійної підготовки фахівців для ІТ-галузі викладено в законодавчих і нормативно-правових актах нашої держави (Закон України «Про вищу освіту» (2014), «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» (2007), Стратегія сталого розвитку «Україна – 2020 року» (2013), «Про Стратегію кібербезпеки України» (2017), «Про Національну програму інформатизації» (2012)).

В умовах розвитку ІТ-індустрії та появи нової спеціальності «Кібербезпека» зростає потреба вивчення досвіду зарубіжних держав, виявлення конструктивних ідей щодо підготовки ІТ-фахівців задля їх творчої імплементації в Україні. Доцільність звернення до досвіду Сполучених Штатів Америки підтверджується потребою встановлення нових засобів контролю за безпекою відносин в інформаційному просторі; необхідністю збереження конфіденційності інформації як державного, так і приватного характеру; лідерськими позиціями США у наданні інформаційних послуг; створенням ефективної системи підготовки фахівців з кібербезпеки, запозиченої багатьма європейськими країнами; функціонуванням потужної мережі закладів вищої освіти, які здійснюють підготовку конкурентноздатних фахівців з кібербезпеки на світовому ринку. За даними журналу «Business Week», зі 100 провідних компаній світу у рейтингу в галузі інформаційних технологій 75 компаній зареєстровані в США, а три з них («America Online», «Dell Computer», «Solectron») посідають в ньому перші позиції. У 2017 році 65% власників ПК у світі були громадянами США, американські користувачі Інтернету від загальної чисельності у становили 68,4%.

Питання інформатизації суспільства та підготовки фахівців ІТ-галузі висвітлено у працях українських науковців (О. Баранов, В. Биков, І. Джалладова, І. Діордіца, Д. Дубов, Л. Зубик, С. Мельник та інші). Специфіку розвитку вищої технічної освіти в зарубіжних країнах проаналізовано у наукових розвідках Л. Акімової, П. Хейфец (Білорусь); Т. Георгієвої, А. Іванової, В. Парал, С. Романової, О. Скрябіна, М. Чванова, Л. Філіпова, Р. Шаран (США); Т. Мостової, Л. Соловійова (Німеччина); Є. Бражник, В. Єлманової, С. Єрковича, С. Коршунова, І. Федорова (Франція), І. Пододіменко (Японія).

Дотичними до проблеми дослідження є праці з проблем професійної підготовки фахівців у системі вищої освіти США, у яких розкриваються різні її аспекти: Р. Беланової (гуманізація підготовки студентів); О. Даневича, О. Романовського (особливості вищої освіти); Д. Джонстоуна (структура, управління, фінансування

системи вищої освіти); Т. Георгієвої (організація педагогічного процесу в американських університетах і коледжах); Г. Глової (методологія розвитку творчого потенціалу майбутніх інженерів у закладах вищої освіти); С. Зап'ягасва (системний аналіз вищої освіти); С. Зарєцької, Г. Семєко, Е. Каверіна (аспекти доступності американської вищої освіти); І. Зварича (оцінювання знань студентів); Т. Кошманової (розвиток педагогічної освіти); Н. Лізунової (теорія і практика відбору змісту навчання в американській вищій школі); В. Паріла (організація вищої технічної школи); Н. Поліхуна, О. Локшиної (механізм вимірювання якості освіти).

Аналіз документальних і наукових джерел свідчить про суттєвий доробок американських дослідників щодо специфіки підготовки фахівців ІТ-галузі, зокрема: дослідження, в яких розкриваються основні положення кібербезпеки та комп'ютерних мереж (А. Бікак (A. Bick)); технології навчання, їх вплив на ефективність освітнього процесу (Д. Бромвіч (D. Bromwich)); технології управління ризиками кіберзагроз (Г. Раттрея (G. Rattray)); теорії мережевого суспільства (М. Кастельса (M. Castells)); питання глобальної безпеки, кіберзахисту і цифрової трансформації, техногенного права, кіберконфіденційності (Т. Ленцнера (T. Lenzner)), інформаційні технології та кібербезпека (Д. Мерфі (D. Murphy)), Д. Пескатора (J. Pescatore)).

Водночас вивчення джерельної бази дає підстави стверджувати, що проблема професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США не була предметом окремого дослідження і потребує всебічного наукового вивчення.

Науковий аналіз теоретичних основ і практичного досвіду підготовки бакалаврів з кібербезпеки у закладах вищої освіти України дає змогу виявити низку суперечностей між:

- стрімким розвитком інформаційних і телекомунікаційних технологій та недосконалістю механізмів визначення потреб у фахівцях із кібербезпеки, що спричиняє незадовільний стан кадрового забезпечення;
- об'єктивною потребою у гарантіях інформаційної безпеки на національному й індивідуальному рівнях та відсутністю освітніх стандартів професійної підготовки фахівців з кібербезпеки і недостатньою увагою до науково-методичного супроводу їхньої підготовки;
- потребами вітчизняної педагогіки у вивченні прогресивних ідей зарубіжного досвіду для реалізації заходів з кібернетичної безпеки та незадовільним станом його об'єктивного аналізу в Україні.

Актуальність проблеми дослідження, важливість її вивчення для зміцнення національної безпеки України у кіберпросторі, необхідність розв'язання виявлених суперечностей, а також доцільність упровадження прогресивних ідей американського досвіду в умовах сучасних реформаційних змін у вищій освіті України зумовили вибір теми нашого дослідження **«Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США»**.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до тематичного плану науково-дослідної роботи Інституту педагогічної освіти і освіти дорослих НАПН України за темою «Тенденції розвитку освіти дорослих у розвинених країнах світу» (РК № 0117U001070). Тему дисертаційного дослідження затверджено вченою радою Інституту педагогічної освіти і освіти дорослих НАПН України (протокол №1 від 30 січня 2017 р.) та узгоджено в Раді

з координації наукових досліджень у галузі педагогічних і психологічних наук України (протокол № 3 від 16 травня 2017 р.).

Об'єкт дослідження – система професійної підготовки фахівців для ІТ- галузі в США.

Предмет дослідження – зміст, форми організації і методи професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США.

Мета дослідження – на основі цілісного наукового аналізу теоретичних і практичних засад професійної підготовки бакалаврів з кібербезпеки у США обґрунтувати можливості творчого використання прогресивних ідей американського досвіду у закладах вищої освіти України.

Відповідно до об'єкта, предмета, мети визначено **завдання дослідження**:

1. Дослідити стан дослідженості проблеми професійної підготовки бакалаврів з кібербезпеки у педагогічній науці та обґрунтувати основні поняття наукового пошуку.
2. Проаналізувати національну стратегію та вплив соціально-економічних і політичних чинників на професійну підготовку фахівців з кібербезпеки в США.
3. Виявити особливості організації освітнього процесу для бакалаврів з кібербезпеки у вищих навчальних закладах США.
4. Розкрити зміст, форми організації і методи професійної підготовки бакалаврів з кібербезпеки в досвіді американських закладів вищої освіти.
5. Розробити науково-методичні рекомендації щодо можливостей творчого використання прогресивних ідей американського досвіду у підготовці бакалаврів з кібербезпеки у закладах вищої освіти України.

Концептуальна ідея дослідження ґрунтується на положенні про те, що професійна підготовка ІТ-фахівців є міждисциплінарною проблемою, що вивчається з урахуванням національної стратегії її розвитку. Дослідження спрямоване на аналіз професійної підготовки фахівців з кібербезпеки як цілісної системи, в архітектоніці якої враховуються освітні траєкторії, побудовані з урахуванням принципу неперервності й особливостей організації освітнього процесу. Ефективність підготовки фахівців з кібербезпеки забезпечується за умов швидкої адаптації освітнього процесу до зовнішніх (глобалізаційні та інтеграційні процеси, набуття інформаційним простором транснаціонального характеру, широке використання сучасних інформаційних технологій в усіх сферах життєдіяльності суспільства, зростання кіберзлочинності й загострення боротьби з нею) та внутрішніх чинників (необхідність узгодження змісту, форм організації і методів професійної підготовки відповідно до галузевих потреб з метою забезпечення конкурентоспроможності цих фахівців на ринку праці). Вивчення й об'єктивне осмислення конструктивних ідей американського досвіду професійної підготовки фахівців з кібербезпеки та з'ясування можливостей їх творчого використання може слугувати орієнтиром для українських науковців та практиків у процесі модернізації професійної підготовки ІТ-фахівців, які становлять вагомий кадровий потенціал національної безпеки України.

Методологічною основою дослідження є провідні положення наукової теорії пізнання щодо взаємовпливу і взаємозалежності явищ об'єктивної дійсності; системний, культурологічний підходи до порівняльного аналізу педагогічних явищ; філософсько-педагогічні ідеї щодо випереджувального підходу у розвитку сучасної освіти; методологічні принципи порівняльно-педагогічних досліджень; ідеї

компаративістичних досліджень на основі діахронічного і синхронічного вивчення педагогічних, соціально-культурних і економічних реалій.

Теоретичною основою дослідження стали: провідні положення філософії освіти (В. Андрущенко, І. Зязюн, В. Кремень, В. Кудін); неперервності й фундаменталізації професійної підготовки (С. Гончаренко, В. Луговий, Л. Лук'янова, Н. Ничкало); концепції інноваційних технологій професійної підготовки фахівців (О. Дубасенюк, О. Кучерявий, О. Лавріненко, М. Солдатенко, Г. Сотська); положення порівняльної педагогіки (Н. Авшенюк, Н. Бідюк, Б. Вульфсон, О. Джурицький, О. Локшина, О. Матвієнко, О. Огієнко, Н. Пазюра, Л. Пуховська, А. Сбруєва); інформатизації освіти (В. Биков, А. Гуржий, М. Жалдак, О. Спірін, О. Пінчук, Ю. Триус); теоретичні і методичні засади підготовки фахівців ІТ-галузі (О. Баранов, Т. Вдовичин, Г. Глотова, Б. Карія, С. Мельник, К. Батіста (С. Battista)); теорії мережевого суспільства (М. Кастельс (M. Castells), Г. Раттрей (G. Rattray)); концепції з питань розвитку кадрового потенціалу ІТ-сфери (С. Гордійчук, Н. Журавська, О. Кисельова, С. Стрілець, А. Туник, О. Шепета).

Для реалізації визначених завдань використано комплекс взаємопов'язаних **методів дослідження**: *теоретичні* – аналіз і синтез для обґрунтування поняттєво-термінологічного апарату наукового пошуку; структурно-функціональний аналіз – для визначення дидактичних засад професійної підготовки бакалаврів з кібербезпеки; компаративно-педагогічний аналіз – для порівняння і виявлення особливостей професійної підготовки бакалаврів з кібербезпеки в американському й українському досвіді; *емпіричні*: спостереження, опитування, бесіди з українськими і американськими студентами і викладачами; статистичний аналіз – для статистичної обробки й систематизації наукових фактів і даних; верифікації отриманої інформації шляхом зіставлення даних, оприлюднених у наукових джерелах; *прогностичні*: екстраполяції – для обґрунтування шляхів використання прогресивних ідей досвіду США у професійній підготовці бакалаврів із кібербезпеки в Україні.

Джерельна база дослідження. На різних етапах наукового пошуку використано 347 джерел, із них 177 – зарубіжних, зокрема:

аналітичні матеріали міжнародних і національних організацій, відомств, асоціацій та агенцій, що опікуються або регулюють підготовку ІТ-фахівців (ЮНЕСКО, Ради Європи, Європейське агентство мереж та інформаційної безпеки (European Agency for Network and Information Security, ENISA), Організація безпеки та кооперації в Європі (Organisation for Security and Cooperation in Europe, OSCE), Міжнародна асоціація комп'ютерних інформаційних систем (International Association for Computer Information Systems), Міжнародне багатостороннє партнерство проти кіберзагроз (the International Multilateral Partnership Against Cyber Threats, ІМПАКТ), Міжнародна телекомунікаційна спілка (International Telecommunication Union), Національне агентство безпеки (National Security Agency), Комітет систем національної безпеки (Committee on National Security Systems), Національний центр академічної майстерності кіберзахисту (National Centers of Academic Excellence in Information Assurance / Cyber Defense), Національний центр захисту інфраструктури (National Infrastructure Protection Center), Агенція захисту інформаційних систем (Defense Information Systems Agency);

законодавчі та нормативно-правові документи США (Presidential Decision Directive 63 (PDD 63), National Strategy to Secure Cyberspace 2003, Homeland Security Act of 2002, Cyber Security Research and Development Act тощо);

науково-методичні й інформаційно-аналітичні матеріали, освітньо-професійні програми, навчальні плани, програми коледжів та університетів США (Walden University, American Military University, Embry-Riddle Aeronautical University, St. John's University, Mercy College, Iona College, Saint Vincent College);

наукові праці вітчизняних і зарубіжних дослідників, зокрема американських (A. Bork, D. Bromwich, A. Bicap, J. Gorgone, P. Gray, J. Franscella, E. Stohr та ін.);

публікації у вітчизняних і зарубіжних науково-педагогічних періодичних виданнях, серед яких – «Освіта для сучасності», «Порівняльно-педагогічні студії», «Порівняльна професійна педагогіка» («Comparative professional pedagogy»), «Journal of Digital Learning in Teacher Education», «Journal of Information Systems Education», «Journal of Learning Analytics», «Program Information Systems Education Journal», «Roadmap for Improving Critical Infrastructure Cyber security» тощо;

офіційні веб-сторінки вищих навчальних закладів США, енциклопедії, довідники, словники тощо.

Організація дослідження. Дисертаційне дослідження проводилося упродовж 2015–2018 рр. й охоплювало три етапи.

На *першому (пошуковому) етапі* (2015–2016 рр.) обґрунтовано теоретичні засади проблеми дослідження, сформовано поняттєво-категоріальний апарат, вивчено джерельну базу, здійснено бібліографічний аналіз та первинну обробку дослідницьких матеріалів.

На *другому (дослідно-аналітичному) етапі* (2016–2017 рр.) проаналізовано автентичні навчальні плани і освітньо-професійні програми підготовки фахівців з кібербезпеки та компоненти організації освітнього процесу у вищих навчальних закладах США.

На *третьому (підсумковому) етапі* (2017–2018 рр.) узагальнено результати дослідження, сформульовано висновки, укладено науково-методичні рекомендації щодо впровадження прогресивних ідей американського досвіду в українських закладах вищої освіти.

Наукова новизна і теоретичне значення одержаних результатів полягає в тому, що:

- *вперше* у вітчизняній педагогічній науці здійснено комплексне дослідження професійної підготовки бакалаврів зі спеціальності «Кібербезпека» у вищих навчальних закладах США, зокрема обґрунтовано положення про вплив соціально-економічних та політичних чинників на оновлення професійної підготовки фахівців з кібербезпеки; схарактеризовано особливості підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США: організаційні (гнучкість, відкритість, автономність, індивідуалізація, орієнтація на потреби роботодавців, диверсифікація форм організації навчання та джерел фінансування, соціальне партнерство основних учасників навчального процесу тощо), змістові (міждисциплінарний характер навчання, підготовка за двома спеціальностями, запровадження спеціалізацій із кібернетичної безпеки у межах інших спеціальностей, інтеграція теоретичного і практичного компонентів підготовки, постійне оновлення змісту відповідно до потреб ІТ-галузі),

технологічні (практико-орієнтовані форми організації навчання, проблемно-пошукові і рефлексивно-орієнтовані методи навчання); з'ясовано можливості творчого використання прогресивних ідей американського досвіду у закладах вищої освіти України;

- *уточнено* змістове наповнення понять «ІТ-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист», «інформаційна безпека», «кібербезпека», «кібербезпекова політика», «ризики», «фахівець з кібербезпеки»; «бакалавр з кібербезпеки», «професійна підготовка бакалавра з кібербезпеки»;

- *подальшого розвитку* набули положення щодо забезпечення якості професійної підготовки бакалаврів з кібербезпеки;

- *до наукового обігу* введено дотепер невідомі і маловідомі в Україні праці американських дослідників, документи, навчально-методичні матеріали, освітньо-професійні програми, теоретичні ідеї і підходи до підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США.

Практичне значення дослідження полягає у підготовці науково-методичних рекомендацій «Професійна підготовка бакалаврів з кібербезпеки: досвід США» для студентів закладів вищої освіти, в яких обґрунтовано шляхи використання прогресивних ідей американського досвіду для модернізації професійної підготовки майбутніх фахівців з кібербезпеки в Україні. Основні положення, теоретичні висновки, джерельна база дослідження можуть бути корисними для розроблення освітніх стандартів підготовки бакалаврів з кібербезпеки, спецкурсів і спецсеминарів для підготовки майбутніх фахівців ІТ-галузі, оновлення навчальних планів і програм, удосконалення організації професійної підготовки майбутніх фахівців з кібербезпеки в Україні. Результати наукового пошуку будуть корисними для науковців, викладачів у здійсненні історико-педагогічного аналізу, компаративістичних досліджень.

Результати дослідження впроваджено в освітній процес Національної академії державної прикордонної служби України імені Богдана Хмельницького (довідка № 107/3–162 від 15.01.2018 р.), Національного Авіаційного Університету (довідка № 183/5–112 від 05.02.2018 р.), Черкаського державного технологічного університету (довідка № 97/13–87 від 22.01.2018 р.), Чернігівського національного технологічного університету (довідка № 101/10–158 від 26.01.2018 р.).

Апробація результатів дослідження. Основні результати дослідження обговорено і схвалено на науково-практичних конференціях, семінарах, читання різного рівня, з-поміж яких: *міжнародні*: «Педагогічна майстерність: методологія, теорія, технології» (Черкаси, 2014, 2015), «Проблеми та інновації в природничо-математичній, технологічній і професійній освіті» (Кропивницький, 2017), «Вища школа: удосконалення якості підготовки фахівців» (Київ, 2017, 2018), «Modern scientific knowledge» (Morrisville, USA, 2017), «Педагогічна компаративістика і міжнародна освіта – 2017 : освітні трансформації у контексті європейської інтеграції і глобалізації» (Київ, 2017), «Освіта і формування конкурентоспроможності фахівців в умовах євроінтеграції» (Мукачево, 2017); *всукраїнські*: «Іншомовна підготовка працівників правоохоронних органів та сектору безпеки» (Київ, 2017), «Актуальні напрями досліджень молодих учених в іншомовному просторі» (Житомир, 2018); *звітні наукові конференції* Інституту педагогічної освіти та освіти дорослих НАПН України (Київ, 2015–2018).

Публікації. Основні результати дослідження висвітлено в 15 публікаціях, з них: 6 статей у наукових фахових виданнях України (у т.ч. 1 – у виданні України, що включено до міжнародних наукометричних баз); 1 стаття у зарубіжному науковому періодичному виданні; 1 методичні рекомендації; 7 публікацій у збірниках матеріалів науково-практичних конференцій.

Структура й обсяг дисертації. Робота складається з анотацій українською й англійською мовами, вступу, трьох розділів, висновків до кожного з них, загальних висновків, списку використаних джерел (усього 347 найменувань, з них 177 – іноземними мовами) та додатків на 43 сторінках. Загальний обсяг дисертації становить 244 сторінки, основний зміст викладено на 182 сторінках. Робота містить ілюстрований матеріал – 14 рисунків та 13 таблиць.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовано актуальність обраної теми; відображено зв'язок роботи з науковими програмами, планами і темами; сформульовано мету, завдання; окреслено об'єкт, предмет, методи дослідження; представлено наукову новизну та практичне значення; подано відомості про апробацію результатів, публікації, структуру й обсяг дисертації.

У першому розділі – **«Професійна підготовка фахівців з кібербезпеки як проблема порівняльної педагогіки»** – схарактеризовано стан дослідженості проблеми професійної підготовки фахівців з кібербезпеки у педагогічній і науково-методичній літературі; визначено основні поняття дослідження; проаналізовано підходи до професійної підготовки фахівців з кібербезпеки у документах міжнародних організацій.

Зважаючи на транснаціональний характер інформаційного простору, зростання кількості злочинів у цій сфері та глобалізований характер кібернетичної безпеки, питання підготовки та підвищення кваліфікації фахівців у зазначеній галузі є принципово важливим як для США, так і для України. Вивчення наукового доробку вітчизняних й зарубіжних науковців і практиків засвідчило, що професійна підготовка фахівців з кібербезпеки є однією зі складових національної безпеки, без якої неможливими є захищене передавання інформації і відповідно – науково-технічний та соціально-економічний розвиток країни. На основі студіювання праць з'ясовано, що в умовах інформаційних війн, замахів на цілісність і суверенітет держави проблема підготовки фахівців з кібербезпеки є не лише педагогічною, а й системною, міждисциплінарною. Основний аспект дослідження українських педагогів стала освітня діяльність у галузі «Інформаційні технології». Ученими (В. Акіменко, Л. Гришко, С. Семеріков, О. Співаковський й ін.) здійснено аналіз стану й проблем становлення вітчизняної системи освіти, підготовки ІТ-фахівців в інших країнах світу (І. Пододіменко, Р. Шаран), запропоновано заходи щодо модернізації освітнього процесу фахівців ІТ-галузі. У роботах В. Баскакова, М. Дімчогло, В. Залізняка, О. Климентьєва, Д. Лобова, Ю. Максименко, М. Микитенко, В. Політило, А. Туніка, О. Шепета закладено методологічні основи формування сучасних освітніх стандартів з професійної підготовки фахівців з кібербезпеки.

Визначено, що відкритими для наукової дискусії є питання змістового наповнення понять: «ІТ-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист», «інформаційна безпека», «кібербезпека», «кібербезпекова політика»,

«ризик», «фахівець з кібербезпеки», «фахівець з інформаційної безпеки» «бакалавр з кібербезпеки», «професійна підготовка бакалаврів з кібербезпеки». Розбіжності у наукових поглядах на ці поняття зумовлюють специфіку структурно-змістових та організаційно-педагогічних засад професійної підготовки фахівців ІТ-галузі в США.

На основі аналізу нормативно-правових документів міжнародних організацій (ЮНЕСКО, НАТО, Європейського Союзу), зокрема «Стратегії кібербезпеки Європейського Союзу» («European Union Cyber Security Strategy: An open, safe and secure cyberspace», 2013), «Директиви Європарламенту щодо атак інформаційних систем» («Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA»), «Пропозицій Європарламенту щодо забезпечення високого рівня мережевої і інформаційної безпеки на теренах Союзу» («Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union», 2009), Концепції кібербезпеки країн Європейського Союзу, Світового форуму кіберекспертів (Global Forum on Cyber Expertise (GFCE)), матеріалів міжнародних конференцій з питань захисту кіберпростору тощо), з'ясовано вимоги ЄС до забезпечення його глобального, відкритого, безпечного характеристик. В документах визначені важливі складові кібербезпекової стратегії розвитку європейського простору: створення необхідної інформаційно-комунікаційної системи та інфраструктури, розроблення спільних стандартів ефективності його функціонування, забезпечення необхідної освіти та підготовки фахівців з кібербезпеки, законодавче урегулювання освітньої діяльності, постійний розвиток та упровадження інновацій в ІТ-галузі, кооперація діяльності світової спільноти у розбудові кіберпростору.

Особливу увагу приділено організаційним, людським, матеріальним, технічним та фінансовим ресурсам, необхідним для створення спеціальних структур, метою діяльності яких є запобігати або мінімізувати наслідки кібератак. У документах наголошується на необхідності врахування різних рівнів економічного, технічного, соціального розвитку країн світу, їх культурних особливостей у процесі розбудови глобального, безпечного кіберпростору. Зазначені документи спрямовані на посилення міжнародної кооперації, розвитку спільного бачення проблеми кіберзагроз, ефективного використання наявного технічного і людського потенціалу, розроблення «дорожньої карти» для злагодженої і послідовної реалізації планів. Міжнародні документи спрямовані на законодавче врегулювання створення національних систем кібербезпеки країн світу. Відповідно виникає необхідність в імplementації положень міжнародних організацій, що спрямоване насамперед на упровадження сучасних освітньо-професійних програм підготовки бакалаврів з кібербезпеки, розроблення сучасних навчальних планів та програм на основі випереджувального підходу для розвитку спеціальних навичок фахівців з кібербезпеки, поліпшення якості професійної підготовки та підвищення продуктивності їхньої діяльності, забезпечення необхідної кількості фахівців, здатних ефективно вирішувати проблеми інформаційної захищеності суспільства.

У другому розділі – «Система професійної підготовки бакалаврів з кібербезпеки у США» – проаналізовано положення Національної стратегії професійної підготовки фахівців з кібербезпеки; виявлено соціально-економічні та

політичні чинники впливу на професійну підготовку майбутніх фахівців з кібербезпеки; викладено загальну характеристику системи професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США; визначено освітні траєкторії у неперервній освіті американських ІТ-фахівців.

З'ясовано, що Національна стратегія США щодо удосконалення інформаційної безпеки, задоволення кількісних та якісних вимог ринку праці до професійної підготовки кадрів з кібербезпеки реалізується шляхом виконання середньострокових та довгострокових завдань: визнання сертифікованих програм підготовки, формування свідомого ставлення суспільства до ризиків кіберзагроз та їх наслідків, підвищення ефективності чинних програм, на основі запровадження соціального партнерства різних зацікавлених структур і навчальних закладів, зростання рівня мотивації приватних компаній щодо розроблення, поширення сертифікованих програм з їх подальшим визнанням на національному рівні.

Виявлено чинники впливу на розвиток та становлення американської системи професійної підготовки фахівців з кібербезпеки: *техніко-технологічні* (науково-технічний та технологічний прогрес, розвиток кібернетичних ресурсів, комунікаційних систем, мережевої інфраструктури та інформаційних технологій, створення єдиного кіберпростору), *політичні* (розвиток національної кібербезпекової політики США, потреба захисту цивільних прав та інтересів бізнесового, наукового, технічного, військового, фінансового потенціалу та потенціалу високих технологій країни, необхідність прогнозування та протидії кіберзагрозам), *соціальні* (набуття людиною нової функції суб'єкта та об'єкта кіберборотьби, виникнення соціального та галузевого запиту на спеціальність, необхідність у формуванні відповідального ставлення населення до національної та індивідуальної інформаційної безпеки), *економічні* (гострий дефіцит кадрів у галузі інформаційних технологій, що стрімко розвивається, нові вимоги ринку праці до фахівців завдяки структурному перерозподілу зайнятості населення).

Проаналізовано основні принципи організації вищої освіти США, а саме: децентралізація управління освітою на рівні штатів; незалежність та повна автономія вищого навчального закладу; рівноправне функціонування державних, приватних і напівприватних вищих навчальних закладів; можливість вільного вибору студентами курсів/дисциплін; демократичність, рівноправність шансів кожної людини у здобутті вищої освіти. Схарактеризовано ступеневу структуру вищої освіти США, в якій функціонують: університети; інтеграційні університети, в яких активно проводяться наукові дослідження; дворічні технічні (Technical Colleges) та молодші (Junior Colleges) коледжі, місцеві або громадські (Community Colleges) коледжі; коледжі вільних мистецтв, де пропонуються курси академічної освіти; коледжі чотирирічного навчання, які за статусом прирівнюються до вищих навчальних закладів; професійні вищі школи. Вимоги до абітурієнтів та здобувачів освітньо-кваліфікаційного рівня «бакалавр» визначаються диференційовано з урахуванням базового освітнього рівня, регіональних потреб штату. Важливо, що кожен здобувач ОКР «бакалавр» зі спеціальності «Кібербезпека» проходить суворий відбір на професійну надійність: студенти, які потенційно схильні до використання сформованих умінь у злочинних цілях, до навчання не допускаються.

Виявлені диверсифіковані освітні траєкторії здобуття освіти та охарактеризовано систему неперервної професійної підготовки фахівців з кібербезпеки в США, що функціонує на засадах відкритості, гнучкості, варіативності, послідовності та спадкоємності засвоєння знань, їх постійного вдосконалення та оновлення відповідно до потреб галузі. З'ясовано, що національну політику країни в ІТ-галузі в США формує Агентство національної безпеки (АНБ). Міністерству оборони США відведена важлива роль щодо розв'язання поставлених завдань на національному рівні, а його спеціальний підрозділ менеджменту програм в галузі кібербезпеки (Information Assurance Program Office) опікується питаннями удосконалення форм та методів навчання фахівців ІТ-галузі. Підготовка компаніями цих фахівців на базі закладів вищої освіти та залучення міжнародних консорціумів з їхньої сертифікації стала традиційною практикою, що забезпечує практичну спрямованість, гнучкість і безперервність освіти. Така інтеграція наукового, академічного, бізнесового та військового секторів й запровадження механізмів здобуття фаху альтернативним шляхом сприяло більш ефективному задоволенню кількісних та якісних потреб ІТ-галузі у кваліфікованих фахівцях з кібербезпеки.

У третьому розділі – «**Дидактичні засади професійної підготовки бакалаврів з кібербезпеки у закладах вищої освіти США**» – визначено змістові і структурно-організаційні особливості теоретичної і практичної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США; схарактеризовано форми і методи організації освітнього процесу бакалаврів з кібербезпеки; виявлено рівні забезпечення якості підготовки бакалаврів з кібербезпеки в американських закладах вищої освіти.

Аналіз освітньо-професійних програм підготовки у 45 американських вищих навчальних закладах 25 штатів США дозволив виявити змістові і структурно-організаційні особливості організації професійної підготовки бакалаврів з кібербезпеки. З'ясовані можливі шляхи здобуття освітньо-кваліфікаційного рівня «бакалавр» зі спеціальності «Кібербезпека» за різними моделями навчання (модель 4-річного навчання в одному закладі (вищий коледж / університет / професійна школа) та модель «2+2» (молодший коледж / технічна школа) + (вищий коледж / університет / вища професійна школа). Така диверсифікація в американській вищій школі зумовлює істотні відмінності у програмах і функціях вищих навчальних закладів відповідно до різноманітних соціально-культурних та соціально-економічних запитів суспільства.

Вивчення навчальних програм вищих навчальних закладів США дозволило виявити та узагальнити обов'язкові вимоги до організації підготовки фахівців для ІТ-галузі зі спеціальності «Кібербезпека»: об'єктно-орієнтоване та практично-спрямоване навчання; активна участь представників галузі та федеральних структур у структуруванні змісту професійної підготовки бакалаврів; забезпечення практичної підготовки студентів означеної спеціальності». В освітньо-професійних програмах визначено перелік необхідних для бакалавра з кібербезпеки компетентностей (інтегральна компетентність, загальні та спеціальні фахові компетентності). На основі аналізу 7 бакалаврських освітньо-професійних програм з кібербезпеки 4 американських університетів (Walden University, American Military University, Embry-Riddle Aeronautical University, St. John's University) та 3 коледжів (Mercy College, Iona College, Saint Vincent College) визначено оптимальний перелік дисциплін циклів загальної професійної та фахової підготовки. До циклу фахової підготовки належать обов'язкові

(«Інформаційна безпека», «Розслідування комп'ютерних інцидентів», «Міжмережіві екрани і виявлення вторгнень», «Безпека бездротових мереж» тощо) та вибіркові дисципліни («Соціальні аспекти інформаційної безпеки», «Дані і інтелектуальний аналіз», «Безпека розподілених баз даних», «Політика інформаційної безпеки», «Практичні питання безпеки» тощо).

Зміст освітньо-професійних програм структуровано з урахуванням принципів послідовності і наступності. Спостерігається збільшення частки дисциплін, що розкривають правозахисні аспекти діяльності фахівців у галузі кібербезпеки відповідно до міжнародного права, особливості розслідування кіберінцидентів, та дисциплін, які спрямовані на вивчення специфіки захисту інтелектуальних прав і використання технологій кібербезпеки у бізнесі. Така тенденція підтверджує пріоритетність міждисциплінарного підходу до підготовки бакалаврів з кібербезпеки, яка забезпечує інтеграцію структурних елементів наукового знання дисциплін різних циклів і значно підвищує конкурентоспроможність випускників на ринку праці. Важливо, що адаптація та постійне оновлення змісту навчання (кожні 90 днів) відбуваються відповідно до технічних змін в ІТ-галузі.

Практична підготовка бакалаврів з кібербезпеки здійснюється в органах силових структур і державного управління, промислової і банківської сфери, в яких студенти оволодівають необхідними професійними навичками та вміннями. Результати практики суттєво впливають на подальшу долю випускника американського університету чи коледжу, а заробітна плата, яку одержують студенти під час практики, може частково покрити витрати на навчання.

Схарактеризовано шляхи підвищення якості професійної підготовки фахівців із кібербезпеки, а саме: поєднання *традиційних* (лекції, практикуми, семінари, лабораторні заняття з елементами дослідження, конференції, консультації) та *інноваційних форм* навчання (онлайн-лекції, лекції-подкасти, робота Fablab «Кібербезпека», демо-зони засобів кіберзахисту, бізнес-інкубаторів для створення стартапів, онлайн-тести, лекція з опорними конспектами; лекція-візуалізація; лекція-дискусія; семінар-дискусія, поєднання міні-лекції з обговоренням проблем у парах чи малих групах тощо); *інтерактивних методів* («круглий стіл», «засідання експертної групи», «дебати», «форум», «навчання від зворотного», ситуаційного навчання, аналізу кризових ситуацій (кібератак, ризиків кіберзагроз), рольових ігор) та використання ІКТ, що сприяє успішній реалізації цілей професійної підготовки бакалаврів з кібербезпеки. Проведений аналіз засвідчив, що американська система демонструє значну диверсифікацію форм звітності академічної діяльності студентів зі спеціальності «кібербезпека» та відсутність можливості перескладати іспити.

Одним із заходів постійного вдосконалення діяльності вищих навчальних закладів США є проведення аудиторських перевірок. Подано загальну характеристику процедури зовнішнього оцінювання американських вищих навчальних закладів, визначальними рисами якої є добровільна основа проходження акредитації, самостійне прийняття рішення щодо її необхідності. Виявлено основні критерії аудиту, як-то: залучення незалежних агенцій професійних асоціацій та університетів у якості аудиторів; відповідність освітньо-професійних програм галузевим вимогам щодо підготовки фахівців із кібербезпеки; забезпеченість освітнього процесу матеріальними, науково-методичними та кадровими ресурсами.

У четвертому розділі – **«Перспективні напрями вдосконалення професійної підготовки бакалаврів з кібербезпеки в Україні»** – розглянуто сучасний стан підготовки бакалаврів з кібербезпеки у закладах вищої освіти України; здійснено порівняльно-педагогічний аналіз особливостей професійної підготовки бакалаврів з кібербезпеки в США та Україні; з'ясовано можливості творчої реалізації конструктивних ідей американського досвіду в системі вищої освіти України.

Виявлення особливостей професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США і України було проведено з урахуванням сукупності критеріїв, що забезпечують його коректність, а саме: *нормативно-правовий* (аналіз законодавчих документів, що регламентують професійну підготовку бакалаврів з кібербезпеки); *організаційний* (особливості організації освітнього процесу, проведення вступних випробувань, практичної підготовки); *змістовий* (обсяг освітньо-професійних програм підготовки бакалаврів, зміст і характеристика професійних компетентностей, цикли підготовки за навчальним планом, змістове наповнення практичної підготовки майбутніх фахівців з кібербезпеки), *технологічний* (форми, методи організації освітнього процесу у вищих навчальних закладах, особливості оцінювання навчальних досягнень студентів у процесі оволодіння професійними компетентностями).

Проведений порівняльно-педагогічний аналіз засвідчив підвищення вимог, що висуваються до рівня теоретичних знань та практичних умінь випускників спеціальності «Кібербезпека» в Україні та США. Водночас в Україні, попри усвідомлення важливості підготовки фахівців з кібербезпеки, не існує державних стандартів та чітко визначених кваліфікаційних характеристик з означеної спеціальності, затверджених на державному рівні, що пояснюється ліквідацією напрямку підготовки «Інформаційна безпека» й запровадження спеціальності «Кібербезпека» в межах галузі знань «Інформаційні технології» з 2016 р.

Виявлено, що в Україні основна підготовка фахівців із кібербезпеки відбувається на освітньо-кваліфікаційному рівні «бакалавр». Вітчизняні заклади вищої освіти (Національний авіаційний університет, Національний технічний університет України «Київський політехнічний інститут», Київський національний університет імені Тараса Шевченка, Київський національний економічний університет імені Вадима Гетьмана, Національний університет «Львівська політехніка» тощо) на законодавчому рівні здобули тимчасове (до введення стандартів вищої освіти України) право на підготовку здобувачів освітньо-кваліфікаційного рівня «бакалавр» зі спеціальності 125 «Кібербезпека». Однак, незважаючи на наявність ліцензій на підготовку бакалаврів з цієї спеціальності, методологічні й методичні засади стандартизації професійної підготовки потребують обґрунтування та оновлення підходів до її розроблення.

Аналіз освітньо-професійних програм, навчальних планів професійної підготовки бакалаврів за спеціальністю «Кібербезпека» українських закладів вищої освіти вказує на їх неузгодженість у змістовому компоненті, недостатню практичну спрямованість, про що свідчить обмежений обсяг спеціалізованих професійно-орієнтованих дисциплін, наявність дисциплін базової підготовки («Алгебра», «Геометрія», «Диференціальні рівняння» тощо) у блоці професійної підготовки. Співвідношення загальноосвітніх дисциплін до професійно-орієнтованих складає 1:3, а співвідношенні між лекційним і практичним заняттями – приблизно 2:1. Відсоток дисциплін за вибором студента дорівнює 33 % від кількості обов'язкових (67 %).

Знівельовано гуманітарну складову професійної підготовки цих фахівців, посилення якої можливе за рахунок включення правничої складової до змісту освіти або предметів для виховання «глобальної культури кібербезпеки». В результаті такої невідповідності спостерігається неузгодженість результатів підготовки у закладах вищої освіти з вимогами майбутніх роботодавців до знань, умінь і навичок випускників, неготовність бакалаврів з кібербезпеки до складання міжнародних фахових іспитів, відсутність у випускників навичок практичної діяльності, що значно знижує їхню конкурентоспроможність на ринку праці.

Доведено, що в практичній підготовці бакалаврів з кібербезпеки в українських закладах вищої освіти бракує інтегративного підходу з метою поєднання навчання в університеті та здобуття практичних умінь на майбутньому потенційному робочому місці; спостерігається недостатньо налагоджене соціальне партнерство із можливими роботодавцями для оволодіння практикантами необхідними галузевими знаннями.

Вивчення досвіду підготовки бакалаврів з кібербезпеки у системі вищої освіти США дозволяють виокремити особливості: абсолютна перевага американських університетів у розмірах фінансування, матеріально-технічному забезпеченні підготовки фахівців цієї галузі; практична орієнтація підготовки, що сприяє розвитку кар'єрних можливостей випускників спеціальності «Кібербезпека» та полегшує їхнє працевлаштування; наявність гнучких освітніх планів, широкого спектру навчальних курсів за вибором, що сприяє мобільності траєкторій навчання; прагматичний практико-орієнтований підхід у структуруванні змісту підготовки; домінування самостійної практичної роботи над аудиторним теоретичним навчанням.

За результатами порівняльно-педагогічного аналізу професійної підготовки бакалаврів з кібербезпеки у закладах вищої освіти України і США обґрунтовано науково-методичні рекомендації щодо використання конструктивних ідей американського досвіду в українських реаліях на таких рівнях: *стратегічному* (удосконалення законодавчої бази, що регламентує діяльність закладів вищої освіти України у процесі організації професійної підготовки бакалаврів з кібербезпеки; розроблення нових професійних стандартів, що сприятиме забезпеченню якості підготовки та професійному розвитку фахівців; здійснення підготовки на засадах компетентнісного підходу; визначення у варіативній складовій освітніх стандартів конкретних компетенцій, пов'язаних із майбутньою професійною діяльністю, що акцентуватиме увагу педагогів на формуванні відповідних знань і умінь у процесі навчання та і сприятиме вирішенню проблеми адаптації на ринку праці тощо), *організаційному* (створення ефективного механізму акредитації закладів вищої освіти відповідно до світових стандартів; розроблення системи відбору абітурієнтів для вступу на спеціальність із застосуванням тестування на професійну придатність та засвоєння норм професійної етики; заохочення на постійній основі фахівців, що працюють в ІТ-галузі, для проведення лекційних та практичних занять; застосування в освітньому процесі активних, творчих, дослідницьких, проблемних, проектних методів навчання, дискусій, ділових ігор, що сприятиме підвищенню мотивації до навчальної діяльності та якісній підготовці майбутніх фахівців тощо), *змістовому* (постійне оновлення змісту підготовки бакалаврів з кібербезпеки відповідно до змін, що відбуваються у галузі; запровадження міждисциплінарного підходу до структурування змісту; створення можливості для оволодіння на якісно новому рівні іноземними мовами, суміжними

дисциплінами, необхідними для роботи у певній галузі; підготовка фахівців з кібербезпеки відповідно до систематизованих відомостей з різних секторів ринку праці, що мають потребу в такій категорії професіоналів; зорієнтованість на збільшення кількості годин, відведених на практичну підготовку; впровадження у практичну підготовку програм інтернатури на потенційному робочому місці тощо).

ВИСНОВКИ

На основі узагальнення результатів наукового пошуку обґрунтовано такі висновки:

1. Аналіз проблеми дослідження засвідчив, що у педагогічному дискурсі вітчизняної педагогічної науки вивчалися лише окремі аспекти проблеми підготовки фахівців з кібербезпеки в США, насамперед визначення особливостей організації освітнього процесу у галузі знань «Інформаційні технології». Ученими здійснено аналіз стану й проблем становлення вітчизняної ІТ-освіти, виявлено особливості підготовки фахівців ІТ-галузі в зарубіжних країнах, запропоновано окремі заходи з модернізації освітнього процесу з урахуванням потреб інформаційного суспільства. Студіювання теоретичних праць з проблеми професійної підготовки бакалаврів з кібербезпеки дозволило з'ясувати, що спектр питань щодо ефективності підготовки фахівців відповідно до вимог сучасного соціуму залишаються відкритими і нерозв'язаними. У результаті наукового пошуку уточнено важливі для нашого дослідження поняття: «ІТ-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист», «інформаційна безпека», «кібербезпека», «кібербезпекова політика», «ризики», «фахівець з кібербезпеки». Проблема професійної підготовки бакалаврів з кібербезпеки потребує проведення системних досліджень на основі аналізу світових тенденцій професійної підготовки фахівців ІТ-галузі з метою творчого використання позитивних напрацювань зарубіжної вищої школи у вітчизняній системі освіти.

2. Вивчення досвіду підготовки фахівців з кібербезпеки у США уможливило доведення, що освітній процес спрямований на реалізацію Національної стратегії, в якій визначено основні завдання середньострокової та довгострокової перспективи (постійне збільшення обсягів інвестицій для ІТ-галузі для її подальшого розвитку; виховання відповідального ставлення громадян країни до ризиків кіберзагроз та їх наслідків; популяризація спеціальностей та мотивація талановитої молоді до здобуття цього фаху; створення, модернізація та підвищення ефективності чинних освітньо-професійних програм підготовки фахівців з кібербезпеки; заохочення галузевого, військового, бізнесового секторів з метою максимального наближення програм навчання до практичних потреб галузі; запровадження нових та визнання чинних програм сертифікації фахівців з кібербезпеки, посилення ролі вищої освіти у підготовці висококваліфікованих фахівців – еліти з кібербезпеки). Необхідність реалізації Національної стратегії зумовлювалася соціально-економічними (набуття людиною нової функції суб'єкта та об'єкта кіберборотьби, гострий дефіцит кадрів з інформаційних технологій, що стрімко розвивається, нові вимоги ринку праці до фахівців в умовах структурного перерозподілу зайнятості населення) і політичними чинниками (зростання кількості кібератак та підвищення загрози кібервійни, необхідність прогнозування та протидії кіберзагрозам). З'ясовано, що професійна

підготовка фахівців з кібербезпеки спрямована на задоволення поточних і перспективних потреб сучасного інформаційного суспільства.

3. До особливостей організації професійної підготовки бакалаврів з кібербезпеки в США, що здійснюється в коледжах й університетах віднесено: вертикальну інтеграцію ступенів навчання; варіативність моделей підготовки, проходження відбору на професійну придатність; об'єктно-орієнтоване та практико-спрямоване навчання; укладання освітньо-професійних програм подвійних спеціальностей; раціональну організацію самостійної і науково дослідницької роботи студентів; активну участь представників цієї галузі у структуруванні змісту підготовки та організації освітнього процесу; підвищення конкурентоспроможності випускників на основі широкопрофільності підготовки; забезпечення проходження практики студентами в установах, організації, на підприємстві, яке є потенційним робочим місцем; цілеспрямоване формування мотивації студента.

В основу організації та функціонування професійної підготовки бакалаврів з кібербезпеки у США покладено принципи прогностичності, диверсифікації, міжпредметності, варіативності, ступневості, демократизації, децентралізації, об'єктивності, відкритості, наступності, професіоналізації, предметної спеціалізації, елективності. Результат такої підготовки – висококваліфікований фахівець ІТ-галузі, який володіє інтегральними, загальними і спеціальними фаховими компетентностями та здатний якісно виконувати професійні завдання.

4. Аналіз змісту, форм організації і методів професійної підготовки бакалаврів з кібербезпеки засвідчив, що її ефективність забезпечується шляхом постійного оновлення змісту освіти відповідно до галузевих потреб та використання широкого діапазону інноваційних форм і методів навчання. Зміст підготовки характеризується міждисциплінарністю та випереджувальним підходом. Доведено, що вивчення обов'язкових та вибіркових дисциплін, спрямованих на оволодіння поглибленими знаннями в ІТ-галузі, виконання студентами дипломного проекту, наукових досліджень, проходження практики на потенційному робочому місці забезпечує зорієнтованість їхньої підготовки на подальше професійне неперервне зростання.

Автономія закладів вищої освіти США уможливило вільний вибір інноваційних форм (онлайн-лекції, лекції-подкасти, Fablab, демо-зони, бізнес-інкубатори тощо) і методів (ділові ігри, дискусії, аналіз ризиків кібератак, симуляція кібербезпекових ситуацій, методи «від зворотного», «мозкового штурму» тощо) навчання, що сприяє формуванню компетентних фахівців, здатних вирішувати найскладніші завдання з метою протистояння правопорушенням у кіберпросторі.

5. Здійснений порівняльно-педагогічний аналіз професійної підготовки у вищих навчальних закладах США та закладах вищої освіти України за нормативно-правовим, змістовим, організаційним та технологічним критеріями дозволив виявити подібне та відмінне у підготовці бакалаврів з кібербезпеки. До подібного віднесено: позитивну динаміку у кількості вступників на освітньо-професійні програми підготовки бакалаврів з кібербезпеки; підвищення престижності цього фаху завдяки можливості подальшого гідного працевлаштування та високої оплати праці; диверсифікація професійної підготовки бакалаврів з кібербезпеки; кредитно-модульна система організації освітнього процесу. Водночас існує низка відмінних ознак у законодавчому, науково-методичному, інформаційному, матеріально-технічному, забезпеченні

освітнього процесу, а саме: абсолютна перевага американських університетів у обсягах фінансування, матеріально-технічних засобах підготовки фахівців цієї галузі; практична зорієнтованість підготовки; гнучкість освітньо-професійних програм тощо. Виявлення прогресивних ідей американського досвіду уможливило розроблення науково-методичних рекомендацій щодо удосконалення системи професійної підготовки фахівців з кібербезпеки в Україні на стратегічному, змістовому й організаційному рівнях.

Проведене дослідження не вичерпує всіх аспектів цієї актуальної проблеми. До подальших напрямів наукового пошуку вважаємо за доцільне віднести: дидактичне обґрунтування особливостей професійного розвитку персоналу ІТ-компаній в США; психолого-педагогічні й організаційні засади підготовки фахівців ІТ-галузі до педагогічної діяльності в умовах інтеграції освітнього та промислового секторів.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації

1. Бистрова, Б. (2016). До питання щодо обґрунтування необхідності досліджень професійної підготовки бакалаврів із кібербезпеки в США. *Гуманізація навчально-виховного процесу*, 6 (80), 150–158.

2. Бистрова, Б. (2017). Особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США. *Вісник Черкаського університету. Серія: Педагогічні науки*, 6, 15–19.

3. Бистрова, Б. (2017). Основні поняття дослідження та концептуальні засади професійної підготовки фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*, (72), 58–70.

4. Бистрова, Б. (2017). Системний підхід до організації професійної освіти в галузі підготовки бакалаврів з кібербезпеки в США. *Наукові записки. Серія: Проблеми методики фізико-математичної і технологічної освіти*, 11 (4), 31 - 39.

5. Бистрова, Б. (2017). Модернізація освітньої програми «Кібербезпека»: реалії та перспективи. *Науковий вісник Мукачівського державного університету. Серія «Педагогіка та психологія»*, 2 (6), 22–24.

6. Bystrova, B. (2017). Comparative analysis of curricula for bachelor's degree in cyber security in the USA and Ukraine. *Comparative professional pedagogy*, 7(4), 114–119.

7. Bystrova, B. (2017). *Comparison of the educational cybersecurity programs of the United States and Ukraine universities*. USA: Lulu Press.

8. Бистрова, Б. (2017). *Професійна підготовка бакалаврів з кібербезпеки: досвід США*. Київ: Альфа-ППК.

Опубліковані праці апробаційного характеру

9. Бистрова, Б. (2014). Особливості підготовки кадрів в області кібербезпеки США. В О.А. Біда (Ред.), *Педагогічна майстерність: методологія, теорія, технології: І Міжнародна науково-практична конференція, Черкаси, 22-23 травня*, (с. 119–121). Черкаси: видавець Чабаненко Ю.А.

10. Бистрова, Б. (2015). Загальна політика США у сфері кібербезпеки. В О.А. Біда (Ред.), *Педагогічна майстерність: методологія, теорія, технології: II Міжнародна науково-практична конференція, Черкаси, 22-23 травня*, (с. 9–10). Черкаси: видавець Чабаненко Ю.А.

11. Бистрова, Б. (2017). Формування сучасного освітнього середовища для підготовки бакалаврів в області кібербезпеки у ВНЗ США. В Н.В. Пазюра (Ред.), *Вища школа: удосконалення якості підготовки фахівців: I міжнародна науково-практична конференція, Київ, 26-29 квітня*, (с. 15–17). Черкаси: видавець Чабаненко Ю.А.

12. Бистрова, Б. (2018). Структура та зміст моделі управління процесом практичного навчання бакалаврів з кібербезпеки у ВНЗ США. В Н.В. Пазюра (Ред.), *Вища школа: удосконалення якості підготовки фахівців: II міжнародна науково-практична конференція, Київ, 26-29 квітня*, (с. 10–13). Київ: Альфа-ППК.

13. Бистрова, Б. (2017). Шляхи розвитку освіти в Україні (спеціальність «Кібербезпека»): реалії та перспективи. В Т.Д. Щербан (Ред.), *Освіта і формування конкурентоспроможності фахівців в умовах євроінтеграції. Матеріали міжнародної науково-практичної конференції, Мукачєво, 26 – 27 жовтня*, (с. 31 – 33), Мукачєво: Вид-во МДУ.

14. Бистрова, Б. (2017). Загальні підходи до реформування системи вищої освіти в галузі підготовки бакалаврів з кібербезпеки в США. *Ініціативна підготовка працівників правоохоронних органів та сектору безпеки: Всеукраїнська науково-практична конференція, Київ, 21 – 22 квітня*. (с.20-22), Київ: Національна академія прокуратури України.

15. Bystrova, B. (2018). The Peculiarities of Professional Training of Bachelors in Cybersecurity: American Model. *Current Trends in Young Scientists' Research V All Ukrainian Scientific and Practical Conference Zhytomyr, 12 April*, (p. 166 – 168), Zhytomyr: ZSTU.

АНОТАЦІЇ

Бистрова Б.В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата педагогічних наук за спеціальністю 13.00.04 – теорія і методика професійної освіти. – Інститут педагогічної освіти і освіти дорослих НАПН України. – Київ, 2018.

У дисертаційній роботі схарактеризовано категоріально-поняттєвий апарат дослідження, проаналізовано стан дослідженості проблеми професійної підготовки фахівців з кібербезпеки у педагогічній і науково-методичній літературі; досліджено підходи до питання підготовки фахівців з кібербезпеки у документах міжнародних організацій.

Подано характеристику Національної стратегії розвитку ІТ-галузі та виявлено соціально-економічні і політичні чинники впливу на підготовку майбутніх фахівців з кібербезпеки у вищих навчальних закладах США; представлено загальну характеристику організації професійної підготовки бакалаврів з кібербезпеки у системі вищої освіти США; виявлено диверсифіковані освітні траєкторії у неперервній освіті фахівців ІТ-галузі. Визначено особливості змісту, схарактеризовано форми, методи професійної підготовки бакалаврів з кібербезпеки; з'ясовано шляхи забезпечення якості професійної підготовки означених фахівців.

Проаналізовано сучасний стан підготовки бакалаврів з кібербезпеки у закладах вищої освіти України. На основі порівняльно-педагогічного аналізу особливостей професійної підготовки бакалаврів з кібербезпеки в США та Україні виявлено подібне та відмінне, з'ясовано можливості творчої реалізації конструктивних ідей американського досвіду в системі освіти України.

Ключові слова: професійна підготовка бакалаврів з кібербезпеки, заклади вищої освіти США, освітньо-професійна програма підготовки, зміст, форми і методи навчання.

Быстрова Б.В. Профессиональная подготовка бакалавров кибербезопасности в высших учебных заведениях США. – Рукопись.

Дисертація на соискание ученой степени кандидата педагогических наук по специальности 13.00.04 – теория и методика профессионального образования. – Институт педагогического образования и образования взрослых НАПН Украины. – Киев, 2018.

В диссертационной работе охарактеризован категориально-понятийный аппарат исследования, проанализирована степень изученности проблемы профессиональной подготовки специалистов кибербезопасности в педагогической и научно-методической литературе; изучены подходы к подготовке специалистов по кибербезопасности в документах международных организаций.

Представлена стратегия развития сферы информационных технологий, выявлены социально-экономические и политические факторы влияния на подготовку будущих специалистов кибербезопасности в высших учебных заведениях США; подана общая характеристика организации профессиональной подготовки бакалавров кибербезопасности в системе высшего образования США; выявлены

диверсифицированные образовательные траектории специалистов в непрерывном образовании. Определены особенности содержания, охарактеризованы формы, методы профессиональной подготовки бакалавров кибербезопасности, выявлены способы обеспечения качества профессиональной подготовки бакалавров кибербезопасности.

Рассмотрено современное состояние подготовки бакалавров кибербезопасности в заведениях высшего образования Украины. На основе сравнительно-педагогического анализа особенностей профессиональной подготовки бакалавров кибербезопасности в США и Украине выявлены подобные и отличительные черты, выяснены возможности творческой реализации конструктивных идей американского опыта в системе образования Украины.

Ключевые слова: профессиональная подготовка бакалавров кибербезопасности, заведения высшего образования США, образовательно-профессиональная программа, содержание, формы и методы обучения.

ABSTRACT

Bystrova B.V. Professional training of bachelors in Cybersecurity in the US Higher Education Institutions. – Manuscript.

Dissertation for the degree of a Candidate of Pedagogical Sciences in specialty 13.00.04 – Theory and methodology of professional education. Institute of Pedagogical and Adult Education of the National Academy of Pedagogical Sciences of Ukraine, Kyiv, 2018.

The aim of this study is to determine the course of research and to highlight its results. Thus, a comprehensive study of bachelors' professional training in the field of 'Cyber Security' at US universities and colleges was conducted. For analysis, 45 universities in 25 states have been selected. In particular, the features of the training structure (flexibility, sociability, autonomy, orientation towards the needs of employers, the diversity of its types, forms of organization and funding sources; social partnership between the State and the community, the interaction of the major participants in the bachelor's study programme in the United States, etc.) have been explored and revealed.

The scientific novelty of the obtained results and the theoretical significance of the study is that for the first time in the national pedagogical science a comprehensive analysis of the bachelors' professional training in the field of 'Cyber Security' in higher education institutions in the United States was carried out; the organizational, pedagogical and didactic principles of the cybersecurity bachelor's professional training in the American higher education system are disclosed; a comparative-pedagogical analysis of the cybersecurity bachelor's professional training in higher education institutions in the United States and universities in Ukraine was conducted.

The peculiarities of the study content are the multidisciplinary nature of teaching and learning, double majors studying, and the introduction of cybernetic security specializations in other specialties, the integration of the theoretical and practical components in the process of specialists training.

With regard to the forms and methods of professional training of bachelors from cybersecurity, they are aimed at research skills development, an independent work organization, interactivity, and total computerization).

The comparative and pedagogical analysis of the cybersecurity bachelor's professional training in higher education institutions in the United States and Ukrainian universities gave the basis for the extrapolation possibilities of American experience constructive ideas into the system of higher technical education in Ukraine on the strategic, organizational, and content levels.

The content of the concepts 'IT industry', 'cyber threats', 'cyberspace', 'cyber defense', 'information security', 'cybersecurity', 'cyber security policy', 'cybersecurity specialist', 'Bachelor in Cybersecurity', 'Professional training of Bachelor's degree in Cybersecurity' has been specified. The further development of regulations to ensure the quality of cybersecurity bachelor's professional training in the American experience has been gained.

The study has become of practical importance due to the preparation of methodical recommendations 'Cybersecurity Bachelor's Professional Training: US Experience', which outlines the possibilities of American experience constructive ideas implementation to upgrade the professional training of cybersecurity specialists in Ukraine.

The study sources, the main features, the theoretical conclusions that may be useful for the educational standards development of cybersecurity specialists training and teachers of comparative pedagogy courses were worked out. Reasonable scientific and methodological recommendations on the constructive ideas creative realization of American experience in Ukraine can be used by Ukrainian scholars and scientists in pedagogical and comparative research as well as in the courses development and special courses in pedagogy of higher education, comparative pedagogy, and special seminars on pedagogical innovations.

Key words: professional training of bachelors in cybersecurity, establishments of higher education, professional education program, contents, forms and methods of education.

Наклад 100 прим.

Підписано до друку 30.05.2018 року

Зам. АУ/295-3

Віддруковано ТОВ «Альфа-ПК».

Посвідчення про внесення суб'єкта видавничої справи до державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції серія ДК №1806
від 25.05.2004р.

01034, м. Київ, вул. Малопідвальна 21/8. тел. 270-73-54.