НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ ПЕДАГОГІЧНОЇ ОСВІТИ І ОСВІТИ ДОРОСЛИХ

Кваліфікаційна наукова праця на правах рукопису

БИСТРОВА БОГДАНА ВАСИЛІВНА

УДК 378.046-021.64:004.492.2(73)

ДИСЕРТАЦІЯ

ПРОФЕСІЙНА ПІДГОТОВКА БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ США

13.00.04 – теорія та методика професійної освіти

Подається на здобуття наукового ступеня кандидата педагогічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів, текстів інших авторів мають посилання на відповідне джерело

_____ / Б. В. Бистрова
(підпис, ініціали та прізвище здобувача)

Науковий керівник:
Пазюра Наталія Валентинівна
доктор педагогічних наук, доцент

Київ – 2018

АНОТАЦІЯ

Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США - Кваліфікаційна наукова праця на правах рукопису

Дисертація на здобуття наукового ступеня кандидата педагогічних наук (доктора філософії) за спеціальністю 13.00.04 «Теорія і методика професійної освіти» (012 - Професійна освіта). Інститут педагогічної освіти і освіти дорослих НАПН України, Київ, 2018

Вивчення наукового доробку вітчизняних й зарубіжних науковців і практиків засвідчило, що професійна підготовка фахівців з кібербезпеки є однією зі складових національної безпеки, без якої є неможливими 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.

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 чинниками.

У дисертаційній роботі особливу увагу приділено організаційним, людським, матеріальним, технічним та фінансовим ресурсам, необхідним для створення спеціальних структур, метою діяльності яких є запобігати або мінімізувати наслідки кібератак. Зокрема, необхідності врахування різних рівнів економічного, технічного, соціального розвитку країн світу, їх культурних особливостей у процесі розбудови глобального, безпечного кіберпростору; посиленню міжнародної кооперації, розвитку спільного бачення проблеми кіберзагрози, ефективного використання наявного технічного і людського потенціалу, розроблення «дорожньої карти» для злагодженої і послідовної реалізації планів. Представлено міжнародні документи, які спрямовані на законодавче врегулювання процесу творення національних систем кібербезпеки країн світу. Обґрунтовано необхідність імплементації положень міжнародних організацій, що спрямовані 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.

Наукова новизна отриманих результатів та теоретичне значення дослідження полягає у 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.

Описано хід та результати комплексного дослідження професійної підготовки бакалаврів зі спеціальності «Кібербезпека» в університетах та коледжах США. Для аналізу обрано 45 вищих навчальних закладів з 25 штатів. Зокрема досліджено та виявлено особливості структури цієї підготовки (гнучкість, відкритість, автономність, орієнтація на потреби роботодавців, різноманітності її видів, форм організації та джерел фінансування; соціальне партнерство держави та громади, взаємодія основних учасників підготовки бакалаврів з кібербезпеки у США тощо).

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 широко-профільності підготовки; забезпечення проходження практики студентами в установі, організації, на підприємстві, яке є потенційним робочим місцем; цілеспрямоване формування мотивації студента.

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.

Набули подальшого розвитку положення щодо забезпечення якості професійної підготовки бакалаврів з кібербезпеки в американському досвіді. 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 напряму підготовки «Інформаційна безпека» й запровадження спеціальності «Кібербезпека» в межах галузі знань «Інформаційні технології» з 2016 р.

Дослідження набуло практичного значення завдяки підготовці методичних рекомендацій «Професійна підготовка бакалаврів з кібербезпеки: досвід США», в яких окреслено можливості використання конструктивних ідей американського досвіду для модернізації професійної підготовки фахівців з кібербезпеки в Україні. Потреба якої підсилюється збільшенням випадків кіберзлочинів та вимог інформаційного суспільства. Опрацьована джерельна база дослідження, основні положення, теоретичні висновки, що можуть бути корисними для

укладачів освітніх стандартів підготовки фахівців з кібербезпеки та викладачів навчальних курсів із порівняльної педагогіки. Обґрунтовані науково-методичні рекомендації щодо творчої реалізації конструктивних ідей американського досвіду в Україні можуть бути використані українськими науковцями в педагогічних та порівняльних дослідженнях, а також при розробці курсів і спецкурсів із педагогіки вищої школи, порівняльної педагогіки, спецсемінарів із проблем педагогічних інновацій.

Ключові слова: *кібербезпека, професійна підготовка бакалаврів з кібербезпеки, освітньо-професійна програма (ОПП), ключові компетенції фахівця з кібербезпеки, американська модель вищої освіти, порівняльна педагогіка, диверсифікація, неперервна освіта, сертифікація, стандартизація, теоретична та практична підготовка бакалаврів з кібербезпеки, методичні рекомендації, інноваційні форми навчання, екстраполяція прогресивних ідей.*

Список публікацій здобувача

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-ПІК.

Наукові праці апробаційного характеру

9. Бистрова, Б. (2014). Особливості підготовки кадрів в області кібербезпеки США. В О.А. Біда (Ред.), *Педагогічна майстерність: методологія, теорія, технології: I 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-ПІК.

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, Мукачево, 26 – 27 жовтня, (с. 31 – 33), Мукачево: Вид-во МДУ.

14. Бистрова, Б. (2017). Загальні підходи до реформування системи вищої освіти в галузі підготовки бакалаврів з кібербезпеки в США. *Іншомовна 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.

ABSTRACT

Professional training of bachelors in Cybersecurity in the US Higher Education Institutions – Qualifying scientific work published as a manuscript.

Dissertation for the degree of a Candidate of Pedagogical Sciences (doctor of philosophy) in specialty 13.00.04 – 'Theory and methodology of professional education' (012 – Professional education). Institute of Pedagogical Education 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: cyber security, cybersecurity bachelors' professional training, *Professional Education Program* (PEP), key competences of cybersecurity specialist, American model of higher education, comparative pedagogy, diversification, continuing education, certification, standardization, theoretical and practical cybersecurity bachelors' training, methodical recommendations, innovative forms of training, extrapolation of progressive ideas.

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ……14

ВСТУП……...16

РОЗДІЛ 1. ПРОФЕСІЙНА ПІДГОТОВКА ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ЯК ПРОБЛЕМА ПОРІВНЯЛЬНОЇ ПЕДАГОГІКИ

1.1. Аналіз стану дослідженності проблеми підготовки фахівців з кібербезпеки у США…….27

1.2. Основні поняття дослідження …….....38

1.3. Проблема підготовки фахівців з кібербезпеки у документах міжнародних організацій …….55

Висновки до розділу 1…….64

РОЗДІЛ 2. СИСТЕМА ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ ІЗ КІБЕРБЕЗПЕКИ У США

2.1.Національна стратегія підготовки фахівців з кібербезпеки у США…67

2.2. Загальна характеристика підготовки бакалаврів з кібербезпеки у закладах вищої освіти США……...…81

2.3. Освітні траєкторії у неперервній освіті ІТ фахівців у США ……91

Висновки до розділу 2…….…….107

РОЗДІЛ 3. ДИДАКТИЧНІ ЗАСАДИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ США

3.1. Змістові та структурно-організаційні особливості теоретичної і практичної підготовки бакалаврів з кібербезпеки в навчальних закладах США……109

3.2. Форми і методи організації навчального процесу бакалаврів з кібербезпеки……..124

3.3. Рівні забезпечення якості підготовки бакалаврів з кібербезбеки у вищих навчальних закладах США…….....…137

Висновки до розділу 3……145

РОЗДІЛ 4. ПЕРСПЕКТИВНІ НАПРЯМИ ВДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ В УКРАЇНІ

4.1. Становлення і розвиток професійної підготовки фахівців із кібербезпеки в Україні…….....148

4.2. Порівняльно-педагогічний аналіз професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США та України.....162

4.3. Обґрунтування можливостей використання прогресивних ідей досвіду США з професійної підготовки бакалаврів з кібербезпеки у вітчизняній системі вищої освіти……183

Висновки до розділу 4……..189

ЗАГАЛЬНІ ВИСНОВКИ.....191

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....195

ДОДАТКИ.....218

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АНБ – Агенція національної безпеки

АПІТУ – Асоціація підприємств інформаційних технологій України

БІР НАП – банк інформаційних ресурсів навчального призначення

ГСВО – галузеві стандарти вищої освіти

ІКТ – інформаційні та комп'ютерні технології

ІНТ – інформаційні науки та технології

ІСМ – інформаційні системи та мережі

ІТ – інформаційні технології

НІТ – новітні інформаційні технології

ННІДС НАУ–Навчально-науковий інститут інформаційно-діагностичних систем Національноий авіаційний університет

НТУУ КПІ – Національноий технічний університет України Київський політехнічний інститут

ОКР – освітньо-кваліфікаційний рівень

ОКХ – освітньо-кваліфікаційна характеристика

ОПП – освітньо-професійна програма

ABET (Accreditation Board for Engineering and Technology) – Рада з акредитації програм у галузі техніки і технологій

ACT (American College Testing) – американське тестування

CALS (Computer Acquisition of Lifesycle of Studying) – система комп'ютерного супроводу навчального процесу

CSP (Cisco Certified Security Professional) – фахівець із безпеки сертифікації Cisco

CEH (Certified Ethical Hacker) – сертифікований етичний хакер

CIP 2010 (Classification of Instructional Programs) – КОП 2010, класифікатор освітніх програм, розроблений Національним центром освітньої статистики США у 2010 році

CISA (Certified Information Systems Auditor) – аудитор сертифікованих інформаційних систем

CISSP (Certified Information System Security Professional) – сертифікованаий фахівець з безпеки інформаційної системи

DISA (Defense Information Systems Agency) – Агентство з захисту інформаційних систем

E-learning (від англ. Electronic Learning) – система електронного навчання

IACIS (International Association for Computer Information Systems) – Міжнародна асоціація фахівців комп'ютерних досліджень

IAPO (Information Assurance Program Office) – Управління програм з інформаційної безпеки

ISO 27001 Lead Implementer (International Organization for Standardization) – Міжнародна організація з стандартизації, головний виконавець

ISO 27001 Lead Auditor (International Organization for Standardization) – Міжнародна організація з стандартизації, головний аудитор

ISO/IEC JTC (International Organization for Standardization / The International Electrotechnical Commission Joint Technical Committee) – об’єднаний технічний комітет №1

GED (General Equivalency Diploma) – диплом про середню освіту

МОС/МЕК – підрозділ Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії, що займається проблемами стандартизації в галузі IT

NIPC (National Infrastructure Protection Center) – Національний центр захисту інфраструктури, що об'єднав представників влади, військових і приватний сектор

O*NET (The Occupational Information Network) – довідкова комп’ютерна мережа Департаменту праці США

ICANN (Internet Corporation for Assigned Names and Numbers) – Інтернет-корпорації з присвоєння імен та номерів

SAT (Scholastic Assessment Test) – схоластичний оцінювальний тест

SOC (Standard Occupational Classification) – стандартний класифікатор професій у США

ВСТУП

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 втручанню 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. Параіл, С. Романової, О. Скрябіна, М. Чванова, Л.Філіпова, Р. Шаран (США); Т. Мостової, Л. Соловйова (Німеччина); Є. Бражник, В. Єлманової, С. Єрковича, С. Коршунова, (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. Бєланової (гуманізація підготовки студентів); О. Данєвича, О. Романовського (особливості вищої освіти); Д. Джонстоуна (структура, управління, фінансування системи вищої освіти); Т. Георгієвої (організація педагогічного процесу в американських університетах і коледжах); Г. Глотової (методологія розвитку творчого потенціалу майбутніх інженерів у закладах вищої освіти); С. Запрягаєва (системний аналіз вищої освіти); С. Зарєцької, Г. Семеко, 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. Bicak)); технології навчання, їх вплив на ефективність освітнього процесу (Д. Бромвіч (D. Bromwich)); технології управління ризиками кіберзагроз (Г. Раттрейя (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 підготовка 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. Джуринський, О. Локшина, О. Матвієнко, О. Огієнко, Н. Пазюра, Л. Пуховська, А. Сбруєва); інформатизації освіти (В. Биков, А. Гуржиій, 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 (C. 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. Тунік, О. Шепета).

Для реалізації визначених завдань використано комплекс взаємопов'язаних **методів дослідження**: *теоретичні* – аналіз і синтез для обґрунтування понятєво-термінологічного апарату наукового пошуку; структурно-функціональний аналіз – для визначення дидактичних засад професійної підготовки бакалаврів з кібербезпеки; компаративно-педагогічний аналіз – для порівняння і виявлення особливостей професійній підготовці 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 Co-operation 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, IMPACT), 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. Bicak , 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 понятєво-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 спецсемінарів 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 контекстів європейської інтеграції і глобалізації (Київ. 2017), «Освіта і формування конкурентоспроможності фахівців в умовах євроінтеграції» (Мукачево, 2017); *всеукраїнські:* «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 статей 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.

РОЗДІЛ І. ПРОФЕСІЙНА ПІДГОТОВКА ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ЯК ОБ'ЄКТ ДОСЛІДЖЕННЯ ПОРІВНЯЛЬНОЇ ПЕДАГОГІКИ

У розділі 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.

1.1. Аналіз стану дослідженості проблеми професійної підготовки фахівців ІТ-галузі

Стрімке поширення інформаційних та телекомунікаційних технологій (ІКТ) та набуття ними повсюдного характеру в сучасному соціумі свідчить про те, що вони є невід'ємною частиною життя сучасної людини, відповідно фундаментально змінило принципи функціонування суспільства в багатьох аспектах. ІКТ надали безпрецендентні можливості та переваги для активного життя кожної людини, долаючи часові, просторові та інші контекстуальні обмеження. У концепції «Цілі розвитку тисячоліття» (Millennium Development Goals) Ради економічного та соціального розвитку об'єднаних націй (United Nations Educational, Scientific and Cultural Organization, 2016, с. 8) зазначено, що «міжнародна спільнота лише починає усвідомлювати потенціал ІКТ у досягненні пріоритетів свого розвитку». Тому ІКТ були визнані засобом уможливлення та підтримки трьох пріоритетів сталого розвитку будь-якого суспільства: соціального та економічного, а також захисту навколишнього середовища.

Водночас із значними можливостями та перевагами поширення цифрових технологій спричинило ряд соціальних та етичних проблем. У світі зростає громадська стурбованість щодо цифрової нерівності різних країн, загрози онлайн-безпеки громадян, ризиків для здоров'я під час використання ІКТ. Крім того, з'явились нові типи злочинів, що відбуваються у кіберпросторі: зловживання інформацією, порушення безпеки передавання даних, порушення

інтелектуальної власності (плагіат і піратство), онлайн-пропаганда, радикалізація. Окремі злочини свідчать про порушення базових прав людини: кібер-знущання, кібер-шахрайство, секс-трафік, розповсюдження порнографії, крадіжки особистих даних тощо. Тривожні доповіді очільників різних держав щодо негативного впливу ІКТ змушують на національному рівні застосовувати цензуру або суворі правила їх використання та доступу до Інтернету, фільтрації та блокування контенту. Безпека в кіберпросторі та попередження кіберзлочинів є критично важливими чинниками загального добробуту суспільства.

Зазначимо, що проблема забезпечення кібербезпеки є надзвичайно актуальною для України, беручи до уваги агресію Російської Федерації, що триває, а заходи з протидії викликам і загрозам у цій сфері перебувають на початковому етапі та не мають комплексного характеру вирішення. Підтвердженням цього стала кібератака 27 червня 2017 р. (цей день отримав назву «чорного вівторка» у контексті кібербезпеки нашої країни) комп'ютерного вірусу «Ransom:Win32/Petya» на приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування тощо.

На жаль, наша держава виявилася неспроможною протистояти такій атаці, яка виявила незахищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору та відсутність можливостей своєчасного виявлення, запобігання і нейтралізації реальних та потенційних загроз національній безпеці у кіберпросторі (Грабовий, 2017).

У нестабільних умовах внутрішньої та зовнішньої політики виникає потреба у професійній підготовці значної кількості компетентних ІТ-фахівців, здатних працювати в інформаційному суспільстві. Ця потреба зумовила необхідність консолідації зусиль світової спільноти у формуванні цілісного

підходу до підготовки кадрів, здатних забезпечити ефективність функціонування кіберпростору та гарантій захищеного статусу його користувачів.

Недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації від кіберзагроз, а також інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України спонукали до невідкладного створення національної системи кібербезпеки як складової системи національної безпеки України. В її основу покладено положення Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV(Верховна Рада України, 2005) . Вимога захисту державних інформаційних ресурсів та інформації встановлена законодавством України щодо основ національної безпеки та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» (Верховна Рада України, 2015).

Проаналізуємо ключові положення відповідних законодавчих документів для виявлення перспектив професійної підготовки фахівців з кібербезпеки. У Стратегії національної безпеки України визначені пріоритети та напрями забезпечення кібербезпеки України, що передбачають підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, виховання комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадження державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту. Крім того, наголошується на необхідності встановлення кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам (Рада національної безпеки і оборони України, 2016).

У Законі України « Про основні засади забезпечення кібербезпеки України» визначено важливі базові поняття в галузі кіберзахисту та кібербезпеки і окреслено права й обов'язки державних органів у цьому напрямі. Стаття 8 наголошує на важливості підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов’язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об’єктів критичної інфраструктури, з урахуванням міжнародних стандартів (Закон України «Про основні засади…» Верховна Рада України, 2017).

На наше переконання, впровадження нових підходів до професійної підготовки фахівців з кібербезпеки неможливе без належного опрацювання досягнень українських та зарубіжних науковців і практиків у цій галузі. До проблеми підготовки інженерів у галузі інформаційно-комунікаційних технологій в Україні та за кордоном зверталося багато дослідників. Важливими працями у контексті нашої проблеми є дослідження В. Бикова (2011), А. Гурджій (2013), Г. Козлакової (2012), Т. Морозова (2005), З. Сейдаметової (2004) та ін. Аналізу специфіки розв’язання завдань у галузі програмування і формування професійних якостей програмістів присвячені праці педагогів та психологів (Ф. Брукс (2012), Г. Вейнберг, Н. Вірт (1989), Е. Дейкстра (1975), С. Макконелл (2010), М. Смульсон (2013), О. Тихоміров (2006), Г. Цейтін, Б. Шнейдерман (2016) та ін.). Дослідження особливостей підготовки ІТ-фахівців здійснено в роботах В. Акіменка, Л. Гришка, С. Семерікова (2009), О. Співаковського (1986, 2004) та ін. Окремі аспекти неперервної освіти і відкритого навчання висвітлено у працях Б. Вульфсона (2002), О. Кареліної (2005), І. Козубовської (2016), В. Кухаренка, Н. Ничкало (2002), Н. Сиротенка, П. Стефаненка (2016), О. Спіріна (2016) та ін.

Академік В. Биков зазначає, що так як інформаційно-комунікаційні технології (ІКТ) належать до високих технологій, а їх розвиток і широке

впровадження на законодавчому рівні віднесено до пріоритетних напрямів розвитку науки и техніки України на період до 2020 року, важливим і складним завданням є підготовка висококваліфікованих кадрів для ІТ-індустрії, де позитивні результати і прогалини в їх підготовці проявляються особливо разюче. Якість підготовки таких кадрів не тільки відображається на їхній індивідуальній конкурентоспроможності на ринку праці, але й безпосередньо впливає на науково-технічний рівень ІТ-продукції, її конкурентоспроможність на міжнародних ринках товарів і послуг, а тому і на загальну конкурентоспроможність економіки України. Вчений підкреслює залежність перспектив інтеграції України у світовий економічний простір та збереження національної безпеки країни від якості підготовки ІТ-фахівців (Биков, 2011).

Здійснений аналіз наукової літератури дозволяє стверджувати, що завдяки транснаціональному характеру кіберпростору в різних країнах світу існують спільні проблеми, а до професійної підготовки фахівців ІТ-галузі висуваються подібні вимоги, що потребують нагального вирішення. Останнім часом особливий інтерес привертає концепція компетентнісного підходу до підготовки фахівців в українській вищій школі. Сьогодні немає сумніву в тому, що компетентнісний підхід – це один із найважливіших чинників, що сприяє модернізації змісту освіти та наближенню її до практичних потреб суспільства. Підготовка ІТ-фахівця є складним процесом, який має певні особливості, пов'язані насамперед зі швидкою зміною технологій програмування, коли технологія, у якій програміст був професіоналом, стає практично незатребуваною. З погляду компанії-виробника програмного забезпечення завжди буде затребувана найбільш сучасна технологія, отже, професіонал повинен постійно відслідковувати зміни, новинки і тенденції у сфері програмування (Власюк, Грицюк, 2013).

Суголосною є думка американських учених (Allabarton, 2015; Weiner, 2014), які підкреслюють, що комп’ютерні науки та інформаційні технології – це дуже динамічна галузь. Результатом цієї динамічності є недостатній зв’язок між освітньою та професійною галузями, що призводить до проблем у процесі

працевлаштування випускників цієї спеціальності. Кібербезпека – це «мішень, що постійно рухається», що є викликом як для освітнього сектору, так і для професійної галузі. Основною вимогою до професійної підготовки фахівців для ІТ-галузі є вимога не відставати від гіперактивних змін, що відбуваються на споживчому та промисловому ринках (Schirf, & Serapiglia, 2017).

Українська дослідниця К. Кірей також дотримується думки щодо актуальності компетентнісного підходу у професійній підготовці фахівців ІТ-галузі. Саме компетентністний підхід дозволяє виокремити й класифікувати типові помилки, які допускають випускники закладів вищої освіти на робочому місці після працевлаштування, та обрати оптимальні дидактичні методи і засоби їх усунення в процесі їхньої підготовки. Так, відомий автор підручників з мов програмування Марк Аллен Уайс включив після кожної навчальної теми у свій навчальний курс перелік типових помилок (Кірей, 2016).

В Україні ж лише нормативні акти, навчальна література та дослідження досвіду дає розуміння того, які знання, вміння та навички мають одержати студенти ІТ-спеціальності у процесі навчання. Однак думка роботодавців щодо знань та вмінь майбутнього ІТ-фахівця є надзвичайно важливою для структурування та оновлення змісту професійної підготовки (Кірей, 2016).

Важливо зазначити, що американські роботодавці відповідно до результатів спостережень також не завжди задоволені підготовкою випускників вищих навчальних закладів. Крім того, невідповідність бажаних та одержаних під час навчання умінь не завжди стосується технічної галузі. Навички вирішення проблем, софт-скіллс, навички міжперсональної комунікації, мотивації, позитивного настрою необхідні і цінуються роботодавцями одночасно зі знаннями мови програмування та іншими спеціальними знаннями та навичками (Schirf, & Serapiglia, 2017).

Український учений С. Гнатюк пропонує власне розуміння шляхів подолання проблем, пов’язаних із підготовкою кадрів для вітчизняної галузі інформаційних технологій. Серед пріоритетних заходів ним визначається системна взаємодія ІТ-освіти та ІТ-індустрії. Акцентується увага на наявності

помітного прогресу у налагодженні широкого діалогу між приватним сектором (комерційними ІТ-компаніями) і закладами вищої освіти, що здійснюють підготовку фахівців для сфери інформатизації: укладаються договори про співпрацю з провідними вітчизняними й міжнародними ІТ-компаніями, завдяки чому українські студенти навчаються, працюють, проходять виробничу і переддипломну практику на базі цих компаній. Учений підкреслює, що географія такого співробітництва не обмежується лише великими містами з провідними навчальними закладами. На жаль, така співпрацю, хоча й вийшла в Україні на рівень системної, виникла стихійно, поза межами втручання держави та її регуляторів (Гнатюк, 2014).

Українські дослідники (Власюк, Грицюк, 2013) наголошують на тому, що часто причиною незадовільних результатів роботи програміста стає недостатність знань, які не стосуються прямої компетенції фахівця. Тобто умовно можна виділити три складові професійної підготовки ІТ-фахівця, необхідні для успішної роботи: фундаментальна і технологічна (забезпечуються на певному рівні закладу вищої освіти) і прикладна – у галузі, з якою буде пов'язана робота програміста, наприклад, бухгалтерія, інженерія, юриспруденція тощо. Такої ж думки дотримується І. Діордіца, який, враховуючи широкий діапазон сфери діяльності фахівців з кібербезпеки, пропонує кореспондувати теоретичні знання і практичні навички, що формуються у закладі вищої освіти з подальшою роботою в конкретних секторах. Передбачаються спеціалізації із кібербезпеки в наступних секторах: сектор державної влади і управління; сектор безпеки і оборони; сектор економіки; сектор науки і техніки (Діордіца, 2017).

Дослідження Т. Каушан присвячено визначенню основних напрямів удосконалення професійної підготовки майбутніх фахівці із комп’ютерних наук. На думку науковця, формування інформаційної культури у майбутніх фахівців з комп’ютерних наук вимагає побудови освітнього процесу на основі застосування сучасних технологій навчання (модульного, особистісно орієнтованого, контекстного), інтерактивних навчальних методів та

рейтингової системи оцінювання результатів навчальної діяльності студентів (Каушан, 2011).

Здійснений аналіз публікацій американських науковців з проблеми дослідження дозволяє зробити висновок, що значна увага приділяється змісту, формам і методам навчання майбутніх фахівців з кібербезпеки. Американські вчені зазначають, що на таких фахівців існує значний попит, який не виявляє тенденцію до зниження, відповідно є потреба у достатній кількості ефективних програм підготовки фахівців, а іноді вимагає залучення додаткових освітніх ресурсів. Американські науковці наполягають на необхідності практично орієнтованої підготовки та активного навчання (Boggs, 1999; Bonwell & Sutherland, 1996; Felder & Brent, 2003). Вони зазначають, що в сучасному світі викладачі в усіх галузях інформаційних технологій повинні відійти від традиційних методів та надати перевагу такому підходу у навчанні, який б підвищив інтерактивну взаємодію зі студентами (Bork, 2000).

У підготовці фахівців з кібербезпеки невід'ємною частиною повинна стати можливість працювати у інтерактивному практичному середовищі. Для розвитку важливих навичок для таких фахівців, зокрема щодо «вирішення проблем», американські науковці пропонують інкорпорацію проблем реального робочого місця у зміст навчання. На їхню думку, це підштовхує студентів до вищого рівня критичного мислення: аналізу, синтезу, оцінювання, які вкрай необхідні для професійної діяльності фахівців з кібербезпеки. Крім іншого, студенти повинні набути «професійного артистизму» для підготовки до сучасної кар'єри у галузі кібербезпеки. Проблеми цієї галузі потребують від фахівців розглядати кібербезпекові проблеми з обох перспектив (нападу та захисту) і бути здатним адаптуватися до загроз, які постійно з'являються. Саме тому лише практична складова може дати найбільш ефективні результати у підготовці фахівців з кібербезпеки (Martin, & Woodward, 2013).

Запровадження нової спеціальності «кібербезпека» згідно з Постановою Кабінету Міністрів України у 2015 р. зумовлює необхідність теоретичного осмислення освітніх стандартів підготовки фахівців цього напряму. Проблема

проектування освітніх стандартів професійної підготовки фахівців з кібербезпеки ускладнюється тим, що Закон України «Про вищу освіту» (2014) вніс принципові зміни щодо розуміння стандартизації освіти і процесів, що її супроводжують. На думку І. Діордіца, основною проблемою стандартизації підготовки фахівців у сфері кібербезпеки є відсутність чітко визначеного правового поля для цього виду професійної діяльності: така діяльність не передбачена державними стандартами та чітко визначеними кваліфікаційними характеристиками, затвердженими на державному рівні (Діордіца, 2017).

Українськими дослідниками запропоновано заходи для формування того ресурсного та інфраструктурного мінімуму, що необхідний для оптимізації системи підготовки кадрів для сфери ІКТ у напрямі своєчасного та адекватного реагування на потреби ринку та галузі. Вирішення таких критичних для адекватного кадрового забезпечення галузі питань пропонується здійснювати у напрямах: подальшого розширення та вдосконалення кластера профільних закладів вищої освіти, підвищення якості освіти на основі розвитку сталих навчально-виробничих зв’язків з науково-дослідними центрами ІТ-підприємств та світових корпорацій, міжвузівського (включаючи міжнародне) співробітництва, координації навчальної роботи із системою шкільної освіти; профільної модернізації та спеціалізації системи шкільної освіти, зокрема створення необхідної кількості закладів (шкіл, спецкласів) для отримання початкових знань та умінь у галузі ІКТ; налагодження профільної системи післядипломної освіти для оперативного підвищення кваліфікації фахівців, їхньої перепідготовки отримання чергової кваліфікації тощо (за моделлю «освіта протягом життя») (Гнатюк, 2014).

Отже, проведений аналіз законодавчих ресурсів, наукових праць дозволяє зробити висновок, що методологічним підґрунтям для вивчення проблеми професійної підготовки фахівців з кібербезпеки є компетентнісний, особистісно-орієнтований, функціональний, аксіологічний, інструментальний, прагматичний підхід.

У межах компетентнісного підходу особлива увага науковців приділена компонентам професійної компетентності фахівців з кібербезпеки, при чому американські вчені наголошують на важливості, крім загальних і спеціальних знань, умінь і навичок, соціального і комунікативного компонентів. Дослідники обох країн акцентують увагу на необхідності врахування особливостей структури і змісту професійної підготовки фахівців з кібербезпеки. Представники функціонального підходу зосереджуються на діяльності навчальних установ, що забезпечують необхідний рівень кваліфікації. Прихильники інструментального підходу зацікавлені у вивченні методів і форм організації освітнього процесу, які сприяють його ефективності. Дослідники особистісно орієнтованого підходу наполягають на важливості розвитку особистісних якостей майбутніх фахівців з кібербезпеки. Представники аксіологічного підходу зосереджують увагу на формуванні професійних якостей майбутніх фахівців з кібербезпеки, що необхідні для їхньої успішної професійної діяльності. Представниками прагматичного підходу є переважно американські вчені, які підкреслюють необхідність такої підготовки фахівців з кібербезпеки, яка б забезпечила їхню конкурентоспроможність на світовому ринку, здатного успішно працювати в умовах завдань, що постійно змінюються, творчо мислити. Головний акцент науковці роблять на практико-орієнтованому навчанні, навчанні у професійно-зорієнтованому середовищі.

У межах проблеми нашого дослідження варто відзначити важливість порівняльно-педагогічних досліджень. Україна як держава, яка інтегрується в європейський індустріальний та освітній простір, у своєму розвитку не може не враховувати всі його вимоги. Тому вирішення означених проблем у професійній підготовці фахівців ІТ-галузі та фахівців з кібербезпеки зокрема неможливе без вивчення, аналізу та імплементації позитивного зарубіжного досвіду. Аналіз компаративістських досліджень свідчить про значний інтерес дослідників у галузі порівняльної професійної педагогіки до питань професійної підготовки фахівців для ІТ-галузі в країнах світу.

Дослідження З. Сейдаметової можна вважати першим значним кроком у висвітленні проблем зарубіжного досвіду підготовки фахівців для ІТ-галузі. Аналізуючи міжнародний освітній стандарт СС 2001 та наявні вітчизняні галузеві стандарти спеціальності «Інформатика» напряму підготовки 0802 «Прикладна математика», дослідниця відзначає істотну і об'єктивну відмінність у методології та принципах формування цих стандартів і пропонує розробляти стандарти для спеціальностей комп'ютінга (напрями підготовки 0403, 0501, 0502, 1701, 0802) з урахуванням міжнародного досвіду і наявних міжнародних стандартів (Сейдаметова, 2004).

До азійського досвіду звернулася І. Пододіменко, яка досліджувала особливості професійної підготовки бакалаврів комп'ютерних наук в університетах Японії. Вона проаналізувала вимоги суспільства до професійної підготовки фахівців у галузі інформаційних технологій в Японії, виокремила позитивні аспекти зарубіжного досвіду та можливості їх творчого використання у вітчизняній педагогічній практиці. І. Пододіменко також підкреслила важливість компетентнісного підходу у підготовці конкурентоздатного ІТ-фахівця у закладах вищої освіти. Вона також переконана, що акцент має бути зміщено з формування певного спектру професійних знань, умінь і навичок у галузі програмування на виховання таких якостей, як: робота в команді; лідерські здібності; відповідальність; здатність до рефлексії, самостійного навчання й освоєння нових технологій протягом життя; самоосвіта; планування діяльності; логічне й алгоритмічне мислення; цілеспрямованість; наполегливість; уміння самостійно ухвалити рішення, швидко адаптуватися до нового завдання; широкий кругозір у предметній галузі (Пододіменко, 2014).

Р. Шаран проаналізував досвід США щодо підготовки магістрів інформаційних технологій у системі дистанційної освіти та визначив можливості його впровадження в Україні. У ході дослідження ученим було виявлено характерні ознаки розвитку галузі ІТ в США, які важливо враховувати при розробленні освітньо-професійних програм професійної підготовки магістрів, зокрема: феномен стрімкого розширення Інтернету; розвиток

технологій мобільного зв'язку з їх інтеграцією з мережею; прогрес у технології розроблення програмного забезпечення та в індустрії інформаційних ресурсів; формування і швидкий розвиток нових напрямів ІТ (електронні бібліотеки, біоінформатика, квантова інформатика, цифрова економіка); постійне зростання ролі міжнародних стандартів для індустрії й ринку продуктів і сервісів ІТ. До особливостей організації дистанційного навчання в університетах США Р. Шаран відносить функціонування трьох груп центрів дистанційної освіти за ступенем «занурення» в Інтернет, які діють при університетах США: центри, робота яких ґрунтується винятково на Інтернет-технологіях; навчальні заклади, що поєднують різні традиційні форми очної й дистанційної форми навчання з нововведеннями в дусі часу; навчальні центри, для яких Інтернет служить лише внутрішнім комунікаційним середовищем (Шаран, 2010).

Отже, аналіз психолого-педагогічних, порівняльно-педагогічних досліджень з проблеми професійної підготовки фахівців з кібербезпеки дозволив представити та охарактеризувати основні підходи науковців України та США щодо вивчення окресленої проблеми. Дослідження проводилось на основі вивчення досвіду підготовки фахівців у галузі знань «Інформаційні технології». У цих роботах закладено вагому методологічну і практичну основу для вивчення проблеми професійної підготовки фахівців з кібербезпеки, запропоновано заходи з модернізації освітнього процесу. У межах кожного з підходів закцентовано увагу на зумовленості чинниками особистісного, практичного, функціонального характеру та важливості професійної підготовки фахівців з кібербезпеки в сучасному інформаційному суспільстві.

1.2. Основні поняття дослідження

У сучасних умовах наукового-технічного та технологічного прогресу інформаційна складова набуває дедалі більшої ваги і як один із найважливіших елементів забезпечення національної безпеки визначається складною взаємодією багатьох факторів, серед яких провідне місце займає «фактор людини». Людина є основним творцем і користувачем комп'ютерних систем і

мереж (КСМ) та/або телекомунікаційних мереж (ТКМ), тому вона виступає основним суб'єктом і об'єктом кіберборотьби. Кіберпростір, кібернетичні ресурси, комп'ютерно-системна і мережева інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Інформаційна безпека та кібербезпека є невід'ємними складовими кожної зі сфер національної безпеки і водночас ІБ та кібербезпека – важливі самостійні складові процесу забезпечення національної безпеки (Соснін, 2005).

На думку дослідника теорії мережевого суспільства, професора Каліфорнійського університету (м. Берклі) М. Кастельса (Castells, 2002), ядром комунікаційної організації сучасного суспільства є не сама інформація, а мережева логіка, яка наповнює інформацію якістю та тими функціями, що системно перетворюють усі основні сфери життєдіяльності людей. Нова комунікаційна система радикально трансформує основні виміри людського життя. У цьому контексті доступ до Інтернету є одним із критеріїв, за яким країни поділяються на високорозвинені та слаборозвинені. Термін «digital divide» (цифрова нерівність) було вперше вжито 1998 року Білом Клінтоном, який порівняв телекомунікацію з епохою розширення «медіакордонів» (Кастельс, 2002).

Рис. 1.2.1. Складові інформації та взаємозв'язок між ними.

На рис 1.2.1. зображено чотирьохкомпонентну структуру поняття інформації та взаємозв'язок між чотирма її складовими, які з метою безпечного зберігання та передачі інформації повинні знаходитися у рівновазі між собою.

Відповідно основними інформаційними компонентами є інформація як невід'ємний компонент існування будь-якої держави; як товар; як суспільне благо; власне сама конфіденційність інформації. У контексті національної кібербезпекової політики США актуальним стало «негайне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин; недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; створення урядової політики в галузі інформації і комунікації» (Соснін, 2005, с. 24-25).

Для досягнення та збереження цієї рівноваги необхідне забезпечення інформаційної та загальної безпеки людини, суспільства, держави з метою протидії тенденціям значного зростання проявів кіберзлочинності й військово-політичного протистояння в кіберпросторі, які у деяких випадках мають ознаки кібервійни, навіть з людськими жертвами.

Вітчизняний фахівець з питань захисту інформації С. Мельник стверджує, що нові виклики часу, активна співпраця України в боротьбі з міжнародним тероризмом, стан розвитку інформаційного суспільства й інформаційної інфраструктури України визначає професійні вимоги державних і приватних структур щодо уведення нових інтегрованих програм професійної підготовки майбутніх фахівців з питань захисту інформації та управління кібербезпекою у вищих навчальних закладах. Обгрунтування концептуальних засад організації професійної підготовки майбутніх фахівців із кібербезпеки у вищих навчальних закладах є актуальною сучасною науково-практичною проблемою (Мельник, 2011, с.79-80).

У контексті нашого дослідження необхідно виділити ключові терміни з метою конкретизації та уточнення їх сутнісних значень. До них відносимо*: «IT-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист»,*

«інформаційна безпека», «кібербезпека», «кібербезпекова політика», «ризики», «фахівець з кібербезпеки», «бакалавр з кібербезпеки», «професійна підготовка бакалаврів з кібербезпеки». Вважаємо, що визначення сутності цих понять надасть можливість охарактеризувати доцільність та обґрунтованість термінологічного наповнення навчальних програм з підготовки фахівців з кібербезпеки.

Експерти ЮНЕСКО дають визначення *«IT-галузі»* як сукупності обчислювальної техніки, її прикладних програм, а також методів її взаємодії з людьми і промисловим обладнанням (Anderson, 2002). Інше тлумачення доповнює це визначення: *IT-галузь* – це сукупність методів, виробничих і програмно-технологічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збирання, зберігання, обробку, висновок і поширення інформації. Інформаційні технології призначені для зниження трудомісткості процесів використання інформаційних ресурсів (Information technology – Guide for ISO/IEC 12207 (Software Life Cycle Processes, 2016)

У Законі України «Про основні засади забезпечення кібербезпеки України» поняття *«кіберпростору»* трактується як простір, під яким пропонується розглядати середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних (Верховна Рада України, 2017).

Важливим для нашого дослідження є поняття «кібербезпека». У «Великому тлумачному словнику української мови» термін *«кібер»* або *«кібернетичний»* – трактується як такий, що походить від терміну *«кібернетика»;* той, що створено та працює на основі принципів та методів кібернетики» (Єрошенко, 2012, с. 308). Термін «безпека» визначає стан, коли кому - та/або чому-небудь ніщо не загрожує, тобто характеризує відсутність небезпеки (Єрошенко, 2012, с. 106). Аргументом щодо цього твердження

виступає етимологічне тлумачення двох складових цієї правової категорії – «кібер» та «безпека». Однак це тлумачення є достатньо звуженим та не розкриває основної сутності поняття.

Визначення терміну «кібербезпеки» тісно пов’язане з конотативним навантаженням поняття *«кіберпростір*». У результаті зіставлення всіх основних просторів («землі», «моря», «повітря», «космосу» як джерел суперництва та могутності), Г. Раттрей (Rattray, 2009), співробітник американської Інтернет-корпорації, пов'язаної зі стабільністю та стійкістю системи доменних імен та корпоративної програми безпеки, безперервності та управління ризиками корпорації з присвоєння імен та номерів – ICANN (Internet Corporation for Assigned Names and Numbers), доводить, що «кіберпростір» насправді є новим п’ятим простором і джерелом могутності. Як правило, могутність зростає у випадку контролю над ключовими аспектами операційного середовища. Нездатність отримати доступ до таких аспектів чи неможливість управляти ними може призвести до обмеження кола політичних, дипломатичних, економічних, військових та інформаційних аспектів могутності» (Rattray, 2009).

За тлумаченням Міжнародної спілки електрозв’язку (ITU–International Telecommunication Union), сукупність взаємопов’язаних інформаційних ресурсів, ПЗ, баз даних та пов’язаної з ними інфраструктури використовується поняття *«кіберсередовище»*, яке вносить плутанину через тотожність із терміном *«кіберпростір».* Адже кіберпростір є інтерактивним інформаційним комунікативним середовищем, що утворюється та функціонує за допомогою комп'ютерних систем. Кіберпростір можна розглядати як локальне середовище, у випадку функціонування засобу комп'ютерної техніки (КТ), що не підключено до мережі та/або розосереджене середовище, у випадку підключення КТ до локальної та/або глобальної мережі передачі даних (Інтернет) (Зубик, 2016, с. 173-174).

Отже, поняття *«кіберпростір»,* на нашу думку, більш доцільно використовувати у контексті дослідження проблеми аналізу особливостей підготовки фахівців з кібербезпеки в США.

Підґрунтям запровадження поняття «кібербезпека» стало розуміння необхідності вирішення проблеми нейтралізації або мінімізації сукупності кіберзагрози. З технологічного аспекту кібербезпека є складовою частиною інформаційної безпеки, оскільки сутність загроз, методів, засобів і заходів є однаковою та стосується лише кіберпростору. З іншої точки зору термін «кібербезпека» розглядається як окремий випадок інформаційної безпеки, введення якого обумовлене використанням комп'ютерних систем і мереж (КСМ) та/або телекомунікаційних мереж (ТКМ). «Кібербезпека» як безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує, передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозами (Діордіц, 2017). Кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем і мереж і мереж та/або телекомунікаційних мереж. Аналіз основних факторів, що негативно впливають на функціонування комп'ютерних систем і мереж та/або телекомунікаційних мереж, показав, що існує ряд чинників, що спричиняють ризики кіберзагрози їх функціонуванню та зумовлюють потребу їх захищеності від кібератак.

У наукових джерелах наявне чітке тлумачення поняття *«кібернетична загроза (кіберзагроза)»* як назва протиправних дій суб'єктів правових відносин ІТ-галузі і як назва наявних та/або потенційно можливих явищ і чинників, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критично важливих об'єктах національної інформаційної інфраструктури (Дубов, 2010).

Наступним ключовим терміном, який дозволяє об'єктивно здійснювати дослідницький пошук, є *«кібератака»* як посилений наступ різних кодів і програм на адресу певних користувачів. Як результат, такі дії здатні нанести велику шкоду. Адже атаки найчастіше спрямовані на установи та організації, спричиняють серйозної шкоди їх діяльності з довготривалими негативними за своїми результатами наслідками. Крім того, наявне трактування поняття

«кібербезпека» як певного стану систем, відповідно до якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах (Баранов, 2017). Вважаємо слушною думку І. Діордіци про те, що ця дефініція є недосконалою через відсутність пояснення, про стан якої саме системи йдеться (Діордіца, 2017).

На рис. 1.2.2. представлено основні чинники негативного інформаційного впливу на КСМ та/або ТКМ. До факторів впливу на комп'ютерні системи і мережі та/або телекомунікаційні мережі, що можуть спричиняти ризики та загрози кібератак, відносять неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації (Брижко, Гальченко, Цимбалюк та ін., 2002).

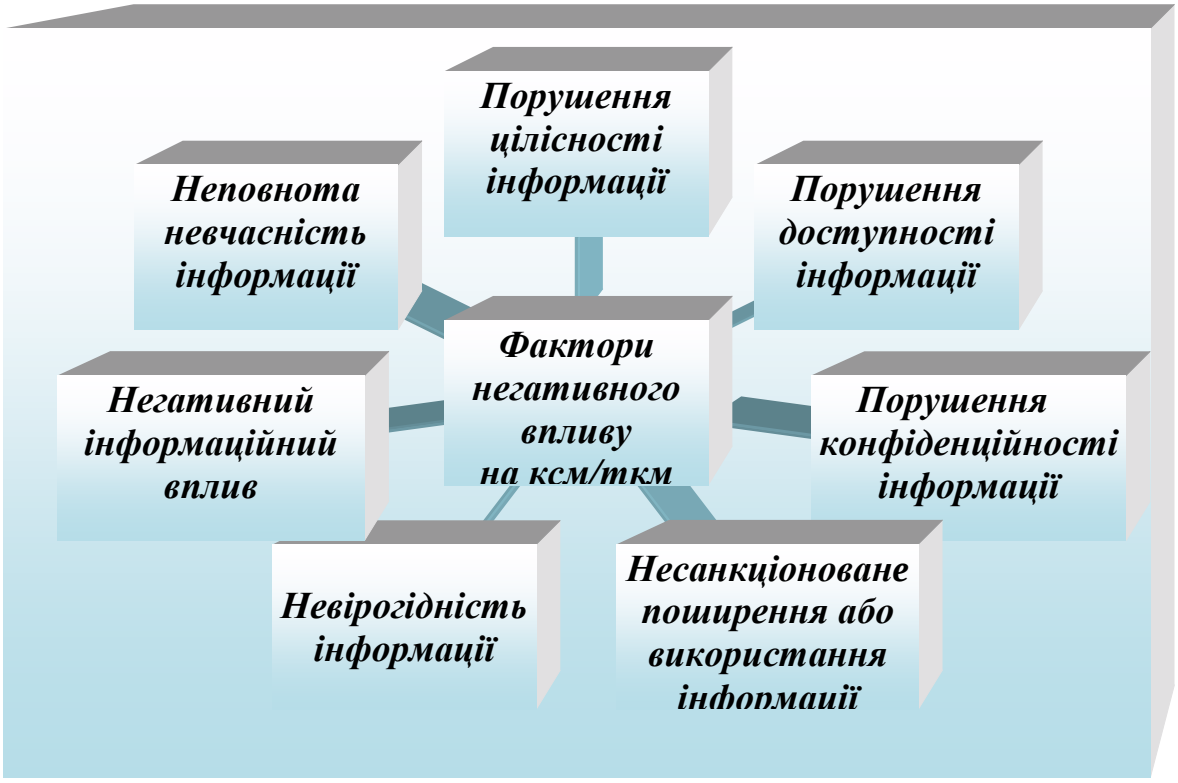


Рис 1.2.2. Чинники негативного інформаційного впливу на комп'ютерні системи та телекомунікаційні мережі (Брижко, Гальченко, Цимбалюк &ін., 2002; Дубов, 2013).

Так як проблема кібербезпеки має глобальний характер, вважаємо за необхідне звернутися до визначення поняття «кібербезпека», що пропонується

Міжнародною спілкою електрозв'язку (International Telecommunication Union) в нормативному документі цієї організації – «Рекомендаціях Міжнародної спілки електрозв'язку» (International Telecommunication Union Regulations). Відповідно до документа кібербезпека визначається як набір засобів, стратегій, принципів забезпечення безпеки, а також керівні принципи, підходи до управління ризиками, певні заходи та технології, професійна підготовка та практичний досвід, які можуть бути використані для захисту кіберсередовища, інформаційних ресурсів організації та користувача (Рекомендації, 2009). Важливим положенням, на нашу думку, є те, що професійна підготовка визначається як одна зі складових кібербезпеки, без якої неможливе захищене передавання інформації.

Ключовою категорією дефініції «кібербезпеки» є «інформація» як основний об'єкт інформаційних відносин, що належать до єдиного кіберпростору. Усвідомлення необхідності вирішення проблеми нейтралізації або мінімізації сукупності загроз дало підґрунтя для запровадження поняття «кібербезпека». Отже, якщо «інформаційна безпека» – це стан безпеки інформації, що належить, зазвичай, організації чи компанії, зокрема в IT-системах, то «кібербезпека» – це стан захищеності IT-систем, тобто обладнання та програм. Зіставлення різних тлумачень цього поняття лише підсилює розуміння того, що кібербезпека має статус самостійної складової національної безпеки.

На основі проаналізованих матеріалів можна зробити висновок про те, що кібербезпека – це стан захищеності життєво важливої інформації особистості, суспільства і держави в умовах використання комп'ютерних систем і мереж та/або телекомунікаційних мереж. Основним із завдань кібербезпеки є кіберзахист КСМ та/або ТКМ шляхом запобігання, мінімізації можливості ризиків кіберзагроз, спричиненої шкоди та усунення кібератак.

Отже, аналіз основного поняття на основі різних джерел дозволило визначити, що *«кібербезпека»* – це комплекс заходів: *технічних*, які застосовуються державою задля гарантій захищеності людини як основного

творця і користувача мережевої логіки (КСМ та ТКМ), як основного суб'єкта і об'єкта кіберзахисту та ІТ-систем (тобто обладнання та програмного забезпечення), а також запобігання, мінімізації можливості ризиків, можливої спричиненої шкоди та усунення кібератак; *педагогічних*, спрямованих на створення умов підготовки фахівців / професіоналів з кібербезпеки шляхом забезпечення ефективної системи та необхідної матеріально-технічної бази для навчання конкурентоспроможних на ринку праці фахівців з кібербезпеки (Проект Стратегії забезпечення кібернетичної безпеки України, 2013).

У цьому контексті доречно звернутися до поняття «фахівець з кібербезпеки», тому що він є основним суб'єктом і об'єктом кіберборотьби та кіберзахисту. На думку І. Діордіци, «термінологічне сполучення *«фахівець із кібербезпеки»* вживається в широкому розумінні, щоб іменувати так осіб, які за видом своєї професійної діяльності можуть використовувати спеціальні знання для попередження потенційних загроз, викриття, нейтралізації або мінімізації наслідків протиправної поведінки правопорушників у комп'ютерному просторі» (Діордіца, 2017).

На думку фахівця із кібербезпеки компанії «Сентурія Інтел» (Senturia Intel), відомого дослідника і впливової особи в галузі безпеки, професора Джованні Баттіста Карія (Battista, 2017), *«фахівець із кібербезпеки»* компанії повинен мати потенціал, який би забезпечував не лише якісне виконання ним професійних обов'язків, а й професійне самовдосконалення». Професор Карія 17 років працює над дослідженням проблем кібербезпеки та хакінгу. Результатом цієї роботи стало видання ґрунтовних праць – «PentTestMag» та «HackerAttack». 31 травня 2017 року на відкритій лекції на факультеті комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, на якій була присутня авторка дисертації, було розглянуто поняття кібербезпеки, кіберзагрози й основних шляхів захисту інформації. Лектор окреслив основні шляхи зниження кіберризику та ознайомив слухачів із методами впровадження безпеки у кіберпросторі.

Вітчизняні науковці з питань підготовки фахівців з інформаційної безпеки В. Бабак, С. Головань, В. Козловський, С. Лєнков, В. Хорошко, Л. Щербак, Д. Чирков (2001), які сьогодні втілюють в життя проект підготовки бакалаврів із кібербезпеки в українській вищій школі, у своїй науковій діяльності розглядали поняття «фахівець» або тотожне до нього поняття «спеціаліст» у сфері інформаційної безпеки. Характеризуючи необхідні професійні якості фахівців із захисту інформації з обмеженим доступом, С. Головань, С. Лєнков, В. Дорошко, Л. Щербак (2008) визначають кваліфікаційні вимоги до фахівця (спеціаліста) з інформаційної безпеки, зазначаючи, що, окрім суто спеціальних знань, пов'язаних з механізмом захисту, він повинен володіти знаннями про об'єкт (предмет) захисту та ефективність застосування даного механізму. Так, *фахівець (спеціаліст) з інформаційної безпеки* (напрям 1701: Безпека інформаційних і комунікаційних систем; системи технічного захисту інформації і управління інформаційною безпекою) повинен оволодіти знаннями не тільки зі своєї галузі, але й суміжних галузей. *Фахівець (спеціаліст) з управління системою обробки інформації,* крім спеціальних знань з теорії управління, повинен оволодіти знаннями технологій обробки інформації та механізмів її захисту. *Фахівець (спеціаліст) з проектування* повинен оволодіти ґрунтовними спеціалізованими знаннями. Така відмінність вимагає здійснення класифікації фахівців/спеціалістів з урахуванням їхнього функціонального включення в систему та розуміння певних базових знань, що ґрунтуються на загальносистемних закономірностях. Так, на думку С. Голованя, В. Дорошко та Л. Щербака (2009), «спеціаліст у сфері інформаційної безпеки має вміти давати оцінку своїй діяльності, а також людям, які входять в систему обробки інформації як її елемент, не тільки з точки зору нанесеного збитку, але й з позицій дотримання правових норм, а також оцінювати відповідність можливостей юридичної бази, впливати таким чином, щоб уникати нанесенню збитку. Значущість інформації і знань, що базуються на них, їх перспективність, цінність, змістовна ємність нерівнозначні з точки зору наслідків їх просочування і несанкціонованого використання.

Відповідно виникає необхідність наявності у студентів уявлень про критеріальний відбір знань, їх оцінку, що вимагає, в свою чергу, вміння обирати такі критерії, якщо не формувати їх залежно від конкретної ситуації, при чому на усвідомленій і обґрунтованій основі (Головань, Хорошко & Щербак, 2009, с. 99-103).

Українські науковці, які досліджують проблеми підготовки фахівців з інформаційної безпеки структурних підрозділів Міністерства надзвичайних ситуацій України, аналізують специфіку підготовки фахівців у Львівському ДУ БЖД з напряму «Управління інформаційною безпекою» кваліфікації *«Фахівець з організації інформаційної безпеки»*, студіюють нормативні документи, що пов'язані з використанням конфіденційної та секретної інформації, з особливостями експлуатації об'єктів інформаційного захисту. Ю. Грицюк, Т. Рак (2011) стверджують, що структура професійних навичок фахівців у галузі захисту інформації визначається сферою, об'єктами і видами їхньої професійної діяльності, зокрема сферою професійної діяльності випускника, основними компетенціями якого є сукупність методів і засобів інформаційної діяльності, спрямованими на захист конфіденційної та секретної інформації.

Найбільш важливими напрямами діяльності *фахівців із захисту інформації,* на думку Ю. Грицюка та Т. Рака (2011), є спостереження, аналіз, оцінювання та прогнозування джерел загроз і рівнів їх небезпек, критичної безпеки інфраструктури, ступеня внутрішньої та зовнішньої уразливості; відпрацювання стратегії та тактики захисту інформації, планування попередження нападу, укріплення потенційних зв'язків, варіювання мережевих ресурсів щодо забезпечення інформаційної безпеки; відбір сил і засобів протидії, нейтралізація та недопущення інформаційних атах, мінімізація шкоди від них; протистояння джерелам загроз природного, технічного або антропогенного характеру системам забезпечення інформаційної безпеки; управління наслідками інциденту (від інформаційних атак, інформаційних операцій, інформаційних воєн).

На думку вітчизняних фахівців з питань підготовки фахівців з інформаційної безпеки в Україні О. Голубенка, О. Петрова та В. Хорошка (2006), структура професійних навичок фахівців у галузі захисту інформації визначається сферою, характером, природою, сутністю і змістом джерел загроз і рівнів їх небезпек, умінням своєчасно їх ідентифікувати.

Професор кафедри комп'ютерної математики та інформаційної безпеки, Київського національного економічного університету імені Вадима Гетьмана І. Джалладова стверджує, що компетентний *фахівець з інформаційної безпеки* зобов'язаний стати еталоном суб'єкта безпечної інформаційної діяльності і при цьому знатися на питаннях інформаційної безпеки в усіх аспектах: юридичних, психологічних, соціально-історичних, педагогічних, програмно-технічних. Адже інформація (інформаційні ресурси, цінності) та її інфраструктура – це та основа, з якою їм доведеться працювати і жити в XXI столітті (Джалладова, 2015).

Вітчизняний учений Л. Зубик вважає, що поняття «бакалавр з інформаційних технологій (ІТ-бакалавр)» слід трактувати наступним чином: «людина, яка успішно завершила навчальну програму першого рівня вищої освіти обсягом 180-240 кредитів ЄКТС, спрямовану на інформаційні технології як узагальнений об'єкт діяльності, і отримала ступінь бакалавра, що підтверджує сформованість у неї професійних компетентностей, достатніх для виконання обов'язків відповідного рівня і передбачених для первинних посад у певному виді економічної діяльності» (Зубик, 2016, с. 19-20).

У процесі тлумачення поняття «фахівець із кібербезпеки» з метою визначення сутності термінів «фах» і «фахівець» звернемося до «Великого тлумачного словника сучасної української мови», де пояснюється, що «фах – це вид заняття, трудової діяльності, що вимагає певної підготовки і є основним засобом до існування; професія… та/або основна кваліфікація, спеціальність… Тоді, як фахівець – це той, хто досконало володіє певним фахом, має високу кваліфікацію, глибокі знання з певної галузі науки, техніки, мистецтва, тощо; спеціаліст» (Великий Тлумачний Словник, 2012, с. 1538).

У Класифікаторі професій ДК 003:2010 України зазначено наступне: «Назва професії «фахівець» може бути розширена за потребою користувача для внутрішнього використання термінами та словами, які уточнюють місце роботи, виконувані роботи, сферу діяльності. Наприклад, «фахівець з інформаційного забезпечення» тощо». На нашу думку, доцільним є застосування рекомендації щодо розширення спеціальності за потребою щодо спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», що суголосно зі спеціальністю *«фахівець із кібербезпеки»*.

На думку Л. Зубик, кваліфікаційні вимоги до фахівців можна визначити наступним чином: *фахівець І категорії* – повна або базова вища освіта відповідного напряму підготовки (спеціаліст або бакалавр); стаж роботи за професією фахівця ІІ категорії не менше 1 року (спеціаліст) або не менше 2 років (бакалавр); *фахівець ІІ категорії* – повна або базова вища освіта відповідного напряму підготовки (спеціаліст або бакалавр); без вимог до стажу роботи (спеціаліст), стаж роботи за професією фахівця не менше 1 року (бакалавр); *фахівець* – базова або неповна вища освіта відповідного напряму підготовки (бакалавр або молодший спеціаліст); без вимог до стажу роботи. (Зубик, 2016, с. 21). Відповідно до класифікатора (Класифікатор професій ДК 003:2010 України, 2010) кваліфікаційні вимоги до фахівців можна екстраполювати на кваліфікаційні вимоги до *«фахівця із кібербезпеки»*, що вимагає конкретизації та уточнення їх сутнісних характеристик.

Незважаючи на поширене хибне уявлення щодо подібності сфери діяльності та компетенції фахівців з кібербезпеки та інформаційної безпеки, вони є відмінними. Підтвердженням думки про необхідність розмежування сфери їхньої діяльності та компетенції є спосіб сертифікації. У світі упроваджено кілька самостійних сертифікацій фахівців з кібербезпеки та інформаційної безпеки.

С. Мельник стверджує, що, виходячи з позиції адекватності освітніх послуг вимогам ринку праці, для визначення змістової частини нової спеціальності «Кібербезпека», у національній системі кібербезпеки України, з

метою обґрунтування можливих спеціалізацій в рамках цієї та інших спеціальностей набуває особливого значення питання співвідношення між поняттями «інформаційна безпека» та «кібербезпека» (Мельник, 2012.).

Найпоширеніші та найбільш популярні у світі види сертифікації для «*фахівця з кібербезпеки»* є*:*

- CEH Сертифікат «етичного хакера» (Certified Ethical Hacker);
- CISSP Сертифікат професіонала з безпеки інформаційної системи (Certified Information System Security Professional);
- CCSP Сертифікат професійнала з безпеки Cisco (Cisco Certified Security Professional),

та для *«фахівця з «Інформаційної безпеки»*:

- CISA Сертифікат аудитора інформаційних систем (Certified Information Systems Auditor);
- ISO 27001 Головний імплементатор (Lead Implementer);
- SO 27001 Головний аудитор (Lead Auditor).

Розглянемо їх більш детально. Так, CEH (сертифікований іспит EC-Council CEH, статусний іспит *312-50v 8* або *EC0-35e*) – це один із провідних варіантів сертифікації для фахівців з кібербезпеки, схвалений Міністерством оборони США. За успішними результатами складання екзамену (4-годинний іспит охоплює 150 тестових питань) кандидати отримують статус «етичного хакера». Сертифікація Certified Ethical Hacker визнана у всьому світі і підтверджує наявність відповідного рівня знань у сфері кібербезпеки мереж. Сертифікований «етичний хакер» є кваліфікованим фахівцем з кібербезпеки, який розуміє і знає, як шукати слабкі місця цільових систем і використовує ті ж знання та інструменти, що і хакер, але для їх захисту.

Вимоги до претендентів на звання CISSP суворі, зокрема передбачено 5 повних років роботи безпосередньо в якості фахівця з кібербезпеки систем в двох або більше з 10 сфер CBK: управління доступом; безпека додатків; планування безперервності бізнесу і відновлення в разі надзвичайної ситуації; криптографія; управління ризиками та безпекою інформаційних систем;

законодавство, регулювання, відповідність та розслідування; безпека операцій; фізичний захист від впливів навколишнього середовища; архітектура і побудова безпеки; безпека телекомунікацій і мереж.

Допуск до сертифікації CISSP відбувається за наявності досвіду, диплому CISSP та на основі підписання кодексу етики *ISC2*. Рівень знань, необхідних для успішного складання іспиту, достатньо високий: 6-годинний іспит охоплює 250 тестових питань, на кожне з яких можливі чотири варіанти відповіді (правильним є тільки один з варіантів). Згодом необхідно підтверджувати кваліфікацію CISSP, отримуючи не менше 120 одиниць неперервної професійної освіти (Continued Professional Education, CPE) протягом кожних наступних трьох років.

Сертифікація CCSP (Cisco Certified Security Professional) створена з метою підтвердження наявних знань і досвіду для забезпечення комплексної безпеки в мережах Cisco. Основна перевага цього типу сертифікації полягає у здобутті необхідних навичок для запобігання ризиків кібератак, одночасно знижуючи сукупну вартість навчання завдяки використанню в освітньому процесі обладнання Cisco. Агентство національної безпеки США (National Security Agency) і Комітет систем національної безпеки (Committee on National Security Systems) підтвердили, що сертифікат CCSP задовольняє стандарт із кібербезпеки №4013 і визнається виробниками ПО і обладнання. Необхідні знання в обсязі сертифікації CCNA Security або CCNA і SND (SND – тест дійсний до 17 листопада 2018 року). Кандидати, які склали тести HIPS, SND або SNPA, можуть використовувати їх для отримання сертифікації CCSP протягом 3 років після тестування. Здобувачі, що пройшли попередні версії тестів 642-503 SNRS або 642-544 MARS, можуть використовувати їх протягом 3 років після складання.

Для ґрунтовного усвідомлення відмінності між поняттями «фахівець кібербезпеки» і «фахівець з інформаційної безпеки» проаналізуємо діяльність деяких представників IT-галузі. Так, фахівці з інформаційної безпеки для проникнення в організацію використовують «фактор людини», який є слабким

місцем у системі. Акцентується увага на таких якостях людини, як: цікавість, довірливість, неуважність, жага наживи. Атака такого типу не дозволяє вчасно її виявити та усунути, тому вона є занадто привабливою для зловмисника.

Один із найрозповсюдженіших звичайних прийомів, який залучає соціальну інженерію з метою ошукування користувача за допомогою телефону, електронної пошти, – це фішинг. Така атака є надзвичайно ефективною, оскільки базується на людській неуважності та довірливості в поєднанні з низьким рівнем комп'ютерної грамотності. Фішинг дуже популярний серед зловмисників, оскільки технічні методи захисту від нього неефективні.

«Хакери» вивчають будову різних ІТ-систем, щоб знайти в них вразливі місця з метою отримання вигоди (фінансової та ін.), тоді як «білі хакери» (White Hats) досліджують будову ІТ-систем та знаходять їх слабкі сторони для запобігання кіберзагрозі, відхилення кібератаки та усунення проблем.

У контексті нашого дослідження ключовими є поняття «бакалавр з кібербезпеки» та «професійна підготовка бакалаврів з кібербезпеки». Так, вітчизняна дослідниця І. Джалладова слушно вважає, що найважливішими проблемами сучасності є безпека інформаційних і комунікаційних систем, захист від атак за наявності інформаційних війн, розроблення при цьому моделі власної поведінки учасника кіберпростору. На її думку, *«підґрунтям для істотної протидії зростанню злочинів у кіберпросторі може стати грамотна політика національних кадрів у галузі інформаційної безпеки»* (Джалладова, 2015). На наше переконання, враховуючи той факт, що галузь інформаційної безпеки в сучасному суспільстві трансформовано у ІТ-галузь, виникає необхідність цілеспрямованої державної політичної векторності, яка б на законодавчо-нормативному підґрунті забезпечувала б підготовку національних кадрів з кібербезпеки.

Відповідно до «Положення про освітньо-кваліфікаційні рівні» (2016) бакалавр – це освітньо-кваліфікаційний рівень фахівця, який на основі повної загальної середньої освіти здобув поглиблену загальнокультурну підготовку, фундаментальні та професійно-орієнтовані уміння та знання щодо

узагальненого об'єкта праці і здатний вирішувати типові професійні завдання, передбачені для відповідних посад, у певній галузі народного господарства (Закон України Про вищу освіту, 2014). Відповідно «*бакалавр з кібербезпеки*» – це освітньо-кваліфікаційний рівень фахівця, який на основі повної загальної середньої освіти здобув поглиблену загальнокультурну підготовку, фундаментальні та професійно-орієнтовані уміння та знання щодо способів, методів протидії злочинності у кіберпросторі. Екстраполюючи думку І. Джалладової щодо політики підготовки національних кадрів з метою протидії зростанню злочинів у кіберпросторі у поєднанні з тлумаченням поняття «бакалавр», зазначимо, що «професійну підготовку бакалаврів з кібербезпеки» необхідно розглядати як важливу складову державної політики з підготовки національних кадрів для боротьби з кіберзлочинністю.

Одним із ключових понять нашого дослідження є «*кібербезпекова політика»* як політика надання гарантії національної безпеки у кіберпросторі. У формуванні кібербезпекової політики, що має на меті продемонструвати аудиторії як в США, так і на міжнародному рівні серйозність намірів американського керівництва у сфері кібербезпеки, центральну роль відведено Білому Дому. Упродовж періоду президентства Б. Обами відбувався процес формування, організації та кадрового забезпечення реалізації кібербезпекової політики США. Важливим питанням кібербезпекової політики американського інформаційного суспільства стало інтенсивне залучення до всіх його сфер висококваліфікованих кадрів.

Отже, аналіз наукової літератури дозволив визначити термінологічне поле дослідницького пошуку, конкретизувати та уточнити сутнісне значення ключових понять дослідження. З’ясовано, що в США підготовка фахівців з кібербезпеки розглядається на національному рівні як важлива умови посилення кібербезпекової політики, захисту цивільних прав, інтересів бізнесу, наукового, технічного, військового, фінансового потенціалу країни. Заходи, спрямовані на досягнення кібербезпеки, передбачають інтеграцію підготовки

кваліфікованих фахівців ІТ-галузі з вихованням відповідального ставлення до національної безпеки у населення країни.

1.3. Проблема підготовки фахівців з кібербезпеки у документах міжнародних організацій

Незважаючи на те, що національна політика будь-якої країни передбачає збереження і захист кордонів й національного суверенітету, інфраструктура, обладнання, та логістика кіберпростору функціонують поза межами цих кордонів, що надає йому міжнародного статусу. Транснаціональний характер кіберпростору вимагає вирішення проблем шляхом регіонального та міжнародного співробітництва. Крім того, у заходах щодо подолання загроз, розроблення відповідних рішень з метою зміцнення безпеки кіберпростору на національному рівні виникає потреба у кооперації дій різних галузей: політичної, економічної, технологічної, правової, управлінської, військової.

У сучасному інформаційному суспільстві спостерігається залежність розвитку економічної, політичної та соціальної сфер від інформаційної та кібернетичної спроможності країни. За підрахунками фахівців можливі збитки від кібератак на онлайнові-банківські та фінансові послуги лише однієї Європейської країни становитиме понад 10 мільйонів євро на день (Radunović, 2013). Тому багато країн розробили та затвердили національну кібербезпекову стратегію, що була підкріплена відповідною законодавчою базою, та запровадили національні механізми реагування на кіберінциденти. Деякі країни проголосили кіберпростір п'ятим військовим об'єктом, а також створили захисні та наступальні кіберкоманди в своїх арміях задля мінімізації ризиків для промисловості та громадян.

Однак здійснений аналіз відповідних матеріалів свідчить про існування різних поглядів та підходів до вирішення проблеми кібернетичних загроз в різних країнах. Відмінність спостерігається у визначенні відповідальних органів: якщо в одних країнах були створені національні організації,

відповідальні за управління кібербезпекою, то в інших відповідальність за реалізацію національної політики покладена на координаційні органи, а управління та імплементація політики була залишена урядовим департаментам.

Незважаючи на створення національних органів, що несуть відповідальність за кібербезпекову політику та специфіку її реалізації в кожній окремій країні, міжнаціональний характер кібернетичного простору потребує вироблення та координації політики передусім на міжнародному рівні. Вивчення матеріалів з проблеми дослідження дозволяє стверджувати, що кількість міжнародних організацій, урядових та неурядових органів, відповідальних за глобальну або регіональну кібербезпеку, постійно зростає. Їх діяльність варіюється від дослідної до регуляторної, спрямованої на вироблення колективного спільного підходу до вирішення проблеми кіберзагрози.

Аналіз законодавчої бази у галузі кібербезпеки різних країн дозволила з’ясувати, що вона є доволі складною і змінюється дуже швидко, причому різниця спостерігається у тому, як країни трактують кібербезпеку в національних законах. Багато країн та національних організацій дотримуються як національних, так і міжнародних законів з кібербезпеки і відповідно до них доповідають про певні типи фінансових або інших типів кіберзлочинів. Існують міжнародні норми правоохоронної діяльності (співпраця, запроваджена Інтерполом). Багатьма країнами були прийняті вимоги щодо інформування про скоєння кіберзлочинів. На сьогодні відбувається робота над створенням міжнародного кодексу кіберетики. До найбільш впливових міжнародних організацій, що реалізують політику із координації і регулювання діяльності країн у галузі безпечного використання кіберпростору, належать: ЮНЕСКО, НАТО, Кіберкоманду американського уряду (U.S. Government Cyber Command, Європол (Europol), Спільний центр досконалого кіберзахисту (Cooperative Cyber Defence Center of Excellence, CCD COE), Європейське агентство мереж та інформаційної безпеки (European Agency for Network and Information Security, ENISA), Міжнародну організацію стандартизації (The International Organization for Standardization, ISO), Організацію для безпеки та кооперації в Європі

(Organisation for Security and Co-operation in Europe, OSCE), Міжнародний форум реагування на інциденти та командної безпеки (Global Forum for Incident Response and Security Teams), Міжнародне багатостороннє партнерство проти кіберзагроз (the International Multilateral Partnership Against Cyber Threats, IMPACT), Асоціацію комунікації та електроніки озброєних сил (the Armed Forces Communications and Electronics Association, AFCEA), Інтернет корпорацію присвоєння імен та номерів (the Internet Corporation for Assigned Names and Numbers, ICANN), Інтернет-форум управління (the Internet Governance Forum, IGF), Міжнародну спілка комунікації (the UN-backed International Telecommunications Union, ITU).

Розглянемо найбільш важливі закони та підзаконні акти, що розробляються міжнародними організаціями для врегулювання різних аспектів функціонування кібернетичного простору.

Організація Північноатлантичного договору (НАТО), яка є осередком колективної оборони, зосереджує свої зусилля на забезпеченні кібербезпеки. НАТО стежить за зростаючою кількістю кіберзагроз, викликаних залежністю суспільства від технологій та Інтернету, і тому діяльність з кіберзахисту була включена у стратегічні та інституційні плани. У 2009 р. Центр підвищення кваліфікації з кіберзахисту (CCD COE) був акредитований НАТО з метою проведення міжнародних досліджень в галузі освіти з кіберправа. Під впливом розвитку кібернетичного простору відбулися зміни в доктринерській структурі організації. 28 держав-членів у 2016 р. погодились оголосити кіберпростір операційної галуззю, окрім повітря, суші та моря.

У 2016 р. НАТО розробила важливий документ «Кібербезпека: навчальний план загального користування» (Cybersecurity a generic reference curriculum) для забезпечення країн партнерів НАТО планом для запровадження курсів поглибленого вивчення та підтримки курсів у галузі кібербезпека. Цей документ є «дорожньої картою» у процесі надання необхідних знань та навичок майбутнім фахівцям з кібербезпеки і дозволяє розвивати кібербезпекову політику на національному та міжнародному рівнях (NATO, 2016, p. 3).

Необхідно зауважити, що в документі визначаються необхідні для майбутніх фахівців професійні знання та навички (NATO, 2016, p. 13), знання міжнародного та національного права з питань кібербезпеки (p. 48), навички менеджменту кібероперaціями на національному рівні (p. 54). Документ пропонує найбільш ефективні форми та методи навчання, насамперед практико-орієнтовані, які мають реалізовуватися у співпраці з представниками галузі (запрошення представників приватних та державних організацій для викладення певних тем, наприклад, кібербезпека приватних компаній) (p. 25).

Гармонізація законодавства на національному рівні та посилення співпраці між країнами Європейського Союзу є найефективнішим механізмом інтеграції в ЄС, що є надзвичайно актуальним для України на сучасному етапі її розвитку. Договори про стабілізацію та асоціацію як ключові документи пов'язані з процесом поширення ЄС, передбачають, зокрема, зобов'язання всіх країн привести їх національне законодавство у відповідність до законодавства ЄС. У сфері комунікаційних та інформаційних системи існують положення законодавства ЄС, що спрямовані на створення спільними зусиллями. кібернетичної безпеки країн-членів.

Шляхом прийняття конвенцій, декларацій країни світу застосовують єдиний підхід у забезпеченні безпеки у кібернетичному просторі, визнаючи, таким чином, необхідність співпраці у цій галузі. Найважливішою міжнародною конвенцією в галузі кібербезпеки вважається Конвенція Ради Європи про кіберзлочинність (Convention on Cybercrime) (Будапештська конвенція) (Council of Europe, 2001). Конвенція є правовою основою для боротьби з кіберзлочинністю, включаючи напади на інформаційні системи. Ця конвенція, доповнена Протоколом про ксенофобію та расизм, поширення якого здійснюється через комп'ютерні системи, є єдиною обов'язковою міжнародною угодою, що стосується кібербезпеки і вважається архетипним шаблоном для всіх країн, які зацікавлені у безпеці кіберпростору. Конвенція підписана 54 країнами (ратифікована 48) з усього світу. Будапештська конвенція вимагає від сторін: прийняття відповідного законодавства проти кіберзлочинів;

забезпечення належних процедурних інструментів для ефективного розслідування та переслідування злочинів, пов'язаних із кіберзлочинністю; запровадження міжнародного співробітництва між всіма країнами, що беруть участь у таких заходах.

Таким чином, Будапештська конвенція запроваджує міжнародні правові стандарти шляхом криміналізації кіберзлочинів, ініціює заходи для управління програмами боротьби з кіберзлочинністю, запроваджує співробітництво у виявленні, екстрадиції, взаємодопомоги, взаємообміну інформацією тощо (Council of Europe, 2001, 10–17).

Директива 2013/40/ ЄС Європейського Парламенту та Ради «Про напад на інформаційні системи» (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) запровадила нові правила криміналізації та покарання за ряд злочинів, спрямованих проти інформаційних систем, таким чином доповнюючи положення Будапештської конвенції. Ці правила вимагають від країн ЄС використання однакових контактних пунктів, узгоджених Радою Європи та Великою вісімкою, для швидкого реагування на загрози застосування передових технологій у злочинних цілях. Основні види кримінальних злочинів, що визначені в цій Директиві, є напади на інформаційні системи, починаючи від атак про відмову в обслуговуванні, призначеної для знищення сервера, до перехоплення даних та атак ботнету. Таким чином, ця директива зосереджується на уніфікації кіберзлочинів для їх криміналізації у всіх державах-членах Європейського Союзу та співпраці правоохоронних органів. З цією метою в країнах ЄС створюються операційні національні осередки контактів.

З метою своєчасного реагування на терористичні акти у кіберпросторі ЄС у 2015 р. Радою Європейського Союзу була затверджена Європейська програма безпеки (The European Agenda on Security) (Council of the European Union, 2015), в якій означені загальні стратегічні рамки ініціатив ЄС щодо забезпечення кібербезпеки та запобігання кіберзлочинності. Програма передбачає

підвищення ефективності правоохоронних органів, зокрема шляхом створення Європейського центру боротьби з кіберзлочинністю (Європол), та вирішення проблем, пов'язаних із кримінальними розслідуваннями щодо кіберзлочинів, зокрема стосовно вільного доступу до доказів таких злочинів. Основні заходи (European Commission, 2015), передбачені цією Програмою, включають оновлення Рамкового рішення про тероризм (Council Framework Decision of 13 June 2002 on combating terrorism) (The Council of the European Union, 2002), посилення діалогу з ІТ-індустрією та зміцнення інструментів боротьби з кіберзлочинністю, вирішення проблем кадрового забезпечення галузі. Програма також підкреслює важливість зміцнення потенціалу Європолу, включаючи створення Європейського контртерористичного центру, який допомагатиме Європолу активізувати підтримку дій національних правоохоронних органів для боротьби з іноземними терористичними злочинцями, фінансуванням тероризму, екстремістським контентом в Інтернеті, та незаконним обігом вогнепальної зброї.

Рамкова політика ЄС щодо кіберзахисту (Cyber defence policy framework), схвалена у 2014 р. (Council of the European Union, 2014), є одним з головних документів, що конкретно стосуються цих питань і слугує основою для протидії загрозам, що виникають в результаті кіберзагроз Згідно з документом визначено п'ять пріоритетних сфер для забезпечення кібернетичної безпеки та спільної оборонної політики: підтримка розвитку можливостей кіберзахисту країн – членів союзу; сприяння співпраці між цивільною та військовою галуззями та поширення політики кіберзахисту в ЄС відповідними національними установами та установами ЄС; підвищення кваліфікації, забезпечення необхідної освіти та можливостей для навчання персоналу; посилення співпраці з відповідними міжнародними партнерами, зокрема НАТО.

З метою активізації заходів щодо забезпечення кібербезпеки Рамкова політика, з-поміж іншого, визначає процедуру надання допомоги державам-членам Союзу, способи пропагування поінформованості щодо можливих

випадків та наслідків кіберзлочинів, забезпечення тренінгів для протидії, а також визначає необхідність подальших ініціатив у співпраці з країнами-партнерами, іншими міжнародними організаціями. Хоча головним пріоритетом в галузі кібернетичної оборони є захист комунікаційних та інформаційних систем, рамкова політика опирається на надійну та безпечну національну інфраструктуру держав-членів Союзу.

Основа для захисту інфраструктури інформаційних та комунікаційних мереж також закладена у низці документів Європейського Союзу. Директива 2008/114 про ідентифікацію та визначення європейських критичних інфраструктур та оцінку необхідності покращення їх захисту в «Європейській програмі захисту критично важливої інфраструктури» (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008**)**. Важливо, що цей документ визначає загальний, «парасольковий» підхід до захисту критичної інфраструктури в ЄС. Директива визначає необхідність визначення критично важливих складових інфраструктури у Співтоваристві, порушення або руйнування яких матимуть значні транснаціональні наслідки, пов'язані з взаємозалежністю між інфраструктурою різних країн. Оцінювання вимог щодо безпеки для такої інфраструктури має здійснюватися відповідно до єдиного підходу, про який йдеться у документі.

Ряд документів Європейського Союзу спрямовується на об’єднання зусиль у забезпеченні безпечного користування кіберпростором. У 2013 р. була прийнята «Стратегія кібербезпеки ЄС: відкритий, безпечний кіберпростір» (Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace) (European Commission, 2013), що стала першим всеохоплюючим документом ЄС у цій сфері. У ньому визначено п'ять стратегічних пріоритетів: досягнення країнами кіберстійкості; запровадження заходів для зниження кіберзлочинності; розвиток відповідної національної політики та можливостей кіберзахисту, пов'язаних із спільною політикою безпеки та оборони; розвиток промислових та технологічних ресурсів для забезпечення кібербезпеки;

встановлення узгодженої міжнародної політики у сфері кіберпростору для ЄС та сприяння розвитку основних цінностей ЄС.

Документ «Цифрова програма дій для Європи» (The Digital Agenda for Europe), що був прийнятий у травні 2010 р. (Council of Europe, 2010), є одним із найважливіших стратегічних документів на рівні ЄС, у якому підкреслюється загальне розуміння того, що довіра та безпека є фундаментальними передумовами поширення ІКТ та досягнення цілей «сталого зростання» відповідно до стратегії «Європа 2020». У розділі «Довіра та безпека» Програми відзначена необхідність об'єднання зусиль усіх зацікавлених сторін, спрямованих на безпеку та стійкість інфраструктури ІКТ, насамперед зосереджуючи увагу на запобіганні кіберзлочинам, готовності до захисту та обізнаності населення у цьому аспекті, достатньому кадровому забезпеченні галузі.

Захист фізичних осіб у кіберпросторі здійснюється у декількох напрямах. Важливою для безпеки функціонування кіберпростору є Конвенція Ради Європи про захист фізичних осіб під час автоматичної обробки персональних даних (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) (Council of Europe, 1981), яка була підписана 47 країнами. Метою цієї Конвенції є посилення захисту даних фізичних осіб у зв'язку з обов’язковою автоматичною обробкою персональних даних. Важливість документу складно переоцінити, особливо враховуючи необхідність правових положень так званого «електронного уряду». Конвенція передбачає механізм співпраці між країнами та встановлює чіткі правила стосовно транскордонної передачі даних, що вводиться в країнах-учасниках через відповідні державні органи, відповідальні за їх захист.

Варто зазначити, що Рада Європи переймається проблемами захисту дітей у кіберпросторі відповідно до Конвенції із захисту дітей від сексуальної експлуатації та насильства (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse) (інша назва – Конвенція Лансароте) (Council of Europe, 2007), у якій відзначається необхідність створення засад

безпечного Інтернет-середовища, функціонування якого спрямовано передусім на забезпечення дітей корисною для них інформацією та можливістю вільного спілкування.

Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства є найсучаснішим стандартом у цій галузі. Конвенцію Лансароте підписали та ратифікували 40 держав. Її важливість полягає в тому, що вона містить багато посилань на використання інформаційних та комунікаційних технологій у контексті запобігання сексуальній експлуатації та сексуального насильства над дітьми. Це вимагає криміналізації таких дій, як навмисне отримання доступу до дитячої порнографії в Інтернеті. Таким чином, цей документ та Конвенція про кіберзлочинність доповнюють один одного.

Важливо зазначити, що увага міжнародних організацій часто прикута до проблеми кадрового забезпечення ІТ-галузі та захисту кіберпростору. Директива про мережеву та інформаційну безпеку (The directive on network and information security), яка набрала чинності в серпні 2016 р. (European Union. (2016), вимагає, щоб кожна держава – член Європейського Союзу – створила команду висококваліфікованих фахівців з питань своєчасного реагування на інциденти в галузі комп'ютерного захисту у межах спеціальної національної організації та запровадила співробітництво груп стратегічного співробітництва. Директива також гарантує поширення інформації між приватним та державним секторами та визначає декілька категорій операторів основних послуг, від яких вимагається прийняття відповідних заходів безпеки та повідомлення відповідних національних органів про серйозні інциденти, що мають місце у кіберпросторі.

На міжнародному рівні вирішуються питання забезпечення необхідної професійної підготовки персоналу для ІТ-галузі. Створення у 2013 р. основної організації на рівні ЄС у сфері здійснення заходів в рамках комунікаційних та інформаційних систем (Європейської агенції мереж та інформаційної безпеки) ставило за мету здійснювати підготовку фахівців шляхом організації регулярних експертних тренінгів з питань кризового менеджменту у

кіберпросторі та надання практичних рекомендацій, проведення досліджень та організації міжнародних конференцій на тему співпраці в кіберпросторі.

Вивчення документальної бази дозволяє зробити висновок щодо фрагментарності діяльності Організації Об'єднаних Націй (ООН) у галузі кібербезпеки, оскільки означена проблема розглядається на різних рівнях в багатьох органах та установах. З метою виправлення цього недоліку у 2013 р. було налагоджене міжвідомче співробітництво між Міжнародною спілкою електрозв'язку та Управлінням ООН з наркотиків та злочинності. У ході подальшої діяльності у 2013 р. було розроблено загальноєвропейську Рамкову програму з кібербезпеки та кіберзлочинності (Cyber defence policy framework) (Council of the European Union. (2014). Цей документ був укладений для покращення внутрішньої координаційної діяльності організацій системи ООН з суміжних питань.

Отже, міжнародні організації відіграють значну роль у забезпеченні функціонування вільного та безпечного кіберпростору для всіх громадян багатьох країн. Їх діяльність спрямована на розроблення необхідних документів, що створюють правову основу для міжнародної співпраці, об’єднання зусиль у запобіганні та реагуванні на кіберзлочини, підготовки кадрів, спроможних гарантувати безпечне користування інформаційними та комунікаційними мережами. Спільна діяльність країн під керівництвом міжнародних організацій дозволяє більш ефективно протистояти кіберзлочинам на національному рівні, одночасно не зменшуючи темпи розвитку ІТ-галузі.

Висновки до розділу 1

На сучасному етапі розвитку науки і техніки кібербезпека країни перетворюється на одну з найважливіших галузей високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах існування суспільство стало вразливим з боку кібернетичних впливів, які все частіше стають ефективним інструментом для досягнення несилового контролю та управління як об’єктами

інфраструктури держави, підприємств, так і окремими громадянами та їх об'єднаннями. Потоки інформації, що передаються, зберігаються та обробляються у кіберпросторі, постійно збільшуються, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Очевидним і безперечним є той факт, що в умовах подальшого розвитку високотехнологічного суспільства потреба у фахівцях з кібербезпеки буде постійно зростати.

З'ясовано, що методологічним підґрунтям для вивчення проблеми професійної підготовка фахівців з кібербезпеки слугували такі підході: компетентнісний, у межах якого професійна підготовка розглядається як процес засвоєння й закріплення загальних і спеціальних знань, умінь і навичок для ефективного виконання професійних завдань майбутнього робочого місця ІТ-галузі; функціональний, який встановлює залежність процесу професіоналізації майбутніх фахівців з кібербезпеки від особливостей діяльності навчальних закладів; інструментальний, що підкреслює важливість оволодіння системою вмінь шляхом застосування відповідних методів і форм організації освітнього процесу; особистісно-орієнтований, що визначає майбутнього фахівця з кібербезпеки як високопрофесійну особистість; аксіологічний, що вивчає професійну підготовку фахівців з кібербезпеки як процес формування їхніх професійних якостей з урахуванням цінностей суспільства.

Узагальнення результатів наукових пошуків українських та американських учених уможливило висновок про те, що необхідність дослідження проблеми професійної підготовки фахівців з кібербезпеки зумовлена потребами національної безпеки та освітньої практики. Відкритими для наукової дискусії є питання змістового наповнення понять *«ІТ-галузь», «кіберзагрози», «кібератака», «кіберпростір», «кіберзахист», «інформаційна безпека», «кібербезпека», «кібербезпекова політика», «ризики», «фахівець з кібербезпеки», «фахівець з інформаційної безпеки» «бакалавр з кібербезпеки», «професійна підготовка бакалаврів з кібербезпеки».* Розбіжності у наукових поглядах щодо цих понять зумовлюють особливості структурно-змістових та

організаційно-педагогічних засад професійної підготовки фахівців ІТ-галузі в США.

На основі узагальнення результатів наукових розвідок поняття «підготовка фахівців з кібербезпеки» необхідно розглядати як: соціально, економічно, політично детермінований феномен; педагогічну систему, яка є важливою складовою системи вищої освіти; цілісний неперервний педагогічний процес, спрямований на засвоєння систематизованих фахових знань, формування умінь і навичок та їх постійного оновлення, наукового світогляду, що здійснюється з урахуванням досягнень технічного і технологічного прогресу, сучасних тенденцій інформаційного суспільства, потреб внутрішнього та світового ринків праці.

Міжнаціональний характер кібернетичного простору вимагає вироблення та координації спільної для всіх країн світу політики щодо гарантій безпечного користування кіберпростором. На основі аналізу міжнародних нормативно-правових документів узагальнено основні напрями діяльності міжнародних організацій у галузі кібербезпеки: створення правової основи для міжнародної співпраці різних країн, об’єднання зусиль у запобіганні та своєчасному реагуванні на кіберзлочини, ефективна підготовка кадрів, спроможних гарантувати безпечне користування інформаційними та комунікаційними мережами.

Зміст розділу викладено в таких наукових працях автора: Бистрова, 2016; Бистрова, 2017b.

РОЗДІЛ 2. СИСТЕМА ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ ІЗ КІБЕРБЕЗПЕКИ У США

У розділі 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.

2.1. Національна стратегія професійної підготовки фахівців з кібербезпеки у США

На сучасному етапі розвитку науки і техніки США кібербезпека перетворилася на одну з найважливіших галузей високотехнологічного суспільства. Як наслідок суперництва США і ЄС з РФ та КНР американське суспільство є частиною світового кіберпростору і відповідно зазнає різних загроз і негативних впливів. Помітним є загострення уваги до питання вирішення проблем із кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у зміцненні безпеки кіберпросторі держави і вирішенні комплексу проблем, пов’язаних із розбудовою національної системи кібербезпеки.

Здійснений аналіз досвіду США щодо реалізації кібербезпекової політики дозволяє стверджувати, що у країні приділяється значна увага посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу тому, що науковий, технічний, військовий, фінансовий потенціал та потенціал високих технологій Сполучених Штатів Америки є національним надбанням американського народу. Відповідно він потребує захисту на державному рівні. Концентрація найбільших фінансових компаній, науково-дослідницьких установ та корпорацій, які суттєво впливають на фінансову стабільність і

економічний розвиток країни, на інтенсифікацію важливих технологічних процесів підсилюють значущість управління кібербезпекою в США. Отже, однією з особливостей кібербезпеки є її бінарний характер: вона є елементом національної безпеки і водночас – явищем глобалізованим, так як інформаційний простір немає кордонів, тому злочини у цій сфері переважно кваліфікуються як транснаціональні.

Нормативно-правові засади здійснення підготовки й підвищення кваліфікації фахівців із кібербезпеки у США розробляються на національному рівні урядом країни. Вважається, що в США вперше термін «кібербезпека» було запропоновано у середині 1990-х років, коли уряд зацікавився проблемою і почав її досліджувати. Саме директива адміністрації Президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) «Захист критично важливої інфраструктури» від 22 травня 1998 року започаткувала цілеспрямовану регулярну організаційну діяльність в ІТ-галузі на національному рівні. Цей документ лежить в основі підписаного у 2000 році президентом Б. Клінтоном «Загальнонаціонального плану захисту інформаційних систем». У ньому сформульовані основні напрями діяльності країни і всього суспільства щодо забезпечення кібербезпеки як складової інформаційної безпеки. Національну політику країни в цій сфері формує Агентство національної безпеки США (АНБ), а першочергові питання розв’язуються, як правило, на рівні Ради національної та внутрішньої безпеки країни. При цьому кібернетичний захист розглядається АНБ як забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в інформаційно-комунікаційних системах. Крім того, сучасна політика інформаційної безпеки США пов’язана з концепціями інформаційного протистояння і пріоритетами співробітництва у форматі «інформаційної парадигми», що передбачає інформаційно-технологічні переваги держави, які здатні зберегти досягнуту в докризовий період стабільність і забезпечити посткризовий розвиток, зробити перебіг соціальних конфліктів більш прогнозованим, запобігти суперечностям у суспільстві (Брижко, Гальченко, Цимбалюк та ін., 2002)

У лютому 2003 року адміністрація президента Джорджа Буша-молодшого розробила документ «Національна стратегія досягнення безпеки в кіберпросторі» (National Strategy to Secure Cyberspace), у якому було визначено п'ять пріоритетних напрямів діяльності США в ІТ-галузі та кібербезпеки країни, розкрито сутність основних завдань в рамках цих пріоритетних напрямів на середньострокову і довгострокову перспективу.

Розглянемо сутність цих пріоритетних напрямів: *напрям 1* – це становлення і розвиток національної системи реагування на події в сфері інформаційної безпеки; *напрям 2* – це реалізація комплексної системи заходів щодо зменшення загроз інформаційній безпеці; *напрям 3* – це забезпечення підготовки фахівців у сфері комп'ютерної безпеки і забезпечення відповідального ставлення всього населення країни до питань захисту ІТ-систем; *напрям 4* – це забезпечення захисту інформаційних систем, що стосуються діяльності державних органів; *напрям 5* – це розвиток різних форм кооперації (зокрема і міжнародної) у сфері інформаційної безпеки (National Strategy to Secure Cyberspace, 2003).

Відповідно до пріоритетного напряму 3 дії американського суспільства спрямовані на забезпечення підготовки фахівців у сфері комп'ютерної безпеки і формування відповідального ставлення всього населення країни до національної безпеки. Формування відповідального ставлення до ІТ-систем та підготовка кадрів у цій сфері зумовлено тим, що джерелом вразливості є недостатня відповідальність певних користувачів, системних адміністраторів і розробників інформаційних систем щодо питань захисту інформації, їх недостатня інформованість. Для забезпечення кіберзахисту держави згідно з «Національною стратегією досягнення безпеки в кіберпросторі» передбачено реалізацію таких основних чотирьох заходів:

- просування багатосторонньої загальнонаціональної програми з інформування та розвитку відповідального ставлення громадян країни до безпеки тих інформаційних систем, до яких вони мають будь-який доступ;

- створення таких програм підготовки фахівців, які б задовольнили кадрові потреби ІТ-галузі;
- підвищення ефективності існуючих програм підготовки фахівців з кібербезпеки;
- підтримка зусиль приватних компаній по створенню, поширенню і забезпеченню загального визнання сертифікаційних програм у сфері інформаційної безпеки.

Фактично «Національна стратегія досягнення безпеки в кіберпросторі» і стала керівництвом до дії державної влади за стратегічними напрямами розвитку цієї галузі. Як наслідок, відбулася модернізація структури державних органів, які забезпечують ІТ-галузь фахівцями зі спеціальності кібербезпеки в країні. Втілення в життя стратегії інформаційної безпеки та кібербезпеки за основними державними пріоритетами у цій сфері є офіційною загальнонаціональною кібербезпековою політикою США.

Як вже зазначалося, розповсюдження інформаційних засобів відкриває можливості для розвитку особистості, актуалізує питання здійснення змін у свідомості людей в умовах постіндустріального суспільства США, у якому формується потреба якісного кадрового забезпечення різних галузей. Глибока зміна особистісних характеристик людини – це процес, властивий сучасному етапу інформатизації суспільного життя у США. Відповідно до найбільш радикальних гіпотез припускається виникнення нового біологічного виду людини, головною рисою якої є інформаційна потреба. Зусилля, яких повинен докладати професіонал, щоб бути конкурентоспроможним на ринку праці, спонукають його до саморозвитку, самовдосконалення, самоосвіти.

У матеріалах Конгресу США, присвячених питанням національної безпеки кіберпростору, зазначено, що у країні кібербезпека та інші сфери інформаційної діяльності, забезпечують зайнятість 2/3 працездатного населення, а решта працює у виробництві, яке перебуває у залежності від інформації. У США проблеми, пов’язані з появою інформаційних технологій та організацією, розробленням ефективної кібербезпекової державної політики, її

стратегії і тактики розвитку, стали джерелами структурного перерозподілу зайнятості населення у бік інформаційної сфери діяльності, сфери захисту інформації та кіберпростору.

Програми підготовки фахівців для галузі знань «Інформаційні технології» почали з'являтися в кінці 1990-х років. Посилення інтересу суспільства до інформаційних технологій було зумовлено багатьма чинниками, зокрема зростанням глобальної мережі Інтернет, великою, можливо, не завжди виправданою увагою до розв'язання проблеми «*Y2K*» (так позначалася проблема можливого збою комп'ютерних календарів при переході до нового тисячоліття)

У США побудова національної моделі кібербезпекової політики відбувається шляхом розроблення першочергових заходів у діяльності державного та приватного секторів щодо захисту кіберпростору та найбільш ефективного вирішення основних завдань кібербезпекової політики (Черноног, 2015).

Після подій 11 вересня 2001 року уряди країн та громадяни всього світу усвідомили небезпеку та загрози інформаційних атак. В США було створено Міністерство внутрішньої безпеки (МВБ), яке відіграє ключову роль у забезпеченні кібербезпеки держави та захисту критично важливої інфраструктури Сполучених Штатів Америки. Відповідно до прийнятого у 2002 році Закону США «Про внутрішню безпеку» (Homeland Security Act of 2002) урядові структури, що займалися безпекою кіберпростору, перейшли під контроль МВБ. Цей закон також посилив відповідальність за кіберзлочини (включаючи довічне ув'язнення), зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив права останніх щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу суду, визначив основні напрями діяльності федеральних органів з підвищення ефективності захисту критичної інфраструктури США від кібератак, зокрема об'єктів стратегічного значення, що перебувають у приватній власності.

Гарантом ефективності кібербезпекової державної політики США є кримінальне законодавство у сфері кіберзлочинності із низкою чинних законів, а саме:

- Закон «Про боротьбу зі спамом» (Controlling the Assault of Non-solicited Pornography and Marketing, 2003);
- Закон «Про злочини, пов'язані з засобами доступу» (Fraud and related activity in connection with access devices,1998);
- Закон «Про злочини, пов'язані з комп'ютерами» (Fraud and related activity in connection with computers,1984);
- Закон «Про злочини, пов'язані з електронною поштою» (Fraud and related activity in connection with electronic mail, 2003);
- Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» (Wire and Electronic Communications in Terception and Interception of Oral Communications, 1970);
- Закон «Про зберігання повідомлень та доступ до записів транзакцій» (Stored Wire and Electronic Communications and Transactional Record Access, 1986).

У сфері питань, пов'язаних з кібербезпекою, діє чинне законодавство. Серед регулюючих законів відзначимо такі:

- Закон «Про національну безпеку» (Homeland Security Act, 2002);
- Закон «Про дослідження та розвиток кібербезпеки» (Cyber Security Research and Development Act, 2002);
- Закон «Про інформаційну безпеку» (Federal Information Security Management Act, 2002);
- Закон «Про недоторканість особистого життя» (Privacy Act,1974);
- Закон «Про електронні транзакції» (Uniform Electronic Transactions Act, 2000);
- Закон «Про захист дітей у XXI ст.» (Protecting Children in the 21st Century Act, 2007-2008);

- Закон «Про захист дітей від сексуального насильства» (Keeping the Internet Devoid of Sexual Predators Act, 2008);

- Закон «Про захист дітей в Інтернеті» (Children's Internet Protection Act, 2000);

- Закон «Про електронні підписи» (Electronic Signatures in Global and National Commerce Act, 2000 р.).

1 жовтня 2009 року у США (перша каденція Б. Обами) оголошено про додатковий набір 1 тис. співробітників до спеціального кібербезпекового департаменту Міністерства внутрішньої безпеки (Department of Homeland Security), які займаються виключно безпекою високотехнологічних систем США. Однак навіть ця кількість співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки, тому основними завданнями національної кібербезпекової політики США визначено підтримку досліджень і розробок у галузі інформації, запровадження нововведень у сферу економіки; вдосконалення інформаційної інфраструктури, дослідження впливу систем на міжнародні, національні та приватні пріоритети шляхом контролю за їх діяльністю; встановлення рівноваги між основними інформаційними цінностями.

Ефективна реалізація кібербезпекової політики держави на початку XXI століття, в рамках якої розробляється комплекс заходів щодо прогнозування та протидії кіберзагрозами, є передумовою розвитку системи необхідних знань. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем професійної підготовки фахівців з кібербезпеки. Підготовка фахівців для ІТ-галузі з кібербезпеки з метою забезпечення потреб галузі у кадрах та формування відповідального ставлення всього населення країни до кіберзахисту вимагає ґрунтовного підходу до організації освітнього процесу. Стратегія становлення системи підготовки кадрів у сфері кібербезпеки, організаційно-педагогічні умови

навчання бакалаврів з кібербезпеки в університетах США спрямовані на реалізацію загальнонаціональної кібербезпекової політики держави.

На рис. 2.1.1. схематично представлено державну стратегію професійної підготовки кадрів через основні заходи її реалізації.

Рис. 2.1.1. Схематичне зображення основних заходів з підготовки фахівців з кібербезпеки відповідно до державної стратегії США (The National Security Strategy of the United States of America, 2015).

Формування та розвиток відповідального ставлення громадян країни й суспільства до ризиків кібератак та їх наслідків, безпеки кіберпростору та інформаційних систем, покладено в основу державної стратегії, що є передумовою виконання американської кібербезпекової політики, просування багатосторонньої загальнонаціональної програми з інформування суспільства про кіберзахист.

Безсумнівно, ефективність освітнього процесу забезпечується насамперед якісним програмним забезпеченням, що неможливо без професійних кадрів із кібербезпеки. Важливо, що розвиток системи підготовки фахівців з

кібербезпеки в США передбачає запровадження соціального партнерства різних структур, гармонійне поєднання зусиль федеральних органів, відомчих структур, приватного сектору та громадських організацій. Адже формування мотивації щодо створення нових програм з підготовки фахівців входить у спектр повноважень згаданих структур. Укладання нових програм підготовки фахівців, підвищення ефективності чинних програм підготовки кадрів передбачає вмотивованість приватних компаній у питаннях розроблення, поширення сертифікованих програм з їх подальшим визнанням та застосуванням.

Для реалізації цього завдання ще в кінці минулого століття урядом та промисловцями США було створено ряд необхідних відомств, асоціацій та агенцій: NSA (National Security Agency) – Агентство національної безпеки; NIPC (National Infrastructure Protection Center) – національний центр захисту інфраструктури, що об'єднав представників влади, військових і приватний сектор; DISA (Defense Information Systems Agency) – агентство з захисту інформаційних систем; IACIS (International Association for Computer Information Systems) – міжнародна асоціація фахівців комп'ютерних досліджень.

За даними аналітиків провідної світової дослідницької консалтингової компанії у сфері інформаційних технологій «Gartner Group» (рік заснування – 1979, м. Стенфорд, штат Коннектикут, США, яка з 2001 року перейменована на Gartner, Inc.), кількість клієнтів сягає 60 тис. з 10 тис. організацій. Ринок праці США у IT-галузі пропонує не менш, ніж 1,6 млн. робочих місць щорічно, причому більше половини вакансій до кінця року так і залишаються вільними через відсутність необхідних фахівців. Значну частину з них становлять фахівці з кібербезпеки.

На рис. 2.1.2. графічно представлений стан забезпечення сертифікованими фахівцями з кібербезпеки в різних країнах світу.

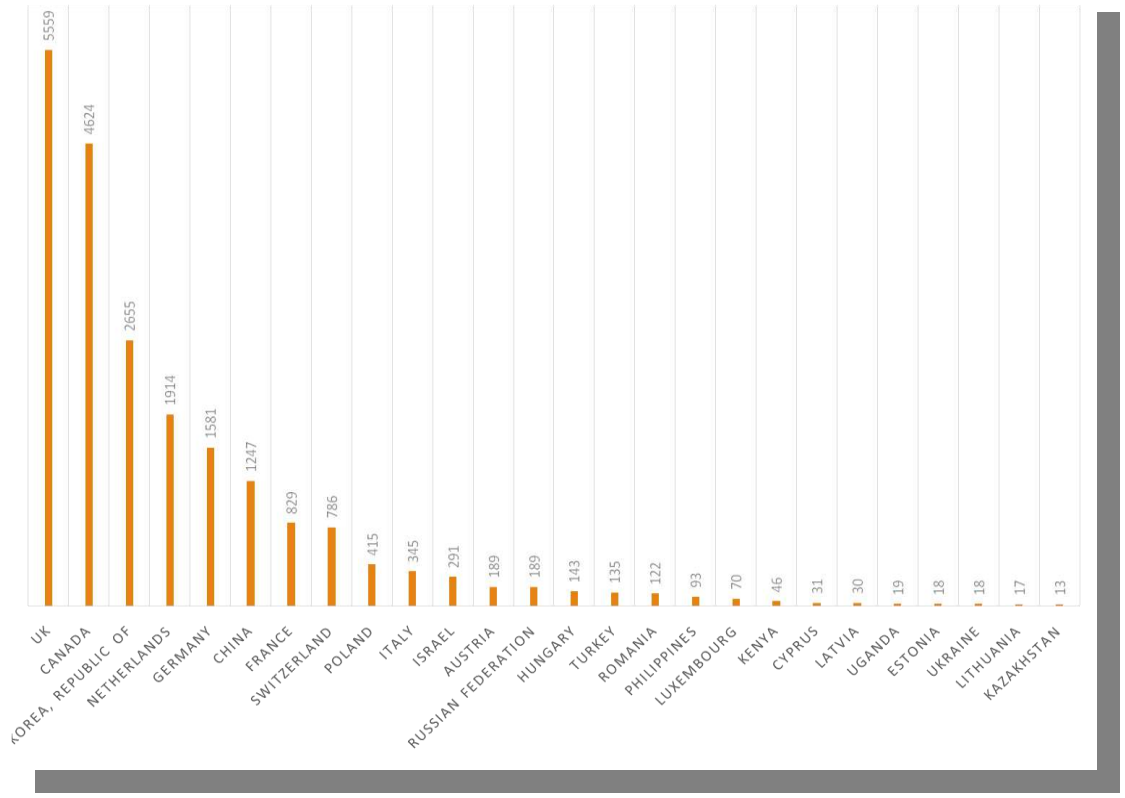


Рис. 2.1.2. Кількість сертифікованих фахівців з кібербезпеки у світі (Кібербезпека: нова пропозиція, 2017).

Як можна бачити, з-поміж інших країн, які мають сертифікованих фахівців з кібербезпеки, зіставлено позиції США та України щодо кількості сертифікованих фахівців з кібербезпеки у світі. За даними 2017 року загальна кількість сертифікованих фахівців з кібербезпеки у світі сягала 108 тис., з них 71 тис. фахівців працювали у США. У контексті питомої ваги із забезпечення галузі сертифікованими фахівцями з кібербезпеки США є лідером, тоді як Україна, на жаль, поки посідає лише 78 місце. Загальна кількість сертифікованих фахівців з кібербезпеки у світі становить 108 тис. осіб, з них на США припадає 71 тис., тоді як потреба ринку в США становить понад 150 тис., що вказує на величезний дефіцит у кадровому забезпеченні галузі.

У США та інших країнах НАТО утворився гостра недостатність кадрів у галузі інформаційних технологій за спеціальністю «Кібербезпека». Так, для комплектування кіберкомандування (Air Force Global Strike Command – штабу бази ВПС в Барксдейлі штату Луїзіана (грудень 2009 – квітень 2010 рр.) чисельністю 26 тис. співробітників, довелось задіяти механізми тимчасового

призову цивільних фахівців інформаційної безпеки в підрозділи національної гвардії.

Розвинена потужна мережа університетів США (45 закладів) забезпечує підготовку фахівців для IT-галузі з кібербезпеки. Але у зв’язку з тим, що, починаючи з 2013 року, ситуація у світі загострилася і кібератаки спричинили людські втрати, було введено термін «кібервійна». У світовому масштабі кількість кіберінцидентів щорічно зростає на 40%. Основними факторами збільшення кібератак стала поява таких явищ, як Internet of Thing – Інтернет-речей; Cloud Computing – хмарні обчислення; різке зростання кількості пристроїв, підключених до мережі, кількість яких до 2020 року сягне 20’000’000’000 (Кібербезпека: нова пропозиція, 2017). За таких масштабів, розслідування комп'ютерної злочинності відчуває гострий дефіцит у фахівцях.

У матеріалах Конгресу США, присвячених питанням національної безпеки кіберпростору (Report to Congress on Cybersecurity - USNI News, 2018) зазначено, що у країні кібербезпека та інші сфери інформаційної діяльності охоплюють зайнятістю 2/3 працездатного населення, а решта працює у виробництві, яке перебуває у залежності від інформації. У США проблеми, пов’язані з появою інформаційних технологій та організацією, розробленням ефективної кібербезпекової державної політики, її стратегії і тактики розвитку стали джерелами структурного перерозподілу зайнятості населення у напрямі інформаційної сфери діяльності, сфери захисту інформації та кібербезпеки. Важливим питанням кібербезпекової політики американського інформаційного суспільства стало інтенсивне насичення всіх його сфер висококваліфікованими кадрами. Технічний директор США і колишній топ-менеджер Google Меган Сміт зазначила, що у найближче десятиліття в США з'явиться 1,4 млн IT-вакансій і лише 400 тис. навчених висококваліфікованих фахівців можуть заповнити їх (Smith, 2017). Це означає, що американська економіка знаходиться перед загрозою гострого дефіциту технологічних кадрів вже у найближчій перспективі.

Щоб заповнити кадровий дефіцит, американські IT-компанії відчайдушно намагаються імпортувати відсутніх фахівців з-за кордону. Тільки в 2017 році федеральний уряд США отримав 233 тис. заявок на видачу робочих віз H1-B іноземцям. Однак, як зазначає Сільвен Калаш (співзасновник освітньої програми для розробників IT-продукції в Сан-Франциско Holberton School) тільки 36 % від квоти на 2017 рік 85 тис. віз були обрані «випадковим чином» тому, що сам механізм відбору багато хто вважає нечесним і схильним до маніпуляцій з боку обізнаних інсайдерів.

Незважаючи те, що Кремнієва Долина вважається епіцентром світової IT-індустрії, статистично більшість високотехнологічних компаній розташовані зовсім не в Каліфорнії. Крім того, IT-фахівців компанії Долини все частіше переводять ключові операції за межі США. За даними різних досліджень (Маслянко, 2017), відсутність інженерних талантів стримує зростання американських IT-компаній, що представляє собою серйозну загрозу для всієї економіки Сполучених штатів. Уряд США добре усвідомлює існування цієї проблеми і докладає значних зусиль для її вирішення.

У березні 2015 року адміністрація Барака Обами оголосила про започаткування ініціативи Tech Hire (національної мережі для громад, педагогів та роботодавців щодо допомоги із забезпечення роботою) з фінансуванням в 100 млн. доларів, метою якої є надання допомоги навчальним закладам, які мають стати «кузнями технічних кадрів майбутнього», у 2016 році бюджет мережі було подвоєно (Tech Hire, 2016).

Зусиллями лідерів IT-індустрії ряд освітніх ініціатив реалізується і в Кремнієвій Долині, яка відома значною щільністю діяльності високотехнологічних компаній, де зосереджено низка провідних університетів, що підпорядковуються неподалік розташованим великим містам. Можливість фінансування нових компаній, географічне розташування, сприяли виникненню і розвитку цього технологічного центру.

Оригінальна назва Долини походить від англійської назви кремнію. Кремній використовується у якості напівпровідника у виробництві

мікропроцесорів. Саме з цієї індустрії розпочалася історія Долини як технологічного центру. Вперше ця назва була використана 11 січня 1971 року журналістом Доном Гефлером (Don Hoefler), коли він почав публікувати серію статей під назвою «Кремнієва Долина США». Так,виконавчий директор Facebook Шеріл Сандберг і засновник Netflix Рід Хастінгс виділили 131 млн. доларів на підтримку інноваційних освітніх організацій. Відразу три венчурних фонди (Trinity Ventures, AME Cloud Ventures і Partech Ventures) інвестували в розвиток Holberton School і її дворічну програму підготовки фул-стек-розробників (full stack developer) програмного забезпечення для IT-галузі (фул-стек-розробник – це фахівець, який володіє знаннями для розроблення веб-проектів від початку до завершення) (Лукидес, 2014).

Відповідно заможні бізнесмени світового рівня найбільш зацікавлені у підготовці фахівців з кібербезпеки. Так, Пітер Тіль засновник Pay Pal в 1998 році, перший зовнішній інвестор Facebook ($ 500 тис.), керуючий партнер в Founders Fund та співзасновник і голова інвестиційного комітету Mithril Capital Management (фонду для інвестицій на пізній стадії) з 2010 року, 30 студентам надає по $ 100 000, щоб вони покинули університет і займалися його проектом. Пітер Тіль в 2014 році здійснив інвестування в Ethereum (з англ. ether – «ефір», «Ефіріум» – платформа для створення децентралізованих онлайн-сервісів на базі блокчейна (децентралізованих додатків), що працюють на основі розумних контрактів), а у 2015 став партнером стартап-інкубатора Y Combinator, який щорічно роздає гранти в розмірі $ 100 000 перспективним IT-підприємцям, закликаючи їх покидати університети і занурюватися в розроблення відповідних продуктів (Business Insider, 2017).

Французький мільярдер і медіамагнат Ксав'є Ніль запустив у 2016 році у Кремнієвій Долині безкоштовну школу програмування «42», яка вже здобула славу у Франції. У найближчі п'ять років в її стінах планують підготувати 10 000 програмістів. Сільвен Калаш стверджує, що хоча ці ініціативи є значущим внеском у справу, але цього недостатньо, щоб заповнити дефіцит технічних кадрів (Dev.by, 2016). Індустрія IT і стартапів зобов'язана збільшити

інвестиції в підготовку інженерних кадрів, щоб вирішити проблему кадрового забезпечення галузі.

У цілому розроблення концепцій й технологій глобальної інформаційної інфраструктури належить до найбільш великомасштабних проектів, реалізованих співтовариством США і покликаним якісно змінити умови життя й діяльності людини (Рудник, 2015).

У кіберпросторі реалізують інформаційну діяльність бізнес-структури і громадяни, зорієнтовані на інформаційні технології. Поява нового покоління користувачів цифрових пристроїв є характерною ознакою американського суспільства. Отже, для боротьби з кіберзлочинністю та у відповідь на соціальні зміни багато урядів і установ запустили ініціативи в галузі кібербезпеки, починаючи з настанов і стандартизації та закінчуючи комплексним законодавством і регуляторними актами (Мельник, 2016, с. 83-84).

Так, на державному рівні з метою посилення боротьби з кіберзлочинністю прийнятий важливий комплекс програмних документів, а саме:

- Міжнародна стратегія для кіберпростору «Безпека, відкритість у мережевому світі» (Security, openness in the network world, 2011);
- План дій з посилення кібербезпеки найважливіших об’єктів інфраструктури (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014);
- Кіберстратегія Міністерства оборони (2015);
- Міжвідомчий план дій з кібербезпеки систем управління (Cross-Sector Roadmap for Cybersecurity of Control Systems, 2014);
- План дій з забезпечення кібербезпеки систем енергопостачання (Roadmap to achieve energy delivery systems cybersecurity, 2014).

У США функціонують відповідальні за кібербезпекову державну політику органи, її стратегію та тактику розвитку. Це координатор органів виконавчої влади з питань кібербезпеки, який виступає в якості помічника Президента. Функції з контролю і координації імплементації національної

стратегії кібербезпеки, політики і згаданих планів дій органами виконавчої влади виконують Міністерство національної безпеки та Міністерство оборони. Стосовно міжвідомчого співробітництва існує ряд програм і планів:

- програми та плани з розподілу повноважень між органами державної влади та приватним сектором; національний план із захисту інфраструктури (National Infrastructure Protection Plan, 2013);

- меморандум між Міністерством національної безпеки та Міністерством оборони про захист важливих цивільних та військових комп'ютерних систем та мереж (2010);

- пілотна ініціатива Міністерства національної безпеки, Міністерства оборони і Центру розповсюдження та аналізу інформації про фінансові послуги (FS-ISAC) із захисту основних мереж та об'єктів інфраструктури у сфері фінансових послуг шляхом обміну чутливою інформацією, що дає підстави для судового переслідування.

Отже, на основі аналізу американського досвіду можемо зробити висновок, що глобалізація світової економіки, модернізація виробництва, динамічні зміни на ринку праці зумовлюють потребу у фахівцях-професіоналах нової генерації в ІТ-галузі і спеціальності «Кібербезпека» та ставлять принципово нові вимоги до їхньої професійної підготовки. Підготовки фахівців з кібербезпеки в США відбувається відповідно до національної стратегії. Її напрями були визначені вимогами Інформаційного суспільства, що характеризується стрімким розвитком інформаційних та телекомунікаційних технологій та потребою у фахівцях для їх обслуговування.

2.2. Загальна характеристика системи підготовки бакалаврів з кібербезпеки у закладах вищої освіти США

Зміни, що відбулися в економічній діяльності установ під впливом недостатності або надлишку інформації, особливості створення кіберпростору та пов'язана з ним потреба забезпечення кіберзахисту актуалізували нові підходи до підготовки бакалаврів з кібербезпеки. На сучасному етапі у США

функціонує найбільш досконала і розвинена система кіберзахисту критично важливої для нації інфраструктури, теоретичними засадами якої є математичне моделювання, цифрове імітування, моделювання систем тощо.

Саме у системі вищої освіти відбувається імплементація аналітичного та системного підходів до підготовки фахівців з кібербезпеки (Pazynyuk, Oreku, &Li, 2008; Seelen, Behrend, 2011). Схарактеризуємо особливості національної системи вищої освіти, приділяючи особливу увагу підготовці бакалаврів в галузі кібербезпеки США насамперед у контексті реалізації принципу ступневості в американській моделі підготовки фахівців.

Особливості державного устрою США визначають відсутність єдиної траєкторії здобуття освіти – кожен штат має право самостійно вирішувати питання щодо структури освіти. Проте більшість штатів надають перевагу традиційній чотирьохступеневій структурі із дошкільною, середньою, професійною і вищою ланками освіти. До особливостей освіти в США можна віднести 12-річне навчання в школі (початковій та середній) і 4-річне навчання у більшості закладах вищої освіти на програмах бакалаврату. Необхідна кількість років для здобуття вищої освіти сягає 16, що відповідає світовим тенденціям і характерно для більшості країн світу (Латвія, Австралія, Польща, Японія та інші).

На рис. 2.2.1. подана схема системи освіти США, яка засвідчує, що задля отримання диплому бакалавра (наприклад, із спеціальності «Кібербезпека») випускник середньої школи повинен вступати на програму підготовки спеціаліста чи магістра, а вступ до аспірантури можливий лише після здобуття повної вищої освіти.

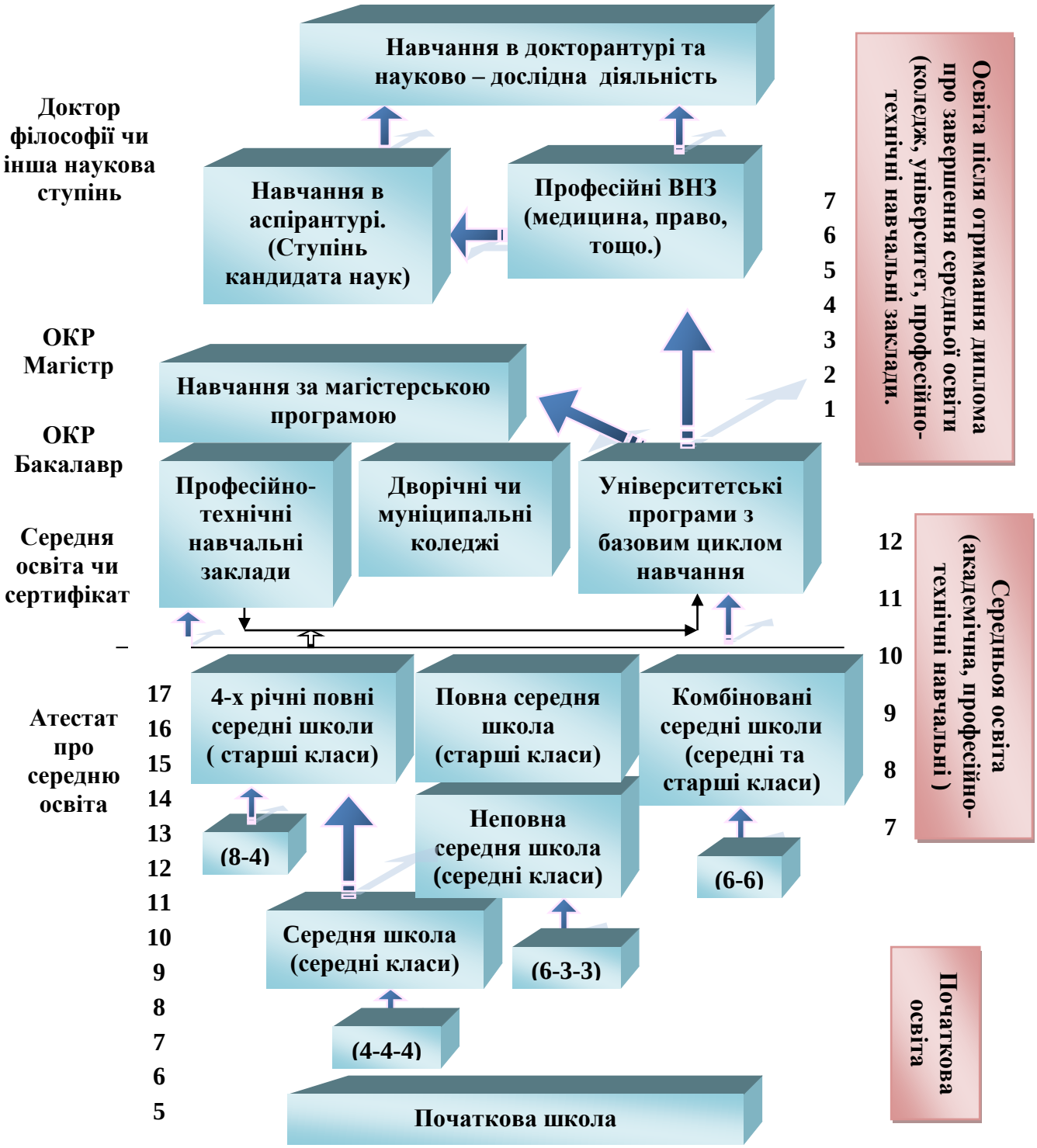


Рис. 2.2.1. Схема ступеневості освіти США (Ничкало, 2002&Романовський, 2002).

Відповідно до сучасної структури системи освіти в США початковою ланкою в цій системі є *початкова школа*, яку відвідують діти з 6-річного віку. *Середню школу* відвідують школярі віком від 14 до17 років, які навчаються з дев'ятого до дванадцятого класів. Здобувачі середньої освіти мають можливість

її здобути у два етапи: спочатку навчання на нижчому ступені молодшої середньої школи. Особливість навчання у цій ланці полягає у відсутності єдиної освітньої програми з чітко визначеними навчальними посібниками, надання учням можливості до восьмого класу самостійно обирати додаткові до основних предмети (англійська мова, математика, суспільствознавство, фізичне виховання та ін.). Вищий ступінь середньої школи передбачає проведення навчання за загальновизнаною програмою, в яку входять такі обов'язкові предмети для вивчення, як: алгебра, англійська мова, природничі і суспільні науки тощо.

Середня освіта в США може поєднувати декілька напрямів. *Академічний напрям* орієнтований на підготовку учнів до вступу у вищий навчальний заклад. Цікаво, що навчання завершується тестом після восьмого року навчання – це тест на визначення коефіцієнту інтелекту. Якщо результат учня менше 90 балів, то доцільність навчання учня на академічному відділенні ставиться під сумнів, і таким учням рекомендують обрати один із професійних профілів навчання. *Професійний напрям* має на меті підготовку учнів насамперед до здійснення професійної діяльності з певної спеціальності і включає проходження практики на потенційному робочому місці з обсягом теоретичних предметів меншим порівняно з академічним профілем. *Загальний напрям* підготовки поєднує два попередні підходи. Слід зауважити, що «...кожна модель 12-річного шкільного навчання надає вищу середню (або повну середню) освіту» (Романовський, 2002, с. 72.).

Характерним є вивчення новітніх технологій та екології у сучасній системі шкільної освіти. На думку дослідниці проблем удосконалення та реформування американської середньої школи М. Шутової (2005) на перший план висуваються інноваційні технології та творчий підхід до навчального процесу з метою трансформації знань і культури на шляху до інформатизації та інтернаціоналізації» суспільства (Шутова, 2005,с. 10).

У ході анлізу американської початкової і середньої освіти нами виділено основні її переваги: 1) реалізація демократичних засад в управлінні та

діяльності шкіл; 2) диференційований підхід до навчання; 3) інноваційний підхід до навчального процесу; 4) безкоштовна державна середня освіти (з 2000р.); 5) державний контроль шкільної освіти; 6) зв'язок середньої школи з вищою шляхом орієнтації на майбутню професійну діяльність.

Підготовка до вступу у вищий навчальний заклад починається ще у середній школі за академічним напрямом. Відповідно особлива увага приділяється важливим дисциплінам (алгебрі, тригонометрії, геометрії, фізиці, хімії тощо), що значно полегшує майбутнім абітурієнтам підготовку до вступу на програму бакалавра в коледжі чи університеті. Цей факт лише підсилює думку про інтеграцію всіх ланок освіти у єдину систему (шкільна, професійна, післядипломна); інтеграцію типів освітніх закладів (молодший коледж, технічна школа, 4-річна вища школа, старша вища школа, молодша вища школа, комбінована вища школа, університет, професійна школа) та кваліфікаційних освітніх рівнів або ступенів (бакалавр, магістр, доктор філософії), що забезпечує можливість отримання загальноосвітніх та професійно-орієнтованих фахових знань і також оновлення й збагачення знань протягом усього життя людини.

Одна із стратегічних цілей освітньої політики США (Америка 2000. Стратегія освіти, 2000) полягає у формуванні компетентності студента для продуктивного використання набутих ним знань у майбутній професійній діяльності у якості відповідального фахівця, громадининав сучасних економічних умовах (Лебідь, 2001, с. 50).

Згідно із структурою системи освіти в США строк навчання у *вищій школі* триває 4 роки. У США немає чіткого визначення поняття «вищий навчальний заклад». До нього відносять будь-який навчальний заклад, де здійснюють підготовку після закінчення середньої школи. Тобто «…коледжі, університети, професійні школи та інші інститути і заклади США післяшкільної освіти традиційно належать до системи вищої освіти»... (Ніколаєнко, 2006, с.77).

Установи вищої освіти поділяються на дві великі групи: *університети,* а також *дворічні технічні* (Technical Colleges) *молодші* (Junior Colleges) і *місцеві* або *громадські* (Community Colleges) коледжі, а також коледжі чотирирічного навчання, які за статусом прирівнюються до закладів вищої освіти. Останні можуть бути як самостійними закладами освіти, так і входити до складу університетів. У категорію університетів входять *інтеграційні університети,* де здійснюються наукові дослідження і викладання; *коледжі вільних мистецтв,* де обмежуються академічною освітою; *професійні вищі школи,* насамперед медицини і права. Університети – найбільш престижні вищі навчальні заклади, які надають освіту на двох рівнях – бакалаврату і магістратури. В університетах студенти мають можливість вибрати різні курси, адже стандартної програми немає. Їм запропоновано 25-35 фахових дисциплін зі спеціальності, 6-8 дисциплін з математики та 2 проекти. Інтерактивний кваліфікаційний проект (IQP, Interactive Qualifying Project) і Головний кваліфікаційний проект (MQP, Major Qualifying Project) – це два обов'язкових великих проекти, які виконуються найчастіше за межами навчального закладу, іноді навіть у різних країнах.

Коледжі надають ступінь бакалавра. Загальна кількість коледжів та університетів перевищує 4000, кількість коледжів – 1900. Чотирирічна вища освіта в США передбачає отримання академічного ступеня бакалавра відповідно до професійної та професійно-технічної кваліфікації.

У США юридично коледжі поділяються на державні та приватні залежно від джерела фінансування. Приватні заклади мають автономну систему управління, тому вартість навчання в них вища, а кількість студентів менша. Значних відмінностей в якості навчання між приватними і державними навчальними закладами не існує. Але це не означає, що всі вони однаково престижні і не відрізняються рівнем матеріального забезпечення. Навчатися у приватному навчальному закладі дорожче, але по закінченню випускник має переваги при працевлаштуванні і для розвитку подальшої кар'єри, тому вибір зробити достатньо складно.

У ході дослідження нами з’ясовано, що багато університетів і коледжів, як приватних, так державних, мають високий ступінь престижності. У них реалізуються цікаві навчальні програми, тому вступники мають можливість здобути престижну освіту. Зауважимо, що США здобули лідерство у підготовці бакалаврів з кібербезпеки завдяки варіативності освітніх програм та розгалуженій мережі вищих навчальних закладів.

У США існує чіткий розподіл щодо престижності навчальних закладів. Вибрати престижний вищий заклад освіти у США дійсно можливо завдяки рейтингу серед вишів та консультантів освітніх агентств. Стати студентом одного з престижних американських університетів – це велике досягнення абітурієнта, адже лише один з десяти абітурієнтів стає студентом. Майже два відсотки осіб вступають до коледжів провідних університетів.

Коледжі бувають різних типів: дворічні технічні, молодші і громадські коледжі, а також коледжі чотирирічного навчання, які за статусом прирівнюються до вищих навчальних закладів. Останні можуть бути як самостійними закладами, так і входити до складу університетів. Дворічний коледж приймає випускників середньої школи та здійснює навчання за кваліфікацією «молодший спеціаліст». Випускники дворічного коледжу переводяться на чотирирічне навчання в інші коледжі або університети з метою здобуття ступеня «бакалавр».

Відповідно до роз’яснювально-інформаційного листа-рекомендації щодо вимог на здобуття ОКР (Bellevue University Nebraska BS-Cybersecurity Degree Information) «бакалавр з кібербезпеки» – це освітньо-кваліфікаційний рівень, який одержує студент, який на базі повної загальної середньої освіти пройшов поглиблену загальнокультурну підготовку, оволодів фундаментальними та професійно орієнтованими знаннями, уміннями та навичками щодо об’єкта праці і який здатний вирішувати типові професійні завдання. Характерні функції його діяльності – обґрунтування потреби та раціональний розподіл обмежених ресурсів управління процесами, забезпечення ефективності

технологічних систем (Bellevue University Nebraska BS-Cybersecurity Degree Information, 2017).

У національних ініціативах США щодо стратегічного плану освіти з кібербезпеки Національного інституту стандартів та технологій (National Institute of Standards and Technology) зазначається, що найбільш конкурентоспроможними дисциплінами освітньо-професійних програм освітньо-кваліфікаційного рівня «бакалавр» галузі знань «Інформаційні технології» є «Розслідування комп'ютерних інцидентів», «Інформаційна безпека», «Кібербезпека», «Комп'ютерна безпека», «Безпека комп’ютерних мереж».

Ступінь бакалавра (The Bachelor’s Degree) надається випускникам, які успішно оволоділи програмою чотирирічного навчання в університеті чи коледжі і пройшли класичну (непрофесійну) загальноосвітню підготовку. Перші два роки навчання у межах реалізації програм підготовки бакалаврів спрямовано на вивчення прикладних дисциплін, останні два роки студент присвячує поглибленому опануванню певного спектру предметів зі спеціалізації (National Institute of Standards and Technology, 2012).

Ступінь доктора філософії (Doctor of Philosophy – PhD) у різних галузях підготовки є найвищим, який надається університетами США. Кандидат на звання PhD повинен володіти більш поглибленими знаннями і навичками у певній спеціалізації у конкретних галузях знань, адже ступінь PhD є вузькоспеціалізованим та вузькопрофільним. Цей ступінь здобувають ті науковці, які виконали самостійне наукове дисертаційне дослідження та захистили його (Романовський, 2002, с. 97).

Проаналізуємо більш детально особливості підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США. У ході дослідження нами було простудійовано освітньо-професійні програми підготовки здобувачів освітньо-кваліфікаційного рівня «Бакалавр» зі спеціальності «Кібербезпека» 45 американських вищих навчальних закладів у 25 штатах США. За кількісними

показниками серед цих вищих закладів 92 % – це університети, 2 % – інститути та 6 % – коледжі (додаток В табл. В 2).

Зазначимо, що в США відсутні уніфіковані освітньо-професійні програми. Кожен навчальний заклад має свою ОПП підготовки бакалаврів, зокрема зі спеціальності «Кібербезпека», яка відрізняється від програм інших закладів навіть у межах одного штату. Варіативність характерна і для номінування спеціальності. У кожному навчальному закладі назва цієї спеціальності може відрізнятися: вибір найменування спеціальності залежить від особливостей та специфіки галузевих потреб конкретного штату. У проаналізованих освітньо-професійних програмах наявні такі варіанти назви спеціальності: конфіденційність та кібершпигунство; інформаційні технології – кібербезпека; обчислювальна техніка з поглибленим вивченням кібербезпеки; кібершпигунство та кібербезпека; інформатика-кібербезпека; кібербезпека.

На нашу думку, варіативність назв спеціальності зумовлена галузевими вимогами на основі врахування міжпредметних зв’язків, тобто взаємодії знань, наслідком чого є нові знання. Така варіативність назв та й власне змісту (дисциплінарного наповнення) спеціальностей насамперед надає можливість фахівцям суміжних спеціальностей розширити поле своєї професійної діяльності та задовольнити галузеві потреби щодо фахівців необхідних спеціалізацій.

У ході дослідження виокремлено найбільш характерні особливості системи освіти США – насамперед це її ступенева структура та диверсифіковані типи навчальних закладів. У цій системі функціонують державні й приватні чотирирічні коледжі, освітні заклади релігійних громад, державні університети, до складу яких можуть входити комунальні коледжі, університети штатів, приватні університети. Способи відбору абітурієнтів у ВНЗ ґрунтуються на засадах демократії та об’єктивності, передбачають проведення диверсифікованих типів завдань, які варіюються від традиційних іспитів на конкурсній основі до популярних сьогодні тестувань і співбесід. У багатьох

навчальних закладах приймаються абітурієнти без вступних випробувань, а лише на підставі свідоцтва про середню освіту.

Отже, вступити до місцевого (громадського) коледжу не складає труднощів для середнього абітурієнта. Він територіально розташований у місті або окрузі та обслуговує місцеву громаду. Головним призначенням таких установ є надання можливості здобути вищу освіту в США практично будь-якому бажаючому, тому вартість навчання в місцевому коледжі порівняно низька (10000 тис. доларів на рік), а широкий вибір предметів дозволяє кожному обрати індивідуальну програму навчання відповідно до індивідуальних потреб та нахилів. Основою програм навчання є дисципліни загальноосвітнього циклу, а також технічного і професійного спрямування. Серед особливо привабливих пропозицій для міжнародних здобувачів освітньо-кваліфікаційного рівня «бакалавр з кібербезпеки» є пільгове навчання, запровадження інтенсивних курсів англійської мови. Такі коледжі надають можливість практично кожному бажаючому здобути освіту.

У таблиці 2.2.2. систематизовано типи навчальних закладів США, у яких можливе отримання освітньо-кваліфікаційного рівня бакалавра зі спеціальності «Кібербезпека».

Таблиця 2.2.2.

Типи навчальних закладів США, що здійснюють підготовку бакалаврів зі спеціальності «Кібербезпека»

№ п/п	Тип навчального закладу		Тривалість Навчання	Примітка
1.	Університети		4 роки	
2.	вищі професійні заклади		4 роки	
3.	вища професійна школа		4 роки	
4.	молодший коледж	вища професійна школа	4 роки	2 та 2
5.	технічна школа	вища професійна школа	4 роки	2 та 2
6.	молодший коледж	вищий коледж	4 роки	2 та 2
7.	молодший коледж	Університет	4 роки	2 та 2

Отже, здобути кваліфікацію бакалавра з кібербезпеки в США можливо ріхними шляхами у вищих навчальних закладах. Продемонстровано, що це можливо здійснити різними шляхами: безпосередньо у вищому коледжі чи університеті або за моделлю «2+2» – перші два роки в молодшому коледжі / або технічної школи, а потім два останні роки – у вищому коледжі / або університеті / або вищій професійній школі. Можливе здобуття ступіня бакалавра безпосередньо у вищій професійній школі, за умови початку навчання (2 роки) в технічній школі.

2.3. Освітні траєкторії у неперервній освіті ІТ-фахівців у США

У контексті реалізації національної кібербезпекової політики США підготовка та перепідготовка кадрів в ІТ-галузі є відповіддю на потреби галузі у кваліфікованих кадрах, важливою складовою комплексу заходів держави щодо протидії загрозам в інформаційній сфері.

Проаналізовані джерела з проблеми дослідження дозволяють зробити висновок, що в США протягом останніх 20 років питанню захисту інформації та кібербезпеки приділяється особлива увага на державному рівні. Так, у 1998 році з метою запобігання, стримування, швидкого реагування та розслідування злочинів, спрямованих проти стабільності національної інформаційної інфраструктури, було створено Національний центр захисту інфраструктури (National Infrastructure Protection Center) та згодом – Міжнародна асоціація фахівців з комп'ютерних досліджень (Міжнародна асоціація комп'ютерних фахівців-розслідувачів). Остання готує спеціалістів для комп'ютерно-технічної експертизи. У кінці 2009 року було створено Національний центр кібербезпеки і зв'язку (National Cyber Security) – центр інтеграції, покликаний допомогти державі у розробленні підходів до вирішення проблем забезпечення інформаційної безпеки, підвищити рівень освіти в цій сфері, а також координувати діяльність всіх національних систем мережевого захисту. Співробітники цього центру займаються моніторингом і попередженням різного типу комп'ютерних атак.

Результатом проведення кібербезпекової політики США та її впливу на процес забезпечення галузі кадрами для кіберзахисту стало запровадження ряду заходів з вирішення проблеми кадрового дефіциту, що схематично представлено на рис. 2.3.1.

Рис. 2.3.1. Провідні тенденції у кадровому забезпеченні ІТ-галузі (спеціальність «Кібербезпека») (Rossett&Vaughan, 2012; Bruce Schneier, 2013; Сьомін, 2016).

У результаті інтенсивного розширення кіберпростору американського суспільства та зростання ролі й стратегічного значення кібербезпеки кадрове забезпечення ІТ-галузі» передбачає реалізацію таких напрямів: визнання підготовки фахівців з кібербезпеки важливим етапом втілення національної стратегії у контексті кібербезпекової політики; стандартизація підготовки фахівців у ІТ- галузі; розроблення програм для навчання фахівців, максимально наближених до практичних потреб галузі та міжнародних сертифікаційних вимог; запровадження новітніх педагогічних технологій у процесі підготовки фахівців, таких, як: дуальне, змішане (Blended learning), практико-орієнтоване навчання (Rossett&Vaughan, 2012); популяризація спеціальностей та вмотивованість талановитої молоді з метою більшої зацікавленості у здобутті

фаху та підвищення престижу і популярності професій, пов'язаних з кібербезпекою; стійке збільшення обсягів інвестицій для ІТ-галузі для подальшого її розвитку з тенденцією зростання кількості робочих місць для фахівців з кібербезпеки; зростання потреби у висококваліфікованих керівних кадрах; підвищення ролі вищої освіти для підготовки висококваліфікованої еліти з кібербезпеки (Сьомін, 2016).

Для реалізації визначених напрямів з метою підвищення національної кібербезпеки та підготовки висококваліфікованих фахівців ІТ-галузі у 2000 році розпорядженням президента США було розширено повноваження АНБ з питань, які стосуються боротьби з кіберзагрозами. Також була створена спеціальна комісія, яку очолив директор АНБ, що отримала завдання виявити і знищити джерела кібератак на урядові мережі. За ініціативою АНБ було сформовано ряд центрів професійної освіти, до яких пізніше підключили 14 провідних університетів США. Одночасно Білий Дім став залучати до навчання 10 тис. урядовців щорічно в рамках федеральної програми забезпечення безпеки інформаційних технологій.

Після терористичного акту 11 вересня 2001 року в містах США було впроваджено масове проведення семінарів, конференцій, зустрічей з проблем кіберзлочинності та кібертероризму. Усі без винятку користувачі інформаційних систем зобов'язані володіти необхідним мінімумом базових знань у ІТ-галузі з кібербезпеки, без яких вони не можуть бути допущені до роботи.

Зауважимо, що національна політика країни в галузі кібербезпеки регулюється Агентством національної безпеки, а першочергові питання розв'язуються, як правило, на рівні Ради національної та внутрішньої безпеки країни (Bruce Schneier, 2013.).

За рекомендаціями АНБ всі урядові мережі повинні відповідати певним обов'язковим вимогам та нормативам:

- урядові мережі мають забезпечувати можливості виявлення кіберзагрози;
- наявність можливості управління системою безпеки;

- особливий підхід до спеціалізованого навчання персоналу;
- наявність електронної охорони периметру найважливіших об'єктів;
- наявність фізичного захисту ключових електронних вузлів системи;
- можливість екстреного оповіщення про аварійні ситуації;
- наявність генерального плану відновлення працездатності мережі.

Міністерству оборони США відведена важлива роль у розв’язанні поставлених завдань на національному рівні. Для вдосконалення методів навчання в Міністерстві оборони США був створений спеціальний Підрозділ з управління програмами в галузі з кібербезпеки (Information Assurance Program Office) IAPO, який виконує функцію удосконалення методів навчання фахівців IT-галузі. Через стрімкий розвиток та постійне удосконалення інформаційного простору передбачено щорічну перепідготовку для персоналу за допомогою програм Education, Training and Awareness (Освіта, навчання та знання).

Крім того, управлінням було розроблено та втілено навчальні програми для військовослужбовців, цивільного персоналу і службовців за контрактом під загальною назвою «Education, Training and Awareness», що є одним із важливих досягнень підрозділу Міноборони. Відповідно до навчальної програми «Education, Training and Awareness» передбачено всебічне навчання, тренування й інформування зазначених категорій слухачів. Також проводилось тестування персоналу інших відомств.

З метою забезпечення галузі у висококваліфікованих фахівцях були задіяні базові заклади вищої освіти Міноборони США, які також готують військових фахівців з кібербезпеки, зокрема для відповідних федеральних відомств. Провідними серед них є:

-Університет інформаційних технологій (Форт Гордоя);

-Технологічний університет (Райт-Патерсон) військово-повітряних сил;

-Військова академія Армії США (Вест-Пойнт);

-Центр і школа спеціальних методів війни імені Дж. Кеннеді (Форт-Брег);

-коледж інформаційного менеджменту Університету національної оборони (Форт Макнейр);

- школа з питань щодо інформаційної війни і прийняття стратегічних рішень та інші.

Важливою тенденцією вважаємо інтеграцію наукового, академічного, бізнесового та військового секторів для задоволення потреб ІТ-галузі. Так, науково-дослідні центри забезпечують високий науковий і практичний рівень сучасної навчально-методичної бази для якісної підготовки фахівців у цих навчальних закладах. Академічний навчальний факультет електронної інженерії і комп'ютерних наук військової академії Вест-Пойнт інтегрований з науково-дослідним центром інформаційних технологій і операцій, у складі якого є «Лабораторія досліджень і аналізу інформаційної війни». Як результат кадети Вест-Пойнту часто стають переможцями навчань-змагань «Змагання з кіберзахисту» (Cyber Defense Exercise) серед шести провідних академій США, організованих Агентством національної безпеки.

Різнорівневі спеціальні навчальні курси з кібербезпеки створені і в інших навчальних закладах, які надають військову освіту та практичну підготовку фахівцям. Серед них є центри інформаційної боротьби всіх видів збройних сил, навчальні курси Net Warfare Training – кібернетичного Командування баз ВПС на авіабазі Барксдейлі. Підготовку фахівців у сфері КБ здійснюють і державні структури: аспірантура Військово-морської академії США пропонує дванадцять різних курсів; Агентство із захисту інформаційних систем – DISA (Defense Information Systems A) – вісім курсів. Бере активну участь в цій роботі і коледж управління інформаційними ресурсами (Information Resource Management College) та ін. Всі види навчання чи перепідготовки у військових навчальних підрозділах, ІТ-центрах є складовою основної освітньо-професійної програми чи післядипломної підготовки.

Іншою важливою тенденцією вважаємо запровадження комерційної курсової підготовки. У США є розвинена потужна система комерційної курсової підготовки та навчальних центрів фірм-виробників ІТ-продукції, що стало важливою складовою загальної системи підготовки фахівців з кібербезпеки. Зазначимо, що серед комерційних компаній, що виробляють ІТ-

продукт, підготовку фахівців для ІТ-галузі зі спеціальності «Кібербезпека» здійснюють відомі у США компанії: «APC», «Allied Telesyn», «Check Point Software Technologies», «Cisco Systems», «Dell Computer», «Internet Security Systems», «Microsoft, Sun Microsystems», «Oracle Corp», «Symantec», «IBM», «Tivoli Systems», «Global Security Laboratory», Консорціум міжнародної сертифікації інформаційних систем безпеки «Internet Security Systems», «Network Associates», «Symantec» тощо. Така підготовка має ряд переваг. По-перше, вона найбільш практично орієнтована і наближена до реалій робочого місця. Це досягається завдяки постійному оновленню змісту навчання, як це, наприклад, відбувається у мережевій академії «Cisco», в якій зміст навчання оновлюється кожні 90 днів. Це пояснюється швидкістю змін, які відбуваються у сфері ІКТ і які зумовлюють необхідністю адаптації до нових умов. Таким чином, курсова підготовка ІТ-фахівців сприяє утвердженню таких вимог до якості освіти – практична спрямованість, гнучкість і безперервність.

На наше переконання, особливої уваги потребує тенденція здобуття фаху альтернативним шляхом. На сучасному етапі підготовка кадрів з кібербезпеки є не тільки реакцією на попит ринку в таких фахівцях, а й виступає важливою складовою комплексу заходів держави щодо протидії загрозам у кіберпросторі. Відповідно відбувається структурування змісту підготовки цих фахівців і формуються чіткі вимоги до освітніх закладів при організації такої підготовки. У загальній системі забезпечення кібербезпеки держави кадровий супровід є самостійною підсистемою, а сама система підготовки фахівців – основа такого супроводу. Тому під підготовкою кадрів для галузі варто розуміти систему, що включає всі рівні професійної освіти, перепідготовки та підвищення кваліфікації фахівців. «В США освіта та підготовка здійснюється за великою кількістю програм та пропонує диверсифіковані шляхи набуття необхідних навичок. Освітні програми передбачають навчання як з набуттям сертифікатів, так і програми, що передбачають одержання освітньо-кваліфікаційного рівня на базі вищих спеціальних або професійних закладів підготовки, а також

програми, що пропонуються працедавцями, інтернатура, учнівство тощо» (Чванова, 2012, с. 122).

На думку Н. Пазюри «традиційна сертифікація» – це засвідчення набутих знань за програмами навчання на базі 4-річних коледжів, що передбачають підготовку студентів та набуття ними базових компетенцій, які оцінюються через виконання письмових екзаменів відповідно до вимог штату. Термін «альтернативний шлях здобуття сертифікату професійної діяльність» використовується в США для визначення всіх видів програм, які передбачають професійну підготовку. Альтернативна сертифікація допускає будь-яке «відхилення» від традиційної освітньої траєкторії та відкриває додаткову можливість одержати освіту за фахом у зручний для здобувача період його життя (Пазюра, 2015).

З метою забезпечення альтернативних шляхів здобуття професійної освіти у ІТ-галузі заохочуються міжнародні консорціуми з сертифікації фахівців у сфері безпеки інформаційних систем. Міжнародні консорціуми забезпечують альтернативу в здобутті сертифікату на професійну діяльність. Світовим лідером сертифікації фахівців з кібербезпеки є Міжнародний консорціум з сертифікації у сфері безпеки інформаційних систем (Консорціум міжнародної сертифікації безпеки інформаційних систем, Inc., або (ISC). Для отримання сертифікату Сертифікований професіонал з безпеки інформаційних систем (CISSP, Certified Information Systems Security Professional) необхідно мати досвід роботи за фахом не менше 4 років (або 3 роки і ступінь бакалавра), скласти непростий іспит, дотримуватися кодексу етики (ISC2) і постійно розвивати свої компетентності. Для підтвердження сертифікації CISSP достатньо кожні 3 роки проходити навчання на авторизованих курсах з інформаційної безпеки, а також брати участь у конференціях за професійним спрямуванням (Чванова, 2012).

Перепідготовка та підвищення кваліфікації мають ключове значення у забезпеченні ІТ-галузі висококваліфікованими фахівцями. Програми перепідготовки і підвищення кваліфікації передбачені для осіб середнього і

старшого віку, які вже отримали базову освіту. Необхідність проведення перепідготовки та підвищення кваліфікації ІТ-персоналу зумовлено стрімким розвитком інформаційно-комунікаційних технологій. За оцінками американських науковців, 5% теоретичних та 20% професійних знань, якими повинні володіти фахівці технічних галузей, зокрема ІТ-галузі, щорічно оновлюється (Altbach, Patricia, Gumport, & Berdahl, 2011). «В США встановлена своєрідна одиниця виміру старіння знань фахівця – так званий період напіврозпаду компетентності. Цей термін, запозичений з ядерної фізики, означає проміжок часу, коли в результаті появи нової наукової та технічної інформації компетентність фахівця знижується до 50%. За останні десятиріччя цей період – період напіврозпаду компетентності – стрімко зменшується. Наприклад, якщо для випускника – інженера в 1940 році «старіння знань» наступало через 12 років, то вже в 1960 році – через 8-10 років, а для теперішніх випускників – 2-3 роки» (Филиппова, 1981, с. 226).

Зазначимо, що перепідготовка працівника передбачає менші фінансові витрати, ніж його заміна. Так, витрати на перепідготовку фахівців ІТ-галузі в США втроє менші, ніж витрати на пошук та прийом нових кадрів. Крім того, ймовірність, що фахівців залишить робоче місце після перепідготовки значно менша. Відповідно до статистичних даних, на підготовку кадрів у приватних компаніях США щорічно витрачається більше 1000 млрд. доларів. Програми щодо підготовки та перепідготовки фахівців мають 76% американських корпорацій з числом зайнятих у цій сфері фахівців більше 500 осіб (Ніколаєнко, 2006). В основі успіху США з вирішення проблеми щодо усунення дефіциту кадрів на ІТ-ринку, зокрема фахівців з кібербезпеки, – багаторівнева система неперервної професійної освіти. Основний принцип її функціонування в умовах глобалізації побудований на послідовності та спадкоємності засвоєння знань, їх постійного вдосконалення та/або оновлення.

У контексті визначення концептуальних засад підготовки фахівців з кібербезпеки тезисно проаналізуємо положення концепції неперервної освіти. Більшість вітчизняних дослідників переконливо доводять, що інтенсивне

насичення висококваліфікованими кадрами всіх сфер життєдіяльності інформаційного суспільства можливе саме на засадах концепції неперервної освіти.

Аналіз аналітичних матеріалів з проблеми дослідження дозволив виокремити декілька типів освітніх траєкторій у системі неперервної освіти ІТ-фахівців в США, а саме: надання другої вищої освіти; нелінійна підготовка фахівців за різними ступенями освіти; запровадження спеціалізацій із кібербезпеки на інших спеціальностях вищих навчальних закладів (юридичних, економічних, управлінських тощо); перепідготовка у процесі післядипломної освіти фахівців із близькоспоріднених із кібернетичною безпекою спеціальностей; використання потенційних можливостей неформальної освіти для підвищення кваліфікації фахівців через проведення тренінгів, круглих столів, міжнародних стажувань тощо (Ліпкан &Череповський, 2014).

Водночас неперервна освіта передбачає інтеграцію всіх видів освіти (шкільну, професійну, післядипломну); інтеграцію типів освітніх закладів (молодший коледж, технічна школа, 4-річна вища школа, старша вища школа, молодша вища школа, комбінована вища школа, університет, професійна школа) та кваліфікаційних освітніх рівнів або ступенів (бакалавр, магістр, доктор філософії) в цілісну систему, що забезпечує можливості отримання загальноосвітніх та спеціальних (фахових) знань і також оновлення й збагачення знань протягом усього життя людини.

Відповідно до концепції неперервної освіти всі етапи навчання підпорядковані діям щодо досягнення чітко визначеної мети, однак у ході навчання передбачено можливе корегування визначених цілей залежно від інтересів, життєвих планів і рішень, пов'язаних із цим завдань професійного визначення, здобуття певної кваліфікації, підвищення кваліфікації або перекваліфікації. Неперервна освіта гарантує людині постійне підвищення освітнього рівня та перекваліфікацію у випадку неактуальності професії через плинність зовнішніх чинників (соціальна структура суспільства, сукупність соціальних чинників, економічних і політичних умов). Неперервна освіта – це

гарантія професійного становлення й розвитку особистості на всіх етапах життя, яка має на меті компенсацію функцій і можливостей людини, що втрачаються з віком, та задовольняє потреби суспільства у постійному розвитку його громадян, зростанні загального та професійного освітнього потенціалу.

У США функціонує велика кількість державних і громадських, формальних і неформальних освітніх структур, об'єднаних взаємною субординацією за рівнями, координацією за спрямованістю й призначенням. Водночас вони належать до єдиної системи, що забезпечують неперервність освіти та можливості за потреби змінювати освітній заклад.

Неперервна освіта – це процес формування й задоволення пізнавальних, духовних потреб кожної людини, розвитку її задатків та здібностей у мережі державно-суспільних навчальних закладів і самоосвіти. У США розвиток неперервної освіти є провідною тенденцією у державній політиці та механізмом розширеного відтворення професійного й культурного потенціалу; умовою прискорення соціально-економічного прогресу країни; способом збереження, розвитку і взаємозбагачення національних культур і загальнолюдських цінностей, важливим чинником і умовою міжнародної співпраці в освітній галузі та вирішення глобальних завдань сьогодення з метою зміцнення національної безпеки США.

Вважаємо за доцільне зупинитися детальніше на характеристиці особливостей розвитку неперервної освіти для ІТ-фахівців.

Надання послуг щодо здобуття другої вищої освіти передбачає здобуття випускником нетехнічного вищого навчального закладу другої вищої освіти, наприклад, за технічним фахом. Отримана кваліфікація відповідно до другої вищої освіти дає можливість реалізувати здобуті знання шляхом поєднання кількох професій. Такий процес здобуття другої вищої освіти характеризується як дієвий, тривалий, високовартісний, з високими вимогами до здобувача.

Надання послуг нелінійної професійної підготовки фахівців за різними ступенями освіти. За таким типом підготовки бакалавр технічного профілю має можливість вступає до магістратури за економічним фахом із метою

подальшої роботи як фахівця з кібербезпеки в банківській сфері. Освітній процес характеризується як дієвий, недовгостроковий, але високої вартості та з високими вимогами до здобувача такої освіти.

Запровадження спеціалізацій із кібербезпеки у межах інших спеціальностей (юридичних, економічних, управлінських тощо). За таким варіантом реалізації неперервної освіти викладач «Інформатики» як фахівець із кібербезпеки шляхом здобуття паралельно спеціалізації із кібербезпеки в іншій сфері (юридичній, економічній тощо) здатний виконувати превентивні (попереджувальні) функції щодо здійснення кваліфікованої роз'яснювальної та виховної роботи. Отже, кібербезпека може виступати не тільки як спеціальність, а й як спеціалізація в межах інших спеціальностей або як окремий компонент освітньої програми підготовки фахівця. Основними характеристиками такого навчання є дієвість, тривалість, поєднанні кількох наукових напрямів, висока результативність, підвищені вимоги до здобувача.

Напрям перепідготовки в контексті післядипломної освіти фахівців із близькоспоріднених із кібербезпекою спеціальностей. Реалізація такої освітньої траєкторії передбачає здобуття післядипломної освіти фахівцями зі спеціальностей, які близькоспоріднені до спеціальності кібербезпека, перепідготовку цих фахівців з метою здобуття кваліфікації за спеціальністю «Кібербезпека». Характерно, що такий освітній процес є дієвим, актуальним, результативним з відносно невеликою затратою часу та коштів, з високими вимогами до здобувача.

Використання потенційних можливостей неформальної освіти для підвищення кваліфікації фахівців-практиків. При такій траєкторії відбувається підвищення кваліфікації фахівців-практиків шляхом поширення досвіду з використанням новітніх педагогічних технологій, проведення тренінгів, круглих столів, міжнародних стажувань тощо. Основні характеристики можливостей неформальної освіти у процесі підвищення кваліфікації практикуючих фахівців – це дієвість, швидкість, актуальність,

результативність, з високими вимогами до здобувача (Ліпкан &Череповський, 2014).

Загалом можна стверджувати, що збільшення кількісних показників у підготовці бакалаврів з кібербезпеки зумовлює певні якісні перетворення, зокрема на рівні прийняття рішень органів державного та міжнародного управління з питань розвитку інформаційних систем та гарантій кібербезпеки (Остроухов, 2015).

Диверсифікація є однією з визначальних тенденцій розвитку вищої освіти США та підготовки бакалаврів освіти в цій системі.

В педагогічній літературі термін «диверсифікація» означає різноманітність, різнобічний розвиток, розширення видів наданих послуг, набуття умінь щодо нових видів діяльності, не властивих раніше (Ничкало, 2001).

Диверсифікація як соціальне явище поєднує в собі:

- процес структурної перебудови, розвитку і трансформації типів закладів вищої освіти;
- принцип структурування освіти і сучасної освітньої політики;
- тенденцію розвитку всіх видів освіти: інституційних структур, рівнів навчання, упровадження багатьох видів освітніх програм, систем, форм навчання, курсів підготовки, номенклатури, характеру і змісту освітніх послуг та їх реалізації;
- напрям реформування і подолання кризи освіти, вдосконалення вищої освіти, вирішення сформованих суперечностей між проголошеної свободою особистості у виборі освітньої траєкторії і реальними умовами для вияву особистісної волі;
- шлях до подолання нерозвиненості, слабкої диференціації і надлишкової централізації.

На рис 2.3.1. представлено основні складові процесу диверсифікації вищої освіти в США, а саме: міжпредметність, варіативність, ступеневість**.**

Завдяки диверсифікації в американській вищій школі з'явилася можливість орієнтувати її на «підтримку істотних відмінностей у програмах і функціях вищих навчальних закладів відповідно до різноманітних соціально-культурних та соціально-економічних запитів суспільства» (Ладиженець, 2001).

Важливою складовою диверсифікації у професійній підготовці бакалаврів з кібербезпеки є міжпредметність. Загалом міжпредметність представлена як міжпредметними зв'язками, так і міжпредметною інтеграцією, тобто взаємодією знань, результатом якої є отримання нових знань.

Рис 2.3.1. Складові диверсифікації вищоїосвіти США (Ничкало, 2002; Ладиженець, 2001).

У табл. 2.3.2. подано узагальнену характеристику етапів формування міжпредметних зв'язків.

Таблиця 2.3.3.

Характеристика етапів формування міжпредметних знань, умінь і навичок здобувачів вищої освіти у вивченні всіх циклів дисциплін (укладено автором на основі дерела: Кошманова, 2002).

ЕТАПИ	**ХАРАКТЕРИСТИКА ЕТАПІВ**
Підготовка	***Формування первинних уявлень***
Інтеграція первинних уявлень Імплементація провідних ідей теми	Актуалізація, відтворення, використання тих понять і висновків, які були засвоєні на підготовчому етапі під час вивчення попередніх дисциплін Послідовний розгляд основних питань теми з різних дисциплін, під час вивчення яких формуються відповідні міжпредметні знання, уміння та навички
Осмислення міжпредметних знань, умінь, навичок Екстраполяція міжпредметних знань, умінь, навичок	Аналіз, конкретизація, узагальнення здобутих міжпредметних знань, умінь і навичок з різних дисциплін Використання здобутих міжпредметних знань, умінь і навичок з різних дисциплін у процесі вивчення наступної навчальної дисципліни, складання міжпредметних державних іспитів.

На нашу думку система інтегрованих занять звільняє здобувачів від формального засвоєння та застосування знань, вимагає обов'язкового врахування міжпредметних зв'язків, дозволяє розкрити ряд понять у більш доступній формі, що відповідає цілям і завданням сучасного освітнього процесу.

Таким чином, міжпредметність – це сучасний принцип навчання, який впливає на відбір і структуру навчального матеріалу цілого ряду дисциплін, посилюючи системність знань здобувачів, активізує методи навчання, орієнтує на застосування комплексних форм організації навчання, забезпечує єдність освітнього процесу. У результаті йдеться про «міжпредметний іспит» – комплексний іспит за навчальними матеріалами цілого ряду дисциплін.

Варіативність вищої освіти закріплена у вибірковій частині освітньо-кваліфікаційних характеристик бакалаврів з кібербезпеки та у варіативній частині освітньо-професійних програм підготовки бакалаврів з цього напряму.

Сутність ступеневості вищої освіти полягає у здобутті різних освітньо-кваліфікаційних рівнів на відповідних ступенях вищої освіти. Професійна підготовка передбачає здобуття освітньо-кваліфікаційного рівня «бакалавр» / «магістр». Зауважимо, що бакалаврська освіта в США є необхідною як для отримання престижної роботи, так і для продовження навчання у магістратурі чи докторантурі.

Аналізуючи особливості вищої освіти в США, необхідно означити таку визначальну тенденцію, як децентралізація управління освітою на рівні штатів, відповідно до якої усі вищі навчальні заклади згідно з чинним законодавством США є незалежними корпораціями, діяльність яких не фінансується і не регламентується Департаментом освіти. Моніторинг їх діяльності здійснюється незалежними від Державного департаменту агентствами з акредитації. Практично всі питання освітньої політики вирішуються саме на рівні штатів, хоча існують і окремі федеральні програми, що фінансуються і контролюються Міністерством освіти США.

Як зазначає американський соціолог М. Троу (Trow, 1998), ще на початку XX століття навчальні заклади США мали можливість вибору освітніх програм, використовували модульний принцип організації освітнього процесу, систему накопичення та визнання залікових одиниць, і від початку функціонували в умовах ринку та автономії університетів, яка відрізнялася кваліфікованим керівництвом й різноманітністю джерел фінансування. США мала організаційну та структурну основи для системи вищої освіти ще задовго до збільшення попиту на неї. Все, що було потрібно, – це зростання попиту.

Вивчення специфіки вищої освіти США дозволила виокремити таку її особливість, як наступність. Було з'ясовано, що підготовку бакалаврів із спеціальності «Кібербезпека», які прагнуть отримати якісну ІТ-освіту, можливо здійснювати як по вертикалі, так і по горизонталі. Основний принцип такої моделі полягає у тому, що ступінь бакалавра можна здобути безпосередньо у вищій професійній школі, при цьому двома шляхами: по вертикалі – початок навчання (перші 2 роки) і останні 2 роки відбуваються в одному і тому ж навчальному закладі; по горизонталі – перші 2 роки навчання триває в одному навчальному закладі (наприклад, в молодшому коледжі), а останні 2 роки – в іншому (у вищій професійній школі) (Додаток В, Таблиця В.1)

На особливості наступності американської освіти акцентує увагу О. Романовський (1997), який зазначає, що «залік, одержаний з предмету в одному університеті, визнається і в інших. Тобто студент може отримати заліки в одному ВНЗ з можливим перезарахуванням їх у іншому та отримати освітньо-кваліфікаційний рівень» (Романовський,1997, с.27.).

Освітні заклади США, які здійснюють підготовку докторів наук, в рамках нормативно-правового поля можуть надавати освітні послуги з підготовки магістрів, бакалаврів та молодших спеціалістів (Associate of Science). Відповідно навчальні заклади вищої освіти, які готують магістрів, можуть також здійснювати підготовку бакалаврів та молодших спеціалістів. Заклади, які навчають бакалаврів, мають право на підготовку молодших спеціалістів. Таким чином, гнучка ступенева неперервна система підготовки фахівців

дозволяє на будь-якому рівні призупиняти навчання, змінювати профіль тощо. На нашу думку, це важлива організаційно-педагогічна умова якісної освіти у США.

Отже, система вищої освіти в США є ступеневою, гнучкою і відкритою для взаємодії з різними освітніми і соціальними системами. Вимоги до абітурієнтів та здобувачів освітньо-кваліфікаційного рівня бакалавра визначаються диференційовано з урахуванням базового освітнього рівня, регіональних потреб штату. В межах системи відбувається забезпечення громадян знаннями, уміннями і навичками з обраної галузі професійної діяльності. Диверсифікація освітніх моделей передбачає функціонування навчальних програм з урахуванням вимог або певного штату, або конкретного замовника кадрів.

У проаналізованих освітньо-професійних програмах вищих навчальних закладів з підготовки бакалаврів з кібербезпеки враховуються основні пріоритети державної політики щодо кібербезпекової спрямованості інформаційної діяльності країни. Вони забезпечують наукове наповнення, реалізацію компетентнісного підходу, наступність, комплексність, інтегрованість, модульність, варіативність, гнучкість підготовки та відповідно підкріплюються академічною автономією вищих навчальних закладів.

Отже, задоволення попиту суспільства щодо фахівців необхідної кваліфікації вирішується шляхом інтеграції наукового, академічного, бізнесового та військового секторів. З’ясовано, що підготовка кадрів для ІТ-галузі – це система, що складається з професійної освіти, перепідготовки та підвищення кваліфікації. Зважаючи на стрімкі зміни у галузі інформаційних технологій, гарантією ефективності підготовки фахівців із кібербезпеки та постійного оновлення їхніх знань виступає система неперервної освіти, що передбачає можливості диверсифікованих освітніх траєкторій для різних категорій населення.

Висновки до розділу 2

Формування системи професійної підготовки фахівців з кібербезпеки відбувалось відповідно до національної стратегії та під впливом економічних, політичних чинників відповідно до соціального запиту та кібербезпекової політики США з метою захисту цивільних прав та інтересів бізнесового, наукового, технічного, військового, фінансового потенціалу та досягнень високих технологій країни, вироблення відповідального ставлення до національної безпеки у населення США.

Визначено основні принципи організації вищої освіти США: 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 дисциплін; демократичність, рівноправність шансів кожного особистості у здобутті вищої освіти.

На основі аналізу нормативно-правових ресурсів було з’ясовано, що система вищої освіти в США є ступеневою, гнучкою і відкритою для взаємодії з різними освітніми і соціальними системами. Розмаїття вищих навчальних закладів та освітніх програм уможливлює здобуття різних освітніх ступенів, одержання ступеня бакалавра з кібербезпеки в різних закладах та за різними моделями навчання, які враховують вимоги або певного штату, або конкретного замовника підготовки фахівців. Вимоги до абітурієнтів та здобувачів освітньо-кваліфікаційного рівня «бакалавр» визначається диференційовано з урахуванням базового освітнього рівня, регіональних потреб штату. В межах системи відбувається забезпечення громадян знаннями, уміннями і навичками з обраної галузі професійної діяльності. З’ясовано, що кожен здобувач проходить суворий відбір на професійну надійність, і до навчання не допускають студентів, які потенційно схильні до використання отриманих навичок в злочинних цілях.

Попит на спеціалістів та дефіцит фахівців ІТ-галузі вимагав реалізації спеціальних заходів щодо диверсифікації здобуття освіти шляхом інтеграції

наукового, академічного, бізнесового та військового секторів для задоволення потреб ІТ-галузі. Гарантією ефективності підготовки фахівців із кібербезпеки у системі американської вищої освіти є система неперервної освіти, що пропонує гнучкі та варіативні типи освітніх траєкторій, надає можливість спеціалістам інших галузей підвищити їхній освітній рівень шляхом перекваліфікації у випадку неактуальності професії через плинність зовнішніх чинників (соціальна структура суспільства, сукупність соціальних чинників, економічних і політичних умов).

Результати дослідження, відображені у розділі, викладено у публікаціях автора: Бистрова, 2014; Бистрова, 2015; Бистрова, 2017d; Бистрова, 2017c.

РОЗДІЛ ІІІ. ДИДАКТИЧНІ ЗАСАДИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ США

У розділі 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.

3.1. Змістові та структурно-організаційні особливості теоретичної і практичної підготовки бакалаврів з кібербезпеки в навчальних закладах США

У результаті стрімкого розвитку інформаційних технологій, інформаційно-телекомунікаційних систем сформувалися принципово нові поняття («інформаційне суспільство», «інформаційний та кібернетичний простори» тощо), які мають практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

У зв'язку з розвитком ІТ-галузі і її проникненням в ключові напрями професійної діяльності людини та освітньої діяльності навчальних закладів існує необхідність у поглибленому аналізі інтеграційних процесів, що відбуваються у галузі кібербезпеки. Крім того, тенденція інтелектуалізації інструментів професійної діяльності фахівця з кібербезпеки передбачає упровадження в освітнє середовище інноваційних розробок.

Першочерговий інтерес до проблеми підготовки бакалаврів для структур, що забезпечують інформаційну безпеку, кібербезпеку країни, полягає у вивченні особливостей функціонування освітніх установ з підготовки цих фахівців.

Виявлено, що напрями, зміст та навчальне навантаження підготовки майбутніх ІТ-фахівців визначаються відповідно до вимог майбутнього місця роботи. Найбільш важливі аспекти, що беруться до уваги, – це ступінь

уразливості об’єктів в кіберпросторі; ступінь розуміння загроз з відповідною адекватною реакцією органів державного управління та чітко визначеними завданнями кадрового забезпечення наявних структур та структур, створення яких передбачено у майбутньому, які відповідають за кіберзахист кожної людини зокрема і суспільства в цілому та держави як гаранта національної безпеки.

Зауважимо, що зростаюча роль інформаційної безпеки повинна адекватно відображатися в освітньо-професійних програмах підготовки фахівців у цій галузі, забезпечуватися розробленням науково-методичного супроводу підготовки фахівців з урахуванням всіх особливостей підготовки бакалаврів з кібербезпеки. Тому поглиблений системний аналіз стандартів ІТ, еталонних моделей, методів роботи зі стандартами й профілями є обов’язковим етапом аналізу особливостей освітнього процесу і запорукою ефективної діяльності американських вищих навчальних закладів з розроблення та впровадження освітньо-професійних програм підготовки бакалаврів з кібербезпеки.

На думку вітчизняних науковців, професійна підготовка фахівців із будь-якої спеціальності (у нашому випадку – «кібербезпека») – це здобуття кваліфікації з даної спеціальності шляхом формування професійної компетенції відповідно до кваліфікаційної характеристики даної професії (Зубик, 2016, с. 14).

У освітньо-професійних програмах університетів США з підготовки бакалаврів із спеціальності «кібербезпека» (Stevens Institute of Technology, 2017) зазначено, що професійна підготовка – це освітній процес, у результаті якого студент отримує сукупність знань і навичок, необхідних для майбутньої професійної діяльності відповідно до вимог класифікаторів стандартів. Здійснений аналіз навчальних програм дозволив виявити і обов'язкові вимоги до організації підготовки фахівців для ІТ-галузі зі спеціальності «Кібербезпека» в американських закладах. З поміж них визначено такі: об'єктно-орієнтована та практична спрямованість навчання; забезпечення конкурентоспроможності наукових і практичних шкіл різних навчальних закладів; обов’язковий обмін

досвідом роботи між працівниками установ та слухачами вишів; залучення до освітнього процесу фахівців відповідних федеральних структур; запровадження навчання «від зворотнього», тобто фахівців з кібербезпеки навчають теорії і практики інформаційної боротьби.

Розглянемо детальніше специфіку професійної підготовки бакалаврів з кібербезпеки, що передбачає озброєння майбутніх фахівців теоретичними знаннями та практичними уміннями й навичками, що дає студентам можливість набувати відповідні технічні та аналітичні компетенції для кіберзахисту даних, файлів, ресурсів комп'ютера, комп'ютерної мережі, застосування кібербезпекової політики в державних органах, бізнесі, а також у критично важливих національних електронних інфраструктурах (Джонстоун, 2003).

Вивчення автентичних матеріалів з проблеми професійної підготовки бакалаврів з кібербезпеки у системі вищої освіти США дало можливість виявити ключові компетентності, які мають бути сформовані у випускників цих програм.

У навчальних програмах визначено перелік компетентностей, які повинен здобути випускник університету ОКР «бакалавр»: інтегральна компетентність (здатність розв’язувати складні спеціальні завдання та практичні проблеми в ІТ-галузі), загальні та спеціальні фахові компетентності (інсталювати і адмініструвати ресурси стандартних операційних систем і пристроїв зберігання даних, виконувати 20 адміністративних функцій, пов'язаних з доступністю інформації та інформаційними технологіями, визначити відносини між інформаційними технологіями та юридичним аспектом комп'ютерної експертизи, застосовувати навички, пов'язані з документуванням обліку даних, отриманих з цифрових пристроїв, застосовувати фундаментальні судові методи у сфері інформаційних технологій, та політику для захисту комп'ютерних систем від кіберзагрози) (Stevens Institute of Technology, 2017.).

Виконання складних завдань у сфері кібербезпеки у поєднанні з необхідністю опанування новітніми технологіями передбачає володіння, серед інших, аналітичною компетентністю, що необхідна для вирішення

кваліфікаційних фахових завдань і є одним із ключових складників професійної компетентності сучасних фахівців. Ця якість є головним компонентом здатності теоретизувати, знаходити причинно-наслідкові зв'язки між явищами, становить основу загальних здібностей і необхідна для успішного освоєння людиною різних видів діяльності.

Тобто до основних компетенцій, якими має оволодіти майбутній фахівець зі спеціальності «Кібербезпека» відносимо:

- розуміти важливу термінологію, знати та вміти використовувати сучасні матеріали та технології;
- володіти загальними навичками з кібербезпеки,
- мати досить високий рівень не лише теоретичних знань, а й професійної майстерності у своїй галузі;
- розуміти процеси, що відбуваються в системі, проводити моніторинг систем безпеки, застосовуючи міжмережеві екрани та системи виявлення вторгнень;
- вміти розробляти, впроваджувати і контролювати виконання заходів безпеки;
- вміло діяти за планом аварійного відновлення даних для операційних систем, баз даних, мереж, серверів і додатків;
- професійно проводити дослідження нових продуктів, послуг, протоколів і стандартів для підвищення рівня безпеки;
- вміти впроваджувати нове програмне забезпечення та / або технології;
- проводити регулярні перевірки відповідності використання операційних систем, баз даних, мереж, серверів і додатків (Додаток В, Таблиця В.1).

Студенти навчаються встановлювати програмне забезпечення систем безпеки, моніторингу мережі з метою виявлення ризиків вторгнень, реагування на кібератаки, основам кіберзахисту, збору даних і доказів (Джонстоун, 2003). Варто зазначити, що особливістю освітніх програм США є відсутність дисциплін з фізичного захисту та інженерно-технічного захисту інформації, що є традиційними для українських освітніх програм, орієнтованих на збереження конфіденційності інформації.

У вимогах ОПП до здобувача ОКР «бакалавр» спеціальності «Кібербезпека» зазначено, що кожен здобувач проходить суворий відбір на професійну надійність; до навчання не допускають студентів, які потенційно схильні до використання отриманих навичок зі злочинною метою (Stevens Institute of Technology, 2017).

Аналіз навчальних матеріалів свідчить про те, що специфічною особливістю підготовки бакалаврів з кібербезпеки є зорієнтованість на поєднання теоретичних знань, отриманих «за партою», з практичною складовою через посилення зв'язків навчального закладу з потенційним місцем роботи випускника. Однією з характерних особливостей підготовки бакалаврів з кібербезпеки США є орієнтованість на практичне застосування знань на засадах демократичних цінностей відповідно до чітко визначених вимог до випускника університету.

Таблиця 3.1.1

Загальна характеристика вимог до здобувачів освітньо-кваліфікаційного рівня «бакалавр» в університетах та коледжах США (ОПП Tennessee Technological University,2017; The University of Tennessee at Chattanooga, 2017; Iona College, 2017; Walsh College, 2017; Stevens Institute of Technology 2017).

АЗВА ВНЗ	ОКР «бакалавр», спеціальність	ЗАГАЛЬНІ ВИМОГИ ДО АБІТУРІЄНТІВ ТА ЗДОБУВАЧІВ ОКР «БАКАЛАВР»
Тенесійський Технологічний університет	**Інформатика-Кібербезпека**	Загальна кількість кредитів для отримання ОКР – 120. Додатково потрібно обрати більше 20 курсів зі спеціальності та спеціалізації. Для вступу середній бал 3.0 або вище. Абітурієнти також повинні мати оцінку ACT[1] або SAT[2]: твір – щонайменше 20, математика – 22.
Технологічний інститут Стивенс	**Кібербезпека**	Першокурсники повинні мати документ щодо результатів успішності про закінчення середньої школи, що включає результати з вивчення англійської мови (4 роки), предметів загальноосвітнього циклу (3 роки), математики (4 роки), включаючи вступ до програмування (1 рік). Від абітурієнтів вимагаються результати АТ або СОТ, есе та дві рекомендації.
Філія Тенесійського Університету в Четтануга	**Інформатика-Кібербезпека**	Вимоги для цієї програми включають наступне: 10 базових курсів з комп'ютерних наук; 7 курсів з кібербезпеки; 3 курси на вибір в комп'ютерних чи технічних сферах; дипломний проект або тези. Студенти також повинні дотриматися ряду вимог щодо математики, в т.ч. обчислення, I та II лінійну алгебру, курс дискретної математики, курс статистики. Абітурієнти GED[3] проходять тестування АТ або СОТ – для заявників віком менше 21 років.
Уолш коледж	**Інформаційні технології – Кібербезпека**	Загальна кількість кредитів для отримання ОКР – 127 семестрових і не менше 45 у коледжі Уолш. Програма коледжу передбачає лише навчання студентів старших курсів, тому абітурієнти повинні мати щонайменше 60 семестрових кредитів з середнім балом 2,0 або вище.
Айона коледж	**Обчислювальна техніка з поглибленим вивченням кібербезпеки**	Студенти цієї галузі повинні мати 25 спеціальних кредитів з інформатики, а також 4 необхідні курси та 2 факультативи з кібербезпеки. Абітурієнти подають диплом про середню освіту та результати підготовчих курсів у ВНЗ. Коледж приймає студентів з GPA[4] 2,75 та результати АТ або СОТ.

З метою візуалізації означеної особливості підготовки бакалаврів з кібербезпеки у табл. 3.1.1 наведено документальні відомості, зокрема з витягу ОПП щодо вимог до вступу та узагальнено дані про здобуття ОКР «бакалавр» зі

[1] ACT (American College Testing) – АТ (Американське тестування) – це стандартизований тест для вступу до коледжів та університетів США, а також при переведенні з одного навчального закладу в інший. Історично стандартизований тест складається з чотирьох тестів: англійська, читання, математика і наукове мислення. У лютому 2005 р. з'явилася можливість опціонально скласти письмовий тест. Усі коледжі та університети з чотирма роками навчання приймають результати АТ, але деякі з них також можуть вимагати додаткові відомості про успішність.

[2] SAT (Scholastic Assessment Test – СОТ (Схоластичний оцінювальний тест) є стандартизованим тестом для вступу до коледжів у Сполучених Штатах АМерики. Мета тесту – оцінити готовність школяра до коледжу. Вперше тест провели у 1926 році, в той час як назва та оцінювання неодноразово змінювалося. Поточний СОТ, впроваджений у 2005 р., на складання цього тесту відводиться три години і сорок п'ять хвилин та коштує $49 ($81 Міжнародний), без податку та мита за запізнілу реєстрацію Можлива кількість балів варіюється від 600 до 2400, об'єднуючи тестові результати з трьох 800-бальних секцій: математика, аналіз тексту і граматика.

[3] GED (General Equivalency Diploma – ДСО (Диплом про середню освіту) – тест на знання програми середної школи, що був уведений у 1942 р. як можливість другого шансу отримати потрібну роботу чи кар'єрного зростання. Облікові дані тесту за програмою середньої школи дають єдині уявлення про еквівалентність знань заявника програмі середньої школи. Результати тесту визнані у всіх 50 штатах. Випускники можуть підтвердити свої академічні навички та знання за основними напрямами: читання, письмова грамотність, математика, наукові та соціальні дослідження. Понад 18 мільйонів людей скористалися ДСО-тестуванням, що проводиться цілорічно в більше ніж у 3400 центрах тестування в усьому світі.

[4] GPA (Grade Point Average) – це СБ (середній бал) усіх оцінок у дипломі / атестаті за період навчання. Певний мінімум середнього балу є необхідною умовою для вступу в більшість університетів США. Насамперед СБ відображає середню успішність з усіх предметів, а не певні захоплення та інтереси. Метод розрахунку СБ в кожному університеті різний. Ряд університетів вимагає бал за останні 3 роки навчання, деякі запитують бал з певних предметів.

спеціальності «Кібербезпека» у декількох університетах, коледжах та інститутах США, а саме: Tennessee Technological University (Тенесійського Технологічного університету), The University of Tennessee at Chattanooga (Філія Тенесійського Університету в Четтануга), Iona College (Айона коледж) у штаті Теннессі, Walsh College (Уолш коледж) у штаті Мічіган, Stevens Institute of Technology (Технологічний інститут Стивенс) у штаті Нью-Джерсі.

Зауважимо, що кожен навчальний заклад висуває різні вимоги до своїх студентів. Так, відповідно до освітньо-професійної програми для здобуття ОКР «Бакалавр» зі спеціальності «Інформатика – Кібербезпека» Тенесійського Технологічного університету здобувачі повинні набрати 120 кредитів загалом, додатково слід також обрати 20 курсів зі спеціальності та спеціалізації.

Для вступу абітурієнти також повинні мати оцінку з національного тестування (ACT – American College Testing): за твір – щонайменше 20 балів, а з математики – 22. В освітньо-професійній програмі Філії Тенесійського Університету в Четтануга визначені інші вимоги щодо вступу та отримання ОКР «Бакалавр» з аналогічної спеціальності «Інформатика – Кібербезпека», а саме: закінчення 10 базових курсів у галузі комп'ютерних наук; 7 курсів з кібербезпеки; курси на вибір у галузі комп'ютерних наук або інших технічних галузях; написання дипломного проекту або іншої наукової роботи.

Студенти університету в Чатануга повинні відповідати ряду вимог щодо знань з математики, включаючи обчислення, лінійну алгебру, дискретну математику та статистику. Абітурієнти повинні мати сертифікат (диплом) про середню освіту (GED – General Equivalency Diploma), а для абітурієнтів, яким не виповнилося 21 рік, додатково необхідно скласти схоластичний оцінювальній тест СОТ (SAT – Scholastic Assessment Test) або пройти національне тестування АТ.

Для вступу в Технологічний інститут Стивенс у штаті Нью-Джерсі на здобуття ОКР «бакалавр» спеціальності «Кібербезпека» абітурієнти подають документ результатів успішності закінчення середньої школи, що включає результати з вивчення англійської мови (за 4 роки навчання), предметів

загальноосвітнього циклу (3 роки), математики (4 роки) та вступу до програмування (1 рік). Від абітурієнтів вимагаються результати АТ або СОТ, есе та дві рекомендації з місця навчання.

Здобувачі ОКР «бакалавр» коледжу Іона спеціальності «Обчислювальна техніка з поглибленим вивченням кібербезпеки» для одержання диплому повинні набрати 25 кредитів у галузі інформатики, а також закінчити чотири обов’язкових курси та два факультативних з кібербезпеки. Абітурієнти повинні мати диплом про середню освіту та мають пройти підготовчі курси у вищій школі. Коледж приймає абітурієнтів з середнім балом усіх оцінок у дипломі (атестаті) за час навчання (GPA – Grade Point Average) 2,75 або вище та вимагає від заявників подавати результати АТ або СОТ.

У коледжі Уолш для здобуття ОКР «бакалавр» зі спеціальності «Інформаційні технології – Кібербезпека» необхідно набрати загальну кількість 127 кредитів, причому не менше 45 кредитів студенти повинні отримати безпосередньо у навчальному закладі. Програма підготовки бакалаврів коледжу Уолша передбачає лише навчання для старших курсів, тому вступники повинні мати щонайменше 60 семестрових кредитів з середнім балом 2,0 або вище.

Загальну характеристику інших американських університетів та коледжів, що здійснюють професійну підготовку бакалаврів за спеціальністю «Кібербезпека», подано у додатку В. Важливо зазначити, що зміст професійної підготовки бакалаврів з кібербезпеки характеризує міждисциплінарність.

Аналіз змісту навчальних планів дозволив виокремити обов’язкові та вибіркові дисципліни, цикли загальної професійної та фахової підготовки. Основними обов'язковими дисциплінами зі спеціальності «Кібербезпека» в американських університетах є: «Інформаційна безпека», «Розслідування комп'ютерних інцидентів», «Міжмережеві екрани і виявлення вторгнень», «Безпека бездротових мереж» тощо. До вибіркових дисциплін відносяться: «Соціальні аспекти інформаційної безпеки», «Дані і інтелектуальний аналіз», «Безпека розподілених баз даних», «Політика інформаційної безпеки», «Практичні питання безпеки». Виходячи з цього, очевидно, в американській

системі навчання фахівців у галузі кібербезпеки дотримуються широкого профілю підготовки (Чванова, 2012).

У таблиці 3.1.2. подано узагальнену інформацію щодо кількості необхідних кредитів з обов'язкових та елективних дисциплін в освітньо-професійних програмах різних університетів США.

Таблиця 3.1.2

Узагальнені дані щодо розподілу кредитів за дисциплінами в ОПП на здобуття ОКР «бакалавр» за спеціальністю «Кібербезпека» в університетах США (опрацьовано автором на основі: ОПП Walden University (2017); American Military University (2017); Embry-Riddle Aeronautical University (2017); Baker College (2017); Iona College (2017) ; Mercy College (2017); Saint Vincent College (2017); Iona College (2017)).

Університет	Загальна кількість кредитів	**General education Requirements**		**Core courses**		**Concentration courses (Specialized Area)**		**Elective courses**		**Final Program Requirements**	
		Кредити	Дисципліни	Кредити	Дисципліни	Кредити	Дисципліни	Кредити	Дисципліни	Capstone Course	Senior Seminar in Cybersecurity
Walden University Університет Уалден	181	46	17	85	17	20	5	20	4	5	5
American Military University Американський військовий університет	106	30	10	54	18	15	5	18	15	3	
Embry-Riddle Aeronautical University Авіаційний університет Ембрі Ріддл	120	40	14	47	15	24	8	12	8	3	3
St. John's University Університет Сент Джон	126	63	21	39	16	15	6	9	3	----	
Baker College	120	27	8	78	15	27	6	9		----	----
Mercy College Коледж Мерсі	138	60	4	42	14	15	5	12	4	12	----
Iona College Айона коледж	120	36	4	48	14	12	6	24	10	----	----
Saint Vincent College Сент-Вінсент Коледж	132	57	16	46	13	15	5	10	3	----	----

Ці відомості дозволяють виявити характерну особливість ОПП університетів та коледжів США з підготовки бакалаврів з кібербезпеки, яка полягає у тому, що значну частину усіх навчальних дисциплін становлять дисципліни, що пов'язані із кібербезпекою відкритих бізнес-систем і електронної комерції. Всі програми підготовки бакалаврів розраховані на чотири роки навчання, після чого здобувач отримує ступінь бакалавра з кібербезпеки за спеціалізацією в обраній галузі. Обов'язкові курси навчання складають вагому кількість предметів і є спеціалізованими.

Включення до навчальних програм як основних, так вибіркових дисциплін значно підвищує рівень захопленості та зацікавленості студентів змістом навчання. Студенти можуть самостійно обрати невелику кількість дисциплін (3–4), спрямованих на засвоєння додаткових знань та навичок в обраній галузі підготовки. До дисциплін за вибором належать: «Соціальні аспекти інформаційної безпеки», «Дані і інтелектуальний аналіз», «Безпека розподілених баз даних», «Безпека електронної комерції», «Політика інформаційної безпеки; прикладна криптографія», «Практичні питання безпеки», «Спеціальні питання інформаційної безпеки» та інші. Виходячи з цього, очевидно, в американській системі навчання фахівців у сфері кібербезпеки дотримуються широкого профілю їхньої професійної підготовки.

У ході аналізу освітніх програм нами виявлено наступні особливості їх змістового наповнення з підготовки бакалаврів з кібербезпеки в США:

- впровадження дисциплін, пов'язаних з розслідуванням комп'ютерних інцидентів;
- збільшення частки матеріалу, зорієнтованого на правозастосовувані технології в ІТ-галузі, спеціальності кібербезпеки, серед них – технології, що ґрунтуються на міжнародному праві;
- включення дисциплін, пов'язаних з впровадженням технологій кібербезпеки в бізнес-структури, електронну комерцію, комерційне застосування інтелектуальних прав.

Упровадження таких дисциплін підтверджує пріоритетність міждисциплінарності, яка сприяє інтегративності змісту курсів у професійній підготовці бакалаврів з кібербезпеки та перенесення структурних елементів наукового знання з одного циклу дисциплін в іншому.

Практичне навчання бакалаврів з кібербезпеки є фундаментом для здобуття кваліфікаційного рівня майбутніми фахівцями ІТ-галузі, у підготовці яких повинна бути задіяна наукова складова. Підготовка висококваліфікованого фахівця неможлива без взаємодії різних типів навчальних закладів з підприємствами на державному та регіональному рівнях, тобто без практичного компонента навчання. Розроблення нових державних стандартів підготовки бакалаврів з кібербезпеки дає можливість скорегувати умови їх практичної підготовки на потенційному місці роботи. Зауважимо, що посилення практичної складової підготовки фахівців є важливим напрямом реформи вищої освіти в Україні, без якого стає неможливою якісна підготовка фахівців та наближення вітчизняної освіти до міжнародних вимог.

У ході дослідження було проаналізовано особливості практичної підготовки бакалаврів з кібербезпеки в американських вищих навчальних закладів. Майбутні бакалаври з кібербезпеки США проходять практику, яка організовується на засадах інтегративного поєднання навчання в університеті та практичної підготовки на майбутньому робочому місці. Уже у першому семестрі студенти у межах практики здійснюють пошук літератури, складають план досліджень та ініціюють наукові роботи за фахом. Студенти старших курсів займаються безпосередньо дослідженням. Іншою складовою практики є стажування, спрямоване на можливість оволодіння важливими навичками і професійними якостями, а також ознайомлення з особливостями роботи в умовах промисловості, у державних, приватних або бізнес-структурах. Закінчується навчання в бакалавраті виконанням бакалаврського проекту під керівництвом викладача або групи викладачів з професорсько-викладацького складу кафедри.

Проектування є основним методом реалізації інноваційної діяльності та складається з низки послідовно виконуваних дій та операцій, що відтворюють зміст і структуру інноваційної професійної діяльності у ІТ-галузі: моніторинг та діагностика інноваційної спрямованості процесу проектування, визначення мети, прогнозування, моделювання, створення концепції проекту, формування умов та засобів його організації, реалізація проекту, моніторинг процесу реалізації, оцінювання й аналіз результатів, внесення змін, оформлення та опис творчої основи процесу, узагальнення результатів проектування інноваційної професійної системи.

Проходження практики американські студенти можуть здійснювати в органах силових структур та органах державного управління, установах виробничої та банківської сфери, в яких студенти оволодівають професійно необхідними навичками та уміннями і, як результат, за наявності достатньої компетенції та знань, здатні до реалізації заходів із забезпечення інформаційної кібербезпеки.

Особливістю професійної підготовки фахівців з кібербезпеки закладів вищої освіти США є те, що майбутній фахівець з кібербезпеки має сам вибирати місце і час проходження практичної підготовки, оскільки це безпосередньо пов’язано з його майбутнім працевлаштуванням, а тому стосується сфери його відповідальності. Студенти заздалегідь повідомляють адміністрацію навчального закладу про місце і час проходження практики. Координатора (керівника) практики призначає центр кооперативних програм практики та укладає відповідні нормативні документами, зокрема чотиристоронні угоди між Центром кооперативних програм, навчальним закладом, роботодавцем та студентом. Допомогу практиканту щодо вибору проекту практики надає Центр Кооперативного навчання і практики (Cooperative Education and Internship program).

Майбутній практикант бере на себе певні зобов’язання (зразок зобов’язань – додаток Н): дотримуватися професійної етики, застрахуватися від нещасних випадків в установі стосовно фінансової допомоги (за наявності

стипендії), не претендувати на компенсацію по безробіттю, надати роботодавцю інформацію про академічні успіхи для зарахування на відповідну посаду і т.п. Варто акцентувати увагу на аспекті фінансової допомоги: студенти, які отримують стипендію більше одного року, повинні проходити практику у Федеральному агентстві, яка має тривати щонайменше 10 тижнів і, як правило, відбувається впродовж літа. Якщо учасник отримує одну або більше пропозицій, він повинен прийняти ту пропозицію, яка була внесена за 3 місяці до запланованої практики. В іншому випадку відповідно до програми SFS студенту обирається місце практики на власний розсуд, якщо на цей період наявні установи з відповідними пропозиціями щодо практики за необхідною спеціалізацією. Якщо учасник отримує пропозицію і не приймає її, відповідно не проходить практику у запланований термін, тривалість навчання у вищому навчальному закладі буде продовжена на один семестр, щоб надати можливість її пройти.

Центр Кооперативного навчання і практики визначає вимоги-рекомендації щодо Проекту практики, нормативних супровідних документів з проходження практики майбутніми фахівцями ІТ-галузі на потенційному місці роботи. Тривалість практики для майбутніх бакалаврів з кібербезпеки складає до півроку та відбувається за проектами Центру Кооперативного навчання і практики. У додатку К вміщено зразки вимог-рекомендацій Центру Кооперативного навчання і практики щодо проекту практики, нормативних супровідних документів. Проект практики містить таку інформацію:

- мета та завдання практики;
- відомості щодо видів діяльності організації, яка надає робоче місце практиканту;
- інформацію про координатора програми;
- перелік запропонованих посад та відповідних посадових інструкцій;
- опис особливі навичок, якими бажано володіти практиканту;
- перелік дисциплін, які потрібно опанувати перед практикою;

- інформація про відповідальних осіб – представників трудового колективу, які будуть допомагати студентові у роботі;
- чітко визначені обов'язки координатора програми, інших учасників практики та студента;
- місце та роль навчального закладу у проекті практики з метою врахування рекомендацій та вимог навчального закладу, у якому навчається студент;
- особлива увага у проекті відводиться координатору (supervisor), практик. Зазначено, що йому необхідно розуміти свою роль та відповідальність щодо практичної підготовки практиканта.

У функції координатора входить: організація знайомства практиканта з колективом; доведення до відома практиканта особливостей роботи; наставництво; вплив на мотивацію практиканта; забезпечення зворотного зв'язку; оцінювання результатів діяльності практиканта на завершення практики.

У документі окреслено вимоги до кандидатури координатора, а саме: координатор – це фахівець, що володіє певними уміннями і навичками; це насамперед професіонал в ІТ-галузі, який старанно ставиться до своїх обов'язків; він повинен мати досвід роботи зі студентами, вміти вирішувати проблемні ситуації; забезпечити баланс між наглядом, управлінням та самостійним навчанням студентів; вміти оцінити досягнуті результати.

Проект практики, основні аспекти організації практики обговорюються з усіма сторонами (учасниками проекту) для того, щоб можна було адресувати запитання, які виникають, безпосередньо компетентній особі та довести до відома кожному учаснику практики її цілі та специфіку. Результати практики суттєво впливають на подальшу долю випускника американського університету чи коледжу. Успішне проходження практики передбачає отримання відповідних кредитів, що полегшує процедуру подальшого працевлаштування.

Кожен вищий навчальний заклад США на завершення практики отримує від студента документ про успішність її проходження у вигляді Анкети Центру Кооперативного навчання і стажування щодо оцінювання практиканта

роботодавцем у США (додаток Й, таблиця Й-3), яка включає два компоненти: показники підготовки та власне шкалу оцінювання.

Показники підготовки визначені з метою об'єктивного оцінювання результатів проходження практики та різносторонньої характеристики практиканта – майбутнього фахівця з кібербезпеки. Загальна кількість показників підготовки складає понад півтора десятка. Шкала оцінювання складається з оцінок, які засвідчують широкий спектр можливостей в оцінюванні, а саме: об'єктивність, різносторонність та повноцінність оцінки отриманих результатів проходження практики: «відмінно», «добре», «задовільно», «гранично прийнятно», «не задовільно», «не прийнятно».

Показники результатів проходження практики включають не лише суто професійні вміння, а й ділові (вміння працювати в команді), етичні (розуміння професійної та моральної відповідальності, навички спілкування) якості, вміння аналізувати та приймати рішення, оформлювати технічну документацію згідно з чинними нормативними документами у сфері інформаційної кібербезпеки, писемну грамотність, усвідомлення необхідності навчатися протягом усього життя, загальну оцінку академічної підготовки студента тощо.

Крім цього, на подальше професійне зростання випускника американського університету чи коледжу впливає заробітна плата, яку одержують під час практики практиканти, що може частково покрити витрати на навчання. У додатку Й представлено дві таблиці: таблиця Й-1 систематизовано представляє оплату праці фахівця залежно від рівня освіти та набутого досвіду роботи; у таблиці Й-2 візуалізує показники щодо середньої заробітної плати відповідно до посади та років професійного досвіду (10 топ-найменувань посад).

Під час проходження практики студенти, які навчалися за проектами підготовки бакалаврів з кібербезпеки у 2016–2017 рр., отримували в середньому 16 доларів за годину, тоді як стартова середня заробітна плата випускників цієї спеціальності у цей же період складала 43,78 долари за годину.

Синтез теоретичного і практичного навчання в університеті, набуття практичних умінь на майбутньому робочому місці доповнюється особливими формами організації освітнього процесу з підготовки фахівців з кібербезпеки, зокрема для читання лекцій з проблем захисту кіберпростору університети постійно запрошують професіоналів з установ відповідного профілю, а викладачі обов'язкових дисциплін періодично проходять стажування у відповідних установах з фаху. Така тісна співпраця з роботодавцями дозволяє навчальним закладам вчасно модернізувати зміст навчання відповідно до вимог робочого місця.

Отже, на підставі аналізу освітньо-професійних програм та навчальних планів професійної підготовки майбутніх фахівців з кібербезпеки, вивчення особливостей організації освітнього процесу в університетах США можемо стверджувати, що зміст підготовки спрямований на формування та розвиток ключових і фахових компетенцій, які забезпечують ефективність виконання професійної діяльності. Серед позитивних характеристик навчальних планів визначаємо значну кількість дисциплін професійного циклу, особливо предметів фахового спрямування, що посилює формування професійної компетенції.

Важливо відзначити, що навчальні заклади мають тісні контакти із роботодавцями, що позитивно впливає на актуальність змісту підготовки. За практичний компонент професійної підготовки несе відповідальність майбутній працедавець та студент, що сприяє формуванню відповідального ставлення молоді до власного кар'єрного зростання.

3.2. Форми і методи організації навчального процесу бакалаврів з кібербезпеки

Стрімкий розвиток технологій, соціально-економічні та політичні чинники, необхідність тісного зв'язку навчальних програм з практикою у державних інституціях, установах збереження чи поширення інформації та структурах, що використовують ІТ у виробничому процесі, підвищують вимоги

до рівня знань та умінь випускників спеціальності «Кібербезпека». Забезпечення ефективного освітнього процесу можливе лише за умов застосування найсучасніших форм, методів, технологій і методик навчання.

На створення ефективного навчального середовища у вищих навчальних закладах США впливають зовнішні фактори: вільний і необмежений доступ студентів та викладачів до інформаційних ресурсів; забезпечення освітнього процесу лабораторіями новітніх технологій та необхідним сучасним обладнанням, обчислювальною технікою і програмними продуктами найвищого рівня та ін.

Специфіка професійної підготовки бакалаврів з кібербезпеки в системі вищої освіти США визначається методологічними підходами. Міждисциплінарний підхід допомагає сформувати у студентів світогляд, вміння оцінювати ефективність новітніх технологій, розвинути нестандартне мислення та організувати практичну реалізацію здобутих знань та навчити студентів самостійно здобувати знання різних галузей (Глотова, 2005.). Інтегративний підхід забезпечує засвоєння методології кіберзахисту, оволодіння професійними уміннями і навичками, здобуття рівня знань відповідно до вимог міжнародних критеріїв і стандартів вищої освіти. Це передбачає ознайомлення з новими зразками засобів захисту, теоретичними розробками, які демонструються на виставках, а також в ході чинних практик у структурах підрозділів безпеки підприємств. Інноваційно-орієнтований підхід передбачає «засвоєння повного циклу інноваційної діяльності і розвиток професійно важливих якостей фахівців, адекватних новим формам організації праці в умовах інноваційного підходу до кіберзахисту» (Глотова, 2005, с. 169).

Багатьма дослідниками доведено, що використання традиційних (пояснювально-ілюстративних) методів навчання у вищій школі малоефективне, тому вони переважно орієнтовані на пам'ять, а не на мислення (Аткінсон, 1980), мало сприяють розвитку творчих здібностей, самостійності, активності студентів. Дослідження американських учених Р. Карнікау і Ф. Макелроя (1975) виявили достовірну закономірність навчання: людина пам'ятає 10 % прочитаного; 20 %

почутого; 30 % побаченого; 50 % побаченого і почутого; 80 % того, що говорить сам; 90 % того, що усвідомлено у процесі самостійної діяльності.

Рис. 3.2.1. Ефективність видів навчальної діяльності щодо засвоєння навчального матеріалу у вищих навчальних закладах США (Карнікау & Макелрой, 1975).

На рисунку 3.2.1. схематично представлена ефективність видів навчальної діяльності у процесі професійної підготовки бакалаврів кібербезпеки. Зазначимо, що найменш ефективні результати досягаються за умов пасивного навчання. У результаті пасивного прослуховування лекції засвоюється лише 5 % поданого матеріалу, тоді як в результаті читання – вдвічі більше – 10 %. Статистичні дані свідчать, що найкращих результатів студенти досягають за умов упровадження інтерактивних видів навчання. Так, у дискусійних групах результат засвоєння інформації сягає 50 %, дієве навчання – 75 %; найбільший відсоток спостерігається в результаті поєднання навчання з практикою (90 %). Звичайно, середньостатистичні дані і в конкретних випадках результати можуть бути дещо іншими, але в середньому таку закономірність може простежити кожен викладач. За визначенням науковців, педагогічна форма – це усталена, завершена організація освітнього процесу в єдності всіх його компонентів. У дидактиці форма – це спосіб організації навчання. Кожна з

організаційних форм навчання характеризується своєю структурою, принципами упорядкованості її елементів (Гончаренко, 1997, с. 362).

Форми навчання у сфері вищої освіти США є універсальними гуманістичними, що передбачають використання широкого спектру технічних засобів, інформаційно-комунікаційних технологій, діалогової взаємодії з викладачем без урахування відстані і часу.

На рис 3.2.2. зображено форми організації навчання у вищих навчальних закладах США та критерії, які лежать в основі її класифікації. Залежно від кількості студентів форми організації навчання можуть бути фронтальні, індивідуальні чи групові. Місце навчання впливає на вибір територіальних форм організації навчання (університет / установа проходження практики). Використовуються різноманітні форми навчальних занять: лекції, практикуми, семінари, лабораторні заняття, конференції, консультації, заліки, іспити тощо.

Рис 3.2.2. Чинники впливу на вибір форм організації навчання у ВНЗ США (укладено автором на основі: Гончаренко, 1997).

Фронтальною формою організації навчання є такий вид діяльності, за яким виконується спільне завдання під керівництвом викладача. При цьому педагог проводить роботу зі всією аудиторією в єдиному темпі. У процесі розповіді, пояснення, показу передбачено одночасний вплив на всіх присутніх,

що забезпечує процес творчої колективної співпраці, стимулювання активності студентів як важливих умов ефективності цієї форми організації навчання.

Індивідуальна форма роботи передбачена для вирішення різних дидактичних завдань та переважає у виконанні домашніх завдань, самостійних і контрольних тестів.

Інформаційно-комунікаційні технології навчання можна вважати одним із головних компонентів (інформаційно-технологічного простору) та важливою умовою забезпечення ефективного освітнього процесу у системі вищої освіти, основою формування нового інформаційно-освітнього середовища зі специфічними дидактичними вимогами. Поряд із цим використання інформаційних технологій зумовлює вторинну індивідуалізацію освітнього процесу, певне повернення (з новою якістю) до технологій навчання та частково виховання, притаманних освітнім системам доіндустріальних суспільств та наявних у сім'ї (Гребньов, 2001).

Інформатизація системи освіти шляхом використання ІТ для підвищення ефективності видів діяльності, що здійснюються в системі освіти, дозволить розширити єдиний інформаційний простір освітньої діяльності (Биков, 2010).

Провідні ідеї означеної концепції відображаються у використанні актуальних сучасних методів і форм підготовки бакалаврів з кібербезпеки. Так, в американській моделі підготовки бакалаврів з кібербезпеки домінують форми групового навчання, які забезпечують розвиток мислення конкурентоспроможного фахівця, формування умінь і навичок кіберзахисту та моральних цінностей для плідної роботи в команді, використовують групове навчання для вирішення складних проблем, що потребують колективного розуму. Гетерогенні групи, які об'єднують студентів із різними здібностями, досвідом, інтересами, мають переваги у створенні можливостей для різноманітних прийомів розв'язання проблем у професійній сфері.

Різний пізнавальний рівень студентів, що входять до складу гетерогенної групи, зумовлює залучення їх у складний процес мислення, встановлення

причинно-наслідкових зв’язків та участь в обговоренні пізнавального матеріалу.

Відзначимо, що в американських вищих навчальних закладах освітній процес менш регламентований, ніж у нашій державі. Тому вибір форм навчання залежить виключно від особистих уподобань викладача, що забезпечує методичну свободу педагога та закладів вищої освіти, які можуть надавати перевагу лекціям чи семінарським, практичним чи лабораторним заняттям.

На основі аналізу навчально-методичних матеріалів з проблеми дослідження можемо констатувати, що форми навчання бакалаврів з кібербезпеки достатньо різноманітні: лекції, практичні заняття, лабораторні роботи, семінари тощо. З’ясовано, що для навчання бакалаврів викладачі використовують комбінацію форм, методів навчання з метою оптимізації процесу навчання. Необхідно відзначити такі інноваційні форми навчання бакалаврів з кібербезпеки: онлайн-лекції, робота Fablab «Кібербезпека», демо-зони засобів кіберзахисту, бізнес-інкубатори для створення стартапів, онлайн-тести та ін.

Виявлено, що забезпечення якості професійної підготовки бакалаврів з кібербезпеки досягається завдяки творчому поєднанню традиційних та інноваційних форм. Обов’язковою є участь студентів у міжнародних наукових конференціях, семінарах та симпозіумах з таких проблем: «Інформаційні технології та системи», «Безпекознавство», «Кібербезпека», «Захист інформації». Ці види діяльності активізують пізнавальну діяльність студентів, формують самостійність судження, уміння захищати власні думки, аргументувати їх на основі наукових фактів, сприяють оволодінню фундаментальними знаннями, допомагають розвивати логічне мислення.

Розглянемо особливості форм навчання за типом занять, що використовуються у процесі професійної підготовки бакалаврів зі спеціальності «Кібербезпека» в університетах США.

В американських університетах лекція суттєво відрізняється від її сучасних вітчизняних пояснювально-ілюстративних аналогів. Зазначимо, що

лекція – це систематичний, послідовний виклад навчального матеріалу, будь-якого питання, теми, розділу, предмета, методів науки (Парил, 1991, с. 189). Лекції у вищих навчальних закладах США проводять як для малих, середніх, так для великих потоків слухачів-студентів кількістю до 1000 осіб. Тривалість лекції – від 50-120 хвилин, початок лекції, як правило, – о 8 ранку. Лектори університетів США мають найвищий ступінь кваліфікації та притримуються двох концепцій проведення лекцій, а саме: колізм – це читання методологічних лекцій крізь призму загальнонаукових дисциплін; а також редукціонізм– це проведення лекцій за попереднім ознайомленням студентів з матеріалами (Парил, 1991, с. 189).

У випадку використання концепції редукціонізму перед лекцією студенту видається готовий конспект. Слухаючи лектора, студент робить необхідні позначки у тексті. Це інтенсивна методика, яка надає можливість широко використовувати технічні засоби навчання. При такому підході студенти не витрачають час на складання конспекту, що сильно мотивує їх до сприйняття лекційного матеріалу.

Аналіз американської системи підготовки бакалаврів з кібербезпеки показав, що має місце чітка тенденція до скорочення лекційних годин у загальному обсязі навчального навантаження. На нашу думку, завдяки цьому змінюється зміст лекційних занять. На лекціях розглядаються лише основні проблеми та відомості з курсів, що висвітлюють найновіші досягнення у конкретних галузях знань. Це вказує на основні ознаки випереджаючого навчання, яке мотивує студентів не до механічного заучування наукових фактів, а залучає до опанування новітніх ІТ-технологій, аналізу і вирішення поставлених проблем, що впливає на формування професійних умінь майбутнього бакалавра з кібербезпеки.

Відомо, що ефективності лекційних занять сприяє їх матеріальне забезпечення. В США роль технічних засобів виконує телебачення. Значна кількість університетів та установ, які включені до переліку баз проведення практик, мають спільну замкнену мережу телебачення, яка дозволяє читати

лекції для великої кількості студентів, різного місця розташування, демонструвати експерименти, ознайомлювати з сучасними інформаційними технологіями. Навчальні передачі проводяться в аудиторіях як університетів, так і відповідних установ зі спеціально оснащеними засобами зв'язку лектором. Це сприяє інтерактивному спілкуванню викладача та студентів, а також студентів між собою, що знаходяться на відстані один від одного.

Лекції проводяться за розкладом для студентів, а також за попередньо визначеною тематикою для співробітників установ. Кожна навчальна лекція записується на відео, і ті, хто пропустили певну лекцію, можуть її переглянути повторно. Переважно відеозаписи зберігаються два семестри (Собчак, 2004, с. 149-155).

Вартим уваги є досвід запрошення експертів (IT-професорів, менеджерів, військових, представників державних установ, фірм, банків галузі) для проведення лекцій-презентацій з метою забезпечення майбутнього працевлаштування студентів. Їхні виступи дають можливість майбутнім бакалаврам з кібербезпеки поглибити свої знання у сфері захисту кіберпростору, сформувати уявлення про характер і напрями кіберзахисту, про виникнення та особливості кіберзагроз, кібератак, ризиків, тощо (Литтл, Брюс, 1997).

Аналізуючи особливості навчання у вищих навчальних закладах США, неможливо не згадати найновішу і найпотужнішу з-поміж багатьох країн матеріально-технічну базу навчальних закладів. Провідні заклади вищої освіти мають можливість використовувати у своїй науково-педагогічній діяльності унікальні експериментальні зразки найновіших досягнень американської промисловості, науки і техніки.

Особливої уваги варті лекції-подкасти, що записують у вигляді потокових відеоповідомлень «подкастів» («podcast») і розміщують на Інтернет-ресурсах університету, забезпечуючи доступ до них через службу «Live Meeting» з переліку програмного забезпечення «Microsoft Office Live Meeting». Служба «Live Meeting» також створює можливості для спільної роботи студентів та

лекторів. Трансляція онлайн-лекції може здійснюватися як на окремі (домашні) комп'ютери чи мобільні комп'ютери (смартфони, айфони, айподи), так і на проектори у навчальних аудиторіях локальних центрів. Лекції-подкасти дають можливість вільного вибору часу навчання, студентів може прослухати матеріал не за розкладом розкладу. Таким шляхом долаються просторові та часові обмеження при проведенні лекцій та забезпечується очний контакт при проведенні онлайн-семінарів при проходженні практики.

Логічним продовженням лекційних занять з метою подальшого опанування змісту дисципліни є семінарські заняття. У ході підготовки бакалаврів з кібербезпеки семінарські заняття у вищих навчальних закладах США за своєю методикою проведення мало відрізняються від українських форм організації навчання Одна варто відзначити, що в США семінарські заняття відкриті для всіх бажаючих. Зауважимо, що відвідування вузькоспеціалізованих (на відміну від семінарів для широкого загалу слухачів) вимагають від студентів суттєвої теоретичної підготовки та набраних «кредитних годин зі спеціальності» (Романовський, 2002, с. 111.). Дуже важливо, що до проведення вузькоспеціалізованих семінарів залучаються студенти магістратури, докторанти, кращі студенти старших курсів.

Основними обов'язковими вимогами щодо участі студента в лабораторних заняттях є наступне: його ґрунтовна теоретична підготовленість до виконання лабораторних робіт; готовність студента до самостійного проведення дослідів; науково-дослідницький характер структури робіт лабораторних занять; лише власний позитивний результат є підставою для позитивної оцінки роботи.

На думку вчених, важливою підвалиною системи вищої освіти з професійної підготовці фахівців США стала концентрація уваги на стимулюванні студентів до самостійного здобуття знань, умінь та навичок. Як зазначає О. Романовський (2002), важливим завданням сучасної американської освіти є тренування інтелекту, логічного мислення засобами загальнонаукового підходу. Тому значна увага у системі вищої освіти США приділяється

самостійним заняттям бакалаврів з використанням найсучаснішого технічного обладнання та методичного забезпечення. Самостійна робота бакалаврів посідає чільне місце в освітньому процесі університетів США. Майбутні бакалаври з кібербезпеки мають можливість самостійно працювати у комп'ютерних лабораторіях, навчально-наукових центрах, бібліотеці, також у домашніх умовах під час канікул (Глузман, 1998). В університетах США самостійна робота майбутніх бакалаврів з кібербезпеки домінує серед інших видів навчальної роботи. Провідним завданням сучасної американської освіти є розвиток інтелектуальних здібностей особистості, логічного мислення засобами загальнонаукового підходу, виховання методологічної культури набуття знань (Пуховська, 2003). Для успішної самостійної роботи створено сприятливі умови. Серед факторів, що відіграють важливу роль у цьому ми можемо назвати наступні (додаток Д , таблиця Д-3):

1) розпочинається навчання з того, що студент може придбати всі необхідні підручники, посібники, тексти лекцій, зошити для виконання тестів і контрольних завдань, комп'ютерне, аудіо- і відеозабезпечення для вивчення дисципліни;

2) можливість використовувати унікальні, експериментальні зразки найновішого обладнання;

3) вільний доступ до світових досягнень науки і техніки через засоби інформаційно-комп'ютерних мереж;

4) право студента в будь-який момент отримати консультацію, допомогу від викладачів та складати іспит (залік) лише після його готовності до участі в контрольних заходах.

Самостійна робота запланована також у групах: групові проекти, аналіз кейсів (рішення реальних проблем з кіберзахисту), презентація отриманих результатів. Значний семестровий обсяг теоретичного матеріалу для опрацювання американськими студентами передбачає також виконання невеликих індивідуальних завдань, які потребують викладення власної точки зору щодо певної проблеми. Практикується підготовка презентацій, написання

коротких есе (7-8 протягом курсу), виконання курсових робіт. Оскільки в системі підготовки майбутніх бакалаврів з кібербезпеки особливу роль відіграють курсові роботи (зокрема при опануванні студентами бакалаврської програми), детальніше зупинимося на методичних аспектах її реалізації (Wratcher, Morrison , Riley& Scheirton, 1997).

Важливо відзначити, що однією з важливих вимог до виконання курсової роботи є надання інформації про тему дослідження (обрану з запропонованих або самостійно сформульовану), обґрунтування мети, визначення передбачуваних результатів, складання розгорнутого календарного плану роботи обсягом 1-2 сторінки наступного дня після отримання завдання з курсової роботи викладачеві.

Рис. 3.2.3. Складові показники загальної оцінки за курсову роботу (Wratcher, Morrison, Riley& Scheirton, 1997).

У ході проведення курсового дослідження студент має організувати презентацію на 7-9 хвилин про отримані результати з використанням унаочнення даних та презентацію на 15 хвилин результатів дослідження перед захистом курсової роботи. На рис. 3.2.3. висвітлено складові загальної оцінки за курсову роботу: 5 % – це оцінка за уміння скласти план роботи та обґрунтувати

мету; 70 % – за якість оформлення пояснювальної записки; 15 % – за успішність захисту; 10 % – оцінка за проміжну презентацію.

З метою вивчення та обговорення актуальних навчально-виробничих проблем в коледжі чи університеті студенти об’єднуються в невеликі групи. Для цього їм надаються відповідні аудиторії чи лабораторії. Наприклад, в Інституті технологій Стівена (Stevens Institute of Technology) у штаті Нью Джерсі студенти на таких зустрічах навіть проводять лекції з наступним обговоренням проблем, які висвітлюються студентом-лектором. Проблемо-аналітичний підхід до навчання дозволяє сфокусувати увагу студентів на аналізі і розв’язанні конкретної проблемної ситуації, вмотивовує їх на оволодіння знаннями з різних галузей, формує творчі здібності.

Традиційно на лекції, семінари, лабораторні роботи відводиться 16 год. на тиждень (зокрема у Stevens Institute of Technology у штаті New Jersey) і на кожну годину аудиторних занять рекомендовано 2 год. самостійної роботи, то сумарне тижневе навантаження студента складає 45-50 год. Вся система підготовки бакалавра з кібербезпеки підпорядковується правилу: адміністрація вищого навчального закладу для студента – консультативний орган, а викладач – інструктор. Вважається, що це одна з найкращих систем самовиховання та самоконтролю (Stevens Institute of Technology, 2017).

Сьогодні основні методичні інновації у вищій школи пов'язані із застосуванням інтерактивних методів навчання, що ґрунтується на принципах взаємодії, активності студентів, опорі на колективний досвід, обов'язкового зворотного зв'язку. Провідними методами навчання, що використовуються з метою мотивації навчальної діяльності майбутніх бакалаврів з кібербезпеки на семінарських, лабораторних та практичних заняттях є ділові ігри, дискусії та ґрунтовний аналіз ризиків, запобігання кібератак, виникнення кібербезпекових ситуацій, підходи до кіберзахисту.

На думку американського дослідника з технології групового навчання Д. Бромвіча (D. Bromwich), на ефективність освітнього процесу позитивно впливає рольова гра, у процесі якої кожен учасник групи виконує певну роль:

аналітика, інспектора, хакера, опонента тощо. При цьому студенти мають змінювати ролі на кожному занятті для того, щоб вони не звикали до них, але виконали кожну роль кілька разів.

За рекомендацією Д. Бромвіча (Bromwich, 2003), варто постійно вводити у сценарій заняття нові ролі, наприклад, творчі: винахідник, мислитель, генератор ідей тощо. Такий підхід до рольової гри та розподілу ролей в ній допомагає студентам формувати навички роботи в команді, уміння спілкуватися, управляти своїм емоційним станом та загалом опановувати особливості майбутнього фаху. Методи орієнтовані на більш широку взаємодію студентів не лише з викладачем, але й один з одним, на посилення їхньої активності у процесі навчання. Широко використовується дискусійний метод, який притаманний теоретичним формам організації навчання, що, на нашу думку, сприяє посиленню мотивації студентів у пошуку і відстоюванні знайденої ними істини.

Аналізуючи обов'язкові вимоги до організації підготовки фахівців для ІТ-галузі зі спеціальності «Кібербезпека», нами визначено, що у закладах вищої освіти США запроваджено навчання «від зворотнього», тобто фахівців з кібербезпеки навчають питанням інформаційної боротьби. Прикладом навчання «від зворотнього» може слугувати таких факт: у курсі дисципліни «Комп'ютерний злам» практикується метод роботи під назвою «студент у шкурі хакера». Цей метод спрямований на практичне закріплення якісних знань щодо вразливості комп'ютерних систем та досягнення студентом високої вірогідності попередження зламу (Stevens Institute of Technology, 2017).

У процесі професійної підготовки бакалаврів з кібербезпеки в університетах США успішно застосовуються методи ситуаційного навчання на основі аналізу ситуацій, «мозкового штурму» – у межах малих груп, при роботі над спільними проектами, під час публічних виступів з комп’ютерними презентаціями, захисту доповідей тощо. На думку американських учених, форми і методи навчання, що використовуються у процесі професійної підготовки бакалаврів з кібербезпеки, зорієнтовані не на запам’ятовування

матеріалу, що мимоволі гальмує розвиток творчих здібностей, а на його розуміння (Gorgone, Gray, Stohr &Davis, 2006). Отже, процес формування у майбутніх фахівців з кібербезпеки важливих ключових компетентностей, які дозволятимуть здійснювати ефективно професійну діяльність, передбачає оптимізацію навчання за допомогою поєднання традиційних та інноваційних форм, методів і технологій навчання.

3.3. Рівні забезпечення якості підготовки бакалаврів з кібербезпеки у закладах вищої освіти США

В інформаційному суспільстві ІТ-галузь виконує стратегічно важливу функцію гаранта національної безпеки. За таких умов дотримання високих стандартів навчання фахівців та проведення систематичних заходів з перевірки якості їхньої підготовки є першочерговими завданнями.

Згідно зі ст. 11 Всесвітньої декларації ЮНЕСКО з вищої освіти (1998) якість у сфері вищої освіти є багатовимірною концепцією, що повинна охоплювати всі її функції та види діяльності: навчальні та академічні програми, наукові дослідження та стипендії, укомплектування кадрами, учнями, будівлями, матеріально-технічною базою, обладнанням, і передбачає роботу на користь суспільства та академічне середовище. Під якістю вищої освіти найчастіше розглядається рівень отриманих особою знань, умінь та професійних навичок відповідно до мети, визначеної вищим закладом освіти. Результатом є якісне і кількісне оцінювання досягнутого рівня відповідних освітньо-професійних характеристик фахівця (Алфьорова, 2015).

Аналіз нормативних документів з проблеми дослідження дозволяє зробити висновок, що в США система забезпечення якості вищої освіти здійснюється на трьох рівнях: на рівні вищого навчального закладу, федеральному (державна і державно-суспільна система контролю) та галузевому. Система сертифікації, яка існує вже у понад 150 закладах (представлена у попередніх підрозділах), функціонує на галузевому рівні і забезпечує підготовку фахівців з кібербезпеки відповідно до потреб ІТ-галузі.

У США існує децентралізований підхід до впровадження стандартів вищої освіти, тому забезпечення якості на федеральному рівні покладається на комісії штатів, які і є регіональними комісіями з акредитації. Оцінювання якості освіти здійснюється незалежними агенціями, тому у США не використовується таке поняття, як державна акредитація освіти та навчальних закладів.

Процедура проходження акредитації / сертифікації є добровільною для американських університетів, які додатково мають власні системи самоконтролю забезпечення якості з огляду на вимоги державної політики у IT-галузі та потреб суспільства.

Основні критерії аудиту стосуються насамперед відповідності освітніх програм вимогам суспільства щодо підготовки фахівців у галузі та забезпечення матеріальними, науково-методичними, кадровими ресурсами освітнього процесу й ефективності управління університетом. Зовнішнє оцінювання проводять незалежні агенції, створені за ініціативою професійних асоціацій та університетів. Серед організацій, залучених до стандартизації і сертифікації підготовки фахівців з кібербезпеки, можна назвати федеральний орган, який вважається найбільш впливовим, ABET (Accreditation Board for Engineering and Technology) – раду з акредитації програм у галузі техніки і технологій. Передусім це стосується спеціальностей: Computer Science – комп'ютерні науки, Computer Engineering – комп'ютерна інженерія, Systems Engineering – системна інженерія.

Незалежні агенції проводять зовнішній аудит діяльності університетів та надають рекомендації щодо поліпшення якості їх діяльності. Так як мета проходження незалежної акредитації – підвищення якості вищої освіти шляхом розроблення критеріїв оцінювання та пропозицій щодо напрямів розвитку навчальних закладів, то висновок про якість підготовки у певних освітніх установах визначається результатами, отриманими від незалежного оцінювання. Рішення щодо необхідності проходження акредитації приймається вищим навчальним закладом самостійно на добровільній основі.

Дотримання єдиної системи критеріїв оцінювання забезпечує об’єктивність оцінки якості вищої освіти, але кожне незалежне американське агентство має свій перелік додаткових критеріїв щодо підготовки кадрів для ІТ-галузі з кібербезпеки. Однак нами було виявлені основні критерії, які є обов’язковими для аудиту вищих навчальних закладів незалежними агенціями з аудиту. До критеріїв, які є обов’язковими для контролю, належать:

- мета підготовки, планування навчального процесу та його ефективність;
- актуальність освітніх програм;
- цілісність установи, достатні фінанси на рахунках, ефективність управління та адміністрування;
- якісні показники забезпеченості професорсько-викладацьким та допоміжним персоналом;
- умови навчання;
- матеріально-технічне забезпечення освітнього процесу (бібліотечний фонд, комп’ютерна база тощо.)

Процедура незалежної акредитації включає подання заявки та пакету документів з боку університету до обраного агентства з оцінювання якості. Паралельно університет здійснює процедуру самооцінювання за критеріями та показниками, розробленими незалежним агентством. Здійснюючи акредитаційний самоаналіз, вищий навчальний заклад визначає відповідність освітніх послуг відповідним критеріям.

Проведення самооцінювання та складання звіту (Self-Evaluation Report) дає можливість освітній установі визначити свої сильні та слабкі сторони з організації освітнього процесу, усвідомити доцільність вибору організацій для проведення практик, та оцінити результати зв’язків із роботодавцями та своїми випускниками. Звіти університетів відсилаються на розгляд у незалежне агентство з оцінювання якості.

Результати незалежної акредитації дають підстави для доцільності візиту експертної комісії до навчального закладу. Зазвичай дії акредитаційної комісії

спрямовані на усунення невідповідностей освітніх програм та/або навчальної діяльності університетів стандартам якості у сфері вищої освіти.

На етапі визначення перспективних напрямів розвитку вищий заклад освіти звертається до незалежних експертів, аудиторів академічних послуг з метою отримання допомоги. Як правило, це люди, які працюють за спорідненими спеціальностями в інших навчальних закладах, члени професійних асоціацій, працівники агенцій з академічного аудиту та відділів ліцензування. Проводиться розширений моніторинг системи управління навчальним закладом, всіх рішень, що приймалися щодо освітньої діяльності, та отриманих результатів.

Кінцевим результатом роботи акредитаційної комісії є висновок із зауваженнями та практичними рекомендаціями, які передбачають шляхи подолання виявлених недоліків. Рішення про можливість надання акредитаційного сертифікату щодо відповідності визначеним стандартам якості вищої освіти навчальному закладу приймається незалежною агенцією за підсумками всіх етапів незалежного оцінювання (Полухін, 2010).

Наступним етапом є аналіз можливостей навчального закладу забезпечувати підготовку фахівців відповідно до сучасних вимог економічного розвитку країни та ІТ-галузі. Для цього відбуваються періодичні відвідування університету експертами вподовж 2-х років з метою аналізу змін підготовки суб’єктів освітнього процесу, аналізуються відзиви випускників, роботодавців щодо рівня підготовленості контингенту навчального закладу, вивчається думка громадськості про якість наданих освітніх послуг. Завершальний етап презентує висновки щодо відповідності показників освітньої діяльності вимогам з акцентом на позитивних зрушеннях, акцентується увага на поліпшенні якісних показників підготовки, отриманих під час комплексної перевірки.

Матеріали акредитаційної справи можуть повертатися на доопрацювання. Експерти, як правило, готують запити щодо надання додаткової інформації, коментарі, тому період акредитації триває до року. Необхідно зазначити, що в

американських університетах акредитація займає більше часу і має на відміну від української практики систематичний, планомірний характер її реалізації, що дозволяє розглядати її як процес, спрямований на постійне удосконалення надання освітніх послуг (Полухін, 2010, с. 86).

Система оцінювання діяльності на рівні вищого навчального закладу передбачає різноманітні форми здійснення контролю (комп'ютерні та паперові тести, анкетування) з метою оцінювання як академічних досягнень студентів, так і їхнього ставлення до освітнього процесу, а також є провідною умовою забезпечення якості підготовки.

Вартим уваги вважаємо практику попереднього анкетування студента на предмет базових знань перед початком навчання за освітньою програмою. Оцінювання показників у динаміці є надзвичайно важливим тому, що дозволяє об'єктивно охарактеризувати підготовчий рівень.

Головна мета анкетування – це зібрання інформації за декількома категоріями даних: демографічні відомості (вік, стать), що спрямовані на встановлення систематичних розбіжностей серед студентів на основі демографічних чинників; дані, що дозволяють спрогнозувати успішність засвоєння програми щодо оволодіння рідною мовою, навичками набору тексту, технічних базових знань, рівня шкільної освіти.

Для виявлення позитивної або негативної динаміки навчання проводиться тестування з базових знань студентів бакалаврської програми, що перевіряє їхні знання на початку навчання. Тест складається із коротких запитань з фахових проблем, на які студенти дають розгорнути відповіді і на основі перевірки яких експерти дають висновки. Оцінювання знань за такою моделлю (розгорнуті відповіді на короткі запитання) допомагає більш глибоко оцінити рівень знань й навичок, здатність бакалаврів до аналізу та синтезу. Таким чином, тест базових знань є формою одержання зворотного зв'язку для корекції помилкових дій у випадку недостатньої успішності студентів.

Зазначимо, що поточний контроль у вищих навчальних закладах США може проводитись у формі тестової самоперевірки отриманих знань за

пройденою темою. Так, в інституті технологій Стівенс (Stevens Institute of Technology) у штаті Нью Джерсі тести з навчальної дисципліни «Системний аналіз» передбачають розгорнуті відповіді на короткі запитання для перевірки знань з системного аналізу та вимагають розв'язання декількох завдань, пов'язаних з предметом вивчення специфічної проблеми (Stevens Institute of Technology, 2017).

У навчальному закладі також проводиться анкетування студентів після закінчення програми, яке має на меті з'ясування їхньої думки щодо якості змісту навчання, актуальності умінь, яких вони набули у процесі підготовки в університеті. У результаті навчання бакалаври дають оцінку тому, скільки часу у них зайняло вивчення певної дисципліни, характеризують виконання окремих видів навчальної діяльності та своє ставлення до проходження практики як важливого компоненту освітнього процесу. Рейтингово-екзаменаційний контроль (підсумковий контроль з метою оцінювання отриманих бакалаврами знань за семестр та їхньої атестації) проводиться у формі комп'ютеризованого міждисциплінарного тесту, який також передбачає надання розгорнутих відповідей. Вважаємо за необхідне звернути увагу на те, що оцінювання знань і умінь здійснюється як за кожною навчальною дисципліною окремо, так і на загальному інтегративному рівні на основі міждисциплінарного підходу.

За кредитною системою американських університетів навчальний матеріал одного модуля відповідає одному заліковому кредиту. Зазначимо, що в університетах США, які здійснюють підготовку бакалаврів з кібербезпеки, упроваджено комбіновану систему оцінювання навчальних досягнень студентів, що поєднує кредити і оцінки (бали).

Усі студенти повинні пройти письмові іспити в кінці кожного терміну з основних курсів, з усіх технічно-інженерних, гуманітарних чи управлінських дисциплін, що вивчаються факультативно та за вибором.

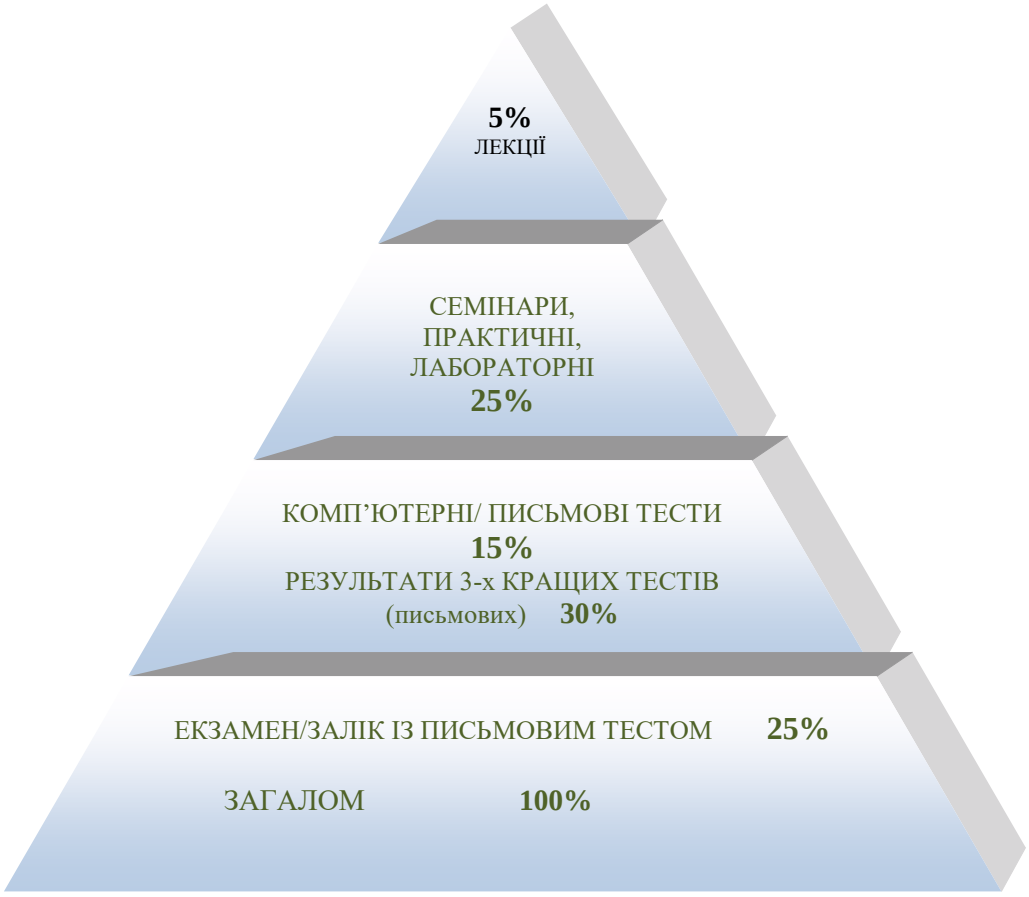


Рис 3.3.1. Сумарний семестровий бал у відсотках за видами занять за курс дисципліни (укладено автором на основі: Романовський, 2002).

На рисунку 3.3.1. представлений загальноприйнятий розподіл балів за видами занять та тестування знань у відсотках для одержання сумарного семестрового балу за курс дисципліни. Зазначимо, що на відвідування лекцій відводиться лише 5 % від загальної оцінки, за відвідування семінарів та виконання практичних та / або лабораторних робіт студенти можуть одержати 25 % від загального балу; виконання тестів (комп'ютерних / письмових) надає додаткові 15 %; високо оцінюються результати трьох кращих щомісячних письмових тестів, на які відводиться 30 %, іспит або залік із письмовим тестом складає 25 %, що дає загальний бал 100 % (Романовський, 2002, с. 107-108).

Проаналізовані матеріали свідчать, що викладачі вищих навчальних закладів здійснюють оцінювання результатів навчання студента відповідно до розширеної шкали оцінювання, що представлена у таблиці 2.4.

Таблиця 3.3.2.

Шкала оцінювання результатів навчання студента у Stevens Institute of Technology (Stevens Institute of Technology, 2017).

Оцінка	A	A-	B+	B	B-	C+	C	C-	D+	D	F
Кількість балів	4	3,67	3,33	3,00	2,67	2,33	2,00	1,67	1,33	1,00	0

Оцінка	P	F	W	Exc
Тлумачення	Складено	не складено	анульовано	звільнено лікарем

Шкала передбачає розподіл за 4-бальною системою, оцінки містять вказані показники якості за кредит на кшталт: A (4.00) – відмінно, B (3,00) – добре, C (2.00) – задовільно, D (1.00) – прохідна, F (0,00) – недостатньо. Оцінка P вказує, що курс пройдено успішно і складено, тоді як F – не складено.

Якщо курс анулюється, за 1 тиждень до останнього заняття семестру ставиться оцінка W; якщо студента звільнив лікар від відвідування фізичної культури ставиться Exc. (скорочено від анг. *excluded*), оцінка Abs. (*absent*) ставиться за відсутність на заняттях; Inc. (*incomplete*) – за їх неповне відвідування.

В Інституті Стівенс система оцінювання якості навчання здійснюється шляхом виведення середнього значення оцінки (GPA). Розрахунок відбувається таким чином: сума балів ділиться на суму відвіданих годин. Для визначення балу якості будь-якого курсу семестрові години множаться на середнє значення оцінки, отриманої за курс.

Таким чином, у процесі вивчення певної дисципліни студент накопичує відсотки. За результатами йому в електронну залікову книжку виставляється оцінка (облік успішності здійснюється за допомогою комп’ютера). Наприклад, якщо навчальну дисципліну оцінено у 3 кредити, і за результатами контрольних заходів студент отримує оцінку «відмінно», то до залікової книжки йому буде внесено 4×3=12 балів. При цьому, що якщо студент набирає 90 % і більше, він

отримує оцінку A; якщо його навчальні досягнення в межах між 80 % і 90 % – B; між 70 % і 80 % – C; між 60 % і 70 % – D. У випадку, коли за результатами навчання студент набрав менше 60 %, він отримує «незадовільно» – F.

Отже, можна констатувати, що система оцінювання діяльності вищих навчальних закладів США функціонує на федеральному, галузевому та локальному (інституційному) рівнях. Використання різних механізмів контролю діяльності навчальних закладів в цілому спрямовано на підвищення ефективності та якості функціонування вищої освіти.

Висновки до розділу 3

Здійснений аналіз дав змогу виявити специфічний підхід у процесі підготовки бакалаврів з кібербезпеки, що полягає у його зорієнтованості на поєднанні теоретичних знань та практичних умінь через посилення зв’язків навчального закладу з установами, які є потенційними місцями роботи випускників. Виявлено, що ефективність підготовки бакалаврів зі спеціальності «Кібербезпека» в університетах США забезпечується як єдністю міждисциплінарного, практико-орієнтованого, інтегративного та проблемно-аналітичного підходів до навчання, так і цілеспрямованим формуванням мотивації студента та втіленням відповідного новим формам організації праці в умовах інноваційного підходу до кіберзахисту.

За результатами компаративістського аналізу на змістовому рівні виявлено, що професійна підготовка бакалаврів з кібербезпеки США спрямована на професійний розвиток студента, активізацію навчально-пізнавальної діяльності та ґрунтується на принципах зв’язку теорії і практики, системності, професійної спрямованості навчання, варіативності, вільного вибору, циклічності, модульності, міждисциплінарності, кар’єрної орієнтації, випереджувального навчання. Визначено основні особливості змісту навчальних програм з підготовки бакалаврів з кібербезпеки в США: впровадження дисциплін, пов'язаних з розслідуванням кіберінцидентів; збільшення частки матеріалу, орієнтованого на правозастосовні та ті, що

засновані на міжнародному праві, педагогічні технології; включення дисциплін, зміст яких спрямований на впровадження технологій кібербезпеки в бізнес, електронну комерцію, комерційне застосування інтелектуальних прав. Формування знань, умінь і навичок забезпечується у межах загальнопрофесійної, професійно-практичної, спеціальної (фахової) підготовки та дисциплін за вибором. Важливо зазначити, що в американській системі навчання фахівців у галузі кібербезпеки дотримуються широкого профілю підготовки, що значно поширює кар'єрні можливості. Пріоритетним є міждисциплінарний принцип, який зумовлює у професійній підготовці бакалаврів з кібербезпеки інтегративні процеси щодо використання структурних елементів наукового знання одного циклу дисциплін в іншому.

Практична підготовка базується на принципах інтеграції знань, умінь, навичок, адаптації, випереджувального навчання, наближення до реальних умов. Визначено, що особливістю практичної складової опанування фаху є те, що студенти проходять практичну підготовку протягом всього терміну навчання, виконуючи різноманітні завчання (пошук літератури, складання плану досліджень, проведення конструкторської роботи за спеціальністю, проходження стажування) в умовах промисловості, державних, приватних або бізнес-структурах. Практична підготовка є основою для здобуття студентами досвіду практичної роботи, розвитку професійного мислення. Забезпечення якісної практичної підготовки можливе за умов поєднання зусиль різних підрозділів та бажання студента відповідати вимогам.

Очікуваними результатами опанування освітньої програми є сформовані професійні компетенції (фахові, технологічні) та базові цінності. Узагальнено вимоги до бакалаврів спеціальності «Кібербезпека», а саме: розуміння важливої термінології, знання та вміння з використання сучасних матеріалів та технологій; мати досить високу практичну майстерність; вміти проводити моніторинг систем безпеки; вміти оперувати заходами безпеки; володіти аварійним відновленням даних ІТ-продукту; професійно досліджувати нові ІТ-

продукти та послуги; впроваджувати нове програмне забезпечення та/або технології; проводити регулярні перевірки на відповідність використання.

З'ясовано, що забезпечення якості професійної підготовки фахівців кібербезпеки досягається завдяки поєднанню традиційних (лекції, практикуми, семінари, лабораторні заняття з елементами дослідження, конференції, консультації) та інноваційних форм (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); використанню інтерактивних методів (дискусія, «круглий стіл», «засідання експертної групи», «дебати», «форум», метод «від зворотного», ситуаційного навчання, рольова гра, аналіз кризових ситуацій (кібератак, ризиків кіберзагроз)), інформаційно-комунікативних технологій, забезпечення освітнього процесу інноваційними матеріально-технічними ресурсами.

Важливим висновком є те, що в США система забезпечення якості вищої освіти здійснюється на трьох рівнях: на рівні вищого навчального закладу, федеральному (державна і державно-суспільна система контролю) та галузевому. Основні критерії аудиту стосуються насамперед відповідності освітніх програм вимогам суспільства щодо підготовки фахівців у галузі та забезпеченості матеріальними, науково-методичними, кадровими ресурсами освітнього процесу та ефективності управління університетом. Зовнішнє оцінювання проводять незалежні агенції, створені за ініціативою професійних асоціацій та університетів. Рішення щодо необхідності проходження акредитації є рішенням навчальної установи і приймається вищим навчальним закладом самостійно на добровільній основі.

Результати дослідження, відображені у розділі, викладено у публікаціях автора: Бистрова, 2017a; Бистрова, 2017j; Бистрова, 2018b; Bystrova, 2018a.

РОЗДІЛ IV. ПЕРСПЕКТИВНІ НАПРЯМИ ВДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ В УКРАЇНІ

У розділі розглянуто сучасний стан підготовки бакалаврів з кібербезпеки у закладах вищої освіти України; здійснено порівняльно-педагогічний аналіз особливостей професійної підготовки бакалаврів з кібербезпеки України і США; з'ясовано можливості творчої реалізації конструктивних ідей американського досвіду в системі вищої освіти України.

4.1. Становлення і розвиток професійної підготовки фахівіц із кібербезпеки в Україні

Особливість функціонування сучасного суспільства полягає в тому, що сьогодні практично не існує організацій, закладів, установ, професійних об'єднань та інших інституцій, які б не потребували фахівців у галузі інформаційних технологій. Оскільки в Україні підготовка та підвищення кваліфікації фахівців із кібербезпеки є відносно новим освітнім напрямом, виникає потреба в обґрунтуванні нормативно-правової основи, окресленні перспектив удосконалення цієї галузі, визначення методологічних орієнтирів розвитку. Необхідно зауважити, що феномен кібернетичної безпеки полягає в її бінарному характері. З одного боку, вона може розглядатись як елемент національної безпеки; з іншого, як явище глобалізоване, адже інформаційний простір є безмежним, для нього не існує кордонів, тому злочини в цій сфері здебільшого кваліфікуються як транснаціональні. Це означає, що питання підготовки та підвищення кваліфікації фахівців у цій галузі є принципово важливим не лише для України, а й для світової спільноти загалом (Діордіца, 2017, с. 199-203).

Необхідність підготовки фахівців у галузі кібербезпеки загострюється у зв'язку із політичною ситуацією в нашій країні та застосуванням методів гібридної війни, що використовуються Російською Федерацією. 8 лютого 2018 р. Палата Представників Конгресу США схвалила проект «Закону про

співпрацю з Україною з питань кібербезпеки» (Палата Представників Конгресу США, 2018), що спрямований на просування активнішої взаємодії між Україною і США у галузі кібербезпеки в умовах протидії російської гібридної агресії. Документ передбачає надання допомоги Україні в удосконаленні стратегії кібербезпеки, зокрема щодо посилення захисту комп'ютерних мереж органів державної влади, зменшення залежності України від російських інформаційний та комунікаційних технологій, сприяння участі України у програмах обміну інформацією.

Основні стратегічні цілі та напрями розвитку інформаційного суспільства в Україні визначені Законом України № 537-V від 9 січня 2007 р. «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Відповідно до цього закону окреслено такі пріоритети: «забезпечення державної підтримки у прискоренні розробки, впровадженні та використанні інформаційно-комп'ютерних технологій в усіх сферах суспільного життя; забезпечення комп'ютерної та інформаційної грамотності населення; створення загальнодержавних інформаційних систем; розвиток національної інформаційної інфраструктури та її інтеграція із світовою інфраструктурою; збереження культурної спадщини України шляхом її електронного документування» (Закон України, 2007). У Ст. 8 розділу 3 визначено завдання організації освітньої діяльності у ВНЗ України з професійної підготовки фахівця для роботи в інформаційному суспільстві та шляхи його реалізації.

Нормативно-правові засади професійної підготовки фахівців з кібербезпеки регулюються Законами України «Про освіту» та «Про вищу освіту». Зокрема відповідно до Ст. 13 Закону України «Про вищу освіту» на центральний орган виконавчої влади у сфері освіти й науки, інші органи, до сфери управління яких належать вищі навчальні заклади, покладаються такі функції, як: проведення аналітико-прогностичної діяльності у сфері вищої освіти, визначення тенденцій її розвитку, впливу демографічної, етнічної, соціально-економічної ситуації, інфраструктури виробничої й невиробничої сфери, формування стратегічних напрямів розвитку вищої освіти з урахуванням

науково-технічного прогресу та інших факторів, узагальнення світового й вітчизняного досвіду розвитку вищої освіти (Про вищу освіту: Закон України, 2014). Методологічне забезпечення використання новітніх технологій у процесі професійної підготовки фахівців для ІТ-галузі, удосконалення основних шляхів розв'язання визначених проблем може бути досягнуто шляхом надання освіти населенню країни відповідно до пріоритетів сьогодення як загальних, так і спеціальних: адаптація до інформаційних систем через знання, модернізація вищої освіти, розроблення нових освітньо-професійних планів, запровадження нових спеціальностей для ІТ-галузі. У розділі «Аналіз підготовки фахівців з інформаційної безпеки в Україні» описані результати досліджень, які показують, що для створення навчальних закладів певної спрямованості необхідно більше 15 років, тоді як для часткової зміни їх завдань у межах традиційної спрямованості, розгортання і упровадження в освітній процес нових навчальних комплексів, формування контингенту студентів необхідно 8-4 роки (Інформаційна Безпека, 2010).

Зауважимо, що система підготовки фахівців є достатньо консервативною і характеризується інерцією, що необхідно враховувати у ході модернізації системи вищої освіти загалом і системи підготовки фахівців ІТ-галузі зокрема. Всі зміни в системі підготовки відбуваються з урахуванням галузевих потреб і галузевих вимог та особливостей змін ІТ-галузі на світовому рівні і відповідно до нового переліку напрямів, за якими здійснюється підготовка фахівців у закладах вищої освіти за освітньо-кваліфікаційними рівнями «бакалавр» і «магістр». Ураховуючи те, що підготовка фахівців з вищою освітою у галузі інформаційної безпеки взагалі була розпочата лише у 1997 році, вона вирізняється інноваційністю і водночас є найбільш динамічною за об'єктом діяльності.

На сьогодні в галузевих стандартах недостатньо враховують стан та перспективи використання методів та засобів підготовки фахівців з кібернетичної безпеки. Постає проблема створення профілю професійної

підготовки бакалаврів щодо кібернетичної безпеки відповідно до найновіших досягнень у галузі розбудови кіберпростору та гарантій кібербезпеки.

Більш детально проаналізуємо особливості підготовки фахівців із захисту інформації в інформаційно-комунікаційних системах за напрямом підготовки 6.170101 – «Безпека інформаційних і комунікаційних систем» відповідно до потреб реального сектору економіки фахівців із захисту інформації в інформаційно-комунікаційних системах. У сучасних умовах сфера професійної діяльності такого фахівця включає, як відомо, сфери науки, техніки й технології, що охоплюють сукупність проблем, пов'язаних із забезпеченням не лише інформаційної, а і кібернетичної безпеки, а також захищеності інформаційного і кіберпросторів держави в цілому або окремих об’єктів їх інфраструктури від ризику стороннього кібернетичного впливу (Богуш & Кривуца, 2004).

Об'єктами його професійної діяльності при цьому є:

− об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні й інформаційно-аналітичні системи, інформаційні ресурси й інформаційні технології в умовах існування кіберзагроз в інформаційній сфері;

− технології забезпечення кібербезпеки об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), які пов'язані з інформаційними технологіями, що використовуються на цих об'єктах;

− процеси управління інформаційною і кібербезпекою об'єктів, що захищаються.

Ураховуючи важливість варіативної частини наявних освітньо-професійних програм підготовки фахівців, що регламентуються нині галузевими стандартами вищої освіти України, необхідно передбачити можливість викладання низки дисциплін, таких, як: «Кібернетичний простір»; «Інформаційні технології та системи кібернетичного простору»; «Технологія організації збору та добування інформації у кіберпросторі, її обробки аналізу і

синтезу»; «Основи автоматизації процесів інформаційної діяльності у кібернетичному просторі» (Бабак, Козловський, Хорошко&Чирков, 2001).

Результатом підготовки фахівців за відповідними програмами має бути формування *компетенцій* (соціально-особистісних, інструментальних, загальнонаукових та професійних), *виробничих функцій* (організаційних, управлінських, дослідницьких, прогностичних, технічних, технологічних, контрольних та функцій щодо проектування) та *вмінь*, якими має володіти випускник-бакалавр, що фактично закладає фундамент для підготовки професіоналів із організації кібернетичної безпеки.

Запровадження згідно з Постановою Кабінету Міністрів України від 29.04.2015 р. № 266 нової спеціальності «Кібербезпека» зумовлює необхідність теоретичного осмислення освітніх стандартів підготовки фахівців зазначеного напряму (Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29.04.2015 р. № 266 (зі змінами, внесеними згідно з постановою Кабінету Міністрів України від 27.09.2016 р. № 674). Проте тому, що спеціальність «Кібербезпека» упроваджено вперше, існують проблеми щодо проектування освітніх стандартів підготовки фахівців з кібербезпеки і як взірець може слугувати лише зарубіжний досвід підготовки аналогічних фахівців.

На думку українських фахівців з інформаційної та кібернетичної безпеки В. Бурячка (2015) та В. Богуша (2004), найбільш цікавими з точки зору майбутніх роботодавців можуть стати знання, які стосуються теоретичних основ кібернетичної безпеки, правових та організаційних засад протидії кіберзлочинності, методів та засобів протидії кіберзлочинності, програмного забезпечення систем кібернетичної безпеки, криптографічних механізмів кібернетичної безпеки, кібернетичної безпеки підприємств, основ кібернетичної безпеки держав тощо.

Зауважимо, що на сьогодні відбулася трансформація вимог за освітніми стандартами з урахуванням принципу автономії навчальних закладів. На

відміну від попередніх стандартів, які передбачали певний набір нормативний дисциплін із визначеною кількістю годин, стандарти нового покоління орієнтовані на результати навчання, а зміст освіти має формувати вищий навчальний заклад. Таким чином, університет відповідає за якість підготовки свого випускника, за його конкурентоспроможність на ринку праці.

Однак Законом України «Про вищу освіту» передбачено, що Міністерство освіти і науки України «формує перелік галузей знань і перелік спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, зокрема за поданням Національного агентства із забезпечення якості вищої освіти, та подає їх на затвердження» (Про вищу освіту: Закон України, 2014). Тобто у Законі визначено, що не всі повноваження щодо запровадження спеціальностей і спеціалізацій віддано університетам, що є стандартною практикою в західних університетах.

Основною проблемою стандартизації підготовки фахівців у сфері кібербезпеки є її наявність поза межами чітко визначеного правового поля. Така діяльність не передбачена ні державними стандартами, зокрема Класифікатором видів економічної діяльності, Класифікатором професій, ні чітко визначеними кваліфікаційними характеристиками, затвердженими в установленому порядку на державному рівні. Тому під час проведення профорієнтаційної роботи заклади вищої освіти по-своєму тлумачать приблизні переліки посад, які обійматиме випускники. Наприклад, у Сумському державному університеті відкрили нову спеціальність – «Кібербезпека». На сайті університету зазначається, що після закінчення навчання за спеціальністю «Кібербезпека» випускники зі ступенем бакалавра можуть бути фахівцями з розроблення й тестування програмного забезпечення, фахівцями з інформаційних технологій, фахівцями з розробки комп'ютерних програм, техніками із системного адміністрування (ОПП Сумського державного університету, 2017).

Про необхідність розроблення стандартів для спеціальності «Кібербезпека» свідчить те, що у жовтні 2016 р. в Міністерстві освіти і науки

України за участю Л. Гриневич відбувся круглий стіл, присвячений підготовці фахівців зі спеціальності «кібербезпека». Міністр наголосила на демонстрації нових підходів до стандартів вищої освіти, що створюються завдяки взаємодії з роботодавцями і тими, хто формує замовлення на певні професійні кваліфікації. Такий підхід до укладання нових стандартів вищої освіти України, які б регламентували галузеві кваліфікаційні вимоги до соціально-виробничої діяльності випускника ВНЗ за напрямом 6(7,8).170101 – «БІКС» має ґрунтуватися на положеннях щодо кібернетичної безпеки та державних вимогах до властивостей і якостей особи, яка здобула вищу освіту з цього напряму. У стандарті має бути визначено термін і зміст навчання та нормативні форми державної атестації, а також встановлено вимоги до змісту, обсягу й рівня освіти та професійної підготовки такого випускника.

Упровадження стандартів підготовки зазначених фахівців дозволить сформувати у нього такі основні компетенції:

− здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства, застосовувати досягнення інформатики й обчислювальної техніки, проводити цілеспрямований пошук і збір інформації з відкритих джерел, а також її добування з відносно-відкритих і закритих електронних джерел;

− здатність виявляти ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;

− здатність організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації й економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації;

− здатність протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ-систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;

− здатність організовувати проведення атестації об'єкта на відповідність вимогам державних або корпоративних нормативних документів;

− здатність брати участь у розробленні підсистем управління інформаційною і кібербезпекою, здійснювати їх адміністрування й експлуатацію;

− здатність до проведення попереднього техніко-економічного аналізу й обґрунтування проектних рішень щодо забезпечення кібербезпеки;

− здатність оформлювати технічну документацію з урахуванням чинних нормативних і методичних документів в області інформаційної і кібербезпеки;

− здатність до програмної реалізації алгоритмів рішення типових завдань забезпечення інформаційної і кібербезпеки й до застосування програмних засобів системного, прикладного й спеціального призначення;

− здатність проводити аналіз інформаційної безпеки об'єктів і систем з використанням вітчизняних і закордонних стандартів;

− здатністю формувати комплекс мір (правила, процедури, практичні прийоми та ін.) для керування інформаційною і кібербезпекою тощо (додаток Ж, таблиця Ж-1).

Організація освітньої діяльності у закладах вищої освіти України здійснюється згідно із Законами України «Про освіту», «Про вищу освіту», державними та галузевими стандартами й іншими чинними нормативними документами. Розглянемо зміст навчання зі спеціальності 125 «Кібербезпека» / 125 «Cyber Security» у галузі знань 12 «Інформаційні технології»/12 «Information technologies» за ступенем вищої освіти «бакалавр», реалізація якого здійснюється відповідно до вимог галузевого стандарту вищої освіти з підготовки бакалаврів (наказ МОН Україні № 492 від 15.06.2004 р.).

На думку І. Зязюна (2005), грані соціальних виявів професійно-педагогічної якості (ППЯ) зазвичай описуються за допомогою таких відомих категорій, як: «кваліфікація», «компетентність», «компетенція» тощо (Зязюн, 2005, с.13). Кваліфікація і компетентність – своєрідні соціально-професійні характеристики, які задають межі й рівень функціональних дій у професії. Вони

визначені нормативно і контролюються соціумом у ході різних атестаційних актів. Кваліфікація формально зумовлюється типом одержаної освіти та документами, що дають право на роботу зі спеціальності, а також слугує основою для надання висхідного тарифного розряду. Кваліфікаційна характеристика фахівця певним чином пов'язана з рівнем освіченості й формує деякі кваліфікаційні очікування, зокрема з приводу технологічної готовності до виконання певних функцій. Однак сам по собі документ про освіту не дає гарантії якості наступної роботи.

Компетентність можна схарактеризувати як здатність вирішувати професійні завдання, що вимагає наявності реальних знань, умінь, навичок, досвіду. Вона виявляється безпосередньо у професійній діяльності як системна характеристика і має чітко визначену структуру. Компетентність може мати кількісний вимір, зокрема за допомогою виокремлення рівнів. Повнота усвідомлення основ професії, механізмів і меж власної діяльності, будучи однією із суттєвих ознак майстерності, зумовлює формування здатності ставити і вирішувати (у межах своєї компетенції) професійні задачі будь-якого рівня складності (Зязюн, 2005).

На думку українського науковця з питань кадрового забезпечення IT-галузі С. Мельника (Мельник, 2016), актуальність підготовки фахівців з кібербезпеки в сучасному світі зумовлена впровадженням нових інформаційних технологій не тільки в економічній сфері. Енергетична безпека як складова національної безпеки, національна безпека в цілому залежать від організації кібербезпеки та контролю інтеграції кіберпростору. Вимоги до рівня професійної підготовки фахівців із кібербезпеки зумовлюється новими викликами часу, активною співпрацею України в боротьбі з міжнародним тероризмом визначають необхідність модернізації змісту й організації, введення нових інтегрованих програм професійної підготовки майбутніх фахівців управління кібербезпекою у вищих навчальних закладах.

Освітньо-професійна програма підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю розроблена відповідно до

Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII, Постанов Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р., «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р.№1187, «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)» від 23.03.2016 р. № 261, методичних рекомендацій «Розроблення освітніх програм» (Методичні Рекомендації, 2014).

Нині в Україні підготовку бакалаврів з кібербезпеки здійснюють такі заклади: Національний технічний університет України «Київський політехнічний інститут», Київській національний університет імені Тараса Шевченка, Київській національний економічний університет імені Вадима Гетьмана, Національний технічний університет «Харківський політехнічний інститут», Ужгородський національний університет, Університет банківської справи та інші заклади, які отримали ліцензію на підготовку фахівців за спеціальністю «Кібербезпека». Освітньою діяльністю в цьому напрямі займаються не лише державні заклади вищої освіти. Так, приватний освітній заклад Kyiv Cyber Academy позиціонує себе як єдиний в Україні навчальний заклад, який готує «фахівців за визнаними міжнародними стандартами» (ОПП, Kyiv Cyber Academy, 2017).

Освітньо-професійна програма визначає передумови доступу до навчання, орієнтацію та основний фокус програми, обсяг кредитів ЄКТС, необхідний для здобуття освітнього ступеня бакалавра, перелік загальних та спеціальних (фахових) компетентностей, нормативний і варіативний зміст підготовки фахівця, викладених у результатах навчання та вимогах до контролю якості вищої освіти; принципи цілісності, логічної послідовності, комплексності, поєднання теоретичних положень із практичними навичками.

Європейська кредитна трансферно-накопичувальна система (ЄКТС) – система трансферу і накопичення кредитів, що використовується в

Європейському просторі вищої освіти з метою надання, визнання, підтвердження кваліфікацій та освітніх компонентів і сприяє академічній мобільності здобувачів вищої освіти (частина перша Ст. 1 Закону України «Про вищу освіту»). Методичне забезпечення залежить від виду контролю: вхідний (визначає початковий рівень набутих знань та сформованих умінь студентів); поточний контроль як аудиторної, так і самостійної роботи студентів; підсумковий контроль (диференційований залік, іспит). Передбачається також обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти. Загальний обсяг освітньо-професійної програми здобуття першого (бакалаврського) рівня вищої освіти «бакалавр» за спеціальністю 125 «Кібербезпека», становить 240 кредитів ЄКТС (табл. 4.1.1).

Таблиця 4.1.1.

Загальний обсяг освітньо-професійної програми для здобуття освітньо-кваліфікаційного рівня «бакалавр» за спеціальністю 125 «Кібербезпека» в Україні (укладено автором на основі: ОПП Житомирського ДТУ, 2017)

Зміст підготовки	***Кількість кредитів ЄКТС***	
ОБОВ'ЯЗКОВА ЧАСТИНА	**178 кредитів**	**74%**
■ Загальна підготовка	53 кредити	30%
■ Професійна підготовка	125 кредитів	70%
ВИБІРКОВА ЧАСТИНА	**62 кредити**	**26%**
■ Загальна підготовка	6,5 кредиту	10%
■ Професійна підготовка	54 кредити	87%
■ Атестація – екзамен з фаху	1,5 кредиту	3%
ЗАГАЛОМ	240 кредитів	

Особа має право здобувати освітньо-кваліфікаційний рівень «бакалавр» за умови наявності в неї повної загальної середньої освіти або ступеня молодшого бакалавра. Професійна підготовка фахівців з кібербезпеки включає практику, яка є завершальним етапом формування професійних якостей бакалавра з кібербезпеки та дає оцінку його готовності до виконання функціональних обов'язків. Результатом навчальної підготовки бакалаврів з кібербезпеки є виконання дипломної роботи, що містить науково обґрунтовані теоретичні

(експериментальні) результати та висновки. Теоретична підготовка включає опанування навчальних дисциплін – загальних та професійно-практичних (фахових).

Вимоги галузевого стандарту вищої освіти з підготовки бакалаврів ІТ-галузі передбачають наступний перелік компетентностей випускника ОКР «бакалавр» спеціальності 125 «Кібербезпека»: компетентності соціально-особистісні, інструментальні компетентності, загальнонаукові компетентності та спеціалізовано-професійні компетентності. У результаті аналізу ОПП на здобуття освітньо-кваліфікаційного рівня «бакалавр» зі спеціальності 125 «Кібербезпека» охарактеризовано кожний блок компетентностей, що систематизовано у додатку Б.

Фахівець з кібербезпеки повинен володіти особистісно-професійними якостями та компетенціями: сприймати як особисту цінність ідеї технологізації професійної підготовки в ВНЗ в межах компетентнісного підходу; володіти змістом професійної освіти, зокрема іноземною мовою на професійному рівні.

Проведений аналіз освітньо-професійної програми на здобуття освітньо-кваліфікаційного рівня бакалавр зі спеціальності «Кібербезпека» дозволяє визначити дисципліни циклів гуманітарної та соціально-економічної, фундаментальної, природничо-наукової професійної та практичної підготовки. У документі міститься інформація про те, що бакалавр зі спеціальності 125 «Кібербезпека» підготовлений для продовження освіти за магістерською програмою, а також до практичної діяльності; адже бакалавр з кібербезпеки є фахівцем з питань захисту кіберпростору.

В освітньо-професійній програмі подано дефініцію поняття кваліфікації як офіційного результату оцінювання і визнання факту здобуття освітньо-кваліфікаційного рівня «бакалавр». Згідно з ОПП диплом бакалавра видається здобувачу у випадку, коли уповноважена установа (компетентний орган) встановила, що особа досягла: компетентностей (результатів навчання) за заданими стандартами відповідно до вимог Закону України «Про вищу освіту»

(Ст. 1, Ч. 1.); очікуваного рівня кваліфікаційної навчально-наукової роботи, яка передбачена на завершальному етапі.

Про відповідність набутих здобувачами результатів навчання (компетентностей) першому рівневі вищої освіти свідчать форми кваліфікаційної роботи, що визначені стандартами вищої освіти, а саме:

а) дипломна робота;

б) публічна демонстрація (захист);

в) сукупність наукових статей;

г) комбінація різних форм вище зазначеного тощо;

ґ) та кваліфікаційний рівень, як структурну одиницю національної рамки кваліфікацій, що визначається певною сукупністю компетентностей, які є типовими для кваліфікацій даного рівня.

Внутрішнє забезпечення якості вищої освіти полягає у виконанні важливих процедур і реалізації заходів щодо забезпечення якості підготовки здобувачів вищої освіти ОКР «бакалавр» зі спеціальності 125 «Кібербезпека», які узагальнено та систематизовано у табл. 4.1.2.

Таблиця 4.1.2.

Узагальнення процедур і заходів щодо забезпечення якості підготовки здобувачів вищої освіти ОКР «бакалавр» зі спеціальності 125 «Кібербезпека» (укладено автором на основі ОПП Stevens Institute of Technology, 2017).

ЗМІСТ ВИМОГ ТА ПРОЦЕДУР СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ
■ здійснення моніторингу та періодичного оновлення освітніх програм;
■ забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; ■ забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;
■ щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному web-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб; ■ забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
■ забезпечення наявності необхідних ресурсів для організації освітнього процесу, зокрема самостійної роботи студентів, за кожною освітньою програмою ■ забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників.

Однією з основних умов ефективної організації професійної підготовки фахівців є вимоги до науково-педагогічних працівників, які забезпечують навчання здобувачів вищої освіти першого (бакалаврського) освітньо-кваліфікаційного рівня зі спеціальності 125 «Кібербезпека». Викладання навчальних дисциплін обов'язкового циклу забезпечують доктори наук, професори, кандидати наук, доценти, які мають певний стаж практичної, наукової та педагогічної роботи. Доцільно, щоб більшість викладачів, які викладають дисципліни циклу науково-природничої, професійної та практичної підготовки, мали наукові ступені в галузі технічних наук.

Процес вивчення обов'язкових дисциплін забезпечується методичними комплексами, що складаються з підручників, методичних розробок до практичних занять, лабораторних практикумів, методичних вказівок до самостійної роботи, методичних матеріалів до курсового проектування, прототипів розробки курсових проектів, екзаменаційних та тестових запитань різної складності (для самоперевірки, для іспитів, для тренінгів) тощо. Викладачі обов'язкових дисциплін повинні мати кваліфікацію відповідно до диплому про вищу освіту та спеціальність за дипломом про здобуття наукового ступеня, які відповідають або споріднені до спеціальності підготовки бакалаврів.

Для подальшого удосконалення професійної підготовки майбутніх фахівців з кібербезпеки у закладах вищої освіти України необхідно активніше упроваджувати сучасні технології навчання; створювати можливості для своєчасного і систематичного підвищення кваліфікації, стажування професорсько-викладацьким складом; використовувати конструктивні ідеї досвіду інших країн для подальшої їх імплементації в освітній процес закладів вищої освіти України.

4.2. Порівняльно-педагогічний аналіз професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США таУкраїни

В умовах інтенсифікації й загострення боротьби з кіберзлочинністю стратегічним завданням освітньої системи України є підготовка принципово нової генерації фахівців, які покликані захищати комп'ютерне середовище від злочинних посягань на економічні та політичні свободи держави. Відповідно системне зіставлення специфіки зарубіжного і вітчизняного досвіду підготовки фахівців з кібербезпеки може сприяти глибшому осмисленню наявних проблем, виправленню помилок і прорахунків, підвищенню ефективності освітньої діяльності українських закладів вищої освіти у напрямі професійної підготовки фахівців з кібербезпеки. Тому порівняльно-педагогічний аналіз досвіду професійної підготовки майбутніх фахівців з кібербезпеки у високорозвинених країнах, зокрема в США, сприятиме удосконаленню фахової підготовки ідентичних фахівців в Україні, встановленню відповідності європейським і світовим стандартам якості навчання. Об'єктивний аналіз досвіду США щодо підготовки кадрів з кібербезпеки може стати цінним джерелом для осмислення конструктивних ідей щодо формування сучасних освітніх стандартів підготовки, нової стратегії та розвитку національної вищої освіти у галузі професійної підготовки фахівців означеної спеціальності.

З метою здійснення ґрунтовного компаративістського дослідження було визначено критерії, за якими здійснювався порівняльно-педагогічний аналіз професійної підготовки фахівців з кібербезпеки у вищих навчальних закладах США та України: нормативно-правовий (до якого включено такі показники: закони, що регламентують професійну підготовку бакалаврів з кібербезпеки, стандарти та стратегії професійної підготовки); змістовий (передбачає дослідження таких показників як обсяг освітньо-професійних програм підготовки бакалаврів освіти, зміст і характеристика професійних компетентностей, цикли підготовки за навчальним планом, змістове наповнення практичної підготовки майбутніх фахівців з кібербезпеки); організаційний (містить особливості організації навчального процесу, вступних випробувань, практичної підготовки);

технологічний (включає форми, методи організації освітнього процесу вищих навчальних закладів, особливості оцінювання навчальних досягнень студентів у процесі оволодіння професійними компетентностями).

Основою для дослідження стали матеріали порівняльно-педагогічного аналізу професійної підготовки бакалаврів з кібербезпеки: нормативні документи, що регламентують підготовку фахівців, освітньо-професійні програми, навчальні плани, навчальні програми дисциплін, графіки організації освітнього процесу, положення про вступні випробування, положення про організацію освітнього процесу, положення про організацію та проведення практичної підготовки фахівців у закладах вищої освіти України.

Для порівняльного аналізу обрано 7 бакалаврських ОПП з кібербезпеки 4 американських університетів: Walden University (Університет Уалден), American Military University (Американський військовий університет), Embry-Riddle Aeronautical University (Авіаційний університет Ембрі Ріддл), St. John's University (Університет Сент Джон) та 3 коледжів: Mercy College (Коледж Мерсі), Iona College (Айона коледж), Saint Vincent College (Сент-Вінсент Коледж) з метою подальшого зіставлення особливостей системи підготовки здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» США та України (додаток В).

Здійснений порівняльно-педагогічний аналіз за нормативно-правовим критерієм показав, що на законодавчому, практичному і науковому рівнях понятійно-категоріальний апарат професійної діяльності у сфері кібербезпеки не є остаточно визначеним. Першим кроком на шляху до модернізації системи вищої освіти України щодо впровадження спеціальності 125 «Кібербезпека» ІТ-галузі було прийняття Постанови Кабінету Міністрів України від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», опублікованої в «Офіційному віснику України» у 2015 р., № 38, ст. 1147; та у 2016 р., № 79, ст. 2647. Відповідно до цього документу було скориговано перелік галузей знань і спеціальностей таким чином: зникла галузь знань 1701 «Інформаційна безпека» зі спеціальностями 170101 «Безпека інформаційних і комунікаційних систем»,

170102 «Системи технічного захисту інформації» та 170103 «Управління інформаційною безпекою»; для галузі знань 12 «Інформаційна безпека» визначено одну спеціальність 125 «Кібербезпека». Вид (види) діяльності затверджується відповідним державним органом, який забезпечує виконання завдань у сфері національної безпеки, за погодженням з МОН.

На думку фахівця сфери національної безпеки України С. Мельника (Мельник, 2016), зазначені напрями професійної діяльності суттєво розвиваються в останні три десятиліття, а сфера кібербезпеки – з 2000-х років (при цьому поняття національної системи кібербезпеки в Україні законодавчо закріплено лише у 2016 р.). Має місце факт: того, що на законодавчому, практичному і науковому рівнях тезаурус сфери кібербезпеки лише формується. Зрозуміло, що кібербезпека – це не лише технології, а передусім ресурс професійних фахівців, які мають справу як із створенням, так і з їх використанням.

Провідні заклади вищої освіти Україні, які позитивно та успішно зарекомендували себе у сфері підготовки фахівців у галузі «Інформаційна безпека» з підготовки бакалаврів зі спеціальностей «Безпеки інформаційних і комунікаційних систем», «Системи технічного захисту інформації» та «Управління інформаційною безпекою» автоматично здобули право підготовки здобувачів ОКР «бакалавр» зі спеціальності 125 «Кібербезпека», але тимчасово – до введення стандартів вищої освіти України.

Серед п’яти найкращих закладів вищої освіти України, що здійснюють підготовку фахівців з кібербезпеки:

- Національний авіаційний університет, в якому три кафедри здобули право підготовки фахівців з означеної спеціальності: кафедра безпеки інформаційних технологій, кафедра захисту інформації Навчально-наукового Інституту інформаційно-діагностичних систем та кафедра комп’ютеризованих систем захисту інформації Навчально-наукового Інституту комп’ютерних інформаційних технологій; (http://www.nau.edu.ua);

- Національний технічний університет України «КПІ імені Ігоря Сікорського», Фізико-технічний інститут, кафедра фізико-технічних засобів захисту інформації (http://lll.kpi.ua /ipo@ipo.kpi.ua/);
- Національний університет «Львівська політехніка», Інститут комп'ютерних технологій, автоматики та метрології, кафедра систем технічного захисту інформації (http://old.lp.edu.ua);
- Київський національний університет імені Тараса Шевченка, Факультет інформаційних технологій, кафедра кібербезпеки та захисту інформації (http://kbzi.knu.ua/).

Багато закладів вищої освіти здобули право на підготовку бакалаврів означеного фаху шляхом ліцензування. Наприклад, Житомирський державний технологічний університет вперше пройшов ліцензування з ОПП підготовки здобувачів ОКР «бакалавр» зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», що здійснюється на кафедрі комп’ютеризованих систем управління та автоматики (http://www.ztu.edu.ua.) та Тернопільський національний технічний університет імені Івана Пулюя (http://tntu.edu.ua/.).

У ході порівняльного аналізу структури освітньо-професійної програми ОКР «бакалавр» зі спеціальності «Кібербезпека» американських університетів та коледжів встановлено, що кожна з досліджуваних ОПП містить таку інформацію: назва вищого навчального закладу, реквізити; освітньо-кваліфікаційний рівень підготовки; галузь знань та спеціальність; вимоги до здобувачів при вступі до закладу вищої освіти та кваліфікаційні вимоги до випускника; загальна кількість кредитів/дисциплін за весь термін підготовки здобувача ОКР; загальна кількість кредитів/дисциплін, назва дисциплін, розподілених відповідно до різних циклів; власне цикли дисциплін (загальноосвітні, професійно-орієнтовані, фахові, вибіркові дисципліни та підсумковий цикл «Capstone course» або «Senior Seminar in Cybersecurity»), якщо такий планувався (додаток В; додаток Д).

Аналіз освітньо-професійних програм за змістовим критерієм професійної підготовки здобувачів ОКР «бакалавр» зі спеціальності

«Кібербезпека» для ІТ- галузі здійснено нами на основі оригінальних матеріалів, які є у доступі на сайтах вищих навчальних закладів. Американський вчений Дж. Ґоргон зазначає, що узагальнена модель навчального плану передбачає перелік взаємопов'язаних циклів дисциплін (Gorgone, Gray & Stohr, 2003).

Можемо зробити висновок, що навчальні дисципліни згідно з американською моделлю ОПП підготовки здобувачів ОКР «Бакалавр» означеної галузі – це насправді цілісна система взаємопов'язаних циклів (блоків) предметів для професійної підготовки компетентного фахівця, сутність якої відображено на рис. 4.2.1.

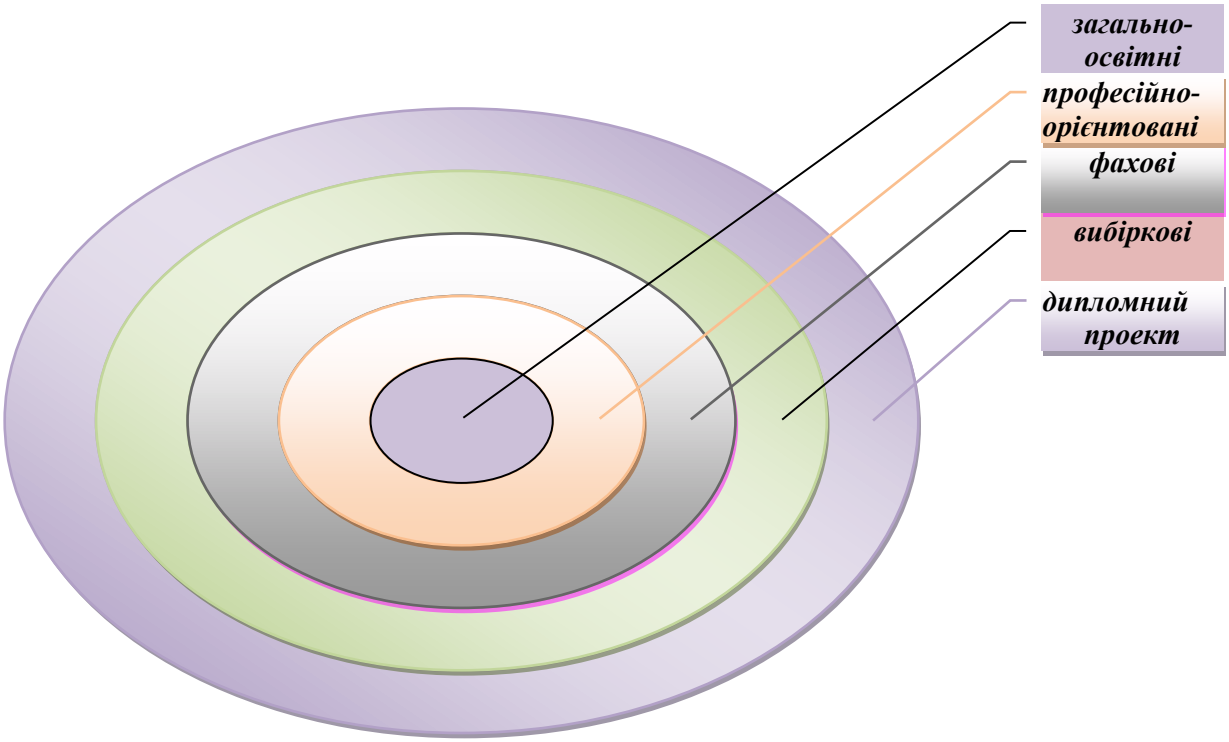


Рис.4.2.1.Узагальнена структура американської моделі ОПП підготовки здобувачів ОКР «Бакалавр» зі спеціальності «Кібербезпека» ІТ-галузі щодо взаємозв'язку циклів навчальних дисциплін (укладено автором на основі: ОПП Авіаційний університет Ембрі Ріддлі Університет Сент Джона, 2017).

Пройшовши ретельний відбір на відповідність вступних вимог, здобувач має можливість розпочати навчання на початковому етапі з циклу

загальноосвітніх дисциплін у межах навчального плану підготовки здобувачів ОКР «Бакалавр» з кібербезпеки, який розроблений з метою адаптації здобувачів з різним рівнем підготовки та розширення сфери знань, слугує фундаментом для вивчення подальших циклів дисциплін. Важливо зазначити, що школярі старших класів можуть записуватися на окремі курси дисциплін, для вивчення та складання іспитів разом зі студентами університету, які потім, після вступу, їм зараховуються. Випускник коледжу, який вступає до університету чи коледжу, також може мати отримані попередньо результати іспиту, які потім зараховуються. На вивчення загальноосвітніх дисциплін в університетах відводиться кредитів/дисциплін відповідно 46/17 – Університет Уалден, 30/10 – Американський військовий університет, 40/21– Авіаційний університет Ембрі Ріддлі, 63/14 – Університет Сент Джона; у коледжах – 27/14 – Коледж Бейкер, 60/17 – Коледж Мерсі, 36/23 – Айона коледж, 56-57/12 – Сент-Вінсент Коледж (додаток В). Ця інформація свідчить про повну автономію вищих навчальних закладів США у структуруванні змісту підготовки.

У додатку Д. подано характеристику циклу професійно-орієнтованих дисциплін ОПП чотирьох американських університетів (Університет Уалден, Американський військовий університет, Авіаційний університет Ембрі Ріддлі Університет Сент Джона) (таблиця Д-1) та коледжів (Коледж Бейкер, Айона коледж, Коледж Мерсі, Сент-Вінсент Коледж) (таблиця Д-2). Цикл професійно-орієнтованих дисциплін вивчається за умови, що студент обере мінімум з циклу загальноосвітніх дисциплін. Лише тоді він обирає основну програму навчання і при цьому додатково може обрати скорочену версію іншої програми. У вітчизняних вищих навчальних закладах студент відразу вступає на конкретну спеціальність, а опанування іншої освітньої програми теоретично можливе, але зазвичай є винятком.

Незважаючи на те, що студенти мають право вільного вивчення курсів/дисциплін, які вони обирають, порядку їх вивчення, вони зобов’язані дотримуватися певної передумови опанування програми певної дисципліни. Так, згідно з освітньо-професійною програмою рекомендується, щоб студенти

дотримувалися щорічних пропозицій, особливо стосовно професійно-орієнтованих курсів першого року навчання. Від цього залежить можливість вивчення подальших дисциплін.

В Україні заклад вищої освіти пропонує студенту систематизований, послідовний підхід стосовно вибору дисциплін та програм, причому студент не може змінювати зміст навчання.

На вивчення циклу професійно-орієнтованих дисциплін у ОПП досліджуваних університетах відводиться наступна кількість кредитів/дисциплін відповідно: 85/17 – Walden University, 54/18 – American Military University, 47/15 – Embry-Riddle Aeronautical University і 39/16 – St. John's University. Здійснений аналіз освітньо-професійних програм засвідчив, що у кожного університету використовується індивідуальний підхід щодо кількості кредитів/дисциплін і свободи вибору дисциплін професійного циклу студентом. Це зумовлено специфікою програми підготовки бакалаврів та особливостями організації освітнього процесу. Так, Університет Walden University пропонує тільки обов'язковий перелік циклу професійно-орієнтованих дисциплін, тоді як три інших університети, які обрані нами для аналізу, запропоновано, крім обов'язкового переліку, по додатковому на вибір здобувача. У коледжах також спостерігається індивідуальний підхід щодо кількості кредитів/дисциплін у переліку циклу професійно-орієнтованих дисциплін в ОПП: 78/14 – Baker College, 43/17 – Mercy College, 48/23 – Iona College, 46-47/12 – Saint Vincent College (ОПП Baker College, Mercy College, Iona College, Saint Vincent College , 2017).

В ОПП як університетів, так і коледжів зазначаються важливі вимоги-рекомендації. Так, у програмах, які не мали у професійно орієнтованому циклі дисципліни «математика», запропоновано спочатку вибрати курс MATH 116 та MATH 201 (а не MATH 115) в рамках загальної вимоги до підготовки. Лише після цього можна вивчати MATH 244. Студенти повинні звернутися до радників факультету або кафедри перед прийняттям рішення щодо вибору MATH 115. Їм буде надана допомога з цього питання. Деякі курси дисциплін

пропонуються лише один раз на рік, тоді рекомендовано звернутися до відділу за поточним графіком пропозицій щодо курсу. Це все свідчить про продуману кваліфіковану організацію освітнього процесу.

В Україні за аналогічною програмою Житомирського державного технологічного університету, який пройшов вперше ліцензування з ОПП підготовки здобувачів ОКР «Бакалавр» зі спеціальності 125 «Кібербезпека» (2016), студенту пропонується цикл загальних дисциплін.

У нормативній частині співвідношення кредитів/дисциплін складає 54/9, у вибірковій частині – 9/2 (при пропозиції для вибору 9 дисциплін). Цикл професійної підготовки нараховує у нормативній частині кредитів/дисциплін 108/20 та у вибірковій частині – 51 кредит (при пропозиції для вибору 18 дисциплін). Крім того, на дисципліни відводиться різна кількість кредитів 3, 4, 6, 7, 8, 9, 10. Загальний обсяг кредитів для здобуття ОКР «Бакалавр» за спеціальністю 125 «Кібербезпека» в Україні у обов'язковій частині сягає 178, з них загальноосвітня підготовка складає 53 (30%) та професійна 125 (70%) кредитів. На вибіркові дисципліни відведено 62 кредити, з них на загальноосвітню та професійну підготовки необхідно відведено відповідно кредитів 6,5 (10%) та 54 (87%). За фаховий іспит пропонується 1,5 (3%) кредитів. Співвідношення загальноосвітніх дисциплін до професійно-орієнтованих прирівнюється 1:3. Дисципліни за вибором складають 33% від кількості обов'язкових, що становлять загалом 67% (додаток Д та табл. 4.1.1).

Робочий план РБ-14-125/17 випускової кафедри безпеки інформаційних технологій Навчально-наукового Інституту інформаційно-діагностичних систем Національного авіаційного університету, чинний на підставі здобуття права підготовки здобувачів ОКР «бакалавр» зі спеціальності 125 «Кібербезпека», має свої особливості щодо наповнення навчальних планів. Так, розподіл між обов'язковою та вибірковою частинами практично однаковий з Житомирським державним технологічним університетом – 180/60 кредитів. Співвідношення дисциплін різних циклів відрізняється: цикл обов'язкової (загальноосвітньої)

підготовки складає 53 (30%), професійної – 125 (70% та практична підготовка) та вибіркової (професійна та військова підготовки).

У робочому плані РБ-14-125/17 ННІІДС НАУ обов'язкові компоненти розподіляються між дисциплінами наступним чином: загальні – 9%, за професійним спрямуванням – 81% та практична підготовка стновить 10% і зовсім відсутня серед вибіркових дисциплін. Вибіркова частина майже у рівних долях 1:1 припадає як на професійну, так і військову підготовку – відповідно 31 та 29 кредитів і 10% складаютьдисциплінизагальної підготовки (табл. 4.2.1.).

Таблиця 4.2.1.

Загальний обсяг ОПП для здобуття ОКР «бакалавр» за спеціальністю 125 «Кібербезпека» в Україні (Укладено автором на основі: РБ-14-125/17 ННІІДС НАУ)

Зміст підготовки	***Кількістькредитів ЄКТС***	
ОБОВ'ЯЗКОВА ЧАСТИНА	**180 кредитів**	**75%**
Загальна підготовка	16 кредити	9%
Професійна підготовка	146 кредитів	81%
Практична підготовка	18 кредитів	10%
ВИБІРКОВА ЧАСТИНА	**60 кредитів**	**25%**
Загальна підготовка	6,5 кредиту	10%
Професійна підготовка	31кредит	52%
Військова підготовка	29 кредитів	48%
ЗАГАЛОМ	240 кредитів	

У більшості вищих навчальних закладів США згідно з вимогами здобуття ОКР «Бакалавр» з кібербезпеки необхідно набрати мінімум 120 кредитів і не більше 130 Capitol Technology University (Технологічний університет Кепітол штату Меріленд). Як факт, констатуємо, що в американській моделі підготовки 1 кредит – 15 аудиторних годин; лекція триває 75 хв.; на 1 аудиторну годину паралельно заплановано 2-3 години самостійної роботи; аудиторні роботи складають 25%.

У вищих навчальних закладах України за освітньо-професійними програмами підготовки бакалаврів з кібербезпеки необхідно набрати 240 кредитів, при чому для більшості курсів 1 кредит складає 30 аудиторних годин, лекція триває 90 хв.

Разом з тим, співвідношення кількості аудиторних годин відрізняється в вищих навчальних закладах США та України. Так, середнє значення 2000 годин в університетах США проти 7200 годин у вищих навчальних закладах України, що зумовлено майже незначною кількістю практичних і лабораторних занять з дисциплін фахової підготовки. Співвідношення годин між лекційним і практичним заняттями проаналізованих програм значно відрізняється. В українських закладах вищої освіти в основному домінують лекційні заняття, а з багатьох дисциплін не заплановано проведення практичних занять.

Аналіз навчальних планів окремих вищих навчальних закладів, зокрема Національного технічного університету України «Київський політехнічний інститут», дав змогу встановити, що підготовка фахівців на бакалаврському рівні за спеціальністю «Кібербезпека» здійснюється за двома спеціалізаціями – «системи і технології кібербезпеки» й «математичні методи кібербезпеки». В інших вищих навчальних закладах спеціалізації в межах зазначеної спеціальності не виокремлюються. Вивчення навчальних планів засвідчило, що гуманітаризації підготовки не сприяє вивчення дисциплін правознавчого спрямування. Так, на блок правових навчальних дисциплін для бакалаврів відводиться лише 2 кредити ЄКТС (60 год.), з яких на аудиторну роботу припадає 36.

В Україні співвідношенні між лекційним і практичним заняттями складає приблизно 1:2. Загалом перелік навчальних дисциплін професійної та практичної підготовки здобувачів вищої освіти ступеня бакалавра за спеціальністю «Кібербезпека» характеризується несистематизованістю і відірваністю від потреб практики. Вкрай важливими для формування фахівця є такі дисципліни, як: «Вступ до кібернетичної безпеки», «Безпека операційних систем та комп’ютерних мереж», «Безпека інтернет-ресурсів», «Управління інформаційною безпекою». Проте викликає сумнів зарахування до дисциплін професійної підготовки таких загальних для усіх інженерів предмети, як: алгебра та геометрія, диференційні рівняння, що належать до блоку базової підготовки.

Згідно із Законом України «Про вищу освіту» (2014) навчальні плани підготовки здобувачів вищої освіти повинні містити 25% дисциплін вільного вибору студента. Під час підготовки фахівців для сфери кібербезпеки блок навчальних дисциплін професійної підготовки має слугувати формуванню компетентностей за спеціалізаціями для майбутньої роботи на посадах. Разом з тим, дисципліни, що пропонуються, ймовірніше, сприяють поглибленню власне математичної підготовки. Так, в у навчальних планах підготовки бакалаврів за спеціальністю «Кібербезпека» НТУУ КПІ загалом не представлені правничі дисципліни, предмети документознавчого спрямування, незважаючи на широке запровадження в компаніях електронного документообігу, цифрових підписів тощо. Відсутні і програми, які б сприяли розповсюдженню глобальної культури кібербезпеки, макро- й мікроекономічних питань щодо технологій захисту від кіберзлочинності.

Здійснений аналіз навчальних планів, програм підготовки фахівців із кібербезпеки показав, що українські освітньо-професійні програми та навчальні плани можуть бути удосконалені шляхом корегування фахового дисциплінарного наповнення. Предметна перевантаженість у системі вищої освіти України порівняно з американською моделлю, де студенти вивчають 3-4 предмети на семестр і відсутня стандартизація дисциплін, формування переліку курсів пов’язане не з потребою галузі, ринку праці й абітурієнтів, а з наявністю кафедр і викладачів, яких необхідно забезпечити навчальним навантаженням. На жаль, констатуємо ситуацію «вибір без вибору», коли фактично не існує практики вибору навчальної дисципліни студентом та відсутній гнучкий варіант вивчення предметів.

Освітньо-професійні програми обох країн враховують регламентуючі вимоги до результатів підготовки – Державного освітнього стандарту в Україні і Ради з акредитації у США. Важливою відмінною рисою у професійній підготовці бакалаврів з кібербезпеки у вищих навчальних закладах двох країн є спрямування системи вищої освіти США на формування самостійного,

ініціативного, креативного фахівця для ІТ-галузі та тісна співпраця американських університетів і коледжів з потенціальними роботодавцями.

Так, у 2017 р. національні центри вдосконалення процесу професійної підготовки в сфері інформаційної безпеки та кібербезпеки США щодо якості знань спільно з авторами Агентства Національної Безпеки (АНБ) та Міністерства Внутрішньої Безпеки (МВБ) США розробили нові кваліфікаційні вимоги до навчальних модулів. Зміст основних вимог стосується мінімального переліку необхідних навчальних модулів, що підлягають обговоренню; навчальних цілей; очікуваних результатів.

В Україні на державному рівні розроблено заходи, щодо стратегії модернізації вищої освіти України на 2017–2018. Серед основних завдань удосконалення системи підготовки фахівців ІТ галузі (з кібербезпеки). До першочергових завдань було віднесено: стандартизація вимог до підготовки фахівців; розроблення програми навчання відповідно до практичних потреб галузі та міжнародних сертифікаційних вимог тощо.

У табл. 4.2.3. зіставлено перелік фахових дисциплін, запропонованих до впровадження в освітній процес підготовки ОКР «бакалавр» із інформаційної та кібербезпеки України у рамках реалізації стратегії модернізації вищої освіти України на 2017–2018, та основні модулі за новими вимогами АНБ та МВБ США. Основні вимоги більш ґрунтовно представлено у додатку Е.

Вважаємо, що найбільш цікавими для майбутніх роботодавців можуть стати знання, які стосуються професійно-орієнтованих (фахових зокрема) дисциплін, запропонованих до впровадження в освітній процес підготовки ОКР «бакалавр» із інформаційної та кібербезпеки України (табл. 4.2.2).

Таблиця 4.2.2.

Перелік професійно-орієнтованих дисциплін, запропонованих до впровадження в освітній процес підготовки ОКР «бакалавр» із інформаційної та кібербезпеки України, та основні модулі за новими вимогами АНБ та МВБ США (укладена автором на основі джерел: РБ-14 - 125 / 17 НАУ НН ІІДС, 2017; National

Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD), 2018)

№	ОСНОВНІ МОДУЛІ ЗНАНЬ (ДИСЦИПЛІНИ)	
	Україна	США
	Вступ	Вступ до аналізу даних
1.	«Кібернетичний простір»	«Основи програмування»
2.	«Основи інформаційної та кібербезпеки (ІКБ)»	«Поняття кібернетичного захисту»
3.	«Кібернетичне право»	«Поняття кібернетичних загроз»
4.	«Хмарні технології в системах ІКБ»	«Фундаментальні принципи проектування безпеки»
5.	«Програмне забезпечення систем ІКБ»	«Введення в криптографію»
6.	«Криптографічні механізм ІКБ»	«Компоненти ІТ-систем»
7.	«Інформаційна та кібербезпека сучасного підприємства»	«Мережеві концепції»
8.	«Інформаційно-аналітичні процеси в системах безпеки державно-інформаційних ресурсів»	«Адміністративна система управління»

Дисципліни, які представлено у нових вимогах АНБ та МВБ США, необхідно взяти до уваги при розробленні нових ОПП для означеної спеціальності. Право вибору дисциплін повинно стати преференцією розробника ОПП та результатом висновків компетентних органів з ліцензування. В українських закладах вищої освіти акцентується увага на вимогах ОПП, що передбачає системне, послідовне засвоєння змісту дисциплін, але не запропоновано можливість вибору гнучких траєкторій освіти та викладача.

Як у США, так і в Україні результати навчання, умови реалізації освітнього процесу відповідно до вимог сертифікації / ліцензування викладені в ОПП. Зазначимо, що в США «традиційна сертифікація» – це програми навчання на базі 4-річних коледжів з напряму «освіта», що передбачає підготовку студентів та набуття ними компетенції, результативність оцінюється через складання іспиту відповідно до вимог штату.

Аналіз сучасного стану підготовки кадрів з означеної спеціальності показав, що у вітчизняній системі вищої освіти у підготовці фахівців з кібербезпеки існує ряд невідповідностей: недостатня узгодженість результатів з практичною професійною діяльністю майбутніх фахівців; неготовність

випускників до складання міжнародних фахових іспитів та працювати за фахом; відсутність у випускників практичних навичок. Однією з причин є те, що зміст підготовки за ОПП як складової галузевого стандарту концептуально має дисбаланс між теоретичною та практичною частинами підготовки бакалаврів ІТ-галузі.

Теоретична підготовка передбачає, що за результатами опанування навчальних дисциплін (як загальних, так і професійно-орієнтованих (фахових)) випускники-бакалаври мають орієнтуватися у положеннях законодавчої та нормативно-правової бази, а також відповідних вимогах, зокрема і міжнародних, стандартах та практиках щодо здійснення професійної діяльності; використання інформаційно-комунікаційних технологій. Майбутні фахівці повинні: здійснювати проектування (розроблення) систем, технологій і засобів інформаційної безпеки; чинити протидію несанкціонованому проникненню в ІТ-системи і мережі; прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем; відновлювати нормальне функціонування ІТ-систем і мереж після здійснення кібератак, збоїв та відмов; виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації; проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з кібербезпеки; формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою; здійснювати управління інцидентами інформаційної та кібербезпеки та управління ризиками інформаційної та кібербезпеки; виконувати моніторинг даних, комп’ютерних зловживань та аномалій; прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.

Аналіз форм та методів навчання бакалаврів зі спеціальності «Кібербезпека» свідчить про виконання українськими студентами значної частини завдань в аудиторії за допомогою викладачів, водночас американські студенти виконують їх самостійно в якості домашніх завдань. Американські студенти фактично не конспектують лекції, оскільки лектор викладає на сайті

великий обсяг інформації і рекомендує студентам підручник, зміст якого суголосний з лекційним матеріалом. Для проведення лекцій з проблем захисту кіберпростору університети постійно запрошують професіоналів з установ даного профілю, а викладачі обов'язкових дисциплін періодично проходять стажування у відповідних установах з фаху. Українські студенти в основному конспектують лекції, оскільки викладач не пов'язує свій курс з одним підручником. Крім того, не завжди на сайті розташовано достатню кількість навчальних матеріалів. Проте при наявності ґрунтовної матеріально-технічної бази в українських закладах вищої освіти це можливо і практикується як передовий досвід.

Формами контролю в Україні є диференційований залік та іспит. Натомість американські студенти мають тільки підсумковий іспит з кожної дисципліни, що включає завдання трьох типів: з відповіддю на вибір, відповіддю у вигляді числа або короткого рядка та розгорнутою відповіддю. В Україні значна частина іспитів приймається в усній формі, що містять питання з переліку, відомого студентам заздалегідь. В США студенти на іспиті мають справу з тестами різних рівнів складності. З кожної дисципліни на початку семестру оголошується система оцінювання до іспиту. Іспит не можна перескласти, але можливо пройти повторний курс. У закладах вищої освіти України іспит не відіграє вирішальної ролі у визначенні остаточної оцінки, що є співвідношенням відповіді та результатів з практичних занять упродовж семестру. В Україні поширена практика перескладання іспитів.

Навчання в США платне для всіх студентів (деяким вдається отримати підтримку різних фондів). Привертає увагу абсолютна перевага американської вищої школи в розмірах фінансування навчальних закладів та забезпеченості матеріально-технічними ресурсами. У 2015–2016 навчальному році для резидентів штату Північна Кароліна загальні витрати на навчання на здобуття ОКР «бакалавр» зі спеціальності «Кібербезпека» склали близько 20 тис. доларів, в Україні співвідношення бюджетних місць для навчання до контрактних становить 1:1 (University of North Carolina at Charlotte, 2017).

Практична підготовка в американських та українських вищих навчальних закладах є завершальним етапом усього навчання. У США вона реалізується на засадах інтегративного поєднання навчання в університеті та здобуття практичних навичок на майбутньому робочому місці. В американських університетах використання досвіду потенційних роботодавців в освітньому процесі є нормою та наповнює його можливістю для здобувачів освіти оволодіти знаннями щодо галузевих потреб, міжнародних сертифікаційних вимог не тільки з теоретичної позиції, а і безпосередньо на потенційному робочому місці, з отриманням заробітної плати. Українські виші не мають такої можливості щодо практики – здобувачі самостійно організовують місце проходження практики. Запозичити такий підхід до отримання практичного досвіду вітчизняним ВНЗ необхідно з метою формування системи дуальної освіти, залучивши провідні українські та міжнародні компанії ІТ-галузі.

Практика носить комплексний характер та реалізується за напрямами: навчальний, технологічний, переддипломне стажування та завершальний (виконання дипломної роботи). Узагальнюючи характеристику напрямів комплексної практичної підготовки, слід зазначити, що всі види практики складають єдиний комплекс: від навчальної, технологічної, виробничої, переддипломної – на завершення навчання виконання дипломної роботи роботи як результат навчальної підготовки бакалаврів з кібербезпеки, що містить науково обґрунтовані теоретичні та експериментальні результати і висновки. На кожен вид практики у ОПП передбачена відповідна кількість кредитів. Практична підготовка складає 18 кредитів і містить наступні дисципліни:

- навчальна практика – 3 кредити;
- технологічна практика – 3 кредити;
- виробнича практика – 3 кредити;
- переддипломна практика – 3 кредити;
- виконання дипломної роботи – 6 кредитів. (Додаток З-2)

Іншою проблемою професійної підготовки є самостійна робота студентів в українських вишах. На нашу думку, необхідно змінити концептуальний підхід

до самостійної підготовки, яка потребує підвищення її ефективності шляхом проведення підготовчої роз'яснювальної роботи щодо практичного її здійснення. Узагальнений зміст форм самостійної роботи систематизовано у додатку Д, таблиця Д-3.

В американській моделі навчання при вступі до вищого навчального закладу студенти отримують спеціальні методичні рекомендації щодо розвитку умінь навчатися. Такий підхід є результативним та успішним фактором процесу підготовки у ІТ-сфері. Орієнтуючись на цей досвід, ми пропонуємо застосовувати різні методики розвитку навичок роботи з навчально-науковою літературою, починаючи з першого курсу. Комплекс позитивних надбань американської системи підготовки характеризує досвід організації індивідуальної самостійної роботи студентів як позитивно результативний. Можливість реального самостійного оволодіння фахом в структурі навчальної роботи американського студента можна екстраполювати у процес професійної підготовки бакалаврів з кібербезпеки в Україні.

У ході дослідження виявлено основні умови ефективності практики, зокрема:

- навчання студентів методиці самостійного формування умінь ефективно працювати з навчально-науковими джерелами, планувати власний час тощо);

- організація індивідуального планування навчальної роботи студентів з обов'язковим контролем за виконанням індивідуальних планів з боку педагогів та навчальної частини закладу;

- доступність структурно-логічної схеми навчальної дисципліни, інформації про викладачів, форми контролю, критерії оцінювання знань, час і місце консультацій;

- розроблення комплексних навчальних посібників для самостійної роботи, що поєднують методичні вказівки, теоретичний та практичний матеріал, які є у вільному доступі для студентів;

- індивідуалізація домашніх завдань і лабораторних робіт, а в умовах групової роботи – чіткий її розподіл між членами мікрогрупи;

- доступність лабораторій, комп'ютерних мереж та інтернет-ресурсу, мультимедійних аудиторій для забезпечення можливостей студенту чи групі самостійно упродовж робочого дня проводити дослідження, використовувати обладнання, устаткування для навчальних потреб;

- створення на кафедрах (спеціальних, випускових) консультаційних пунктів, залів курсового проектування з кафедральними електронними архівами навчального матеріалу та з можливостями доступу до нього.

Підготовка кадрів в США для галузі передбачає ряд кваліфікаційних вимог до фахівця на завершення університетської підготовки, а саме: розуміти важливу термінологію, матеріали, технології; бути спроможним володіти загальними навичками з кібербезпеки; мати достатньо високу майстерність з практики у своїй галузі; здійснювати моніторинг систем безпеки, застосовуючи між мережеві екрани та системи виявлення вторгнень; вміти створювати, впроваджувати і контролювати виконання політики безпеки; вміло діяти за планом аварійного відновлення даних для операційних систем, баз даних, мереж, серверів і додатків; професійно здійснювати дослідження нових продуктів, послуг, протоколів і стандартів для підвищення рівня безпеки; проводити регулярні перевірки на відповідність використання.

Такий елемент узагальненого американського позитивного досвіду, як професійна орієнтація навчальних дисциплін, має забезпечуватися певними вимогами (додаток З, таблиця З-1). Зупинимося детальніше на них:

- відбір і виклад навчального матеріалу необхідно спрямовувати на досягнення цілей, зазначених в ОКХ, для розуміння здобувачами його прикладного значення;
- методологічно спрямоване формування узагальнених навичок та умінь бакалаврів з кібербезпеки має бути відображеним у змісті навчальних дисциплін ОПП;
- теоретична частина навчальної дисципліни є фундаментальним ядром знань;

- практична частина навчальної дисципліни спрямована на застосування теоретичних знань у майбутній професійній діяльності;
- міждисциплінарні зв’язки допомагають здобувачам оволодіти цілісною картиною світу та сучасною методологією пізнання;
- при конструюванні навчальних завдань необхідно формулювати їх зміст у контексті кіберзахисту кіберсередовища та попередження кіберзагрози.

Аналіз особливостей підготовки фахівців з кібербезпеки в США засвідчив, що відповідно до цих вимог усі ОПП американських навчальних закладів з підготовки здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» та їх компоненти мають відповідати наступним узагальненим критеріям (додаток З, таблиця З-1):

- навчальні плани і методи навчання повинні підпорядковуватися основним цілям, місії і очікуваним результатам конкретного вищого навчального закладу, що здійснює підготовку фахівців з кібербезпеки;
- компонентами програми є чіткий план організації, реалізації та оцінювання конкретної сфери дослідження;
- залучення досвіду потенційних роботодавців у процес планування і організації ОПП;
- особливу увагу приділяти постійному контролю і корегуванню ОПП з урахуванням стрімких змін у світовому кіберпросторі;
- ОПП у галузі сфери дослідження мають допомагати студентам розвивати уміння вчитися, навички критично мислити, науково сприймати проблеми та розв’язувати їх, відкрито усвідомлювати зміни світового рівня і парадигми, здатність до самостійного навчання протягом життя;
- галузева освіта має бути достатньою за тривалістю, відповідати можливостям навчання, враховувати складність завдань з метою підготовки бакалаврів з кібербезпеки до здійснення професійної діяльності;

- залучення досвідчених практичних фахівців до створення ОПП;
- ОПП має бути пов’язана теоретично і практично з науковою школою і місцем майбутньої професійної діяльності.

На нашу думку, для усунення наявних невідповідностей у професійній підготовці фахівців в українських закладах вищої освіти необхідно відповідно до концептуальних засад викладання задіяти проектну технологію навчання, що забезпечує оволодіння уміннями виконання різних ролей, у сфері майбутньої професійної діяльності (лідер, виконавець, опонент тощо) для погодженої дії в команді. У ході аналізу методів та форм навчання та оцінювання знань фахівців з кібербезпеки в університетах та коледжах США було встановлено, що в освітньому процесі освітня роль припадає на проектні технології. Американські педагоги (Becker 2001; Bromwich, 2003) переконані, що з боку студентів є необхідність обов’язкового вміння самостійно здобувати ґрунтовні теоретичні знання та використовувати їх у подальшій реальній професійно-практичній діяльності.

Доречно акцентувати увагу на вимогах до реалізації методу проектів: наявність у вихідних даних розроблення проекту проблеми дослідження; теоретична, практична і пізнавальна значущість передбачуваних результатів; використання методів наукового пошуку (визначення проблеми та завдань проектування; формулювання гіпотези; аналіз наукових джерел; розроблення методики дослідження; експериментування; узагальнення результатів наукового пошуку; обґрунтування висновків та практичних рекомендацій); виконання проекту малими групами студентів та спільний захист (презентація) розробниками проекту варіантів розв’язання практичної проблеми.

Визначено низку критеріїв оцінювання виконаних проектів в американських вищих навчальних закладах:

- практичне значення результатів проекту;
- аргументація та спосіб вибору теми (пропозиція викладача, самостійний вибір студента);
- частка самостійного виконання та завершеності проекту;

- доказова база, аргументи, рівень творчості та оригінальності запропонованих рішень поставленої проблеми.

Зазначена технологія, на нашу думку, є актуальною і для вітчизняної практики підготовки бакалаврів для ІТ-галузі.

Виважений аналіз конструктивних ідей досвіду США дасть змогу модернізувати та удосконалити систему професійної підготовки фахівців у галузі кібербезпеки в Україні, зумовлену певними соціально-економічними і політичними чинниками розвитку суспільства. У додатку Ж систематизовано та узагальнено прогресивні ідеї досвіду підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США з метою екстраполяції у вищу освіту України. Модернізація насамперед передбачає екстраполяцію кращих зразків гнучкого нормативно-правового супроводу, до якого включено закони, що регламентують процес професійної підготовки бакалаврів з кібербезпеки, стратегії професійної підготовки, щодо розвитку методичного, навчального та кадрового секторів та державних стандартів для системи вищої освіти з підготовки бакалаврів з кібербезпеки; постійне оновлення ОПП для здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» з метою удосконалення відповідно до світових вимог та обов'язкове їх ліцензування; відображення специфіки професійної підготовки фахівців з кібербезпеки стосовно змісту, форм, методів навчання; запозичення високого технологічного рівня американської моделі підготовки фахівців у вищих навчальних закладах, особливостей оцінювання навчальних досягнень студентів у процесі оволодіння професійними компетентностями; впровадження новітніх педагогічних технологій на основі співпраці та партнерства; особистісно-орієнтованого науково-методичного супроводу та кадрового забезпечення; орієнтація змісту та організаційних форм навчання на збалансований взаємозв'язок теорії з практикою; створення дієвих стимулів професійного розвитку майбутнього фахівця в Україні; запровадження грантів на професійну підготовку фахівців з кібербезпеки.

4.3. Обґрунтування можливостей використання прогресивних ідей досвіду США з професійної підготовки бакалаврів з кібербезпеки у вітчизняній системі вищої освіти

Нові умови життя в епоху інформаційного суспільства зумовили потреби реформування професійної підготовки фахівців з кібербезпеки в Україні з урахуванням зарубіжного досвіду. Проведення порівняльно-педагогічних досліджень сприяє розв'язанню ряду суперечностей між: зростанням суспільних вимог до професійно кваліфікації фахівців з кібербезпеки та наявним рівнем їхньої підготовки; сучасними світовими тенденціями розвитку вищої освіти та недосконалістю нормативно-правового, змістового, технологічного, науково-методичного забезпечення професійної підготовки фахівців з кібербезпеки; вимогами до якості практичної підготовки та недооцінюванням її ролі у професійному вихованні фахівців з кібербезпеки; необхідністю ґрунтовного наукового аналізу конструктивних ідей зарубіжного досвіду професійної підготовки бакалаврів з кібербезпеки та відсутністю його системного вивчення, узагальнення, впровадження у вітчизняній педагогічній теорії та практиці.

Дослідження проблеми професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США та України базувалось на положенні про те, що інформаційна безпека в США та Україні розглядається як важливий компонент національної безпеки. Концепція дослідження професійної підготовки бакалаврів з кібербезпеки ґрунтується на порівняльному аналізі, що здійснюється на основі визначених та обґрунтованих критеріїв порівняння. Порівняльний підхід забезпечує можливість здійснення аналізу системи підготовки у галузі інформаційних технологій в США та України, їх зіставлення та порівняння з вітчизняною освітою з метою виокремлення напрямів використання зарубіжного досвіду у системі вітчизняної освіти. Компаративістський аналіз дозволив виокремити мережі навчальних закладів США та України; виявити спільні та відмінні ознаки змісту, форм, і методів підготовки бакалаврів з кібербезпеки; обґрунтувати перспективні напрями

використання досвіду професійної підготовки фахівців з кібербезпеки у вищих навчальних закладах США та України.

Визначені ідеї підготовки бакалаврів з кібербезпеки у системі вищої освіти США дозволяють виокремити особливості, які позитивно відрізняють американський досвід від українського, а саме:

- абсолютна перевага американських університетів у розмірах фінансування, матеріально-технічних засобах підготовки фахівців цієї галузі;
- практична зорієнтованість підготовки, що полегшує процес працевлаштування та сприяє розвитку кар'єри випускників;
- наявність в американських навчальних закладів гнучких навчальних планів, що включають широкий спектр навчальних курсів, за вибором; водночас відсутність гнучкості у вивченні навчальних дисциплін в український вищий школі, неможливість вибору викладача, мобільних траєкторій освіти;
- предметна перевантаженість процесу навчання у вітчизняній моделі підготовки бакалаврів з кібербезпеки порівняно з американською.

Серед позитивних ознак підготовки бакалаврів з кібербезпеки в Україні варто відзначити:

- неперервну тенденцію до зростання кількості бажаючи навчатися за програмами підготовки бакалаврів з кібербезпеки, зростання престижності цієї спеціальності завдяки можливості одержання гідного працевлаштування та високої заробітної плати;
- відчутність процесів диверсифікації професійної підготовки бакалаврів з кібербезпеки.

На основі аналізу особливостей професійної підготовки бакалаврів з кібербезпеки можемо виокремити ідеї та положення, які є актуальними, перспективними для підготовки бакалаврів з означеної спеціальності в Україні на відповідних рівнях:

На стратегічному рівні:

- Адаптація законодавства України до потреб ІТ-галузі, адаптація до постійних змін у попиті на послуги фахівців з кібербезпеки.

Зростання потреби у формуванні нової системи неперервної освіти впродовж життя, що стає невід'ємною умовою професійного зростання фахівців з кібербезпеки, забезпечує доповнення, оновлення, осучаснення здобутих під час базової освіти знань, умінь, навичок в умовах стрімкого розвитку технічного прогресу. На засадах концепції безперервної освіти можливі декілька варіантів навчання: надання другої вищої освіти (наприклад, випускник технічного вищого навчального закладу здобуває другу вищу освіту за правничим фахом); застосування нелінійної схеми підготовки фахівців за різними ступенями освіти, що стало можливим завдяки новим нормам, закріпленим у Законі України «Про вищу освіту» (наприклад, бакалавр технічного профілю вступає до магістратури за економічним фахом з метою подальшої роботи як фахівця з кібербезпеки в банківській сфері); запровадження спеціалізацій із кібернетичної безпеки на інших спеціальностях (юридичних, економічних, управлінських тощо); перепідготовка у процесі післядипломної освіти фахівців із близькоспоріднених із кібернетичною безпекою спеціальностей; використання потенційних можливостей неформальної освіти для підвищення кваліфікації фахівців-практиків через проведення тренінгів, круглих столів, міжнародних стажувань тощо.

На наше переконання, напрями підготовки й підвищення кваліфікації фахівців із кібербезпеки доцільно проектувати відповідно до Конвенції про кіберзлочинність, прийнятої Радою Європи 23 листопада 2001 р. і ратифікованою Верховною Радою України 7 вересня 2005 р. Кожен із виокремлених у ній аспектів може кореспондуватись зі змістом освіти за спеціальностями, за якими в Україні здійснюється підготовка здобувачів вищої освіти.

- Здійснення підготовки на засадах компетентнісного підходу, сфокусованого на розвитку здібностей та умінь, що дозволяють орієнтуватися фахівцю в розмаїтті складних, швидко змінюваних виробничих ситуаціях.

- Удосконалення нормативно-законодавчої бази, що регламентує діяльність закладів вищої освіти України загалом і процесі професійної підготовки бакалаврів з кібербезпеки зокрема; розроблення нових професійних стандартів, що сприятиме забезпеченню якості підготовки та професійному розвитку фахівців.

На організаційному рівні:

- Створення ефективного механізму акредитації вищих навчальних закладів, які здійснюють підготовку бакалаврів з кібербезпеки, що буде відповідати європейським, світовим вимогам, сприятиме підвищенню якості професійної підготовки фахівців.

- Розроблення нової, більш вимогливої системи відбору абітурієнтів на спеціальністю із застосуванням тестування на професійну придатність, яке дасть змогу виявити готовність вступника до навчання за обраним фахом.

- Створення системи підготовки викладачів, що реалізують професійну підготовку бакалаврів з кібербезпеки, практикують залучення до викладацької діяльності на постійній основі фахівців, що працюють в галузі, для проведення лекційних та практичних занять.

На змістовому рівні:

- Розроблення нових стандартів для бакалаврів, які забезпечують оновлення змісту підготовки бакалаврів з кібербезпеки із орієнтуванням на оволодіння на якісно новому рівні іноземними мовами, суміжними спеціальностями, необхідними для роботи у певній галузі (юридичними, економічними тощо). Створюючи стандарти підготовки, необхідно орієнтуватися на сертифікаційні програми професійних асоціацій, на підставі яких укладаються посадові інструкції. Таким чином, можливе максимальне наближення до потреб практики і забезпечується ефективність професійної підготовки бакалаврів. Стандартизація освіти фахівців із спеціальності

«кібербезпека» надала можливість не тільки охопити діяльність вищих навчальних закладів, а й порушити питання перед асоціаціями роботодавців щодо відпрацювання сертифікаційних програм, аналогічних в інших державах.

- Створення та постійна адаптація освітніх програм з урахуванням сучасних світових тенденцій у ІТ-галузі, підготовка фахівців з кібербезпеки відповідно до систематизованих відомостей щодо секторів ринку праці, які мають потребу в такій категорії професіоналів для роботи в зазначеному сегменті.

Можна передбачити запровадження спеціалізації у таких сферах, як сектор державної влади і управління (для супроводження процесів безпечного електронного урядування, державних інформаційних ресурсів, забезпечення безперешкодної роботи інформаційно-аналітичних інституцій); статистичні підрозділи (з метою дієвої протидії кібератакам на сайтах державних установ і організацій); сектор безпеки та оборони (забезпечення національної та інформаційної безпеки в кіберпросторі, боротьба з кіберзлочинністю, протистояння кіберзагрозам, захист інтересів держави засобами комп'ютерної техніки й технологій в інформаційних і гібридних війнах, забезпечення робочого стану криптографічних засобів захисту інформації); сектор економіки (превенція випадки промислового шпіонажу, викрадення ноу-хау, комп'ютерного шахрайства з електронними платіжними документами, заволодіння конфіденційними даними економічного характеру; унеможливлення противоправних дій із платіжками та кредитними картками, викрадення коштів з електронних рахунків, замовлення товарів і послуг за чужий рахунок тощо); сектор науки і техніки (протистояння виявам кібершпигунства; розробка програмного забезпечення, що перешкоджає проникненню в комп'ютерні системи, розповсюдження вірусів, руйнації бази даних).

- Орієнтація на збільшення кількості годин, відведених на практичну підготовку. Впровадження у практичну підготовку проектів стажування на майбутньому робочому місці.

- В освітніх програмах перевага повинна надаватись практично орієнтованим дисциплінам. Такий прагматичний підхід властивий американським вищим навчальним закладам, проте є принципово новим для української вищої освіти, де традиційно домінувала фундаментальна підготовка. На часі вирішення ще одного питання під час стандартизації: пропорційне співвідношення теоретичних та практичних складових процесу навчання, виділення під час навчання здобувачів вищої освіти в галузі інформаційних технологій резерву часу для набуття інших компетенцій (наприклад, правничих) задля опанування нормативно-правовими засадами інформаційного права, права інтелектуальної власності, нормативно-правового забезпечення діяльності в кібернетичному просторі.

На нашу думку, потенціал удосконалення освітніх стандартів бакалаврів з кібербезпеки полягає в тому, щоб кореспондувати теоретичні знання і практичні уміння, що формуються у закладі вищої освіти з подальшою роботою в конкретних секторах.

- Збільшення частки вибіркових дисциплін, що сприяє розширенню можливостей для вільного вибору дисципліни, які відповідають професійним інтересам майбутніх фахівців з кібербезпеки.

- Застосування в освітньому процесі активних, творчих методів навчання, дослідницьких, проблемних, проектних методів, дискусій, ділових ігор, самостійної навчально-пошукової діяльності студентів, що сприяє підвищенню мотивації до навчальної діяльності та якісній підготовці майбутніх фахівців.

- Виокремлення у варіативний компоненті освітніх стандартів конкретних компетенцій, пов’язаних із майбутньою професійною діяльністю, що буде акцентувати увагу педагогів на формуванні відповідних компетенцій у процесі навчання і сприятиме вирішенню проблеми адаптації на ринку праці.

У додатку Ж., таблиці Ж-4. подано рекомендований узагальнений обсяг годин/кредитів за видами занять, навантаження, відведеного на роботу з викладачем на самостійну роботу студента в українських закладах вищої освіти на ОКР «бакалавр» зі спеціальності «Кібербезпека», та співвідношення між

ними у відсоткових показниках. Очевидно, рекомендоване співвідношення збільшує значущість обсягу годин, відведених на самостійну роботу, щодо обсягу годин, відведених на роботу з викладачем, та право розподілу обсягу годин/кредитів – це преференція розробників ОПП та компетентних органів з ліцензування.

На нашу думку, при такому співвідношенні обсягу годин/кредитів спостерігається позитивна зміна акцентів у навантаження на самостійну роботу та опанування фахом. Реально спостерігається зменшення обсягу годин/кредитів за видами занять, а також зменшення навантаження на роботу з викладачем майже учетверо за кількістю годин та удвічі за кредитами, проте баланс співвідношення у відсотках суттєво не змінився. Кількість годин, рекомендованих на самостійну роботу, майже не змінено, однак покращення якості підготовки в цілому стало можливим. Інший суттєвий висновок щодо вартості самого навчання – можна отримати економію заробітної плати. Проте наші рекомендації носять рекомендаційний характер, адже це преференція розробників ОПП та фахівців з формування фонду заробітної плати. ОПП визначає передумови доступу до навчання, орієнтацію та основний фокус програми, обсяг кредитів ЄКТС, необхідний для здобуття ОКР «бакалавр», перелік загальних та спеціальних (фахових) компетентностей, нормативний і варіативний зміст підготовки фахівця, сформульований у результатах навчання та вимогах до контролю якості вищої освіти.

Отже, результати проведеного дослідження свідчать на те, що використання прогресивних ідей досвіду США у вітчизняній теорії і практиці підготовки бакалаврів з кібербезпеки сприятиме підвищенню мотивації до навчальної діяльності та підвищенню якості підготовки фахівців з метою отримання позитивних результатів.

Висновки до розділу 4

Проведений аналіз американського досвіду професійної підготовки на здобуття ОКР «бакалавр» з спеціальності «Кібербезпека» дозволив визначити

можливості використання його прогресивних ідей у системі вищої освіти України, зокрема: забезпечення інформаційної підтримки довідкових інтернет-ресурсів; розроблення й удосконалення змісту ОПП на здобуття ОКР бакалавра; організація практичної підготовки бакалаврів з кібербезпеки в США, яка здійснюється на засадах інтегративного поєднання навчання в університеті та здобуття практичних умінь на майбутньому робочому місці. Як аргумент такого узагальнення є факт читання лекцій за фахом в американських вишах досвідченими професіоналами з установ відповідного профілю, а викладачі обов'язкових дисциплін періодично проходять стажування у відповідних установах з фаху. Комплекс позитивних надбань американської системи підготовки характеризує досвід організації індивідуальної самостійної роботи в структурі навчальної роботи американського студента можна екстраполювати у процес професійної підготовки. Основна з умов успішності цієї практики полягає у наступному: навчання студентів методиці самостійного формування умінь ефективно працювати з навчально-науковими джерелами, планувати власний час тощо.

Між вимогами ринку праці та практичними результатами освітньої діяльності закладів вищої освіти України утворився відчутний розрив, а саме: відсутність умінь та навичок практичної роботи за спеціальністю, знань сучасних технологій і, як наслідок, збільшення періоду адаптації випускників на первинних посадах, ускладнення працевлаштування й зниження престижу вищої освіти. Загалом викликає занепокоєння Міністерства освіти і науки України питання щодо обсягів практичної підготовки студентів, особливо в відносно новій ІТ-галузі, яка стрімко розвивається та потребує ефективного кібернетичного захисту.

Основні наукові результати, викладені в розділі, відображені автором у публікаціях: Бистрова, 2017e; Bystrova, 2017f; Bystrova, 2017g; Бистрова, 2017i; Бистрова, 2017h.

ЗАГАЛЬНІ 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 установі, 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 уможливлює 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 Україні 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 використаних джерел

Алфьорова, О. (2015). Якість освіти як головний критерій оцінювання діяльності вищого навчального. *Теорія та практика державного управління*, Retrieved from URL:http://nbuv.gov.ua/.

«Америка 2000. Стратегія освіти». (2001). Retrieved from URL: https://eric.ed.gov/.

Анурьева, М. (2013). О приоритетах образовательных программ в области информационной безопасности в разных странах *Психолого-педагогический журнал «Гуадеамус»,* 1(21), 102–109.

Бабак, В., Козловський, В., Хорошко, В. &Чирков, Д. (2001). «Підготовка фахівців із захисту інформації в Україні» *Захист інформації*, 4, 92–99.

Баранов, О. (2014). Про тлумачення та визначення поняття «кібербезпека», Правова інформатика, 2(42), 54-62.

Бєланова, Р. (2001). Концептуальні ідеї гуманізації підготовки студентів в класичних університетах (Україна – США). В М.Б. Євтуха (Ред.) *Теоретичні питання освіти та виховання.* (Збірник наукових праць). Київ. ВЦ КДЛУ, 17, 126–130.

Биков, В. (2010a). Сучасні завдання інформатизації освіти. *Інформаційні технологій і засоби навчання*, 1(15). Retrieved from URL: http://www.nbuv.gov.ua/e-journals/.

Биков, В., Лапінський, В. , Пилипчук, А., Шишкіна, М. & ін. (2010 b). *Засоби інформаційно комунікаційних технологій єдиного інформаційного простору системи освіти України*. (Монографія). В В.Ю. Биков (Ред.), К.: *Педагогічна думка*, 160 с.

Биков, В. (2011a). Технології хмарних обчислень – провідні інформаційні технології подальшого розвитку інформатизації системи освіти України. *Комп'ютер у школі та сім'ї*, 6, 3-11.

Биков, В. (2011b). Технології хмарних обчислень, ІКТ-аутсорсінг та нові функції ІКТ-підрозділів навчальних закладів і наукових установ. *Інформаційні технології в освіті. Збірник наукових праць*, 10, 8-23.

Биков, В. (2011). Упровадження інформаційно-комунікаційних технологій в освіті – імператив її модернізації. *Національна доповідь розвитку освіти України,* 118-124.

Биков, В.Ю. (2012). Інноваційний розвиток засобів і технологій систем відкритої освіти. В І.А.Зязюн та ін. (Ред.) *Сучасні інформаційні технології та інноваційні методики у підготовці фахівців: методологія, теорія, досвід, проблеми*.(Збірник наукових праць), 29, 32-40.

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.

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

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

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

Бистрова, Б. (2017b). Основні поняття дослідження та концептуальні засади професійної підготовки фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*, (72), 58–70. doi: 10.24139/2312-5993/2017.08/058-070.

Бистрова, Б. (2017 c). 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.

Бистрова, Б. (2017d). 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.

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

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

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

Бистрова, Б. (2017 h). *Професійна підготовка бакалаврів з кібербезпеки: досвід США*. Київ. Альфа-ПІК, 74с.

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

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

Bogdana Bystrova (2018a). 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 2018* (p.166–168), Zhytomyr: ZSTU.

Бистрова, Б. (2018b). Структура та зміст моделі управління процесом практичного навчання бакалаврів з кібербезпеки у ВНЗ США. В

Н.В. Пазюра (Ред.), Вища освіта: удосконалення якості підготовки фахівців: ІІ міжнародна науково-практична конференція, Київ, 26-29 квітня, (с. 10–13). Київ. Альфа-ПІК.

Бідюк, Н. (2009), *Професійне навчання безробітних у США: теорія і практика.* (Монографія). В Н.Г.Ничкало, (Ред.). Хмельницький: ХмЦНТЕІ, 542 с.

Бідюк, Н. (2011). Специфіка підготовки педагогічного персоналу для роботи з дорослими у США. *Порівняльна професійна педагогіка*,1,107-115.

Бідюк, Н. (2011). Основні напрями державної політики США щодо забезпечення зайнятості та освітньої підтримки безробітних. *Актуальні проблеми професійної орієнтації і професійного навчання.* (Збірник наукових праць, за матеріалами ІІ міжнар. наук.- практ. конф.), (с. 123-133). Київ, ІПК ДСЗУ.

Бідюк, Н. (2012). Формування міжкультурної комунікативної компетентності фахівців міжнародних відносин. *Вісник Чекарського університету. Серія: Педагогічні науки*, 135, 141–146.

Бідюк, Н. (2013). Співпраця освітніх інституцій та громадських організацій щодо розвитку та підтримки освіти жінок у США. *Порівняльна професійна педагогіка*, 1, 58-66.

Богуш, В., Богуш, В., Кривуца, В. & Кудін, А. (2004). *Інформаційна безпека : термінологічний навчальний довідник*. В В.Г. Кривуци (Ред.). К.: ООО «Д.В.К.», 508 с.

Брижко, В., Гальченко, О. , Цимбалюк, В. & ін. (2002). *Інформаційне суспільство – дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція*. Київ, Інтеграл, *220с.*

Бусел, В., (Ред.), (2005). *Великий тлумачний словник сучасної української мови (з дод. і допов.)* Ірпінь, ВТФ «Перун», 1728с.

Бурячок, В., Невойт, Я. & Бурячок Л. (2015). Вплив загроз антропогенного і техногенного характера на стан безпеки ІТ-систем та соціальних інститутів провідних країн світу і України. *Сучасний захист інформації,* 4, 15 – 27.

Вдовичин, Т. (2016). Використання мережних технологій відкритих систем у навчанні бакалаврів інформатики: загальні висновки. *Інформаційні технології в освіті,* 27, 167-185.

Власюк, А. & Грицюк, П. (2013). Підготовка фахівців з інформаційних технологій у контексті сучасних вимог. *Нова педагогічна думка,* 11, 109-111.

Всесвітня декларація про вищу освіту для XXI століття: підходи та практичні заходи. Retrieved from URL: http://www.sde.ru/.

Вульфсон, Б.(2002). Методы сравнительно-педагогических исследований. *Педагогика*, 2, 70-80.

Глотова, Г. (2005). *Развитие творческого потенциала будущих инженеров в вузах США и Западной Европы.* (Дис. канд. пед. наук), Казанский государственный технологический университет. Казань.

Голубенко, О. & Петров, О. (2009). Особливості підготовки фахівців з інформаційної безпеки в Україні. *Інформаційна безпека,* 2, 5-17.

Глузман, А. (1998). *Профессионально-педагогическая подготовка студентов университета: теория и опыт исследования.* (Монографія). К.: Поисково-издательское агентство, 252 с.

Гнатюк, С. (2014). Пріоритетні напрями підготовки в Україні фахівців з інформаційних технологій. *Стратегічні пріоритети*, 4 (33), 119-124.

Головань, С., Хорошко, В. & Щербак, Л. (2009). Напрями системи знань фахівців із інформаційної безпеки. *Захист інформації,* 1, 99-103.

Гончаренко, С., (Ред.), (1997). Український педагогічний словник. К.: Либідь, 376 с. Retrieved from URL: http://irbis-nbuv.gov.ua.

Грабовий, А. (2017). Закон про кібербезпеку та стратегія кібербезпеки України. *Електронне видання Юрист та Закон*, 26. Retrieved from URL: http://uz.ligazakon.ua/.

Грицюк, Ю. & Рак, Т. (2011). Підготовка фахівців з інформаційної безпеки для потреб Міністерства надзвичайних ситуацій України. *Шоста Міжнародна конференція Нові інформаційні технології в освіті для всіх: навчальні середовища матер. наук.-практ. конф. ITEA-2011(22-23 листопада 2011 р., м. Київ),* (с. 123-129). К.: Міжнародний науково-навчальний центр інформаційних технологій і систем.

Грицюк, Ю. & Сташевський, З. (2013). Значення моделей компетенцій у системі управління освітнім проектом підготовки фахівця з інформаційної безпеки. Retrieved from URL: http://cience.lpnu.ua/.

Грущенко, Л. (2007). Формування професійно-орієнтованого ставлення до дисциплін психолого-педагогічного циклу у студентів економічного університету. Retrieved from URL: http://www.umo.edu.ua/.

Даник, Ю. (2011). Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України України. *Інформаційні системи,* 5, 5-22.

Джалладова, І. (2015). Політика інформаційної безпеки: науково-прикладні аспекти і проблеми підготовки фахівців. В В.К. Галіцина *Моделювання та інформаційні системи в економіці,* ДВНЗ «КНЕУ ім. Вадима Гетьмана», 57–75.

Джонстоун, Д. (2003). Система высшего образования в США: структура, руководство, финансирование. *Университетское управление,* 5. Retrieved from URL: http://www.umj.ru/index.php/.

Десятов, Т. (2003). Система неперервної професійної освіти. *Педагогіка і психологія,* 1, 75–80.

Діордіца, І. (2016). Стан підготовки фахівців у сфері кібербезпеки. *Visegrad journal on human rights*, 6(1), 53-68.

Діордіца, І. (2017a). Кваліфікаційні вимоги до компетенції фахівців із кібербезпеки. *Інформаційне право,* 2, 215–219.

Діордіца, І. (2017b). Напрями підготовки та підвищення кваліфікації фахівців із кібербезпеки. *Інформаційне право,* 3, 199–202.

Діордіца, І. (2017 с). Освітні стандарти підготовки фахівців із кібербезпеки. *Національний юридичний журнал: теорія і практика*, 1 (23), 50- 53.

Діордіца, І. (2017d). Поняття та зміст кіберзагрози на сучасному етапі. *Адміністративне право і процес,* 4, 99–107.

Дубов, Д. (2010). Кібербезпекова політика контексті трансформації політики безпеки США за адміністрації Б.Обами. *Політичний менеджмент,* 1, 155-163.

Дубов, Д. (2013a). Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети*, 4, 119-127.

Дубов, Д. (2013b). Модернізація інформаційної інфраструктури як чинник забезпечення національних інтересів . Retrieved fromURL: http://nbuv.gov.ua

Дубов, Д.(2014). *Кіберпростір як новий вимір геополітичного суперництва.* (Монографія). Київ, НІСД, 328 с.

Дюжев, Д. (2004). *Інформаційне суспільство: соціально-правова парадигма суспільного розвитку.* (Автореф. канд. філос. наук). Донецький національний університет. Донецьк, 18 с.

Елманова, В. (1989). *Высшее образование за рубежом: (США, Великобритания, Франция, ФРГ, Япония, КНР).* Учебн. пособие. ЛГУ, 50с.

Єрошенко, О., (Ред.), (2012). *Великий тлумачний словник сучасної української мови.* Донецьк: ТОВ «Глорія Трейд», 3018 с.

Житомирський державний технологічний університет кафедрі комп'ютеризованих систем управління та автоматики. (2017). *ОПП*. Retrieved from URL: http://www.ztu.edu.ua/.

Зарецкая, С. & Семеко, Г. (2002). Тестирование и прием в высшие учебные заведения: опыт США. *Экономика образования,* 5, 37–51.

Зарецкая, С. & Семеко, Г. (2003). Федеральная помощь студентам и доступность высшего образования США. *Актуальные проблемы экономики образования,* 1, 59–66.

Зубик, Л. (2016). *Формування професійних компетентностей майбутніх бакалаврів з інформаційних технологій у процесі вивчення фахових дисциплін.* (Дис. канд. пед. наук). Національний університет водного господарства та природокористування. Рівне.

Зубик, Л. (2016). Аналіз структури підготовки бакалаврів з Інформаційних технологій. *Молодь і ринок*, 3(134), 173–174.

Зязюн, І. (2001a). Технологізація освіти як історична неперервність. *Неперервна професійна освіта: теорія і практика,* 1, 73–85.

Зязюн, І. (2001b). Філософія педагогічної якості у системі неперервної освіти. *Вісник Житомирського державного університету імені Івана Франка*, 25, 13–18.

Інформаційна безпека. (2010). *Аналіз підготовки фахівців з інформаці*йної безпеки в Україні. Навчальні матеріали он-лайн. Retrieved from URL: http:// info. pidruchniki.com/.

Кастельс М. (2002). *Информационная эпоха: экономика, общество и культура.* В О. И. Шкаратана (Пер. &Ред.), М.: ГУВШЭ, 608 с.

Київський національний університет ім. Тараса Шевченка, факультет інформаційних технологій, кафедра кібербезпеки та захисту інформації. (2017). Retrieved from URL: http://kbzi.knu.ua/.

Каушан, Т. (2011). Особливості підготовки майбутніх фахівців із комп'ютерних наук у вищому навчальному закладі І-ІІ рівнів акредитації. *Науковий вісник МДУ імені В.О. Сухомлинського, Педагогічні науки*, 1,112-115.

Кірей, К. (2016). Методичні підходи щодо підготовки майбутніх фахівців з інформаційних технологій. *Педагогіка*, 258 (270), 17-20.

Коваленко, О. (2010). Неперервна педагогічна освіта у США: сучасний стан і перспективи розвитку. *Педагогічні науки: теорія, історія, інноваційні технології, 6(8)*, 127-132.

Ковалюк, Т. (2013). Стан підготовки ІТ-фахівців в Україні. *Вища школа,* 8, 21–36.

Кошманова, Т. (2002*). Розвиток педагогічної освіти у США (1960–2000 рр.).* (Дис. д-ра пед. наук). Інститут педагогіки і психології професійної освіти АПН України, 589 с.

Куцаєв, В., Живило, Є., Срібний С. & Черниш Ю. (2014). *Розширення термінології сучасного кіберпростору.* Retrieved from URL: http://mino.esrae.ru/.

Лебідь Ю. (2001). Сучасні реформи освіти США, їх вплив на розвиток освітніх процесів в середовищі української діаспори. *Теоретичні питання освіти і виховання.* (Зб. наук. праць). К.: ВЦ КДЛУ, 18, 49–51.

Лєнков, С., *Головань С., Хорошко В. & Щербак Л.* (*2008*). Напрями формування системи знань фахівців захисту інформації з обмеженим доступом. *Вісник КНУ ім. Т. Шевченка. Військові спеціальні науки,* 20,40-44.

Ліпкан, В. & Череповський, К. (2014). *Інкорпорація інформаційного законодавства України.* (Монографія). В В.О. Ліпкана (Ред.), К.:ФОП Ліпкан О.С., 408 с.

Лозинський, О. & Грицюк, Ю. (2012). Підготовка фахівців з інформаційної безпеки у Львівському Державному Університеті Безпеки Життєдіяльності. *Актуальні питання навчання Системи обробки інформації*, 5 (103), 172–175.

Лукидес, М. (2014). Full-stack разработчики. Программисты, понимающие весь стек, обычно создают более качественные приложения. Retrieved from URL: https://dev.by/lenta/main/.

Макаренко, Є. (2012). Геополітіка и прагматика стратегії зміцнення світового лідерства США у XXI столітті. *Дослідження світової політики*, 4(61), 3–12.

Маслянко, О. (2017). Кремнієва Долина. Retrieved from UTL:http://eizvestia.com/uk/.

Матвійчук, Л. & Романюк, А. (2016). Програмні продукти у процесі викладання інформатики студентів гуманітарних ВНЗ в умовах модернізації вищої освіти. *Молодь і ринок.* 2, 80-84.

Матвійчук-Юдіна, О. (2017). Ключові компетентності фахівців спеціальності «Кібербезпека» з предмету «Комп'ютерна графіка» згідно індустріальної

моделі промисловості. *Вісник Житомирського державного університету імені Івана Франка*, 4 (90), 93-98.

Матійків, І. (2006). Компетентнісний підхід до професійної підготовки майбутніх фахівців. *Педагогіка і психологія професійної освіти : наук.-метод. журнал,* 3, 44–53.

Мей, Кристофер (2004). *Інформаційне суспільство. Скептичний погляд.* В М. Войцицька (Пер.) К.: *К.І.С*., 220 с.

Мельник, С. & Матросов, В. (2012). Перспективи розвитку системи експорту освітніх послуг в Україні. *Вища школа*, 1, 43 – 53.

Мельник, С., Тихомиров, О. & Лєсков, О. (2011). До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Київського національного університету імені Тараса Шевченка*. К.: ВІКНУ, 30, 165-172.

Мельник, С. (2016). Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. *Інформаційні технології і засоби навчання,* 55 (5), 187 – 197.

Морозова, Т. (2005.) Образовательные стандарты подготовки ИТ-специалистов в Украине. *Современные информационные технологии и ИТ-образование*. Retrieved from URL: http://2005.it-edu.ru /docs/1/1-08.

Морська, Л. (2007). *Теоретико-методологічні засади підготовки вчителя іноземних мов до використання інформаційних технологій.* (Монографія). Тернопіль,ТНПУ ім. В. Гнатюка, 243 с.

Національний авіаційний Університет, НН ІІДС, кафедра БІТ; кафедра ЗІ; НН ІКІТ, кафедра КСЗІ. Retrieved from URL: http://www.nau.edu.ua/.

Національний технічний університет України «КПІ імені Ігора Сікорського». (2017). *ОПП.* Retrieved from URL : http://lll.kpi.ua/.

Нечитайло, В. (1996). *Інформаційне суспільство»: критичний аналіз космополітичних концепцій майбутнього людства*. (Автореф. дис.д-ра філос. наук). НАН України, Інститут філософії, 46 с.

Ничкало, Н. (2000). Неперервна професійна освіта: міжнародний аспект. В І. А. Зязюн (Ред.), *Неперервна професійна освіта:проблеми, пошуки, перспективи*. (с. 58 –80). Київ, Віпол.

Ничкало, Н. (2001). Неперервна професійна освіта як філософська та педагогічна категорія. *Неперервна професійна освіта: теорія і практика*, 9-22.

Ничкало, Н. (2001). Теоретико-методологічні проблеми і перспективи досліджень з неперервної професійної освіти. *Неперервна професійна освіта: теорія і практика***.** (Зб. наукових праць). Інститут педагогіки і психології проф. освіти, 1, 35–41.

Ничкало, Н. (Ред.) (2002). *Державні стандарти вищої освіти: теорія іметодика.* Хмельницький: ТУП, 334с.

Ничкало, Н. & Кудін, В. (Ред.) (2002). *Професійна освіта в зарубіжних країнах: порівняльний аналіз*. Черкаси, Вибір, 322с.

Ничкало, Н., Левовицький, Т., Вільш, І. & Зязюн І., (Ред.) (2003). Національна доктрина розвитку освіти, педагогічна наука в Україні. *Професійна освіта: педагогіка і психологія,* 4, 421–438.

Нікітченко, М. & Нікітченко, М. & Омельчук, Л. (2013). Порівняльний аналіз українського стандарту освітньо-професійної підготовки з інформатики та міжнародного стандарту «Computer Science». *Актуальні проблеми підготовки спеціалістів ІКТ(АППСІКТ-2013)* (с. 130– 134), *Хмельницький*.

Ніколаєнко, С. (2006). *Стратегія розвитку освіти України: початок XXI століття*. Київ, Знання, 253с.

Падалко, Н. (2008). *Формування професійних знань в майбутніх програмістів у процесі вивчення математичних дисциплін.* (Автореф. канд. пед. наук). Теорія і методика професійної освіти. Житомирський державний університет ім. Івана Франка, 20 с.

Пазюра, Н. (2015a). Загальна характеристика альтернативної педагогічної освіти в США. Вісник Національного авіаційного університету. *Педагогіка. Психологія*. (Збірник наукових праць). Київ, НАУ, 92 – 98.

Пазюра, Н. (2015b). Особливості підготовки фахівців з середньою кваліфікацією в США. *Науковий вісник мукачівського державного університету, «Педагогіка та психологія».* 2 (2), 120– 125.

Панченко, В. (2010). *Гуманітарна та технологічна складові у визначенні поняття «інформаційна безпека».* Актуальні проблеми управління інформаційною безпекою держави. (Зб. матер, наук.-прак. конф.), 17 березня 2010 року, (с. 205-206), Київ. Наук.-вид. відділ НА СБ України.

Парил, В. (1991). Профессорско-преподавательский состав высшей школы США. *США. Экономика. Политика. Идеология,* 1, 52–64.

Пацевко, Н. (2004). *Еволюція теорії і практики навчання у Сполучених Штатах Америки першої половини XX століття*. (Дис. канд. пед. наук). Національний університет ім. Тараса Шевченка. Київ, 248 с.

Поліхун, Н. & Локшина, О. (2010). *Акредитація як механізм вимірювання якості освіти: досвід університетів США.(матеріали науково-практичного семінару), (Київ, 17 черв. 2010р.).* НАПН України та ВНЗ України. В О. І. Локшиної та Н. І. Поліхун. (Ред.), (с.85-89). *Київ, «Інформаційні системи»*.

Пододіменко, І. (2014). Сучасні вимоги суспільства до професійної підготовки фахівця у галузі інформаційних технологій в Японії. *Comparative Professional Pedagogy*, 4(2), 190-196.

Рекомендация МСЭ-Т X.1205. (2009). Обзор кибербезопасности. *Женева: МСЭ*, Retrieved from URL: http://www.itu.int.

Романовський, О. (1997). Хроніка вищої освіти США (діяльность державних і недержавних закладів). *Київ, НПУ ім. М. П. Драгоманова*, 78 с.

Романовський О. (2001). *Теоретичні і методичні основи підготовки інженера у вищому навчальному закладі до майбутньої управлінської діяльності.* (Автореф. д-ра пед. наук) Національний педагогічний університет, ім. М. П. Драгоманова, Київ, 40 с.

Романовський, О. (2002). *Теорія і практика зарубіжного досвіду в підприємницькій освіті України.* (Монографія). Київ, Деміур, 400с.

Сбруєва, А. (2004). *Тенденції реформування середньої освіти розвинених англомовних країн в контексті глобалізації (90-ті рр. XX – початок XXI ст.).* (Монографія). Суми: Сум. обл. друкарня: Козацький вал, 500 с.

Сейдаметова, З. (2004). Нові технології навчання. *Науково-методичний центр вищої освіти*, 39, 27-33.

Сейдаметова, З. (2012). Підготовка магістрів в ІТ-*галузі Комп'ютерно-оріентовані системи навчання, Науковий часопис НПУ ім. М.П.Драгоманова, 2. Комп'ютерно-оріентовані системи навчання,* 12(19), 48-53.

Семеріков, С. (2009). *Теоретико-методичні основи фундаменталізації навчання інформатичних дисциплін у вищих навчальних закладах* (Дис. д-ра пед. наук.), Національний педагогічний університет імені М. П. Драгоманова, Київ.

Скрипник, Л. (2013). Щодо кібербезпеки СТСЗИ, 2(24), 126-130.

Собчак, Н. (2004). *Зміст і форми професійної підготовки соціальних працівників у системі неперервної освіти США.* (Дис. канд. пед. наук) Тернопільський держ. пед. ун-т ім. Володимира Гнатюка. Тернопіль, 228 с.

Соснін, О. (2005). *Державна політика в галузі управління інформаційним ресурсом України* (Дис. д-ра. політ. наук). Одеська національна юридична академія, Одеса. 124-128.

Сьомін, С. (2016). *Система підготовки кадрів для сил безпеки України: проблеми та перспективи розвитку.* (Аналітична доп.) *В В.П. Горбуліна (Ред.) Київ, НІСД,* 50 с.

Спірін, О. (2007). *Теоретичні та методичні засади професійної підготовки майбутніх учителів інформатики за кредитно-модульною системою*. (Монографія). *Житомир. Вид-во ЖДУ ім. І. Франка*, 300 с.

Спірін, О. (2014). *Досвід підготовки наукових кадрів з інформаційно-комунікаційних технологій в освіті* (до 15-річчя Інституту інформаційних технологій і засобів навчання НАПН України). Комп’ютер у школі та сім’ї. 2 (114), 3–8.

Сумський ДУ.(2017). *ОПП*. Retrieved from URL: http://sts.sumy.ua/.

Сухомлин, В. (2003). *Введение в анализ информационных технологий*. М.: Горячая линия.Телеком, 457 с.

Тернопільський Національний технічний університет імені Івана Пулюя. (2017). *ОПП.* Retrieved from URL: http://tntu.edu.ua/.

Тернопільський НТУ імені Івана Пулюя. (2017). *Державний стандарт компетентностей.* Retrieved from URL: http://tntu.edu.ua/.

Тихомиров, О. (2014.) *Забезпечення інформаційної безпеки як функція сучасної держави.* (Монографія). *В Р.А. Калюжний (Ред). Центр навч.-наук. та наук.-практ. вид. НА СБ України.1*96 с.

Україна. Класифікатор професій ДК 003:2010. (2010). *К.: Держспожив стандарт,* 2608 с.

Україна. (2016). Парламентські слухання Верховної Ради України. *«Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України».*Retrieved from URL: http://zakon2.rada.gov.ua/laws/.Україна. *Постанова Кабінету Міністрів України. (2006). 674.* Retrieved from URL: http://zakon.

Україна. Рада національної безпеки і оборони України. (2016). *Стратегія кібербезпеки України*. Retrieved from URL: http://zakon3.rada.gov.ua/.

Україна. Верховна Рада України. (2017). *Закон України Про основні засади забезпечення кібербезпеки України.* Retrieved from URL: http://zakon5.rada.gov.ua/.

Україна. *Офіційний вісник України (2016 р). 79,. Закон України. Про вищу освіту. ст. 2647.* Retrieved from URL: http://zakon2.rada.gov.ua/laws/.

Україна. *Про внесення змін до постанови Кабінету Міністрів України 266. (2015).* Retrieved from URL: http://zakon2.rada.gov.ua/laws/.

Україна. *Указ Президента Про Доктрину інформаційної безпеки України.* (2009). Retrieved from URL: http://zakon4.rada.gov.ua/.

Україна. *Проект Стратегії забезпечення кібернетичної безпеки України.*(2013). Retrieved from URL: http://www.niss.gov.ua.

Україна. Законом України № 537-V. (2007). «*Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки*».

Україна. Закону України *«Про вищу освіту»* №1556-VII. (2014).

Україна. *Конвенція Ради Європи про кіберзлочинність.* (2001). Retrieved from URL: http://zakon2.rada.gov.ua.

Україна. *Конституції України. Стаття 17.* Retrieved from URL: http://zakon4.rada.gov.ua/laws/show/.

Україна. Верховна Рада. (2013). «*Стратегія сталого розвитку «Україна – 2020»*. Retrieved from URL: http://zakon3.rada.gov.ua/laws/show/5/2015.

Україна. Перелік із змінами, внесеними згідно з постановами КМ. Retrieved from URL: № 674 від 27.09.2016, та № 53 від 01.02.2017.

Україна. Постанова Кабінету Міністрів України. (2015). *«Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)»*.

Україна. Постанова Кабінету Міністрів України № 261. (2016). Про розробку методичних рекомендацій: *«Розроблення освітніх програм. Методичні рекомендації».*

Україна. Постанова Кабінету Міністрів України. (2011). *«Про затвердження Національної рамки кваліфікацій».*

Україна. Постанова Кабінету Міністрів України №1187. (2015).*«Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти».*

Україна. *Про затвердження Положення про освітньо-кваліфікаційні рівні ...* (2001). Про освітньо-кваліфікаційні рівні (ступеневу освіту). Retrieved from URL: http://*zakon.rada.gov.ua/*.

Україна. Наказ Міністерства освіти і науки України № 99. (2010). *Про Концепцію організації підготовки бакалаврів в Україні»*. Retrieved from URL: http://osvita.ua/.

Україна. *Проект Стратегії забезпечення кібернетичної безпеки України.* (2013). Retrieved from URL: http://zakon2.rada.gov.ua/laws/show/.

Україна. Розпорядження Кабінету Міністрів України № 356. (2013). *«Про схвалення Стратегії розвитку інформаційного суспільства в Україні».*

Україна. Указ Президента України № 449/2014. (2014). Про рішення Ради національної безпеки і оборони України. «*Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»*.

Україна. Указ Президента України № 96/2016 (2016). «Про рішення Ради національної безпеки і оборони України, *«Про Стратегію кібербезпеки України».* Урядовий кур'єр.(2016). 03, 52.

Україна. Kyiv Cyber Academ. (2017). *ОПП.* Retrieved from URL: http://channel4it.com/.

Филиппова Л. (1981). *Высшая школа США.* М.: Наука, 328 с.

Чванова М. & Анурьева М. (2012). Подготовка кадров в области информационной безопас-ности в США. *Вестник Тамбовского университета. Сер.: Гуманитарные науки. Тамбов,* 112, 126-133.

Черкаський державний технологічний університет, кафедра інформаційної безпеки та комп'ютерної інженерії. (2017). *ОПП.* Retrieved from: http://chdtu.edu.ua/.

Черноног О. (2012). Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління Retrieved from URL: http://mino.esrae.ru/.

Шаран, Р.(2009). Кваліфікаційні напрями підготовки фахівців інформаційних технологій в США. *Вища освіта України. Педагогіка вищої школи: методологія, теорія, технології,* 3 (1), 611–614.

Шаран, Р. (2010). Досвід США з підготовки магістрів інформаційних технологій в системі дистанційної освіти та можливості його впровадження в Україні. *Порівняльно-педагогічні студії* , 1–2, 29-35.

Шутова, М. (2005). *Проблеми реформування загальної середньої освіти в США (1950-ті – 1990-ті рр.).* (Автореф. дис. канд. пед. наук.) Київ. 24 с.

Ярова, М. (2015). Кібербезпека в Україні: у 2015 році наша країна – «найгарячіша» точка Європи. Retrieved from URL: http://news.finance.ua/.

Action on Cybercrime and Cyber Security. (2013). Retrieved from URL: http://www.unsceb.org/content/action-cybercrime-and-cyber-security.

An Act to establish the Department of Homeland Security, and for other purposes.(2018,). Retrieved from URL: http://www.dhs.gov/

Agency of accreditation. (2017). Retrieved rom URL: http://ope.ed.gov/accreditation.

Association of Specialized and Professional Accreditors. (2011). Retrieved from URL: http://www.aspa-usa.

Allabarton, R. (2015). The skills gap is widening – but here's how you can close it. Retrieved from URL: http://thenextweb.com/insider/.

American association of community colleges. (2002). *Protecting information: the role of community colleges in cybersecurity education*, Community college press, Washington, 139 p.

Athey T. (1998). Nontraditional Universities Challenge Twenty-First Century Higher Education. *On the Horizon*, 6 (5), 5–7.

Baker College. (2017). Retrieved from URL: https://www.baker.edu/

Becker, H. (2001). A model for improving the performance of integrated learning systems. *Educational Technology*, 2, 6–15.

Bellevue University Nebraska. (2017). Retrieved from URL: https://www.unomaha.edu/

Boggs, G. (2003). President's report to the board of directors American association of community colleges, *Washington*, 11, 13–18.

Boggs, G. (1999). What the learning paradigm means for faculty. *New Directions for Teaching and Learning*, 51(5), 3–5.

Bork, A. (2000). *Learning technology.* Educause Review, 35(1), 74–81.

Bork, A. (2001).Tutorial distance learning-rebuilding our educational system. *New York. Kluwer Academic,Plenum*, 197p.

Bonwell, C., & Sutherland, T. (1996). *The active learning continuum: Choosing activities to engage students in the classroom*. San Francisco: Jossey-Bass, Inc. (3-16).

Boud, D. (1981). *Developing Student Autonomy in Learning*. London. Kogan Page. 222 p

Bromwich, D. (2003). Politics by Other Means: Higher Education and Group Thinking. *NY ,Yale UP*, 178 p.

Brigham Young University-Provo. (2017). Retrieved from URL: https://catalog.byu.edu/

Business Insider. (2017). *The startup incubator Y Combinator quietly stopped.* Retrieved from URL: www.businessinsider.com/.

Bruce Schneier, (2013). *How to remain secure surveillance*. Retrieved from URL: http://www.theguardian.com/ world/e.

California State Polytechnic University-Pomona. (2017). Retrieved from URL: http://bulletin.csusb.edu/colleges /.

California State University-San Bernardino. (2017). Retrieved from URL: https://www.csusb.edu/.

Capitol Technology University. (2017). Retrieved from URL: https://www.captechu.edu/

Chabrow, E. (2001). *Cybersecurity as a Campaign Issue*. Retrieved from: http://www.govinfosecuritycom/blogs.

Children's Internet Protection. (2012). Retrieved from URL: https://www.webjunction.org/.../webjunction/Children_039_s.

Chvanova, M. & Anureva, M. (2012). Personnel training in information security sphere in the U.S.A. *Bulletin of the University of Tambov. Series: Humanities, Tambov*, 8(112), 126-133.

Curriculum Guidelines for Undergraduate Degree Programs in Cyber security. (2017). Retrieved from URL: http://csec2017.org/.

Cyber Security Strategy for Germany. (2018). Retrieved from URL: https://www.enisa.europa.eu/.

Caria Giovanni Battista. (2017). *«HackerAttack»*. Retrieved from URL: http://www.deseco.admin.ch/.

Computer Science Curricula. (2013). *Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. Retrieved from URL: http://www.acm.org/education/.

Conceptual Foundations. (2017). *Strategy Paper on Key Competencies. An Overarching Frame of Reference for an Assessment and Research Program – OECD (Draft).* Retrieved from URL: http://www.rada.gov.ua/.

Council for Higher Education Accreditation. (2017). Retrieved from URL: http://www.chea.org.

Council of Europe. (2001). *Convention on Cybercrime*, No. 185. Budapest, European Treaty Series, 22 p.

Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 201. *Lanzarote, Council of Europe Treaty Series*, 19 p.

Council of the European Union. (2002). Council Framework Decision of 13 June 2002 on combating terrorism, *Official Journal*, 164(3), 1-5.

Council of the European Union. (2014). *Cyber defence policy framework*, Brussels, 14 p.

Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*,108. Strasbourg, Council of Europe Treaty Series, 9 p.

Council of Europe. (2010). *A Digital Agenda For Europe*, The European economic and social committee and the committee of the regions, 19 p.

Council of the European Union. (2015). *The European agenda on security*. Brussels, the European economic and social committee and the committee of the regions, 20 p.

Cybersecurity Overview. Geneva: ITU, (2009). Retrieved from URL: http://www.itu.int/ITU-T/ipr/.

Cyberwellness Profile United States (2010). Retrieved from URL: http://www.itu.int/en/ITU.

Cyberwellness Profile United States. (2013). Retrieved from URL: http://www.itu.int/en/ITU**.**

Cyber Security Research and Development Act. (2017). Retrieved from URL: https://www.law.cornell.edu/.

Davis, G.(2002). Information Systems as an Academic Discipline: Explaining the Future, *Journal of Information Systems Education* (4)4, 2-7.

Davis, G. &Gorgone, J. (Eds.) (1997, Winter). IS'97 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems, *The Data Base for Advances in Information Systems,* (28)1.

DEV.BY (2016). Retrieved from URL: https://dev.by/lenta/main/it-industriy.

Denning, P. (2007). Computing is a natural science. *Communications of the ACM*. 50(7) 13. doi:10.1145/1272516.1272529.

Detert, K. (2011). *Are General Subjects Relevant to Engineering Education*. (p. 59-67). Proceeding of the 3rd World Congress on Engineering Education and Training, Cairo, Egypt 1.

DHS (Department of Homeland Security). (2012). Task Force on CyberSkills, Cyber Skills Taks Force Report, D.o.H. Security. *Washington, DC*.,1-41.

Electronic Signatures in Global and National Commerce.(2000). Retrieved from URL: www.law.cornell.edu/.

European Commission. (2013). *Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace.* Brussels, The European economic and social committee and the committee of the regions, 20 p.

European Commission. (2015). *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime*. Retrieved from URL: http://europa.eu/.

European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union,* L 345/75, 1-8.

European Commission. (2012). *Final communication from the Commission to the European Parliament*, Brussels, the European economic and social committee and the committee of the regions European strategy for a better Internet for children, 17 p.

European Union. (2013). 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, *Official Journal of the European Union*, L 218/8, 1-7.

Embry-Riddle Aeronautical University (2017). Retrieved from URL: https://erau.edu/degrees/bachelor/cyber-intelligence-security/.

European Union. (2016). Directives of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union the European Parliament the Council of the European Union, *Official journal of the European Union,* 194(1),1-32.

Felder, R., & Brent, R. (2003). Learning by doing. Chemical Engineering and Education, 37(4), 282–283.

Franscella, J. (2002). Cybersecurity vs. Cyber Security: When, Why and How to Use the Term. Retrieved from: www.infosecisland.com/.

Florida Polytechnic University. (2017). Retrieved from: https://www.florida edu/.

Fontbonne University. (2017). Retrieved from URL: https://www.fontbonne.edu/.

George Mason University.(2017). Retrieved from URL: https://volgenau.gmu.edu/.

Walsh University Undergraduate Catalog 2001-2002. (2001, August), *West Hartford, Connecticut, USA,* XLV (3), 221 p.

Georgia Armstrong State University. (2017). Retrieved from: https://www.armstrong.edu/.

George Fox University. (2017). Retrieved from URL: https://www.georgefox.edu/.

Gorgone, J.&P. Gray, et al. (2000, January), MSIS 2000; Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems *Communications of the Association for Information Systems,* (7)1.

Gorgone, J. & Davis, G. (2003). *MSIS* 2002: Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems. *Communications of the Association for Information Systems, (11) 1, 1-63.*

Gorgone, J. & Kanabar ,V. (2003, August). Prospective Tracks in the MSIS 2000 Model Curriculum Framework*, Proceedings of the Americas Conference on Information Systems, Data Base, 31*(3), 1-69.

Gorgone, J., Gray P., Stohr E. et al. (2006). Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems. *Communications of the Association for Information Systems.* 17, 1–56.

Gorgone, J. & Gray, P. (2005). MSIS 2006 Curriculum Preview" *Communications of the Association for Information System,* (15) 30.

Harrisburg University of Science and Technology .(2017). Retrieved from URL: http://harrisburgu.edu/.

Henderson, E. (1979). The Concept of School-Focused Inservice Education and Training. *British Journal of Teacher Education*. 51, 1. p. 17–25.

Hilburn, T. (2002). The Impending Changes in Software Education. *IEEE Software.* 19 (5) , 22–24.

Hislop, G. (1997). Evaluating an asynchronous graduate degree program Frontiers in Education. (p. 437–440). *Conference, 27th Annual Conference: Teaching and Learning in an Era of Change* . Proceedings, 1.

Higher Education in the US. (2017). Retrieved from URL: http:// www.iclass.ru/study_abroad_high_usa/.

Holdaway, E. (1994). Practices and Opinions Reported by Coordinators of Graduate Programs . *Interchance.* 25, 1, 65–86.

Johnson, M. (2007a). Definitions and Models in Curriculum Theory. *Educational Theory.* 17 (2), 127–140.

Johnson, M. (2007b). Intentionality in Education. A Conceptual Model of Curricular and Instructional Planning and Evaluation. *New York: Centre for Curriculum Research and Services,* 264p.

Information technology. (2017). *Guide for ISO/IEC 12207 (Software Life Cycle Processes)*. Retrieved from URL: http://webstore.iec.ch/.

International Strategy for Cyberspace. (2011). Retrieved from URL: https://www.enisa.europa.eu/.

Impagliazzo, J & Gorgone, J. (2002). "Professional Accreditation of Information Systems Programs, *Communications of the Association for Information Systems, (*9)3 , 50-63.

Iona College. (2017). Retrieved from URL: https://www.iona.edu/.

Innovation in education. (2004). Alternative routes to teacher certification. U.S. department of education, office of innovation and improvement. *Washington, D.C.*, 70 p.

Indiana University of Pennsylvania-Main Campus. (2017). Retrieved from URL: https://www.iup.edu/c.

Information Security. (2017). Retrieved from URL: http://csrc.nist.gov/drivers/documents/.

Karnikau, R. (1975). Communication for the safety professional. *Chicago,* 215 p.

KIDS Act. (2008). Retrieved from URL: https://www.law.cornell.edu/.

Knuth, D. (1996). Selected Papers on Computer Science. Stanford, *California: Center for the Study of Language and Information,* 59, 274 p.

Koumi, J. (2015). Matching media Attributes to Teaching Functions and Hence to Learning Objectives. Retrieved from URL: http://www.bme-tk.bme.hu/.

Kyiv Cyber Academy. (2017). Retrieved from URL: http://channel4it.com/.

Lindenwood University. (2017). Retrieved from URL: http://www.lindenwood.edu/

Louisiana Tech University. (2017). Retrieved from: http://catalog.latech.edu/.

Louisiana Southern University and A&M College. (2017). Retrieved from URL: http://www.subr.edu/.

Martin, N. & Woodward, B. (2013). Building a Cybersecurity Workforce with Remote Labs. *Information Systems Education Journal*, 11 (2), 57-62.

Master of Science in Information Assurance and Security. (2015). Retrieved from URL:https://www.mercy.edu/ arts/http

Matviychuk-Yudina O. (2009) Information Technologies of the Higher Education System, Publishing house Education and Science, Dil. 11, pp. 9-15.

Matviychuk-Yudina O. (2017 a). Key competencies of specialists in the specialty Cyber security on the subject Computer graphics according to the industrial model of industry, Bulletin of Zhytomyr State University, No. 4 (90), pp. 93-98.

Matviychuk-Udina, O. (2017 b). Domestic and foreign experience of the content formation of computer graphics education for future bachelors of cyber security *Information Technologies and Learning tools,* 11 (2), 57-62.

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations– An Analysis of the UN's Activities Regarding Cyber-security*" Belfer Centre for Science and International Affairs, Harvard Kennedy School.

Megan, S. (2017). First Female CTO Of The U.S. Hopes Tech's History

Moore, M. & Kearsley, G. (2005). Education: A Systems View. Belmont CA: Wadsworth Publishers, 146–151.

Morze, N & Buinytska. O. (2001).Open E-environment – The Key Instrument of the Education Quality Social Sciences, Education, Media studies, *Communication studies Wydawnictwo Uniwersytetu Śląskiego,* 27-46.

Morze, N. & Buinytska, O. (2015). The Key Instrument Of The Education Quality, International Journal of Research in E-learning, 1 (1), 25-47.

Morze N. & Buinytska, O. (2016). Curriculum of the Politechnika Poznańska Kierunek. Retrieved from URL: http://fee.put.poz . The National Security Strategy of the United States of America. (2015). Retrieved from URL: http://nssarchive. us/national-security-strategy.

National Centers of Academic Excellence in Information Assurance. (2017). Cyber Defense (IA/CD). Knowledge Units. *Jointly Sponsored by the National Security Agency (NSA).*

National Strategy to Cyberspace Secure - US-CERT (2013). Retrieved from URL: https://www.us-cert.gov/sites/.../cyberspace_strategy.

NATO. (2008). *Partnership Action Plan on Defence Institution Building reference curriculum.* Canada: Canadian Defence Academy, 75 p.

NATO. (2016). *Cybersecurity: a generic reference curriculum*, Kingston, ON Canada: NATO graphics & printing, 72 p.

NATO (2017). Cooperative Cyber Defence Centre of Excellence. Retrieved from URL: https://ccdcoe.org/sites/default/files/multimedia/.

Natalya Pazura. (2015). Features of training specialists with secondary qualifications in the USA. *Scientific Bulletin of Mukachevo State University. Series of "Pedagogy and Psychology" – a collection of scientific articles*. 2 (2), 120-125.

NIST, National Initiative for Cybersecurity Education Strategic Plan, National Institute of Standards and Technology (2012). Retrieved from URL: http://nvlpubs.nist.gov/.

NIPP (2013a). Partnering for Critical Infrastructure Security and Resilience Retrieved from URL: http://www.dhs.gov/.

NIPP (2013b). *Partnering for Critical Infrastructure Security and Resilience* Retrieved from URL: http://www.dhs.gov/.

Northeastern State University. (2017). Retrieved from URL: https://academics.nsuok.edu/.

Nunamaker, Jr., Couger, J. & Davis, G. (Eds.) (1982). Information Systems Curriculum Recommendations for the 80s. *Undergraduate and Graduate Programs, Communications of the ACM* (25)11, 781-805.

Pazynyuk, T., Oreku, G. & Li, J. (2008*). Mathematical model for wireless sensor nodes security.* (p.1305–1310). International Conference of Machine Learning and cybernetics (ICMLC 2008), China, 3.

Pazynyuk, T., Oreku, G. & Li, J. (2008). *Reliable data aggregation protocol for wireless sensor networks.* (p.13–16).Third International Conference on Digital Information Management (ICDIM), London.

Pododimenko, I. (2014). Current requirements of the societyto the professional training of specialists in information technology industry in Japan. *Comparative Professional Pedagogy* 4(2), 23-29.

Protecting Children in the 21st Century Act. (2011). Retrieved from URL: https://www.law.cornell.edu/.

Radunović, V. (2013). DDoS - Available Weapon of Mass Disruption. (p.5-9). *Proceedings of the 21st Telecommunications Forum (TELFOR),* 33(1), Recommended Computer Science Core Curriculum (BS) for Information Assurance and Cyber Security Career Focus Report to Congress on Cybersecurity USNI News. Retrieved from URL: https://news.usni.org/.

Rattray, G. (2010). Cambridge, MA Retrieved from URL: http://www.tandfonline J..com/doi/abs/.

Roadmap for Cybersecurity of Control Systems. (2011). Retrieved from URL: https://ics-cert.us-cert.gov/.

Roadmap for Improving Critical Infrastructure Cybersecurity. (2014). Retrieved from URL: http://www.nist.gov/cyberframework/upload/.

Roadmap to Achieve Energy Delivery Systems Cybersecurity. (2011). Retrieved from URL: http://e nergy.gov/.

Rossett, A. & Vaughan, F. (2003). Blended learning CEO Epic Group plc, 52 Old Steine, Brighton BN1 1NH, Retrieved from: http://www.obs.ru/.

Rubino, N., Soltys, M., Wright, G. &Young. R. (1994). Alternative Teacher Certification: An Avenue for Quality and Diversity in Public Education. *Wilmington College*, 35, 23- 31.

Saint Vincent College.(2017). Retrieved from URL: http://www.stvincent.edu/.

Schirf, E. & Serapiglia, A. (2017). Identifying the Real Technology Skills Gap: A Qualitative Look Across Disciplines, *Information Systems Education Journal* , 15 (6), 72-82.

Semin, S. (2014). The training system the Security Service of Ukraine: Institute for Strategic Studies (NISS). Retrieved from URL: http www://.niss.gov.ua.

Southern Arkansas University (2017). Retrieved from URL: https://web.saumag.edu/.

Southeast Missouri State University. Retrieved from URL: http://semo.edu/.

Seelen, W.& Behrend, K. (2015). Principles of Neural Information Processing. Cognitive Systems Monographs. Springer International. *Publishing AG Switzerland is part of Springer Science+Business Media,* 76–77. Retrieved from: www.springer.com.

Stevens Institute of Technology. (2017). Retrieved from URL: https://www.stevens.edu/.

St. John's University. (2017). Retrieved from URL: https://www.stjohns.edu/.

Tarasova, O. (2011). *Priorities for higher education in the United State.* Statistic bulletin of the State Border Guard Service of Ukraine for 2011. Retrieved from URL:http://nbuv.gov.ua/.

Tech Hire. (2016).Retrieved from URL:https://hightech.fm/2016/08/23/silicon-valley.

The Strategy Project of Providing Cybernetic Security of Ukraine. (2013). Retrieved from: http://www.niss.v.ua/.

Tennessee Technological University. (2017). Retrieved from URL: http://catalog.tntech.edu/.

The University of Tennessee at Chattanooga. Retrieved from URL: https://www.utc.edu/.

The Carnegie Classification of Institutions of Higher Education-2000 Edition. Menlo Park. CA: Carnegie Foundation for the Advancement of Teaching. (2001). 198 p.

The Department Of Defense Cyber Strategy. (2015). Retrieved from URL: http://www.defense.gov/.

The University of West Florida. (2017). Retrieved from: https://uwf.edu/.

Trow, M. (1988). American Higher Education: Past, Present, Future / Martin Trow // Educational Researcher. 14, 13–23.

Watson, C. (2008). *U.S. national security: a reference handbook.* Santa Barbara, California: ABC-CLIO, 59 p.

Weiner, J. (2014). The STEM paradoxes: Graduates' lack of non-technical skills, and not enough women. Retrieved from URL: https://www.washingtonpost.com/blogs/.

University of Connecticut (2017). Retrieved from URL: https://catalog.uconn.edu/.

University of Nebraska at Omaha. (2017). Retrieved from URL: https://www.unomaha.edu/.

University of South Alabama. (2017). Retrieved from URL: http://www.southalabama.edu/.

United Nations Educational, Scientific and Cultural Organization. (2016). *A policy review: building digital citizenship in Asia-Pacific through safe, effective and responsible use of ICT*, France and UNESCO Bangkok Office, 130 p.

Uniform Electronic Transactions Act. (1999). Retrieved from URL: http://www.uniformlaws.org/.

University of Southern Maine. (2017). Retrieved from URL: https://usm.maine.edu/.

University of Maryland-College Park. (2017). Retrieved from URL: http://undergrad.cs.umd.edu/.

University of Michigan-Dearborn. (2017). Retrieved from URL: https://umdearborn.edu/.

University of MemphisTexas A & M University-Corpus Christi. (2017). Retrieved from URL: http://sci.tamucc.edu/.

University of Central Missouri. (2017). Retrieved from URL: https://www.ucmo.edu/.

University of North Carolina at Charlotte. (2017). Retrieved from URL: https://academics.uncc.edu/.

University of Wisconsin-Stout. (2017). Retrieved from URL: https://wwwprod.uwstout.edu/.

University of Charleston. (2017). Retrieved from URL: http://www.ucwv.edu/.

University of Washington-Seattle Campus. (2017). Retrieved from URL: https://www.uwb.edu/.

U.S. Code Chapter 103, (2015). *Controlling the Assault of Non-Solicited Pornography and Marketing.* Retrieved from URL: https://www.law.cornell.edu/uscode/text/15/chapter-103.

U.S. Code § 1029, (2011). *Fraud and Related Activity in Connection with Access devices.* Retrieved from URL: www.law.cornell.edu/uscode/text/18/1029

U.S. Code § 1030, (2011). *Fraud and related activity in connection with computers.* Retrieved from URL: www.law.cornell.edu/uscode/text/18/1030.

U.S. Code § 1037. (2012). *Fraud and related activity in connection with electronic mail.* Retrieved from URL: www.law.cornell.edu/uscode/text/18/1037.

U.S. Code Chapter 119 (2011). *Wire and electronic communications in terception and interception of oral communications*. Retrieved from URL: www.law.cornell.edu/.

U.S. CodeChapter 121. (2011). *Stored wire and electronic communications and transactional records access*. Retrieved from URL: https://www.law.cornell.edu/.

U.S. Code § 552a (2011). *Records maintained on individuals* Retrieved from URL: www.law.cornell.edu/.

Webster University. (2017). Retrieved from URL: http://www.webster.edu/.

Whiting, R. (2005, September) Business and Industry Knowledge Will Be a Priority for IT Staffs in 2008 *Information Week*, 13.

Wheelwright, S. (1992). Revolutionizing Product Development. *Quantum Leaps in Speed, Efficiency and Quality New York : Free Press,* 90 p.

Wikipedia. (2009). *The Free Encyclopdia.* Retrieved from URL: http://en.wikipedia.org/wiki/.

Willimson, M. and Herbert, J. (2004). Testing student learning, evaluating teaching effectiveness. *Stanford, Calif : Hoover Institution Press,*337 p.

Word Book Encyclopedia : in 22 V.(2001). *Chicago: A Scott Fetzer Company,* 6, 470 p.

Wratcher, M., Morrison,E. , Riley,V. &Scheirton L. (1997). Curriculum and program planning: a study guide for the core seminar: programs for higher education. *Nova Southeastern University*, 1, 112 p.

Zais, R. (1982). *Curriculum: Principles and Foundation*. 144 p. Retrieved from URL: http://eizvestia.com/uk/.

Zygierewicz, A. (2013). *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*, Brussels, European Parliamentary research service, 8 p.

ДОДАТКИ

Додаток А

Довідка про впровадження результатів дослідження.

Додаток А-1

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

вул. Шевченка, 95, Чернігів, 14027, Україна

тел. +38(04622) 3-16-51;
факс +38(04622) 3-42-44
E-mail: cstu@stu.cn.ua
www.stu.cn.ua
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

CHERNIHIV NATIONAL UNIVERSITY OF TECHNOLOGY

95, Shevchenko str., Chernihiv, 14027, Ukraine

26.11.2018 № 101/10-158

На № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження Бистрової Богдани Василівни на тему: «Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США»
за спеціальністю 13.00.04 - теорія і методика професійної освіти

Результати дисертаційного дослідження Бистрової Богдани Василівни з теми «Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США» було апробовано і впроваджено у навчальний процес Чернігівського національного технологічного університету впродовж 2016-2017 років.

Дисертанткою здійснений аналіз особливостей професійної підготовки майбутніх бакалаврів з кібербезпеки в США. На особливу увагу заслуговує аналіз понятєво-категоріального апарату дослідження, законодавчої бази, виявлення особливостей навчальних програм, форм, методів навчання. Доповнення змісту навчально-педагогічних курсів новими змістовними матеріалами сприяє кращому розумінню закономірностей здійснення освітніх реформістських процесів у США і надає підґрунтя для подальшого використання їх ключових ідей в Україні.

Позитивні результати апробації дисертаційного дослідження Б. В. Бистрової дозволяють стверджувати про доцільність використання у освітньому процесі розроблених автором матеріалів.

Проректор
з науково-педагогічної роботи В.В.Кальченко

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ * 05460798

Система управління якістю сертифікована за ДСТУ ISO 9001:2009 (ISO 9001:2008)

The quality management system is certified according to the ISO 9001:2008

Додаток А-2

ЗАТВЕРДЖУЮ:
Проректор з навчальної
та виховної роботи
Національного авіаційного
університету
_____ І. Іванова
"05" 02 2018 р.

АКТ

про впровадження результатів дисертаційного дослідження
Бистрової Богдани Василівни на тему: «**Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США**»
за спеціальністю 13.00.04 - теорія і методика професійної освіти

Апробація результатів дисертаційного дослідження Богдани Василівни Бистровоїза темою «Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США» здійснювалась впродовж 2016-2017 років в Національному авіаційному університеті, на кафедрі безпеки інформаційних технологій (БІТ) в процесі викладання дисциплін для бакалаврів, спеціальності 125 «Кібербезпека».

Теоретичні та практичні аспекти досліджуваної Б.В. Бистровою проблеми, представлені у методичних рекомендаціях «Професійна підготовка бакалаврів з кібербезпеки: досвід США»,що успішно використовувались у процесі розробки навчальних планів та підготовки майбутніх фахівців з кібербезпеки, сприяли підвищенню зацікавленості та мотивації студентів до навчання, формування у них готовності до використання інноваційних ідей американського досвіду у їх майбутній професійній діяльності.

Цінність результатів дисертаційного дослідження вбачається й у розробці науково-методичних рекомендацій, щодо творчого використання прогресивних ідей американського досвіду у модернізації системи освіти України з професійної підготовки фахівців для ІТ-галузі. Це доводить практичну спрямованість проведенного дослідження і доцільність широкого впровадження його результатів у процесс підготовки бакалаврів з кібербезпеки.

Голова комісії,
завідувач кафедри БІТ,
лауреат Державної премії України
в галузі науки та техніки, д.т.н., проф.,
IEEE Senior Member — О. Корченко

Члени комісії:
доцент кафедри БІТ,
к.т.н., доц. — С. Гнатюк

доцент кафедри БІТ,
к.т.н., доц. — С. Казмірчук

Додаток А-3

ЗАТВЕРДЖУЮ:
Проректор з науково-дослідної роботи
та міжнародних зв'язків Черкаського
державного технологічного університету
д.т.н., проф.
_____ В.М. Рудницький
"___" _____ 2018

АКТ

про впровадження результатів дисертаційного дослідження
Бистрової Богдани Василівни на тему: «**Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США**»
за спеціальністю 13.00.04 - теорія і методика професійної освіти

Впровадження результатів дисертаційного дослідження Богдани Василівни Бистрової з теми «Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США» здійснювалась впродовж 2016-2017 років в навчальний процес Черкаського державного технологічного університету на кафедрі інформаційної безпеки та комп'ютерної інженерії.

Впровадження в практику роботи положень та вказівок, які містяться у методичних рекомендаціях «Професійна підготовка бакалаврів з кібербезпеки: досвід США», наукових статтях Б.В. Бистрової сприяло виробленню нових підходів щодо професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ України, мотивації студентів до засвоєння змісту навчального матеріалу, активізації їхньої науково-дослідної діяльності під час підготовки до семінарських та практичних занять та стимулювання самостійної роботи студентів.

Вважаємо, що дисертаційне дослідження Б.В. Бистрової має теоретичне і практичне значення, тому його результати доцільно екстраполювати у практику навчального процесу навчальних закладів України, що здійснюють професійну підготовку бакалаврів з кібербезпеки з метою модернізації освітньої програми.

Голова комісії,
завідувач кафедри ІБ та КІ,
к.т.н., доц. І.М. Федотова-Півень

Члени комісії:
доцент кафедри ІБ та КІ,
к.т.н., доц. І.В. Миронець

доцент кафедри ІБ та КІ,
к.т.н., доц. Л.А. Шувалова

Додаток А -4

ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО

вул. Шевченка, 46, м. Хмельницький, 29000 тел. 79-59-11, факс 72-08-02, e-mail: nadpsu@pvu.gov.ua

№_____

на №_____

ЗАТВЕРДЖУЮ

Заступник директора Національної акад
Державної прикордонної служби України і
Богдана Хмельницького з наукової роботи
доктор військових наук, професор
полковник В. А. Кириленко

2018 року

Акт

про реалізацію результатів дисертаційного дослідження здобувача наукового ступеня кандидата педагогічних наук Бистрової Богдани Василівни

Комісія у складі голови – начальника науково-дослідного відділу кандид психологічних наук, старшого наукового співробітника О. Ю. Андрощук; чл комісії: начальника кафедри тактики прикордонної служби кандидата педагогіч наук, доцента О. Г. Трембовецького; професора кафедри педагогіки та соціаль економічних дисциплін доктора педагогічних наук, професора О. В. Торічн склала цей акт про те, що результати дисертаційного дослідження Богдани Васил Бистрової з теми «Професійна підготовка бакалаврів з кібербезпеки у вищ навчальних закладах США» здійснювалась впродовж 2016-2017 років у Національ академії державної прикордонної служби України імені Богдана Хмельницького процесі викладання курсів «Технічні засоби охорони кордону», «Теорія і практ наукових досліджень» та у науково-методичній роботі.

Теоретичні й практичні аспекти досліджуваної Б.В. Бистровою пробле

представлені у методичних рекомендаціях «Професійна підготовка бакалавр кібербезпеки: досвід США», успішно використовувались викладачами у наук методичній роботі, впроваджувались у процес організації різних видів наук дослідної роботи студентів напряму підготовки «Охорона та захист держави кордону».

Цінність результатів дисертаційного дослідження вбачається й у розр науково-методичних рекомендацій щодо творчого використання прогресивних американського досвіду у модернізації системи вищої освіти України. Це довод практичну спрямованість проведеного дослідження і доцільність широк впровадження його результатів у процес професійної підготовки фахівців.

Начальник науково-дослідного відділу
кандидат психологічних наук, с. н. с.
полковник О. Ю. Андрощук

Начальник кафедри тактики прикордонної служби
кандидат педагогічних наук, доцент О. Г. Трембовецьк

Професор кафедри педагогіки
та соціально-економічних дисциплін
доктор педагогічних наук, професор О. В. Торічний

Додаток Б

Таблиця Б 1

Перелік компетентностей здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» за вимогами ОПП Житомирського державного технологічного університету.

ІНСТРУМЕНТАЛЬНІ КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КІ 1	Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.

ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
КЗ2	Знання та розуміння предметної області та розуміння професії.
КЗ3	Здатність спілкуватися рідною та іноземною мовою як усно та письмово.
КЗ4	Здатність здійснювати професійну діяльність згідно з вимогами охорони праці, техніки безпеки та протипожежної безпеки.
КЗ5	Вміння виявляти, ставити та вирішувати проблеми.
КЗ 6	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ 7	Навички міжособистісної взаємодії.
КЗ 8	Прагнення до збереження навколишнього середовища, знання структури і методів роботи з базами даних та знань.
КЗ 9	Здатність діяти соціально відповідально та громадянсько свідомо.
КЗ10	Здатність вчитися і бути сучасно навченим.
КЗ11	Здатність приймати обґрунтовані рішення.
КЗ12	Здатність до адаптації та дії в новій ситуації.
КЗ13	Дотримання та пропагування здорового способу життя.
КЗ14	Здатність бути критичним та самокритичним.
КЗ15	Креативність, здатність до системного мислення.

СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КФ 1	Здатність використовувати законодавчу та нормативно-правову бази, вимоги відповідних, зокрема і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
КФ 2	Здатність до використання інформаційних і комунікаційних технологій.
КФ3	Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки.
КФ 4	Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі.
КФ5	Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем.
КФ 6	Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов.
КФ 7	Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТ.
КФ 8	Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки.
КФ 9	Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.

КФ 10	Здатність здійснювати управління інцидентами ІБ та кібербезпеки.
КФ 11	Здатність здійснювати управління ризиками ІБ та кібербезпеки.
КФ12	Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій.
КФ13	Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.
КФ14.	Здатність проводити дослідження у практичній професійній діяльності.

Систематизовано автором на основі джерела: ОПП Житомирського ДТУ.

Таблиця Б 2

Перелік компетентностей здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» за вимогами ОПП Тернопільського національного технічного університету імені Івана Пулюя

КОМПЕТЕНТНОСТІ СОЦІАЛЬНО-ОСОБИСТІСНІ	
ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КСО 01	розуміння та сприйняття етичних норм поведінки відносно інших людей
КСО 02	здатність організувати роботу відповідно до вимог безпеки життєдіяльності й охорони праці
КСО 03	здатність учитися
КСО 04	здатність до критики й самокритики
КСО 05	креативність, здатність до системного мислення
КСО 06	адаптивність і комунікабельність
КСО 07	Толерантність
КСО 08	екологічна грамотність

ІНСТРУМЕНТАЛЬНІ КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТ І
КІ 01	здатність до письмової й усної комунікації рідною мовою
КІ 02	знання іншої мови (мов)
КІ 03	навички роботи з комп'ютером
КІ 04	навички управління інформацією
КІ 05	дослідницькі навички

ЗАГАЛЬНОНАУКОВІ КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КЗН 01	базові уявлення про основи філософії (філософії безпеки), психології, педагогіки, що сприяють розвитку загальної культури й соціалізації особистості, схильності до етичних цінностей, знання вітчизняної історії, економіки й права, розуміння причинно-наслідкових зв'язків розвитку суспільства й уміння їх використовувати в професійній і соціальній діяльності
КЗН 02	базові знання фундаментальних розділів математики, фізики в обсязі, необхідному для володіння математичним апаратом відповідної галузі знань, здатність використовувати математичні методи у сфері захисту інформації
КЗН 03	базові знання в галузі інформатики й сучасних інформаційних технологій; навички використання програмних засобів і навички роботи в комп'ютерних мережах, уміння створювати бази даних і використовувати Інтернет ресурси
КЗН 04	базові знання в галузі, необхідні для освоєння загально професійних дисциплін

ЗАГАЛЬНОПРОФЕСІЙНІ КОМПЕТЕНТНОСТІ

ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ

КЗП 01	знання архітектури комп’ютера
КЗП 02	знання організації інформаційно-обчислювальних процесів і систем
КЗП 03	сучасні уявлення про призначення, структуру та принципи побудови інформаційних і комунікаційних систем
КЗП 04	знання структури і методів роботи з базами даних та знань
КЗП 05	володіння методами та засобами програмування мовами високого рівня, знання технологій створення програмних продуктів
КЗП 06	знання принципів роботи операційних систем
КЗП 07	знання методів та систем штучного інтелекту
КЗП 08	знання протоколів передачі даних в інформаційних системах
КЗП 09	знання комп’ютерної графіки, web-дизайну та технологій проектування та оцінювання людино-машинних інтерфейсів
КЗП 10	здатність планувати й реалізувати відповідні заходи, щодо захисту інформації в інформаційних і комунікаційних системах
КЗП 11	знання правових основ і законодавства України в галузі кібербезпеки
КЗП 12	здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, навички роботи в команді
КЗП 13	знання платіжних систем, фінансових ринків та технологій дистанційного банківського обслуговуван
СПЕЦІАЛІЗОВАНО-ПРОФЕСІЙНІ КОМПЕТЕНТНОСТІ	
ШИФР	ЗМІСТ КОМПЕТЕНТНОСТІ
КСП 01	здатність використовувати професійно профільовані знання в галузі математики (математичної статистики), для статистичної обробки експериментальних даних і математичного моделювання у сфері захисту інформації
КСП 02	здатність використовувати математичний апарат для освоєння теоретичних основ і практичного використання криптографічних методів
КСП 03	здатність використовувати сучасні міжнародні та вітчизняні стандарти з інформаційної безпеки при проектування інформаційних систем безпеки
КСП 04	здатність використовувати теоретичні знання й практичні навички в сфері математики, фізики, програмування для оволодіння теорії й методів захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах
КСП 05	здатність проводити тестування на проникнення
КСП 06	професійно профільовані знання й уміння в галузі управління
КСП 07	професійно профільовані знання й уміння в галузі правового забезпечення
КСП 08	професійно профільовані знання й уміння в галузі програмування
КСП 09	професійно профільовані знання й уміння в галузі адміністрування інформаційних систем

Додаток систематизовано автором на основі джерел: Державний стандарт. Тернопільського НТУ імені Івана Пулюя

Додаток В

Таблиця В.1

Довідник з реквізитами ВНЗ США з підготовки бакалаврів зі спеціальності «Кібербезпека»

№ п/п	ШТАТ	УНІВЕРСИТЕТ	РЕКВІЗИТИ
1	Alabama	University of South Alabama	http://www.southalabama.edu/
2	Arizona	Embry-Riddle Aeronautical University	https://erau.edu/degrees/bachelor/cyber-intelligence-security/
3	Arkansas	Southern Arkansas University	https://web.saumag.edu/academics/program/computer-science-privacy-cyber-security-option-3 /
4	California	California State Polytechnic University-Pomona	http://bulletin.csusb.edu/colleges-schools-departments/social-behavioral-sciences/criminal-justice/criminal-justice-crime-analysis-ba/
5	California	California State University-San Bernardino	https://www.csusb.edu/
6	Connecticut	University of Connecticut	https://catalog.uconn.edu/school-of-engineering/computer-science/
7	Florida	Florida Polytechnic University	https://floridapoly.edu/degree/computer-science/
8	Florida	The University of West Florida	https://uwf.edu/cse/departments/computerscience/undergrad majors/cybersecurity/
9	Georgia	Armstrong State University	https://www.armstrong.edu/academic-departments/ cs-it-bachelor-information-technology
10	Louisiana	Louisiana Tech University	http://catalog.latech.edu/preview_program.php?catoid=3&poid=911&returnto=113
11		Southern University and A & M College	http://www.subr.edu/search?q=Computer+Science
12	Maine	University of Southern Maine	https://usm.maine.edu/tech/bs-cyber-security-0
13		Capitol Technology University	https://www.captechu.edu/academics/undergraduate-academics/bachelor-degree-programs/cyber-information-security
14	Maryland		http://www.ece.umd.edu/
15		University of Maryland-College Park	http://undergrad.cs.umd.edu/degree-requirements-cs-major
16		Baker College	https://www.baker.edu/academics/undergraduate-studies/college-of-information-technology/computer-technologies/information-technology-and-security-concentration-in-information-assurance-and-cyber-defense
17	Michigan	Northern Michigan University	http://www.nmu.edu/bulletin/programs?processtype=self&action=ProgsByDept&phase=phase5&elementid=&subaction=1254169024&
18		University of Detroit Mercy	https://liberalarts.udmercy.edu/academics/cis/index.php

19		University of Michigan-Dearborn	https://umdearborn.edu/cecs/departments/computer-and-information-science/undergraduate-programs/bs-cybersecurity-and-information-assurance
20		Walsh College	https://www.walshcollege.edu/bachelors-bs-degree-information-technology
21		Fontbonne University	https://www.fontbonne.edu/academics/departments/mathematics-and-computer-science-department/cyber-security/
22		Lindenwood University	http://www.lindenwood.edu/academics/academic-schools/school-of-accelerated-degree-programs/undergraduate-programs/cyber-security/
23	Missouri	Southeast Missouri State University	http://semo.edu/study/cybersecurity.html
24		University of Central Missouri	https://www.ucmo.edu/majors/print/4yearplan.cfm?ftd=336&wi=Cybersecurity.cfm
25		Webster University	http://www.webster.edu/catalog/current/undergraduate-catalog/majors/computer-science-cybersecurity.html
26	Nebraska	University of Nebraska at Omaha	https://www.unomaha.edu/academics/majors-and-programs/index.php
27		University of Nebraska at Omaha	
28	New Jersey	Stevens Institute of Technology	https://www.stevens.edu/schaefer-school-engineering-science/departments/computer-science/undergraduate-programs/cybersecurity
29		Iona College	https://www.iona.edu/academics/school-of-arts-science/departments/computer-science/majors/ba-with-concentration-in-cyber-security.aspx
30	New York	St. John's University	https://www.stjohns.edu/academics/schools-and-colleges/college-professional-studies/programs-and-majors/cyber-security-systems-bachelor-science
31	North Carolina	University of North Carolina at Charlotte	https://academics.uncc.edu/sites/academics.uncc.edu/files/media/Computer-Science-BS-BINF-CS-SIS-Depts.pdf
32	Oklahoma	Northeastern State University	https://academics.nsuok.edu/criminaljustice/DegreePrograms/CyberSecurity.aspx
33	Oregon	George Fox University	https://www.georgefox.edu/college-admissions/academics/major/cyber-security-concentration.html
34		Harrisburg University of Science and Technology	http://harrisburgu.edu/courses/computer-and-information-science-bs/
35	Pennsylvania	Indiana University of Pennsylvania-Main Campus	https://www.iup.edu/compsci/undergrad/cyber-security-computer-science-bs/
36		Saint Vincent College	http://www.stvincent.edu/academics/majors-and-programs/cybersecurity
37		Tennessee Technological University	http://catalog.tntech.edu/preview_program.php?catoid=23&poid=2800&returnto=4535
38	Tennessee	The University of Tennessee at Chattanooga	https://www.utc.edu/records/academic-majors-minors.php
39		University of Memphis	

40	Texas	Texas A & M University-Corpus Christi	http://sci.tamucc.edu/CSCI/COSC/undergrad.html
41	Utah	Brigham Young University-Provo	https://catalog.byu.edu/engineering-and-technology/school-of-technology/information-technology-bs
42	Wisconsin	University of Wisconsin-Stout	https://wwwprod.uwstout.edu/cyber-security-concentration
43	West Virginia	University of Charleston	http://www.ucwv.edu/Academics/Degree-Programs/Undergraduate-Programs/Cyber-Security/
44	Washington	University of Washington-Seattle Campus	https://www.uwb.edu/css/undergraduate
45	Virginia	George Mason University	https://volgenau.gmu.edu/program/view/20490

Додаток систематизовано автором на основі джерел: Сайти досліджуваних вищих навчальних закладів США.

Таблиця В.2.

Загальна характеристика ВНЗ США з підготовки бакалаврів, спеціальності «Кібербезпека».

Штат	Університет	Спеціальність	Вимоги
Alabama Алабама	University of South Alabama Університет Південної Алабами	Cyber Assurance Забезпечення кібербезпеки	Для отримання диплому бакалавра, студенти повинні отримати 57 кредитів з базового курсу «Кібербезпека», 6 кредитів з курсу вивчення комп'ютерної грамотності, пройти практику або стажування. Студенти повинні відвести щонайменше 320 годин на стажування або практику, що затверджується кафедрою.
Arizona Арізона	Embry-Riddle Aeronautical University Авіаційний університет Ембрі Ріддл	Cyber Intelligence and Security Кібер-розвідка та безпека	Кандидати повинні подати атестат успішності середньої школи або сертифікат загальноосвітнього рівня підготовки (GED) та два рекомендаційні листи. Студенти можуть також подати есе, бали SAT або ACT, а також резюме академічних та позакласних заходів, спрямованих на підтримку їхніх шансів на вступ.
Arkansas Арканзас	Southern Arkansas University Південний університет штату Арканзас	Computer Science – Privacy and Cyber Security Комп'ютерні науки – конфіденційність та Кібербезпека	Це 120-кредитний бакалаврська програма. Студенти, які подають заяву до Південного Арканзасу, повинні мати сертифікат ACT або SAT, а також табель шкільної успішності середньої школи або сертифікат загальноосвітнього рівня підготовки .
California Каліфорнія	California State Polytechnic University-Pomona Каліфорнійський політехнічний університет (Помона)	Computer Science – Cyber Security Career Focus Комп'ютерні науки – Кібербезпеки	Це 180-кредитна бакалаврська програма. Кандидати повинні подати атестат успішності середньої школи або сертифікат загальноосвітнього рівня підготовки (GED) та два рекомендаційні листи.
	California State University-San Bernardino Каліфорнійський	Criminal Justice – Crime Analysis, Technical Proficiency Cyber Security	Студенти можуть отримати ступінь бакалавра наук з адміністративного менеджменту у кібербезпеці, який вимагає від них отримати 44 кредити з курсової роботи з кібербезпеки.

	державний університет – Сан-Бернардіно	Кримінальне правосуддя - аналіз злочинності, технічна кваліфікація кібербезпеки	
		Інформаційні системи та технології – інтелектуальна безпека в галузі кібербезпеки	Ступінь бакалавра наук у галузі інформаційних систем та кібербезпеки вимагає, них отримати 28 кредитів з курсової роботи з кібербезпеки.
Connecticut Конектікут	University of Connecticut Університет штату Коннектикут	Computer Science – Cyber Security Career Комп'ютерні науки – спеціалізація кібербезпеки	Університет вимагає від студентів отримати щонайменше 15 кредитів з дисциплін, що відносяться до додаткової спеціалізації, повинні заробити С або вище на кожному курсі.
Florida Флорида	Florida Polytechnic University Політехнічний університет штату Флорида	Computer Science: Information Assurance & Cyber Security Комп'ютерні науки: інформаційне забезпечення та кібербезпека	Навчальна програма вимагає, щоб студенти склали 120 кредитів, у тому числі 37 кредитів загальної освіти, 13 кредитів з вищої математики та науки, 48 кредитів в галузі комп'ютерних наук, 12 кредитів в контексті забезпечення інформації та кібербезпеки та 6 кредитів дипломний проект. Абітурієнти повинні мати диплом про середню освіту з (GPA grade point average) принаймні 3,0. Такі студенти повинні подати оцінки ACT або SAT.
	The University of West Florida Університет Західної Флориди	Computer Science – Cyber Security Career Комп'ютерні науки – спеціалізація кібербезпеки	Курс з кібербезпеки передбачає обрання принаймні 48 встановлених кредитів зі спеціалізації, а також чотирьох факультативних дисциплін. Крім того, коледж рекомендує студентам молодших курсів пройти курс з бухгалтерського обліку, мікроекономіки та основ комунікативних навичок, перед початком навчання на старших курсах. Студенти повинні підтримувати середній бал 2.5 з усіх предметів зі спеціалізації загалом.
Georgia Джорджия	Armstrong State University Армстронгський державний університет	Information Technology – Cyber Security Інформаційні технології – спеціалізація кібербезпеки	Студенти повинні отримати 39 кредитів з комп'ютерних наук та інформаційних технологій, 9-15 кредитів з відповідних курсів та 42 кредити на загальноосвітні вимоги.
Louisiana Луїзіана	Louisiana Tech University Технологічний університет штату Луїзіана	Computer Science – Cyber Security Career Комп'ютерні науки із спеціалізацією в галузі кібербезпеки	Щоб отримати цей ступінь, студенти повинні скласти 120 кредитів, включаючи загальноосвітні предмети, предмети з комп'ютерних наук та предмети з кібербезпеки. Спеціалізація з кібербезпеки передбачає обрання 2-х обов'язкових курсів з кібербезпеки та 2-х факультативних. Обов'язковий середній бал варіює відповідно до SAT чи ACT сертифікатів.. Студенти з вищими балами можуть бути прийняті з середнім балом не менше 2,0, а студенти з нижчими балами потребують 2,5.

	Southern University and *Agricultural* and Mechanical College Південний Університет і механіко-сільськогосподарський коледж	Computer Science – Cybersecurity Комп'ютерні науки із спеціалізацією в галузі кібербезпеки	Навчальна програма для цього курсу вимагає від студентів 41 кредит з основного курсу та 18 кредитів зі спеціалізації. Студенти також повинні отримати 12 кредитів з природничих наук, 14 кредитів з математичних та відповідати загальноосвітнім вимогам університету. Першокурсники повинні скласти 19 основних навчальних програм, які штат Луїзіана встановлює для учнів середніх шкіл, і відповідає мінімальним вимогам GPA або ACT / SAT.
Maine Мен	University of Southern Maine Південний університет штату Мен	Computer Science – Cybersecurity Комп'ютерні науки із спеціалізацією в галузі кібербезпеки	Програма вимагає, щоб студенти отримали 121 кредит, включаючи основні курси університету, основні курси кафедри технології та технічні курси з кібербезпеки. Всі студенти повинні пройти курс дипломного проекту, під час якого вони завершують індивідуальний або командний проект. Першокурсники повинні подати табель шкільної успішності середньої школи або SAT або ACT бал, рекомендаційний лист та особисту заяву. Студенти, які переходять з іншого навчального закладу, повинні надіслати табель шкільної успішності середньої школи, особистий реферат та результати ACT або SAT, якщо вони є.
Maryland Меріленд	Capitol Technology University Технологічний університет Кепітол	Cyber and Information Security Інформаційна безпека та кібербезпека	Ступінь бакалавра вимагає від студентів отримати у межах 127 і 130 кредитів, включаючи 31 кредит з комп'ютерних наук, 27 з інформаційної безпеки, шість кредитів з управління та 17 кредитів з математики та науки.
	University of Maryland-College Park Меріленський університет (Коледж-Парк)	Computer Engineering with Specialization in Cybersecurity Комп'ютерна інженерія із спеціалізацією в галузі кібербезпеки	Студенти зобов'язані обрати сім курсів, пов'язаних з кібербезпекою. П'ять з них є обов’язковими, а інші два – за власним вибором студентів.
		Computer Science with Specialization in Cybersecurity Комп'ютерні науки із спеціалізацією в галузі кібербезпеки	Студенти повинні отримати 122 кредити, щоб отримати ступінь бакалавра. Спеціалізація з кібербезпеки вимагає, щоб студенти обрали п'ять курсів з затверджених відповідних дисциплін.
Michigan Мічіган	Baker College Бейкер Коледж	Cyber Defense Кіберзахист	Абітурієнти повинні мати диплом про середню освіту з (GPA grade point average) принаймні 2.0. Для отримання ступеня, студенти повинні отримати 120 кредитів, в тому числі 72 кредити з основних дисциплін, 27 кредитів із спеціалізації.

	Northern Michigan University Північний університет штату Мічиган	Information Assurance/Cyber Defense Захист інформації / Кіберзахист	Щоб отримати ступінь, студенти повинні набрати 122 кредити, в тому числі 32 кредити з основних дисциплін, 18 кредитів з основ інформаційних систем та 16 кредитів з дисциплін. Студенти, які подають заяви на отримання ступеня бакалавра в Північному Мічигані, повинні мати диплом про середню освіту або GED. Коледж шукає студентів із середньою освітою та середнім балом 2,25 або вище, і всі заявники повинні подати результати ACT або SAT.
	University of Detroit Mercy Університет Милосердя Детройту	Computer & Information Systems – Cybersecurity Major Комп'ютерні та інформаційні системи – спеціалізація кібербезпеки	Навчальний план вимагає від студентів 42 кредити із спеціалізації. Більше половини курсів із спеціалізації є факультативними щоб студенти могли адаптувати свою освіту до своїх кінцевих цілей кар'єри. Щоб вступити до Коледжу ліберальних мистецтв та освіти, який пропонує програму кібербезпеки, заявники повинні мати принаймні середній бал 3,0 та оцінки ACT / SAT.
	University of Michigan-Dearborn Мічиганський університет у м. Дірбон	Cybersecurity and Information Assurance – Cybersecurity and Privacy Concentration Інформаційна безпека та кібербезпека - спеціалізація кібербезпеки та конфіденційності	Студенти повинні пройти 123 кредити, щоб отримати ступінь. При розгляді заяв щодо вступу, коледж розглядає успішність середньої школи та результати SAT / ACT. Середній бал складає 2,75.
	Walsh College Коледж Уолш	Information Technology – Cyber Security Інформаційні технології – Кібербезпека	Ступінь вимагає 127 семестрових кредитів, і студенти повинні пройти не менше 45 кредитів через коледж Уолш. Програма Уолша передбачає лише навчання для старших курсів, тому вступники повинні мати щонайменше 60 семестрових кредитів з середнім балом 2,0 або вище.
Missouri Міссурі	Fontbonne University Фонтбон університет	Cyber Security Кібербезпека	Навчальна програма включає предмети з інформатики та математики, а також предмети з кібербезпеки.
	Lindenwood University Університет Линденву	Cyber Security Кібербезпека	Спеціалізація із кібербезпеки вимагає від студентів накопичення 57 кредитів з кібербезпеки.
	Southeast Missouri State University Південно-східний державний університет штату Міссурі	Cyber Security Кібербезпека	Південно-східний державний університет штату Міссурі пропонує ступінь бакалавра наук з кібербезпеки. Студенти проходять щонайменше 88 кредитів зі спеціалізації та необхідні загальні предмети для отримання 120 кредитів, необхідних для випуску.
	University of Central Missouri Університет штату Міссурі	Cyber Security Кібербезпека	Навчальна програма для отримання ступеня включає проходження 10 необхідних основних курсів, 5 курсів у галузі спеціалізації та 1-3 факультативів.

	Webster University Вебстерський університет	Computer Science – Cybersecurity Комп'ютерні науки – спеціалізація кібербезпеки	Щоб отримати ступінь, студенти повинні пройти 128 кредитів, в тому числі 42 кредити в галузі комп'ютерних наук та в кібербезпеці. Кандидати, які є традиційними першокурсниками, повинні закінчити підготовчі курси середніх шкіл у складі 19 навчальних закладів. Приймаються студенти, як правило з середнім балом GPA не менше 3,0. Заявники повинні подати результати ACT або SAT, і можуть попросити інші документи, такі як рекомендаційний лист.
Nebraska Небраска	University of Nebraska at Omaha	Computer Science – Cybersecurity Комп'ютерні науки – спеціалізація кібербезпеки	Щоб отримати ступінь, студенти повинні пройти 120 кредитів. У межах галузі студенти отримують 21 кредит з інформаційно-технологічних дисциплін, 30 кредитів з курсів з кібербезпеки, 8 кредитів з факультативних в галузі кібербезпеки та 12 кредитів на (in co-requisite courses) необхідних курсах, включаючи два курси з політології. Програма навчання вимагає від студентів, GPA 2,5. Абітурієнти, які вперше є першокурсниками, повинні подати табель успішності середньої школи та SAT або ACT.
	Stevens Institute of Technology Технологічний інститут Стівенса	Cyber Security Кібербезпека	Першокурсники повинні мати табель про закінчення середньої школи, що включає чотири роки англійської мови, трьох років науки та чотири роки математики, включаючи рік обчислення. Кандидати повинні подати результати ACT або SAT, табель успішності середньої школи, есе та двох рекомендацій.
New York Нью-Йорк	Iona College Айона коледж	Computer Science with Concentration in Cyber Security Комп'ютерні науки – спеціалізація кібербезпеки	Студенти цієї галузі повинні пройти 25 спеціальних кредитів в галузі інформатики, а також чотири необхідні курси та два факультативи з кібербезпеки. Кандидати повинні мати диплом про середню освіту та повинні були пройти підготовчі курси у вищій школі. Коледж приймає студентів з GPA 2,75 або вище та вимагає від заявників подавати результати SAT або ACT.
	St. John's University Університет Сент Джон	Cyber Security Systems Система кібербезпеки	Студенти повинні набрати 126 кредитів, щоб отримати ступінь. Першокурсники повинні мати диплом про середню освіту або GED, а середній бал має бути близько 3,5.
North Carolina Північна Кароліна	University of North Carolina at Charlotte Університет Північної Кароліни в місті Шарлотт	Software and Information Systems, Cyber Security Concentration Програмне забезпечення та інформаційні системи – спеціалізація кібербезпеки	Студенти повинні набрати 126 кредити, щоб отримати ступінь. Вхідні першокурсники повинні мати диплом про середню освіту або GED, а середній бал має бути близько 3,5.

Oklahoma Оклахома	Northeastern State University Північно-східний державний університет	Cybersecurity Кібербезпека	Навчальний план включає 49 кредитів на відповідні курси в галузі, включаючи курси з кримінального правосуддя, інформатики та інформаційних систем, а також 12 кредитів у відповідних факультативах. Всі спеціалісти з кібербезпеки повинні написати дипломний проект. Студенти також повинні пройти щонайменше 46 кредитів за загальноосвітніми вимогами. Кандидати повинні мати диплом про середню освіту і повинні мати (15 specific units) 15 спеціальних підрозділів середньої школи. Кандидати повинні мати GPA від 2.7 або вище та повинні подати бали ACT .
Oregon Орегон	George Fox University Університет Джорджа Фокса	Computer Science – Cyber Security Concentrationi Комп'ютернаука – спеціалізація кібербезпеки	Щоб отримати ступінь, студенти повинні отримати 45 кредитів з дисциплін що належать до комп'ютерних наук, 9 кредитів за дисциплін на вибір і 29 кредити з кібер безпеки. Студенти можуть перерахувати деякі класи з кібер безпеки на користь факультативних. Першокурсники повинні бути випускниками середньої школи, а більшість прийнятих студентів мають середню бал GPA, який набагато перевищує 3,0. Нещодавні випускники середньої школи повинні подати результати ACT або SAT. Всі повинні подати довідковий і особистий твір.
Pennsylvania Пенсильванія	Harrisburg University of Science and Technology Гаррісберзький університет науки і техніки	Computer and Information Sciences – Cyber Security Комп'ютер та інформатика – кібербезпека	This program requires a total of 50 semester hours: 1) 27 semester hours from the core courses listed below and 2) 23 semester hours completed in one of the following concentrations: Computer Science, Cyber Security, Software Engineering and Analysis, Computational Biology, and Machine Learning. The semester hour value of each course appears in parentheses
	Indiana University of Pennsylvania Індіанський університет штату Пенсильванія	Computer Science – Cyber Security Track Комп'ютерні науки – спеціалізація кібербезпеки	Спеціалізація з кібербезпеки передбачає проходження додаткового курсу з кримінології. Навчальна програма для цієї програми вимагає 120 кредитів, в тому числі 43 кредити в області інформатики, 15 кредитів в криміналістиці та 48 кредитів на необхідні курси ліберального навчання. Студенти з GPA від 3.3 мають більше шансів для вступу. Необхідні також оцінки SAT або ACT.
	Saint Vincent College Сент-Вінсент коледж	Computer Science – Cyber Security Concentration Комп'ютерні науки – спеціалізація кібербезпеки	Студенти повинні пройти 43 кредити з основ обчислювання та кібербезпеки та шість кредитів у відповідних факультативах. Вони також повинні вибрати принаймні один клас у численні. Сент-Вінсент вимагає від абітурієнтів подавати табелі успішності та бали середньої школи з SAT або ACT. Кандидати можуть також надсилати рекомендації та особисті нариси, якщо вони обирають.

Tennessee Теннесі	Tennessee Technological University Технологічний університет штату Теннесі	Computer Science – Cyber Security Комп'ютерні науки – Кібербезпека	Слід заробити в загальній складності 120 кредитів, також взяти більше 20 курсів зі спеціальності та спеціалізації. Для вступу середній бал 3.0 або вище. Абітурієнти також повинні мати оцінку ACT за твір щонайменше 20, а з математики – 22.
	The University of Tennessee at Chattanooga Університет штату Теннессі в Чаттануга	Computer Science – Cyber Security Комп'ютерні науки – Кібербезпека	Вимоги для цієї програми включають 10 базових курсів в галузі комп'ютерних наук, сім з кібербезпеки, три на вибір в галузі комп'ютерних наук або інших технічних областях і дипломний проект або тези. Студенти також повинні пройти ряд вимог щодо математики, включаючи числення, I та II, лінійну алгебру, курс дискретної математики і статистики курс. Абітурієнти повинні мати GED. SAT або ACT необхідні для заявників, яким не виповнилося 21.
Texas Техас	Texas A & M University-Corpus Christi Техаський Ей-енд-еМ університет – Корпус-Крісті	Cyber Security and Infrastructure Кібербезпека та інфраструктура	Студенти цієї спеціальності повинні заробити від 121 до 123 кредитів, в тому числі 42 кредити з обов'язкової навчальної програми, 40 кредитів зі спеціальності та 39 кредитів з предметів спеціалізації, що стосуються кібербезпеки та інфраструктури. Абітурієнти повинні мати диплом про середню освіту або GED, а також подати заяву ACT або SAT. Студенти повинні відповідати мінімальним оцінкам тестів.
Utah Юта	Brigham Young University Університет Брігама Янга	Information Technology emphasis in Cyber Security Інформаційні технології в галузі кібербезпеки	Студенти цієї програми завершують свій останній курс, беручи участь у дипломному проекті протягом 2 семестрів, в якому команди студентів разом із спонсорською організацією вирішують справжню проблему кібербезпеки.
Wisconsin Вісконсин	University of Wisconsin-Stout Університет Вісконсін-Стаут	Applied Mathematics and Computer Science – Cyber Security Concentration Прикладна математика та інформатика – спеціалізація кібербезпеки	Навчальна програма вимагає 120 кредитів, у тому числі 43 кредити за загальноосвітні предмети та 77 кредитів із спеціалізації. Серед основних курсів – математика, статистика, комп'ютерні науки та мережі. Кандидати повинні мати найвищі бали з випускного класу або мати середню бал GPA не менше 3,0. Абітурієнти повинні мати оцінку математичної шкали ATC щонайменше 22, бал ACT з математики – 22 або більше.
West Virginia Вірджинія	University of Charleston	Кібербезпека	Ступінь вимагає 28 кредитів за загальнообов'язкові предмети, дев'ять кредитів з дисциплін з кібербезпеки, 15-18 програми для вибору з кібербезпеки та 18 кредитів з додаткової спеціалізації.
Washington Вашингтон	University of Washington Університет Джорджа Вашингтона	Information Assurance & Cybersecurity Забезпечення Кібербезпеки	INFO 310 is the foundational course for the IAC option. students.) To meet the requirements for this you must take 11-15 credits of IAC electives in addition to INFO 310. Only one basic networking elective (either INFO 341, CSS 432, or T INFO 250) may count toward the IAC option.

Virginia Вірджинія	George Mason University Університет Джорджа Мейсона	Cyber Security Engineering Інженерія кібербезпеки	Кандидати повинні мати 25 років, досвід роботи в галузі кібербезпеки та інформаційних технологій. У програмі перераховані 10 спеціальних курсів з інформаційних технологій, які повинні бути завершені в коледжі, перед входом в Б.А.С. програму.

Додаток систематизовано автором на основі джерел: ОПП досліджуваних вищих навчальних закладів США.

Таблиця В 3.

Довідник щодо реквізитів закладів вищої освіти України з підготовки бакалаврів зі спеціальності 125 «Кібербезпека» у галузі знань 12 «Інформаційні технології».

	НАЗВА ВНЗ	***РЕКВІЗИТИ***
1.	Національний авіаційний Університет, НН Інститут ІДС, кафедра БІТ; кафедра ЗІ; НН Інститут Комп'ютерних інформаційних технологій кафедра КСЗІ	Офіційний веб-сайт http://www.nau.edu.ua/ (044) 497-41-05 Київ Проспект Комарова 1
2.	Національний технічний університет України «КПІ імені Ігора Сікорського», Фізико-технічний інститут, кафедра фізико-технічних засобів захисту інформації;	044)204-92-10, Київ, пр. Перемоги, 37, корп. 1, (офіс 40, к. 5) http://lll.kpi.ua/ ipo@ipo.kpi.ua|
3.	Тернопільський Національний технічний університет імені Івана Пулюя. Retrieved from:	http://tntu.edu.ua/
4.	Національний університет «Львівська політехніка», Інститут комп'ютерних технологій, автоматики та метрологіїкафедра систем технічного захисту інформації ;	Офіційний веб-сайт http://old.lp.edu.ua
5.	Київський національний університет ім. Тараса Шевченка Факультет Інформаційних технологій, Кафедра кібербезпеки та захисту інформації ;	Сайт кафедри: http://kbzi.knu.ua/
6.	Житомирський державний технологічний університет кафедрі комп'ютеризованих систем управління та автоматики,	Офіційний веб-сайт http://www.ztu.edu.ua.
7.	Сумський Деравний Університет	Офіційний веб-сайт http: // sts.sumy.ua/education/u-sumdu-vidkrili-novu-spetsialnist-kiberbezpeka.html
8	Kyiv Cyber Academy	http://channel4it.com/publications/V-Ukran-pochali-navchati-profesyam-maybutnogo-vdkrito-Kyiv-Cyber-Academy-22590
9	Білоцерківський інститут економіки і управління відкритий міжнародній університет развитку людини «Україна»	http://bc-uu.com.ua/ (04563) 8-66-80; 3-20-3 Київська обл., м. Біла Церква, 2-й Комсомольський провулок 42

Додаток систематизовано автором на основі джерел: Сайти досліджуваних вищих навчальних закладів України.

.

Додаток Д.

Таблиця Д-1.

Характеристика циклу професійно-орієнтованих дисципліни ОПП підготовки ОКР «Бакалавр» спеціальності «Кібербезпека» ІТ-галузі університетів США

	ЦИКЛ ПРОФЕСІЙНО-ОРІЄНТОВАНИХ ДИСЦИПЛІНИ		
№	ШИФР	НАЗВА КУРСУ / ДИСЦИПЛІНИ	КРЕДИ-ТИ
		УНІВЕРСИТЕТ УАЛДЕН	
1	ITEC 1010	ІТ-інфраструктура	5
2	ITEC 1020	Введення в програмування	5
3	ITEC 1030	Структури даних	5
4	ITEC 2010	Основи теорії ІТ	5
5	ITEC 2020	Основи та адміністрування операційних систем	5
6	ITEC 2030	Системний аналіз	5
7	ITEC 2040	Дизайн систем	5
8	ITEC 2050	Системи управління базами даних	5
9	ITEC 2060	Взаємодія людини та комп'ютера	5
10	ITEC 2070	Веб-програмування	5
11	ITEC 2080	Мобільні та всеосяжні технології	5
12	ITEC 3010	Основи комп'ютерної безпеки	5
13	ITEC 3020	Управління ІТ-проектами	5
14	ITEC 3040	Адміністрація мережі	5
15	ITEC 4010	Статистичні поняття	5
16	STAT 3401	Системна інтеграція	5
17	ITEC 4030	Структури даних	5
		Загальна кількість кредитів за цикл курсу дисциплін	85
		АМЕРИКАНСЬКИЙ ВІЙСЬКОВИЙ УНІВЕРСИТЕТ	
1	ENTD261	Мови сценаріїв для адміністратора	3
2	ISSC325	Біометрія	3
3	ISSC342	Операційні системи	3
4	ISSC343	Бездротові мережі	3
5	ISSC351	Комп'ютерна криміналістика	3
6	ISSC361	Забезпечення інформації	3
7	ISSC362	ІТ-безпека: Атака та захист	3
8	ISSC366	ІТ-безпека: криптографія	3
9	ISSC421	Комп'ютери та мережева безпека	3
10	ISSC422	Інформаційна безпека	3
11	ISSC431	Безпека баз даних	3
12	ISSC452	Кібербезпека	3
13	ISSC481	ІТ-безпека: планування та політика	3
14	ITMG481	Етика в інформаційних технологіях	3
15	MATH302	Статистика	3
		Усього	45
		Вибрати 3 курси дисциплін з наступних:	9
1	CMRJ320	Захист прав інтелектуальної діяльності	3
2	ENTD412	Системна інженерія	3
3	INFO321	Системи управління базами даних	3
4	INTL434	Аналіз загрози	3

5	ISSC331		Правові проблеми інформаційної безпеки	3
6	ISSC368		IT-безпека: фізична і периферійна оборона	3
7	ISSC451		Кіберзлочинність	3
8	ISSC456		Цифрова криміналістика: розслідування бездротових мереж та пристроїв	3
9	SCMT371		Правові та етичні питання управління безпекою	3
			Загальна кількість кредитів	54
			АВІАЦІЙНИЙ УНІВЕРСИТЕТ ЕМБРІ РІДДЛ	
1	BA 201		Принципи управління	
2	BA 210		Фінансовий облік	3
3	BA 312		Управлінський облік	3
4	BA 329		Судова експертиза бухгалтерського обліку та шахрайства	3
5	CI 119		Введення в систему Cyber Security	3
6	CI 320		Етичний хакер - тестування	3
7	CI 410		Аналіз шкідливих програм	3
8	CS 125		Комп'ютерні науки I	3
9	CS 213		Вступ до комп'ютерних мереж	3
10	CS 225		Комп'ютерні науки II	3
11	CS 304		Введення до комп'ютерної криміналістики	3
12	CS 315		Структура даних та аналіз алгоритмів	3
13	CS 317		Файли та систем бази даних	3
14	CS 420		Операційні системи	3
15	MA 225		Вступ до дискретних структур	3
			Загальна кількість кредитів	47
			УНІВЕРСИТЕТ СЕНТ ДЖОН	
1	CUS	1 115	Основи комп'ютерного програмування	3
2	CUS	1116	Основи комп'ютерного програмування II	3
3	CUS	1185	Безпека даних та криптографія	3
4	NET	1001	Передача даних	3
5	NET	1011	Основи мережі	3
6	NET	1015	Маршрутизатори та концепції маршрутизатора	3
7	CSS	1005	Основи кібербезпеки	3
8	CSS	1011	Мережева безпека	3
9	CSS	1012	Безпека мережевого периметру	3
			Усього	27
			12 додаткових кредитів можна вибрати з наступних курсів дисциплін	12
1	CSS	1001	Введення в інформаційну безпеку	3
2	CSS	1008	Інформаційна безпека в охороні здоров'я	3
3	CSS	1015	Бездротова безпека	3
4	CSS	1021	Кіберзахист та етика	3
5	CSS	1025	Linux і UNIX	3
6	CSS	1032	Кібер-загрози і їх виявлення	3
7	NET	1031	Бездротові мережі	3
			Загальна кількість кредитів за цикл	39

Додаток систематизовано автором на основі джерел: ОПП досліджуваних університетів США.

Таблиця Д -2.

Характеристика циклу професійно-орієнтованих дисципліни ОПП підготовки ОКР «Ббакалавр» зі спеціальності «Кібербезпека» ІТ-галузі коледжів США

№	ШИФР	НАЗВА КУРСУ/ДИСЦИПЛІНИ	КРЕДИ-ТИ
		ЦИКЛ ПРОФЕСІЙНО-ОРІЄНТОВАНИХ ДИСЦИПЛІНИ	
		КОЛЕДЖ МЕРСІ	
1	IASP 330	Аварійне відновлення	3
2	CISC 335	Комп'ютерна мережа II	3
3	CISC 337	Система управління базами даних	3
4	IASP 355	Тестування проникнення та етичне хакерство	3
5	CISC 385	Криптографія / Комп'ютерна безпека	3
6	IASP 420	Мережева безпека	3
7	IASP 455	Судова експертиза / електронне відкриття	3
8	IASP 470	Безпечне та інтелектуальне програмування	3
9	CISC 335	Система безпеки	3
		Усього	27
		Вибрати 5курсів дисциплін з наступних:	
1	CISC 311	Об'єкт / Структура / Алгоритмит I	3
2	CISC 339	Штучний інтелект	3
3	IASP 340	Політика та процедури безпеки	3
4	CISC 341	Комп'ютерна архітектура	3
5	IASP 380	Досвід роботи в сфері кібербезпеки I	3
6	IASP 381	Досвід роботи в сфері кібербезпеки II	3
7	IASP 395	Спеціальні теми в галузі кібербезпеки	3
8	CISC 370	Системний аналіз та дизайн	3
9	CISC 395	Спеціальні теми Comp Info Systm	3
10	CISC 411	Об'єкт / Структура / Алгоритмит II	3
11	CISC 421	Операційні системи	3
12	IASP 397	Незалежне вивчення кібербезпеки	15
		Усього	3
		Загальна кількість кредитів за цикл курсу дисциплін	42
		СЕНТ-ВІНСЕНТ КОЛЕДЖ	
1	CS 102 *	Основи інформатики та обчислювальної техніки	3-4
2	CS 110 C++	Основи IT та обчислювального програмування	3
3	CS 111C++	Основи IT та обчислювального програмування II	3
4	CS 170	Дискретні структури I	3
5	CS 221	Структури даних	4
6	CS 225	Кібербезпека	3
7	CS 310	Мови програмування	4
8	CS 265	Управління інформаційними системами	3
9	CS 330	Архітектура комп'ютера та операційні системи	3
10	CS 350	Концепції баз даних та інформаційні структури	3
11	CS 351	Аналіз та проектування інформаційних систем	3
12	CS 355	Інженерія програмного забезпечення - 3 кредити	3
13	CS 358	Теоретична та прикладна Інформатика Проект II	2
14	CS 357	Теоретична та прикладна Інформатика проект I	2
15	CS 375	Прикладна криптографія	3
		Загальна кількість кредитів	46-47
		АЙОНА КОЛЕДЖ	
		Компютерні науки із спеціалізацією «кібербезпека »	
1	CS 202	Комп'ютерні науки II	4

2	MTH 310	Дискретна математика	3
3	MTH 270	Прикладна статистика	3
4	MTH 408	Автомати та офіційні мови	3
		Усього	13
1	CS 231	Data Structures and Algorithms	3
2	CS 301	Computer Organization and Architecture	4
3	CS 311	Database Design and Implementation	3
4	CS 321	Operating Systems	3
5	CS 451	Software Project Development: Design	3
6	CS 481*	Software Project Development: Implementation	3
		Усього	23
1	CS 315	Структури даних та алгоритми	3
2	CS 409	Комп'ютерна організація та архітектура	3
3	CS 475	Розробка та впровадження баз даних	3
4	CS 477	Операційні системи	3
5	CS 443/444	Розробка програмного забезпечення: дизайн	6
6	CS 472/473	Розробка програмного забезпечення: впровадження	6
		Вибирається одна пара з п.5 тап.6	
		Усього	18
		Загальна кількість кредитів	54

Додаток систематизовано автором на основі джерел: ОПП досліджуваних університетів, інститутів та коледжів США.

Таблиця Д -3.

Узагальнення змісту самостійної роботи здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» в університетах США

№ п/п	Фактори організації та форми самостійної роботи студента	Шляхи реалізації	Вимоги до виконання самостійної роботи
1	доступ до необхідного навчального матеріалу; формування навичок самостійної роботи	методичні рекомендації щодо здобуття навичок та вмінь самостійної роботи	бажання навчитися
2	забезпечення інформацією щодо змісту навчальних дисциплін; робота над навчальним матеріалом	підручники; посібники; тексти лекцій; зошити для виконання тестів і контрольних завдань; комп’ютерне, аудіо- та відео забезпечення	готовність та вміння самостійно навчатися
3	доступ до засобів використання новітніх технологій; виконання практичних завдань	можливість користуватися найновішим експериментальним, обладнанням	ґрунтовна теоретична підготовленість студента

4	доступ до лабораторій, комп'ютерних класів, обладнаних Wi-Fi-мережі Інтернет; пошук та аналіз наукової інформації;	вільний доступ до світових досягнень науки і техніки через засоби інформаційних комп'ютерних мереж;	готовність самостійно проводити дослідження;
5	доступ до консультативних центрів викладачів; бесіда; дискусія	право студента отримати кваліфіковану консультацію від викладачів	готовність студента, з проблемного питання
6	доступ до лабораторій; виконання лабораторних робіт	науково-дослідницький характер лабораторних робіт	готовність до самостійного виконання лабораторних робіт
7	доступ до комп'ютерних класів самоконтролю; тестування	право студента перевірити свою готовність до участі в контрольних заходах;	позитивний результат студента
8	можливість роботи у групі; виконання групових проектів;	аналіз кейсів (рішення реальних проблем з кіберзахисту);	уміння працювати в команді вирішувати різнобічні проблеми; комунікативні навички
9	можливість самостійного наукового досдження; індивідуальні завдання	підготовка презентацій	презентація отриманих результатів
10	можливість опрацювання теоретичного матеріалу; аналіз наукових матеріалів	написання коротких есе (7-8 протягом курсу)	викладення власної точки зору
11	можливість поєднання теоретичного та практичного дослідження; виконання курсових робіт	вибрати тему зі списку чи власний варіант, обґрунтовану мету, очікувані результати, розгорнутий календарний план роботи на 1-2 стор. подають на наступний день після отримання завдання подати викладачеві	володіння навиками . наукової роботи
12	можливість застосування знань та навичок при виконанні кваліфікаційної роботи; дипломна робота	самостійне дослідження	володіння навичками . наукової роботи та ґрунтовними знаннями за фахом

Додаток систематизовано автором на основі джерел:

Додаток Ж.

Таблиця Ж-1.

Зміст освітньо-професійної програми підготовки здобувачів ОКР «бакалавр» зі спеціальності «Кібербезпека» Житомирського державного технологічного університету

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ		
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА		
Галузь знань 12 «Інформаційні технології»		
Соціологія	3	
Техніко-економічна оцінка проектних рішень	3	
Логіка	3	
II Цикл професійної підготовки 1. Нормативна частина	108	20
Основи програмування	7	
Архітектура комп'ютера	4	
Об'єктно -орієнтоване програмування (в т.ч. курсова робота)	7	
Теорія електричних і магнітних кіл	4	
Веб-дизайн	6	
Основи та нормативно-правове забезпечення кібербезпеки	3	
Електроніка (в т.ч. курсова робота)	8	
Бази даних	6	
Інженерна та комп'ютерна графіка	3	
Операційні системи	4	
Теорія інформації та кодування	3	
Комп'ютерні мережі	9	
Прикладна криптологія	7	
Системи технічного захисту інформації в кіберпросторі	10	
Захист інформації в інформаційно-комунікаційних системах	10	
Комплексні системи захисту інформації: проектування, впровадження, супровід	8	
Управління та організаційне забезпечення кібербезпеки	3	
Комплексний курсовий проект «Розробка захищеної інформаційно-комунікаційної системи»	3	
Комплексний курсовий проект «Розробка комплексу засобів захисту інформаційно-комунікаційних систем»	3	
2. Дисципліни на вибір	51	16
Студентнт має вибирати дисципліни загальним обсягом 51 кредит з урахуванням тижневого навантаження.		

Іноземна мова професійного спрямування	6	
Системи підтримки прийняття рішень	6	
Мікропроцесори в задачах захисту інформації	3	
Комп’ютерна стеганографія	6	
Теорія систем та системний аналіз	6	
Інтелектуальні системи захисту інформації в кіберпросторі	3	
Надійність та діагностування систем	3	
Інформаційно-аналітичне забезпечення кіберсистем	6	
Комп’ютерне проектування та моделювання кіберсистем	6	
Системи контролю та управління доступом	6	
Мікроконтролери в задачах захисту інформації	3	
Адміністрування комп’ютерних систем та мереж	6	
Інтернет-програмування	9	
Цифрова обробка сигналів та зображень	3	
Інформаційні технології	9	
Безпровідні мережі	6	
3.Практична підготовка	18	5
Навчальна практика	3	
Технологічна практика	3	
Виробнича практика	3	
Переддипломна практика	3	
Виконання дипломної роботи	6	
Усього	240	59

Додаток систематизовано автором на основі джерел: ОПП Житомирського ДТУ.

Таблиця Ж- 2.

Зміст освітньо-професійної програми з підготовки здобувачів ОКР «Бакалавр» зі спеціальності «Кібербезпека» Тернопільського національного технічного університету імені Івана Пулюя.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ імені Івана Пулюя		
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА		
Галузь знань 12 «Інформаційні технології» ОКР «Бакалавр» спеціальності 125 «Кібербезпека»		
ОСНОВНІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ	**Кредити**	**Кілк.дисц.**
І. Цикл загальної підготовки		
1. Обов язкова частина	**53**	**10**
Українська мова (за професійним спрямуванням)	5	
Історія і культура України	5	
Іноземна мова професійного спрямування	5	
Філософія	4	
Лінійна алгебра та аналітична геометрія	4	
Фізика	8.5	
Математичний аналіз	6	
Дискретна математика	6.5	
Теорія ймовірностей і математична статистика	3	
Інформаційні технології	5	
2. Дисципліни на вибір	**6.5**	**2**
Основи права .	3.5	
Соціологія	3	
ІІ Цикл професійної підготовки		
1. Обов язкова частина	**109**	**22**
Об’єктно -орієнтоване програмування (в т.ч. курсова робота)	4.5	
Кростплатформне програмування	5	
Паралельні та розподілені обчислення	4.5	
Електроніка Веб-дизайн	4.5	
Основи теорії електричних і магнітних кіл	4.5	
Операційні системи	4	
Алгоритмізація та програмування	4	
Комп’ютерні мережі	5	
Адміністрування комп'ютерних систем та мереж	6.5	
Комп’ютерна графіка	3	

Теорія інформації та кодування Прикладна криптологія	6 9	
Системи технічного захисту інформації в кіберпросторі Захист програм та даних	4 4.5	
Захист інформації в в операційних системах Захист інформації в комп'ютерних системах	5 4	
Комплексні системи захисту інформації: проектування, впровадження, супровід Управління інформаційною з безпекою	8 4	
Техноекологія та цивільна безпека (диф.зал.) Веб-технології	4 4.5	
Вступ до інформаційної безпеки	4	
Безпека життєдіяльності, основи охорони праці (диф.з.)	4	
2. Дисципліни на вибір	**53.5**	**14**
Нормативно-правове забезпечення інформаційної безпеки . Комп'ютерна стеганографія	4	
Захист інформації в банківських системах Методи та системи штучного інтелекту	3.5 4	
Іноземна мова професійного спрямування Якість і тестування програмного забезпечення	3 6	
Методології аудиту захищеності ІКС Інтелектуальний аналіз даних	3.5 3	
Архітектура і програмування мікроконтролерів. Архітектура комп'ютерних систем	3.5 4.5	
Обробка сигналів та зображень 3 Організація баз даних та знань	3 5.5	
Чисельні методи Управління ІТ	3 9	
III. Практична підготовка	**16.5**	**4**
1. Обов язкова частина		
Навчальна практика Проектно-технологічна	**3** **3**	
Виробнича практика Стажування з фаху	**3** **7.5**	
Державна атестація		
Екзамен з фаху	**1,5**	
Всього за обов'язковою та вибірковими частинами:	**240**	

Додаток систематизовано автором на основі джерел: ОПП Тернопільського НТУ ім. Івана Пулюя.

Таблиця Ж-3.

Зміст робочої програми з підготовки здобувачів ОКР «Бакалавр» зі спеціальності 125 «Кібербезпека» Національного авіаційного університету , ННІІДС

УЗГОДЖЕНО

Начальник навчально-методичного відділу

_____Л.Бородінова

"___"_____2017 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

РОБОЧИЙ НАВЧАЛЬНИЙ ПЛАН

№ РБ - 14- 125 / 17

Галузь знань:	**12**	**Інформаційні технології**
Спеціальність:	**125**	**Кібербезпека**
Спеціалізація - 01:		**Адміністративний менеджмент у сфері захисту інформації**
Кваліфікація бакалавра:	**3439**	**Фахівець з організації інформаційної безпеки**
Спеціалізація - 02:		**Системи та технології кібербезпеки**
Кваліфікація бакалавра:	**3439**	**Фахівець з кібербезпеки**

І. Графік навчального процесу

КУРС	Вересень				29	Жовтень			27	Листопад				Грудень				29	Січень			26	Лютий				Березень				30	Квітень			27	Травень				Червень				29	Липень		
I	1	8	15	22	IX	6	13	20	X	3	10	17	24	1	8	15	22	XII	5	12	19	I	2	9	16	23	2	9	16	23	III	6	13	20	IV	4	11	18	25	1	8	15	22	VI	6	13	20
	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	29	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26
	X	XI				XI				I				II				I	II												IV				V								VII			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
I																		=	=	::	::																		::	::	X	X	=	=	=	=	=
II																		=	=	::	::																		::	::	O	O	=	=	=	=	=
III																		=	=	::	::																		::	::	X	X	X	=	=	=	=	=
IV																		=	=	::	::																	::	Д	Д	Д	Д	Д	=	=	=	=	=

Таблиця Ж -4.

Узагальнена інформація щодо обсягу годин/ кредитів за видами занять в українських закладах вищої освіти ОКР «бакалавр» зі спеціальності «Кібербезпека»

ОБСЯГ РОБОТИ СТУДЕНТА (ГОДИН/ КРЕДИТІВ)							
ВСЬОГО		**Робота з викладачем**					
КРЕДИТІВ	**ГОДИН**	Аудиторних занять	Лекції	(семінарські)	Лабораторні заняття	Індивідуальні заняття	Самостійна робота
240	**7200**	**НАУ, НН ІПДС кафедра БІТ**					
		3600 Годин	1536 годин	619 годин	1235 годин	**210** годин	***3620***
		120 кредитів	48 кредитів	21 кредит	38 кредитів	7 кретитів	
%		**50%**	19%	15%	17%		***1:1***
		РЕКОМЕНДОВАНО (за аналогією до американської моделі)					
120	**1800**	**900**	300	150	300	***150***	***3600***
		60 кредитів	20 Кредитів	10 кредитів	20 кредитів	10 кредитів	
%		**50%**	17%	8 %	17%	8%	***1:4***

Додаток систематизовано автором на основі джерел: робочий план РБ-14-125/ 17 ОКР «Бакалавр» Національного авіаційного університету, ННІІДС.

Додаток З.

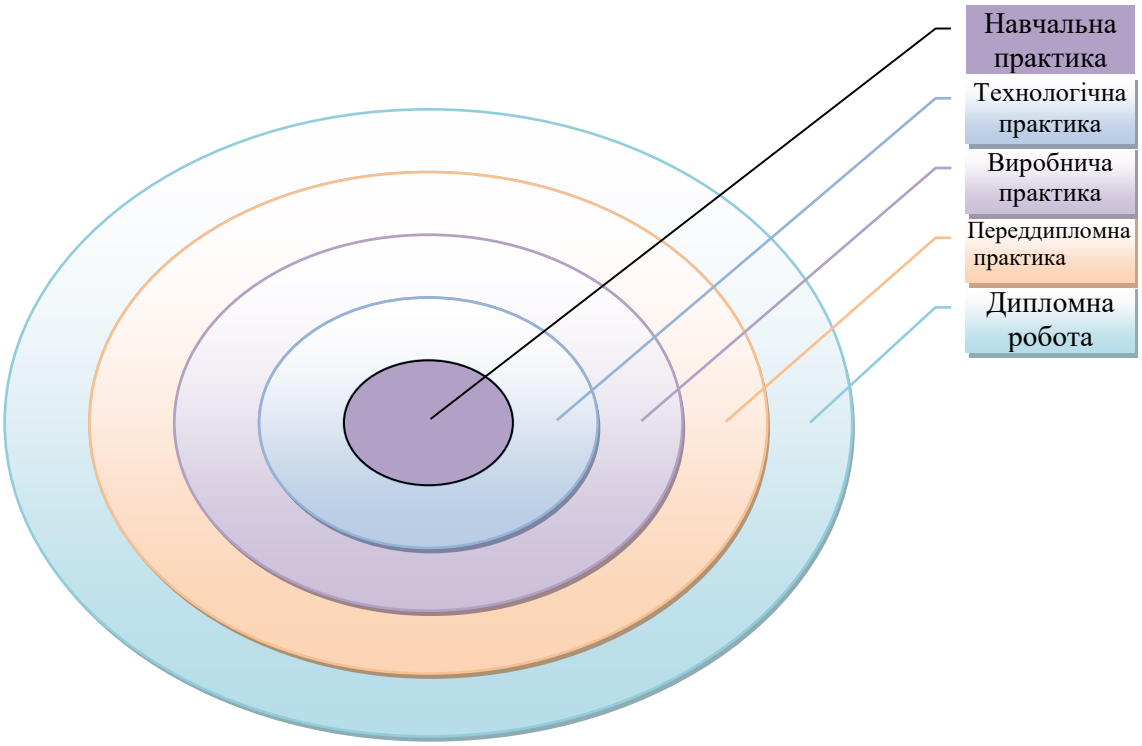
Таблиця 3-1.

Узагальнені критерії оцінювання компонентів ОПП та вимоги щодо професійної орієнтації змісту навчальних дисциплін вищих навчальних закладів США з підготовки здобувачів ОКР «бакалавр» з кібербезпеки

ЗМІСТ КРИТЕРІЮ	***ЗМІСТ ВИМОГ***
відповідність основним цілям, місії і очікуваним результатам	відповідність навчального матеріалу цілям, ОКХ для розуміння здобувачами його прикладного значення
відповідність меті підготовки бакалаврів з кібербезпеки щодо здійснення професійної діяльності наявність чіткого плану організації, реалізації та оцінювання конкретної галузі сфери дослідження	методологічна спрямованість навчального матеріалу на формування узагальнених навичок та умінь теоретична частина навчальної дисципліни є фундаментальним ядром знань
процес планування і організації ОПП за участю потенційних роботодавців залучення досвідчених практичних фахівців до створення ОПП	практична частина навчальної дисципліни має своє міце задачі практичної частни застосування теоретичних знань у майбутній професійній діяльності
контроль за актуалізацією ОПП вдповідно до галузевих вимог досліджуваної сфери відповідність щодо розвитку уміння вчитися; навичок наукового підходу до вирішення проблем; критичного мислення та самосвіти.	наявність міждисциплінарних зв’язків відповідність змісту навчальних завдань контекстові кіберзахисту кіберсередовища та попередженню кіберзагрози
відповідність щодо достатньої тривалості галузевої освіти відповідність щодо складності завдань дисциплін	відповідність змісту навчальних дисциплін сучасній методології пізнання забезпечення формування уяви цілісної картини світу
відповідність щодо зв'язку теоретичної і практичної частини ОПП відповідність щодо зв'язку з науковою школою і потенційним місцем професійної діяльності.	

Додаток систематизовано автором на основі джерел: ОПП вищих навчальних закладів США.

Додаток 3-2.



Характеристика напрямів комплексної практичної підготовки з ОКР «Бакалавр» спеціальності «Кібербезпека».

Додаток И.
Таблиця И-1

Система узагальнених прогресивних ідей досвіду підготовки бакалаврів з кібербезпепеки у вищих навчальних закладах США для екстраполяції у вищу освіту України

Рівень	АМЕРИКАНСЬКА МОДЕЛЬ ПІДГОТОВКИ	УКРАЇНСЬКА МОДЕЛЬ ПІДГОТОВКИ
Концептуальний	орієнтація системи вищої освіти США на формування здібного самостійно працювати фахівця;	орієнтація системи вищої освіти України на систематичне, послідовне засвоєння змісту дисциплін ОПП;
	підхід американських університетів і коледжів до організації проходження практик: співпраця з структурами потенційного місця роботи випускників;	формальний підхід до організації проходження практик у ВНЗ України
	позитивний та результативний підхід щодо вибору навчальних дисципліни університетів та коледжів США;	відсутність гнучких варіантів вивчення предметів в українській вищій школі (фактично не існує практики вибору навчальної дисципліни);
	баланс між теоретичною та практичною частинами начального процесу в американській моделі підготовки(3-4 предмети на семестр);	предметна перевантаженість процесу підготовки бакалаврів з кібербезпеки у системі вищої освіти України;
	високий рівень забезпеченння студентів необхідною навчально-методичним матеріалом та доступом до лабораторій, аудиторій новітніх технологій;	недостатній рівень забезпеченння навчального процесу
	взаємна відповідальність американських студентів і викладачів за якість освіти	в українській системі вищої освіти ступінь відповідальності на неналежному рівні;
Організаційно-педагогічний	Характерна диверсифікація та гнучкість структури і змісту ОПП та навчальних планів, форм і методів навчання бакалаврів ІТ.	Урахування перспектив розвитку ІТ галузі; орієнтація на модернізацію системи вищої освіти з підготовки здобувачів ОКР «Бакалавр» з«Кібербезпеки»;
	Основні принципи організації їх підготовки:самостійність, свобода вибору, неперервність, індивідуалізація, диференціація, гнучкість системність.	Основні принципи організації їх підготовки:комплексна поглиблена підготовка фахівців, здатних здійснювати проекти практично-професійної спрямованості;
	Високий рівень науково-методичного супроводу та кадрового забезпечення. орієнтація змісту та організаційних форм навчання на збалансований взаємозв’язок теорії з практикою	впровадження новітніх педагогічних технологій на основі співпраці та партнерства, особистісно-орієнтованого навчання

Рівень	АМЕРИКАНСЬКА МОДЕЛЬ ПІДГОТОВКИ	УКРАЇНСЬКА МОДЕЛЬ ПІДГОТОВКИ
Законодавчо-методичному	Гнучка законодавчо-правова база, спрямована на активну розробку та оперативну реалізацію програм розвитку освіти сфери дослідження; запровадження грантів на професійну підготовку фахівців з кібербезпеки. Постійне оновлення ОПП з метою удосконалення, відповідно до світових стандартів, вимог сучасності.	Створення гнучкого забезпечення нормативно-правового супроводу, щодо розвитку методичного, навчального та кадрового секторів та державних стандартів для системи вищої освіти з підготовки бакалаврів з кібербезпеки. Ліцензування ОПП для здобувачів ОКР «Бакалавр» з «Кібербезпеки»;
Фінансовий	Абсолютна перевага американської вищої школи в розмірах у фінансування, матеріально-технічних ресурсах Основним джерелом університетів та коледжів у США, крім держави, є комерційні структури, що прагнуть підвищити рівень кваліфікації своїх співробітників; кошти від оплати за навчання та ґранти.	Недостатня можливість забезпеченн доступу до високотехнологічних джерел сучасної наукової інформації та навчального матеріалу у вишах України; Використання альтернативних джерел фінансування; збільшення обсягу інвестицій у розвиток ІТ галузі та освітні програми; забезпечення професійної підготовки бакалаврів
Міжнародний	Інтенсивний розвиток міжнародної співпраці з проблем підготовки бакалаврів з кібербезпеки, розробка та участь у міжнародних проектах, активна реалізація програм міжнародного співробітництва.	Впровадження у вітчизняну освітню практику досліджених та оґрунтованих прогресивних ідей зарубіжного досвіду підготовки бакалаврів з кібербезпеки: американська модель. Орієнтація процесу модернізації на сучасні тенденції вищої освіти.

Додаток систематизовано автором на основі джерел: ОПП, навчальні та робочі плани вищих навчальних закладів США та України.

Таблиця И-2.
Сфери зайнятості ОКР «бакалавр» зі спеціальності «Кібербезпека» ІТ-галузі у США та України.

№ п/п	*СФЕРА ЗАЙНЯТОСТІ США*	*СФЕРА ЗАЙНЯТОСТІ Україна*
	Керівник відділу ІТ-безпеки	фахівець з організації захисту інформації;
	Судовий експерт	фахівець з інфокомунікацій;
	Фахівці швидко/оперативного реагування на інциденти	технік з сигналізації;
	Етичний Хакер	технік із конфігурованої комп'ютерної системи;
	Адміністратор безпеки	технік з обслуговування інженерно-технічних засобів охорони;
	Аналітик з питань безпеки	технік (сфера захисту інформації);
	Архітектор локальних мереж	технік із системного адміністрування (адміністратор ІС системний, мережевий);
	Аудитор у сфері безпеки	фахівець з інформаційних технологій;
	Директор з питань безпеки	інспектор з організації захисту секретної інформації;
	Консультант з інформаційної безпеки	фахівець з режиму секретності;
	Інженер з інформаційної безпеки	фахівець із організації інформаційної безпеки;
	Менеджер з інформаційної безпеки	прикладний програміст;
	Розробник програмного забезпечення	системний програміст;
		web-програміст;
		інженер з експлуатації засобів захисту інформації;
		адміністратор баз даних;
		спеціаліст з проектування систем захисту інформації;
		спеціаліст з проектування комп'ютерних мереж.

Додаток систематизовано автором на основі джерел: ОПП вищих навчальних закладів США та України.

Додаток Ї.

Національні центри академічної досконалості (ЦАД) з питань інформаційної безпеки та кіберзахисту (ІБ/КЗ)

Одиниці знань

Спільно підтримується Агентством національної безпеки (АНБ) та Міністерством внутрішньої безпеки (МВБ)

Метою модифікацій академічних вимог до програм з ІБ/КЗ ЦАД було їх оновлення. Було схарактеризовано структуру одиниць знань (ОЗ) та ключових напрямків (КН), щоб спростити вимоги у майбутньому та дозволити диференціювання серед шкіл шляхом визнання конкретних областей, в яких вони зосереджують свої дослідження та / або освітні пропозиції (наприклад, судово-медична експертиза, інженерна система безпеки, безпечне розроблення програмного забезпечення).

Обов'язкові предмети

(2 - річні програми)

Аналіз даних
Основи написання сценаріїв або вступ до програмування
Кіберзахист
Кібер-загрози
Основні принципи проектування безпеки
Основи ІБ
Введення в криптографію
Компоненти ІТ-систем
Мережеві концепції
Політика, законодавство та етика
Системне адміністрування

Обов'язкові предмети

(4 - річні програми)

Бази даних
Мережева оборона
Мережеві технології та протоколи
Концепції операційних систем
Ймовірність та статистика
Програмування

Предмети за вибором

• Розширена криптографія
• Розширені мережеві технології та протоколи
• Алгоритми
• аналогові телекомунікації
• Хмарні обчислення
• Планування та управління кібербезпекою
• Адміністрування даних
• структури даних
• Системи управління базами даних

• Цифрові комунікації
• Цивільна судова експертиза
• Криміналістика пристроїв
• Проведення судово-медичної експертизи
• Медіа-криміналістика
• Мережа криміналістика
• Вбудовані системи
• Судова бухгалтерія
• Формальні методи
• Запобігання шахрайству
• Апаратне проектування
• Апаратне забезпечення / прошивка безпеки
• Архітектура ІБ
• Відповідність вимогам ІБ
• Стандарти ІБ
• Незалежне / Дирекційне дослідження / Дослідження
• Системи промислового контролю
• Вступ до теорії обчислень
• Виявлення вторгнень
• Безпека життєвого циклу
• Низький рівень програмування
• Мобільні технології
• Адміністрування мережевої безпеки
• загартування операційних систем
• Теорія операційних систем
• Огляд кібер-операцій
• Тестування проникнення
• QA / Функціональне тестування
• Принципи РФ
• Захист практики програмування
• Управління програмою безпеки
• Аналіз ризиків безпеки
• Software Assurance
• Програмне забезпечення зворотної інженерії
• Аналіз безпеки програмного забезпечення
• Безпека постачання
• Системне програмування
• Системи сертифікації та акредитації
• Системи безпеки інженерії
• Технології віртуалізації
• Аналіз вразливості
• Бездротові сенсорні мережі

Національні центри ІБ/КЗ з академічної досконалості в інформаційній безпеці / підрозділи знань з кіберзахисту CAE

Таблиця Й-1

Дохід фахівців за рівнем освіти та досвідом роботи

Додаток Й

ОСВІТА/*ДОСВІД*	**0-3 роки**	**4-6 років**	**7-16 років**	**11-15 років**	**16-20 років**	**+ 20 років**	**Середній дохід**
Диплом середньої школи	$47.917	$75,938	$115,000	$86,235	$102,222	$123,333	$89,013
Диплом коледжу /технічної школи	$66,761	$86,560	$100,726	$115,662	$116,436	$117,073	$101,014
Диплом молодого спеціаліста	$62,302	$85,000	$93,418	$107,569	$101,528	$106,756	$90,601
Диплом бакалавра	$71,564	$84,619	$100,862	$115,782	$123,56	$127,733	$98,510
Навчання у магістратурі	$79,479	$87,069	$100,952	$122,842	$177,500	$177,667	$106,439
Диплом магістра	$82,036	$97,109	$100,319	$170,964	$137,816	$175,464	$109.705
Ступінь доктора філософії	$121,667	$114,231	$126,462	$119,600	$150,000	$116,250	$125,244

Таблиця Й-2.

Середній дохід за назвою посади та роками досвіду (*10 топ найменувань посад*)

CISO/CSO	**0 – 3**	**4 – 6**	**7 – 10**	**11 – 15**	**16 – 20**	**Середня**
Директор або менеджер з інформаційних технологій	$89,500	$97,750	$125,400	$138,529	$148,000	$133,989
Керівник відділу IT–безпеки	$108,846	$105,189	$120,381	$128,379	$134.538	$124.798
Інженер-програміст з інформаційної безпеки	$96,429	$104,242	$107,184	$123,588	$114,070	$112,014
Інженер з безпеки або архітектор	$70,238	$97,128	$105,828	$119,568	$123,358	$106,630
Системний інженер або інтегратор	$89,444	$89,706	$108,750	$115,556	$129,615	$105,773
Мережевий інженер або архітектор	$91,944	$85,000	$107,179	$107,625	$109.118	$103,065
Судовий експерт	$67,273	$83,625	$101,000	$123,448	$159,286	$99,457
Аудитор	$65,278	$82,600	$97,143	$107,115	$113,333	$96,529
Аналітик з питань безпеки	$72,393	$ 79,034	$93,498	$101,618	$109.915	$87,829
Системний адміністратор	$62,679	$75,000	$85,469	$87,333	$91,000	$80,351

Таблиця Й-3.

Анкета Центру Кооперативного навчання і практики щодо оцінювання практиканта роботодавцем у США

№ п/п	Показники підготовки	Відмінно	Добре	Задов.	Гранично прийнятно	Не задов.	Не прийнятно
1	Вмінн проводити пошук і збір інформації з відкритих , відносно-відкрити і закритих електор. джерел						
2	Вміння використовувати знання про сутність і значення інформації в розвитку сучасного суспільства						
3	Вміння використовувати інформаційні технології						
4	Вміння протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ истем і мереж						
5	Вміння забезпечити стійкість роботи, ІТ систем і мереж та відновлення їх нормального функціонування після здійснення кібернападів						
6	Вміння аналізувати дані						
7	Вміння атестувати об'єкт згідно вимогам нормативних документів						
8	Вміння оформлювати технічну документацію згідно діючих нормативних документів в області інформаційної і кібербезпеки						
9	Здатність проводити аналіз інформаційної безпеки об'єктів						
10	Здатність формувати комплекс мір (правила,прийоми процедури, тощо) для керування кібербезпекою						
11	Вміння працювати в команді						
12	Розуміння професійної та моральної відповідальності						
13	Навички спілкування						
14	Писемна грамотність						
15	Усвідомлення необхідності навчатися протягом усього життя						
16	Загальна оцінка академічної підготовки студента						

Додаток К.

Додаток К-1.

Зобов'язання майбутнього фахівця з кібербезпеки щодо проходження практики

згідно Проекту Центру Кооперативного навчання і практики

Стосовно Академічного статусу

Я_____розумію, що для участі у програмі практики, мені слід мати середній бал, не нижчий, ніж 2;

Я _____ проінформований щодо умов участі у Проекті практики та стосовно документів, які слід завірити у координатора практики.

Стосовно фінансової допомоги *(за наявності стипендії)*

Я _____ розумію, що зобов'язаний самостійно зв'язатися з Офісом Фінансової Допомоги Студентам (Office of Student Financial Aid) стосовно стипендії та позичок залежно від певного виду діяльності під час практики.

Стосовно професійної етики

Я _____ усвідомлюю, що є представником (назва навчального закладу) і тому повинен дотримуватися професійної етики під час проходження практики / стажування;

Я _____ розумію, що як практикант, я повинен (повинна) самостійно обговорити з координатором питання стосовно своєї посадовуої інструкції, умов праці, компенсацій та мотивації.

Стосовно Страхування від нещасних випадків

Я _____ розумію, що в моїх інтересах мати страховку від нещасних випадків на час підписання договору. (назва навчального закладу) не несе відповідальності за нещасні випадки, що можуть трапитись зі мною на виробництві.

Стосовно Грошової компенсації по безробіттю

Я _____ розумію, що як практикант, я не маю право подавати позов на підприємство, де проходжу практику, або (назва навчального закладу) щодо виплати компенсації по безробіттю.

Стосовно Доступу до персональних даних

Я _____ погоджуюся надати відповідальній особі за практику / стажування інформацію про мої академічні успіхи для того, щоб роботодавці могли оцінити мою придатність тій чи інвідповідність щодо запланованої посади.

Я _____(за бажанням) дозволяю координатору та службовому персоналу з проходення практики зробити результати моєї практики доступними для всіх бажаючих ознайомитися з ними.

Я_____повинен вчасно повідомити про початок своєї практики координатора програми. Зобов'язуюсь дотримуватись посадової інструкції вимог роботодавця та навчального закладу, щодо графіку проходення практики. Розумію, що моя зайнятість в організації обмежується термінами, вказаними у договорі.

Підпис студента _____ Дата _____

Підпис координатора проекту _____ Дата_____

Додаток систематизовано автором на основі джерела: ОПП університету Стівенс.

Додаток К-2.

Зразок вимог-рекомендацій Центру Кооперативного навчання і практики щодо проекту практики, нормативних супровідних документів майбутніми фахівцями ІТ галузі на потенційному місці роботи

Розробляючи проект проходження практики слід *:*

1) Перш за все визначити цілі практики. Створити документ – Проект практики щодо видів діяльності організації. Слід визначити місце та роль навчального закладу в програмі практики, включити інформацію про координатора програми, перелік пропонованих посад та відповідних посадових інструкцій, особливі навички, якими бажано володіти практиканту, перелік предметів, які потрібно пройти перед практикою;

2) Зазначити терміни практики та узгодити з графіком навчальних занять навчального закладу у проекті практики. Встановити строки вирішення поставлених завдань з метою найефективнішого використання часу.

3) Визначити відповідальних осіб з числа робочого колективу, які будуть допомагати студентові. Визначити та чітко описати обов'язки координатора (керівника) програми, інших учасників практики, студента.

4) Проект практики та основні аспекти організації практики обговорити з усіма сторонами-учасниками проекту для того, щоб можна було адресувати запитання, які виникають, безпосередньо до компетентної в цьому особи та довести до відома кожного учасника практики цілі та специфіку роботи.

5) Врахувати у програмі рекомендації та вимоги навчального закладу, у якому навчається студент.

Координатору (supervisor), *практики слід:*

6) Розуміти, що під час практики студент знаходиться під його наглядом;

7) Координатор у ході практики повинен ознайомити студента з особливостями роботи, бути його наставником, заохочуючи роботу студента та забезпечучи зворотній зв'язок, в кінці практики дати оцінку результатів діяльності студента.

8) Координатор – це фахівець, що володіє певними уміннями і навичками: це перш за все професіонал у ІТ- галузі та старанно ставитися до своїх обов'язків; мати досвід роботи зі студентами, вміти вирішувати проблемні питання; забезпечити баланс між наглядом, управлінням та самостійним навчанням студентів; вміти дати оцінку досягнутим результатам.