МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ДРАГОМАНОВА

Кваліфікаційна наукова
праця на правах рукопису

МАГІЛЕВСЬКИЙ Владислав Віталійович

УДК 378.091.33:004.056-051:[006.91+621.3] (043.3)

ДИСЕРТАЦІЯ

ПРОФЕСІЙНА ПІДГОТОВКА МАЙБУТНІХ ФАХІВЦІВ ДО РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ЕЛЕКТРОНІКИ, МЕТРОЛОГІЇ ТА РАДІОТЕЛЕКОМУНІКАЦІЙ

011 – Освітні, педагогічні науки
01 – Освіта/Педагогіка

Подається на здобуття наукового ступеня доктора філософії.

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

_____ В.В. Магілевський

(підпис, ініціали та прізвище здобувача)

Науковий керівник: Рідей Наталія Михайлівна,
доктор педагогічних наук, професор

Київ – 2026

АНОТАЦІЯ

Магілевський В.В. Професійна підготовка майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 011 «Освітні, педагогічні науки» – Український державний університет імені Михайла Драгоманова, Київ, 2026.

У ході дисертаційного дослідження досягнуто мету, яка полягала у розробці, теоретичному обґрунтуванні та експериментальній перевірці моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Вирішено завдання дослідження, а саме: здійснено аксіологічний та порівняльний аналіз тезаурусу, стану і перспектив педагогічної проблеми досліджень у академічних надбаннях; проведено контент-, формально-логічний та компаративний аналізи міжнародного та національного нормативно-правового забезпечення особливостей професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки для сфери електроніки, метрології та радіотелекомунікацій за функціональним призначенням; розроблено, обґрунтовано проєктування моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації; експериментально перевірено її ефективність у виокремлених педагогічних умовах на основі розробленого критеріального апарату оцінювання рівня сформованості професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації.

Визначено, обґрунтовано та розкрито науковий апарат дослідження, а саме: об’єкт дослідження як процес професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та

радіотелекомунікацій; предмет дослідження як модель організації (зміст, форми та методи) формування професійної компетентності до реалізації інформаційної безпеки майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Виокремлено наукову новизну захисних положень педагогічного дослідження – уперше: обґрунтовано теоретичні та методичні засади педагогічної проблеми професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій; розроблено, обґрунтовано та верифіковано модель організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій; «КВАРТЕТ» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах професійної підготовки майбутніх фахівців для галузі знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелекомунікації» (соціальна та інформаційна політика, метрологія, інформаційні менеджмент та безпека, технології); розроблено, обґрунтовано та верифіковано педагогічні умови реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій (формування сприятливого середовища плекання інформаційної культури – навчальний проєкт «Інформаційна розвідка: від ланцюгів пошуку даних до визначення їх достовірності»; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу – окреслено абриси структури сучасного інформаційно-технологічного забезпечення та сервісу у ЗВО, запропоновано алгоритм застосування наукометричних сервісів в освітньому процесі «Науково-метричний цифровий профіль молодого дослідника» та мережева інформаційна безпека системи – розроблено інтенсив-спецкурс «Кібербезпека в сфері освіти, науки й інноватики: від навчання до компетентності» та пам'ятку з кібергігієни для здобувачів освіти); критеріальний апарат діагностики рівнів (достатній,

середній та високий) сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у критеріях (системно-управлінський, нормативний та мотиваційний); конкретизовано методологічні та розкрито інформаційно-технологічні аспекти забезпечення формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій; сформульовано у авторському тлумаченні дефініції – «професійна підготовка майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій», «процес професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій»; верифіковано за бальним оцінюванням ефективності моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій; подальшого розвитку набули методологічні положення змістового наповнення та науково-методичного, інформаційно-технологічного супроводу професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій.

Практичне значення одержаних результатів полягає у тому, що: розроблено і апробовано «КВАРТЕТ» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах дисциплін і практик професійної підготовки майбутніх фахівців для галузі знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелекомунікації» – соціальна та інформаційна політика, метрологія, інформаційні менеджмент та безпека, технології; запропоновано модернізований зміст програмних результатів навчання, загальних компетентностей, спеціальних (фахових) компетентностей задля формування пропозицій до оновлення Стандарту вищої освіти України за спеціальністю 015 «Професійна освіта (за спеціалізаціями)» для першого

(бакалаврського) рівня вищої освіти; розроблено засоби методичного супроводу освітніх компонентів для спеціалізацій «Цифрові технології» – «Вступ до спеціальності», «Основи кібербезпеки», «Технології навчання, інформаційні технології (мережеві)» та «Електроніка, метрологія та радіотелекомунікації» – «Вступ до фаху», «Інформаційна безпека та захист інформації», «Цифрові освітні та комунікативні технології в галузі».

Ключові слова: *професійна підготовка, інформаційна безпека, національна безпека, захист даних, електронні системи, безпечна передача даних, контролювання доступу, інформаційні технології, заклад вищої освіти, майбутні фахівці, електроніка, метрологія, радіотелекомунікації, інформаційно-комунікаційні технології, комунікації, цифровізація, теорія і методика професійної освіти, бакалаври професійної освіти, засоби хмарних технологій, освітній процес, організація освітнього процесу.*

ANNOTATION

Mahilevskyi V.V. Professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications. – Qualifying scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 011 "Educational, Pedagogical Sciences" – Drahomanov Ukrainian State University, Kyiv, 2026.

The dissertation research achieves its goal, which consists in the development, theoretical substantiation, and experimental verification of a model for organizing the formation of professional competence for the implementation of information security in future specialists for the field of electronics, metrology, and radiotelecommunications.

The research tasks have been solved, namely: an axiological and comparative analysis of the thesaurus, state, and prospects of the pedagogical problem in academic achievements was performed; content, formal-logical, and comparative analyses of international and national regulatory and legal support for the professional training of future specialists were conducted; the design of a model for organizing the formation of professional competence of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications was developed and substantiated; the effectiveness of the model was experimentally verified under specific pedagogical conditions based on a developed criteria apparatus for assessing the level of professional competence.

The scientific apparatus of the study is defined, substantiated, and disclosed: the object of the study is the process of professional training of future specialists to ensure the acquisition of professional competence for information security implementation; the subject of the study is the organizational model (content, forms, and methods) of forming professional competence for information security implementation for future specialists in the field of electronics, metrology, and radiotelecommunications.

The scientific novelty of the findings of the pedagogical research is highlighted – for the first time: the theoretical and methodological foundations of the pedagogical problem of professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications were substantiated; an organizational model for forming professional competence for the implementation of information security in future specialists for the field of electronics, metrology, and radiotelecommunications was developed, substantiated, and verified; a "QUARTET" of educational modules was introduced according to the cycles of general, professional, and special training in the educational components of professional training of future specialists for Knowledge area A Education, specialty A15 Professional Education, specializations "Digital Technologies" and "Electronics, Metrology, and Radiotelecommunications" (social and information policy, metrology, information management and security, technologies); pedagogical conditions for the implementation of professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications were developed, substantiated, and verified (formation of a favorable environment for fostering information culture – educational project "Information Reconnaissance: from data search chains to determining their reliability"; equipping the toolkit of information-technological support/service – the outlines of the structure of modern information-technological support and service in HEIs were defined, an algorithm for applying scientometric services in the educational process "Scientometric digital profile of a young researcher" was proposed, and network information security of the system – an intensive special course "Cybersecurity in the field of education, science, and innovation: from training to competence" and a guide on cyber-hygiene for students were developed); a criteria apparatus for diagnosing levels (sufficient, average, and high) of the formation of professional competence for the implementation of information security in future specialists for the field of electronics, metrology, and radiotelecommunications in criteria (systemic-managerial, normative, and motivational); methodological aspects were specified and information-technological

aspects of ensuring the formation of professional competence of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications were disclosed; definitions were formulated in the author's interpretation – "professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications", "the process of professional training of future specialists to ensure the acquisition of professional competence for the implementation of information security in the field of electronics, metrology, and radiotelecommunications"; the effectiveness of the model for organizing the formation of professional competence for the implementation of information security in future specialists for the field of electronics, metrology, and radiotelecommunications was verified by scoring assessment; methodological provisions of content filling and scientific-methodological, information-technological support of professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications were further developed.

The practical significance of the results obtained lies in the fact that: the "QUARTET" of educational modules has been developed and tested across the cycles of general, professional, and special training in the educational components of disciplines and practices of professional training of future specialists for the field of knowledge A Education, specialty A Professional Education, specializations "Digital Technologies" and "Electronics, Metrology, and Radiotelecommunications" – social and information policy, metrology, information management and security, technologies ; the modernized content of program learning outcomes, general competencies, and special (professional) competencies has been proposed for the formation of proposals for updating the Standard of Higher Education of Ukraine for specialty 015 "Professional Education (by specializations)" for the first (bachelor's) level of higher education ; means of methodological support for educational components have been developed for the specializations "Digital Technologies" – "Introduction to the Specialty," "Fundamentals of Cybersecurity," "Learning

Technologies, Information Technologies (network)" and "Electronics, Metrology, and Radiotelecommunications" – "Introduction to the Profession," "Information Security and Data Protection," "Digital Educational and Communicative Technologies in the Field".

***Keywords**: professional training, information security, national security, data protection, electronic systems, secure data transmission, access control, information technologies, higher education institution, future specialists, electronics, metrology, radiotelecommunications, information and communication technologies, communications, digitalization, theory and methodology of professional education, bachelors of professional education, cloud technology tools, educational process, organization of the educational process.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковано основні результати дисертації

Статті в наукових фахових виданнях України

1. **Магілевський В.В.** Формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних. *Педагогічна Академія: наукові записки*. 2025. №14. URL: https://pedagogical-academy.com/index.php/journal/article/view/572.

2. **Магілевський В.В.** Підготовка майбутніх фахівців до інтеграції сучасних методів захисту даних у сфері електроніки та метрології. *Інноваційна педагогіка*. 2025. №82, Том 2.С. 99-107.

3. **Магілевський В.В.** Використання сучасних стандартів інформаційної безпеки у професійній підготовці фахівців радіотелекомунікацій. *Інноваційна педагогіка*. 2025. №83, Том 2. С. 111-117

4. **Магілевський В.В.**, Рідей Н.М. Оцінка ефективності освітніх програм для підготовки фахівців до інформаційної безпеки у сфері радіотелекомунікації. *Наукові інновації та передові технології*, 2025. Випуск №9(49). С. 1927-1945.

Статті у зарубіжних наукових періодичних виданнях

5. **Mahilevskyi V.** Content analysis of technical regulation means for training future specialists to implement information security in the field of electronics, metrology, and radiotelecommunications. *Paradigm of knowledge*. 2025. Vol 5, № 69. URL: https://naukajournal.org/index.php/Paradigm/issue/view/276.

Наукові праці, які засвідчують апробацію матеріалів дисертації

6. **Магілевський В.В.** Цифрові інструменти педагогічного супроводу майбутніх фахівців радіотелекомунікацій у сфері інформаційної безпеки. *Збірник матеріалів VIII Міжнародної науково-практичної конференції «Сучасні світові тенденції розвитку науки та інформаційних технологій»*, 29–30 травня 2025 р. м. Одеса. С. 8-14.

7. **Магілевський В.В.** Педагогічні умови формування готовності майбутніх фахівців до забезпечення інформаційної безпеки у сфері телекомунікацій. *Збірник матеріалів XVI Міжнародної науково-практичної конференції «Актуальні проблеми сучасної науки та освіти»,* 7-8 листопада 2025 року, Львів. С. 66-69.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CCDCOE – Центр передового досвіду з кібероборони (з англ. – Cooperative Cyebr Defence Centre of Excellence)

COBIT – IT-стандарт «Контрольні цілі для інформаційних та суміжних технологій» (з англ. – Control Objectives for Information and Related Technologies)

CSBMs – Заходи довіри та безпеки (з англ. – Confidence- and Security-Building Measures.

DPIA – Проведення оцінки впливу на захист даних (з англ. – Data Protection Impact Assessment)

GCA – Глобальний порядок денної кібербезпеки (з англ. – Global Cybersecurity Alliance)

GDPR – Директиви загального регламенту про захист даних (з англ. – General Data Protection Regulation)

GGE – Група урядових експертів (з англ. – Group of Governmental Experts)

IEC – Міжнародна електрична комісія International (з англ. – Electrotechnical Commission)

IOT – Інтернет речей (з англ. – Internet of Things)

ISO – Міжнародна організація стандартизації (з англ. – International organization for Standartisation)

ITU – Міжнародний союз електрозв'язку (з англ. – International Telecommunication Union)

NIS – Мережеві та інформаційні системи (з англ. – Network and Information Systems)

NIST (CSF) – набір добровільних інструкцій, розроблених, щоб допомогти організаціям оцінити та покращити здатність запобігати, виявляти та реагувати на ризики кібербезпеки (з англ. – Cybersecurity Framework)

OEWG – Відкриті робочі групи (з англ. – Open-ended Working Group)

ДСТУ – Державний Стандарт України

ЗУ – Закон України

ЗУН – Знання / Вміння / Навички

ІКТ – інформаційно-комунікаційні технології

КСЗІ – Комплексна система захисту інформації

НАЗЯВО – Національне агентство із забезпечення якості вищої освіти

НАТО – Організація Північноатлантичного договору/Північноатлантичний альянс (з англ. – North Atlantic Treaty Organization)

ОБСЄ – Організація з безпеки і співробітництва в Європі (з англ. – Organization for Security and Co-operation in Europe)

ООН – Організація Об'єднаних Націй

СУІБ – Система управління інформаційною безпекою

ШІ – штучний інтелект

ВСТУП

Актуальність теми дослідження. У сучасних умовах глобалізації та стрімкого розвитку цифрових технологій питання інформаційної безпеки постає як одне з ключових для стабільності держави й суспільства. Від її ефективного функціонування залежить не лише захищеність стратегічних секторів економіки, але й надійність систем державного управління та критичної інфраструктури. В умовах цифрової трансформації національного господарства гарантування інформаційної безпеки вимагає не лише технологічних рішень, але й системної підготовки висококваліфікованих фахівців, здатних реалізовувати комплексний підхід у проєктуванні, впровадженні, захисті та експлуатації інформаційних систем. Формування у майбутніх фахівців професійних компетентностей до реалізації інформаційної безпеки потребує чітко структурованої та імплементованої нормативно-правової бази до міжнародних, що б забезпечило гармонійне поєднання міжнародних стандартів, національного законодавства та стратегій освітніх політик. Наразі перед українською системою вищої освіти постає завдання не лише адаптації до глобальних вимог у сфері інформаційної безпеки, але й активного впровадження інституційних механізмів для забезпечення резервів кадрового потенціалу в галузі знань 01 Освіта/Педагогіка (нині – А Освіта).

Електроніка, метрологія та радіотелекомунікації – це галузь знань – інженерний напрям, що забезпечує триаду взаємодії процесно-апаратних комплексів гарантує точність достовірної метрики вимірювань та безпеки інформаційної та кіберзахисту систем зв'язку. Майбутні фахівці галузі задіяні у процесах проектування, обслуговування і сервісної підтримки телекомукаційних мереж, радіоапаратури та систем метрологічного контролю за достовірністю і якістю вимірювань параметрів надійності, оперативності комунікацій зв'язку. Структурно-змістові компоненти галузі: електроніка – наука, яка вивчає взаємини електронів з електромагнітними полями, що застосовується у приладобудуванні, параметральній метриці вимірювань

показників та комунікаціях; метрологія – наука з вимірювань, що забезпечує цілісність і точну достовірність результатів у процесах стандартизації, верифікації обладнання, апаратних комплексів; радіотелекомунікації – техніко-інженерні системи для передачі інформації (радіо-, теле-, мобільного зв'язку комп'ютерних та соціокультурних мереж); технічна галузь та сфера спеціальної діяльності , що реалізує трансляцію інформації на відстанях при використанні радіохвиль, передбачає проєктну, експлуатаційну та сервісну діяльність бездротових мереж, радіозв'язку, телерадіомовлень та глобального позиціонування систем; сертифікації, аудиту, моніторингу, експертизи, паспортизації, надання ліцензій та підтвердження на право діяльності;

Аспекти державної політики у сфері інформаційної безпеки, засоби технічного регулювання вивчали у контексті міждисциплінарного бачення: В. Арістова, Д. Сулацький; Є. Архипова; М. Грайворонський, О. Новіков; А. Гуз; О. Довгань; Д. Дубов; К.Захаренко; О. Золотар; О. Корченко; К. Молодецька-Гринчук; О. Рибальський, В. Хахановський, В. Кудінов; І. Сердюк; В. Шемчук. Питання правового регулювання інформаційної безпеки досліджували науковці відповідно: О. Баранов; В. Гурковський; Б. Кормич; А. Нашинець-Наумова; О. Олійник; Д. Ланде, В. Фурашев, К. Юдкова; І. Арістова, О. Баранов, К. Бєлякова О. Дзьобань; І. Бєляков. Наукові розвідки учених у контексті інформаційної безпеки як складової національної безпеки держави здійснювали автори щодо: О. Архипов, О. Муратов; І. Доронін; А. Качинський; В. Ліпкан; В. Ліпкан, Ю. Максименко, В. Желіховський; В. Ліпкан, К. Череповський; Т. Перун; В. Петрик, О. Семченко; Г. Пєвцов, С. Залкін; А. Тарасюк; О. Тихомиров; Т. Ткачук; В. Торічний. Інформаційно-технологічні аспекти формування архітектури інформаційної безпеки для впровадження й удосконалення інформаційно-комунікаційних технологій в освітньому просторі України з метою забезпечення сприятливого інформаційного середовища та відкритої освіти розглядали учені: В. Биков, В. Лапінський, А. Пилипчук, М. Шишкіна; Ю.Жук, Н. Задорожна, Т.Омельченко; О. Білоус, Ю. Богачков; Р. Гуревич, Ю. Кадемія; А.Гуржій,

Л.Карташова; К. Кірей, Л. Кірей; Л. Панченко; О. Співаковський; О. Спірін. Теоретико-методологічні засади професійної підготовки фахівців з інформаційних технологій та кібербезпеки досліджували науковці: І. Бардус; В.М. Богуш, В.В. Богуш, В. Бровко, В. Настрадін; І. Діордіца; П. Малежик; О. Матвійчук-Юдіна; Я. Сікора; В. Артемов; А. Васильєв, Ю. Зубань, Ю. Коровайченко, С. Шкарлет; С. Воскобойніков; Ю. Іванчук; О. Ілляшенко; О. Трифонова; Л. Зубик; М. Газдик; Т. Гончаренко; Г. Лебедь. *Аналіз останніх досліджень і публікацій у періодичних виданнях дав змогу виокремити компетентні розвідки дослідників у питаннях щодо:* В.Богуш, М.Хмельницький; Ю. Борсуковський, В. Бурячок; П. Складанний, В. Борсуковська; В. Горлинський; Ю.Даник, Ю. Супрунов; Л. Дегтярьова, В. Ляшевський; О. Дубровін, В. Коваль; О. Євсюкова; Л. Козубцова, І. Козубцов, В. Ліщина, С. Штаненко; В. Кудлай; О. Лаврова; С. Мельник; А. Міночкін; О. Самойленко; Ю. Сачук; В. Семко.

Виокремлено особливості формування професійних компетентностей на засадах компетентнісного підходу у ЗВО. Дослідження здійснено фахівцями у профілі педагогічних розвідок: Л. Васіна; Т. Гончаренко; О. Жарова; О. Ігнатюк; А. Кокарєва; К. Лебедєва; Г. Луценко; Л. Марцева; В. Петрук; М. Вінник; О. Гура; О. Джеджула; Ф. Лясова; Л. Сергеєва, Т. Стойчик, К. Мартиненко; К. Стрюк; І. Хом'юк; В. Татарчук; А. Коломієць; С. Петрович; О. Сажієнко. *Уточнено практично-корисний зарубіжний досвід професійної підготовки фахівців-інженерів, в тому числі з кібербезпеки:* Г. Артюшин, К. Тушко; Б. Бистрова; Н. Бідюк; Б. Брайко; О. Павленко; І. Пододіменко; Р. Шаран; А. Кузьмінський, О. Кучай, О. Біда.

Методологічні, інституційні та нормативні та засади розвитку й забезпечення метрологічної діяльності в Україні, що сформували системну основу для підготовки та професійного розвитку висококваліфікованих фахівців у системній єдності метрики, вимірювань, стандартизації ґрунтовно представлені в наукових доробках щодо: О. Величко; І.Дудич; Л.Коломієць, Т. Гордієнко; Л. Віткін, Ю. Кузьменко; Д.Луценко; Є. Володарський,

І. Потоцький; Л.Кошева; Ф. Гриневич; С.Таранов; Б. Гриньов, Ю. Даниленко, В. Любинський; О. Жихарєва, В. Ігнаткін, Н.Єфіменко, Ю. Туз; Ю. Кузьменко, С. Черепков, В.Дуля; М. Козаченко, О. Панченко; В.Мотало, А.Мотало, Б.Стадник. *Визначено, що значну роль у забезпеченні нарощення когнітивного потенціалу здобувачів освіти забезпечено авторами посібників та підручників:* В. Бабак, С. Бабак, В. Єременко; Р. Бичківський; Л. Боженко; Є. Володарський, В.Кухарчук, В.Поджаренко та Г.Сердюк; І. Григоренко, С.Кондрашов І. та С.Григоренко; А. Гуржій, Л. Возненко, Н.Поворознюк та В.Самсонов; М. Дорожовець, В.Мотало та Б.Стадник; В. Ігнаткін, О.Томашевський та В. Матюшин; В.Кухарчук, В.Кучерук, Є.Володарський та В.Грабко; Л.Коломієць, П.Воробієнко та М.Козаченко; П. Орнатський; Ю. Павленко та І. Захаров; В. Поджаренко та В. Кухарчук; В. Поджаренко, П. Кулаков, О.Ігнатенко та О.Войтович; Є.Поліщук, М. Дорожовець та В.Яцук; В. Сиротюк, С. Хімка та С. Сиротюк; І. Солтис та О.Деревянчук; В. Топольник та М. Котляр; В. Цюцюра та С.Цюцюра; Н.Яворський, В.Теслюк та Є.Литвинова.

Аналіз досліджень вказує на наявність вагомих *суперечностей*, які обумовлюють проблему дослідження між :

– специфікою динамічно модифікованими видами загроз інформаційної безпеки (також кіберзагроз) у критичній інфраструктурі за видами економічної діяльності та недостатнім рівнем сформованості професійної компетентності випускників ЗВО до оперативного реагування в умовах соціальної турбулентності та цифровізації суспільства;

– соціальним замовленням на майбутніх фахівців, які здатні реалізувати інформаційну безпеку у сфері електроніки, метрології та радіотелекомунікації і традиційними підходами до формування їх професійної компетентності;

– необхідністю цілісної моделі організації професійної підготовки майбутніх фахівців з компетентностями до реалізації інформаційної безпеки у сфері електроніка, метрологія та радіотелекомунікації та переважно

фрагментарним висвітленням проблем інформаційної безпеки у змісті освітніх компонентів спеціальності А15 Професійна освіта;

– потребою у розробці науково-обґрунтованого критеріального апарату оцінювання рівнів сформованості професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій та відсутністю відповідного діагностичного інструментарію у сфері професійної освіти;

Виявлені об'єктивні суперечності зумовили вибір теми наукового дослідження: «**Професійна підготовка майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій**».

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до теми Зведеного плану НДР сфери освіти, науки та інноватики у межах виконання теми «Освітня політика якості й безпеки життєдіяльності соціокультурних форм для сталого розвитку України» (ДР № 0122U000046, 2022-2024 рр.). Тему дисертації затверджено вченою радою Українського державного університету імені Михайла Драгоманова (протокол № 14 від 27 червня 2025 р.).

Мета дослідження: полягає в розробці, теоретичному обґрунтуванні та експериментальній перевірці моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Реалізація поставленої мети передбачає вирішення **завдань дослідження:**

1) здійснити аксіологічний та порівняльний аналіз тезаурусу, стану і перспектив педагогічної проблеми досліджень у академічних надбаннях;

2) провадити контент-, формально-логічний та компаративний аналізи міжнародного та національного нормативно-правового забезпечення особливостей професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки для сфери електроніки, метрології та радіотелекомунікацій за функціональним призначенням;

3) розробити, обґрунтувати проєктування моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації;

4) експериментально перевірити ефективність моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій у виокремлених педагогічних умовах на основі розробленого критеріального апарату оцінювання рівня сформованості (професійної компетентності).

Об'єкт дослідження – процес професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій.

Предмет дослідження – модель організації (зміст, форми та методи) формування професійної компетентності до реалізації інформаційної безпеки майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Для вирішення поставлених завдань було використано комплекс **методів дослідження**:

– *теоретичні методи*: методи аналізу (аксіологічний, порівняльний, контент-, формально-логічний, функціональний) понятійно-категоріального апарату педагогічної проблеми дослідження, правового та технічного регулювання професійної підготовки кадрів для сфери електроніки, метрології та радіотелекомунікацій, зіставлення та порівняння поглядів учених на проблему дослідження, визначення предметно-об'єктного поля дослідження та тезаурусу стану та перспектив обраної теми у академічних надбаннях; моделювання (розробка моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій); логічне узагальнення (висновки та рекомендації щодо системної організації освітнього процесу);

– *емпіричні методи*: вивчення досвіду застосування методів, форм і засобів організації професійної підготовки майбутніх фахівців, оцінювання навчальних досягнень студентів; експертні оцінки, анкетування,

спостереження, тестування; педагогічний експеримент (констатувальний, формувальний) спрямовано на вивчення стану традиційної та перевірки ефективності розробленої моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікації;

– *методи математичної статистики:* кількісний і якісний аналіз емпіричних даних.

Наукова новизна одержаних результатів полягає у тому, що *уперше*:

– *обґрунтовано* теоретичні та методичні засади педагогічної проблеми професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій;

– *розроблено, обґрунтовано та верифіковано* модель організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій; «КВАРТЕТ» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах професійної підготовки майбутніх фахівців для галузі знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелекомунікації» (соціальна та інформаційна політика**,** метрологія, інформаційні менеджмент та безпека, технології);

– *розроблено, обґрунтовано та верифіковано* педагогічні умови реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій (формування сприятливого середовища плекання інформаційної культури – навчальний проєкт «Інформаційна розвідка: від ланцюгів пошуку даних до визначення їх достовірності»; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу – окреслено абриси структури сучасного інформаційно-технологічного забезпечення та сервісу у ЗВО, запропоновано алгоритм застосування наукометричних сервісів в освітньому процесі

«Науково-метричний цифровий профіль молодого дослідника» та мережева інформаційна безпека системи – розроблено інтенсив-спецкурс «Кібербезпека в сфері освіти, науки й інноватики: від навчання до компетентності» та пам'ятку з кібергігієни для здобувачів освіти);

– критеріальний апарат діагностики рівнів (достатній, середній та високий) сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у критеріях (системно-управлінський, нормативний та мотиваційний);

– *конкретизовано* методологічні та *розкрито* інформаційно-технологічні аспекти забезпечення формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій;

– *сформульовано* у авторському тлумаченні дефініції – «професійна підготовка майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій», «процес професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій»;

– *верифіковано* за бальним оцінюванням ефективності моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій;

– *подальшого розвитку набули* методологічні положення змістового наповнення та науково-методичного, інформаційно-технологічного супроводу професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій.

Практичне значення одержаних результатів полягає у тому, що :

– розроблено і апробовано «КВАРТЕТ» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах

дисциплін і практик професійної підготовки майбутніх фахівців для галузі знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелекомунікації» – соціальна та інформаційна політика, метрологія, інформаційні менеджмент та безпека, технології;

– запропоновано модернізований зміст програмних результатів навчання, загальних компетентностей, спеціальних (фахових) компетентностей задля формування пропозицій до оновлення Стандарту вищої освіти України за спеціальністю 015 «Професійна освіта (за спеціалізаціями)» для першого (бакалаврського) рівня вищої освіти;

– розроблено засоби методичного супроводу освітніх компонентів для спеціалізацій «Цифрові технології» – «Вступ до спеціальності», «Основи кібербезпеки», «Технології навчання, інформаційні технології (мережеві)» та «Електроніка, метрологія та радіотелекомунікації» – «Вступ до фаху», «Інформаційна безпека та захист інформації», «Цифрові освітні та комунікативні технології в галузі».

Результати дослідження впроваджено в освітній процес Українського державного університету імені Михайла Драгоманова (акт упровадження № 332 від 30.10.2025 р.); Бердянського державного педагогічного університету (довідка № 57-02/67 від 12.12.2025 р.); Харківський національний автомобільно-дорожній університет (довідка № 157/31 від 04.12.2025 р.).

Особистий внесок дисертанта. Результати дослідження, які представлено в дисертації, автором отримано особисто. У фаховій статті у співавторстві з науковим керівником [4] здійснено аналіз стану і структури освітніх програм до інформаційної безпеки у сфері радіотелекомунікацій, встановлено їх відповідність сучасним стандартам і потребам ринку праці, охарактеризовано застосування симуляційних середовищ, віртуальних лабораторій та моделей кіберзагроз у професійній підготовці фахівців до інформаційної безпеки у сфері радіотелекомунікації.

Апробація результатів дисертації. Основні результати дисертаційної

роботи представлено у доповідях на *міжнародних* конференціях: III Міжнародна науково-практична конференція «Проблеми та інновації професійної і технологічної освіти: реалії, досвід, перспективи» (Чернігів, 2024); VIII Міжнародна науково-практична конференція «Сучасні світові тенденції розвитку науки та інформаційних технологій» (Одеса, 2025); XVI Міжнародна науково-практична конференція «Актуальні проблеми сучасної науки та освіти» (Львів, 2025); Міжнародна науково-практична конференція «Наука в добу глобальних трансформацій: інтеграція знань, інновацій та суспільного розвитку» (Київ, 2025); VIII Міжнародна науково-методична конференція «Передові технології реалізації освітніх ініціатив» (Переяслав, 2025).

Публікації. Основні положення та результати дисертаційного дослідження відображено у 7 наукових працях, серед них 4 статті у наукових фахових виданнях України у галузі педагогіки, стаття у зарубіжному науковому періодичному виданні, 2 наукові праці, які засвідчують апробацію матеріалів дисертації.

Структура та обсяг дисертації. Дисертація складається з анотації українською й англійською мовами, вступу, трьох розділів, висновків до розділів, загальних висновків, списку використаних джерел. Загальний обсяг дисертації становить 295 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ДО РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ЕЛЕКТРОНІКИ, МЕТРОЛОГІЇ ТА РАДІОТЕЛЕКОМУНІКАЦІЙ

1.1 Аксіологічний та порівняльний аналіз тезаурусу, стану і перспектив педагогічної проблеми дослідження у академічних надбаннях

Проблема професійної підготовки висококваліфікованих майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій зумовлена стрімким зростанням кіберзагроз, розвитком бездротових технологій та підвищенням складності технічних систем зв'язку. Збільшення обсягів переданих даних, поява нових стандартів мобільних мереж та впровадження технологій Інтернету речей створюють умови для виникнення вразливостей, що потребують системного підходу до захисту інформації. Традиційні освітні програми не завжди враховують сучасні тенденції розвитку галузі, зокрема інтеграцію криптографічних рішень, застосування штучного інтелекту для виявлення атак та забезпечення стійкості радіоканалів до навмисних завад, що визначає необхідність перегляду методології навчання та підготовки професійних кадрів, здатних не лише застосовувати стандартизовані протоколи безпеки, але й розробляти інноваційні рішення для захисту критично важливих інформаційних ресурсів. Обрана проблематика дослідження тісно пов'язана з важливими науковими завданнями, серед яких створення адаптивних систем протидії кіберзагрозам, розробка нових методів аналізу захищеності мереж та побудова математичних моделей безпеки для телекомунікаційних середовищ. У прикладному вимірі ефективність професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки визначається рівнем захищеності національної інформаційної інфраструктури, що є критично важливим для стабільного функціонування державних та

комерційних систем зв'язку, а також для гарантування інформаційного суверенітету країни.

Здійснено аксіологічний аналіз тезаурусу, стану і перспектив педагогічної проблеми досліджень у академічних надбаннях учених. *Аспекти державної політики у сфері інформаційної безпеки, засоби технічного регулювання вивчали у контексті міждисциплінарного бачення:* В. Арістова та Д. Сулацький [2] – інформаційну безпеку користувачів телекомунікаційного сервісу й обслуговування; Є. Архипова[8] – соціально-філософський аналіз інформаційної безпеки; М. Грайворонський та О. Новіков[60] – безпекові засади інформаційно-комунікаційних мереж; А. Гуз[64, 65, 66, 67] – сучасне бачення проблем ЄС, державно-правові механізми провадження інформаційної політики, становлення та еволюції міжнародних стандартів інформаційної безпеки; О. Довгань[87] – щодо гарантій безпеки інформаційних середовищ у глобалізаційному вимірі; Д. Дубов[93] – щодо сучасного виміру геополітичного суперництва кіберпростору; К.Захаренко[101] – щодо інституційної архітектури інформаційної безпеки України у стратегічних орієнтирах; О. Золотар[102] – у теоретичних і практичних аспектах інформаційної безпеки людини; О. Корченко[126] – систем регулювання захисту інформації; К. Молодецька-Гринчук[161] – методології розбудови систем формування інформаційної безпеки держави (соціальні сервіси); О. Рибальський, В. Хахановський та В. Кудінов[204] – у аспектах інформаційної безпеки та технічного захисту інформації; І. Сердюк[211] – організаційних засадах публічного регулювання інформаційної суспільної безпеки ментального здоров'язбереження; В. Шемчук[244] – державного функціоналу інформаційної безпеки.

Питання правового регулювання інформаційної безпеки досліджували науковці відповідно: О. Баранов[10] – правового захисту інформаційної галузі у теоретичних, методологічних і практичних аспектах; В. Гурковський[74, 75] – організаційно-правничих засад взаємин уповноважених органів державного регулювання національної інформаційної безпеки; правового та метрологічного забезпечення інформаційних систем захисту; Б. Кормич[124, 125] –

організаційно-правничих засад інформаційної безпеки та її політичних гарантій; А. Нашинець-Наумова[167] – у питаннях правового захисту у сфері інформаційної безпеки; О. Олійник[170] – теоретико-методологічних аспектів адміністративних і правових гарантій інформаційної безпеки України; Д. Ланде, В. Фурашев і К. Юдкова[179] – базиси інформаційних і соціально-правових моделей; І. Арістова, О. Баранов, К. Бєлякова та О. Дзьобань [245] – щодо юридичної відповідальності за вчинені правопорушення в інформаційних середовищах деліктології; також у редакції І. Бєлякова[246] – юридичної відповідальності за правопорушення в інформаційній сфері.

Наукові розвідки учених у контексті інформаційної безпеки як складової національної безпеки держави здійснювали автори щодо: О. Архипов, О. Муратов[7] –критеріїв визначення потенційної шкоди національній безпеці України при витоках інформації державної таємниці; І. Доронін[89] – національної безпеки України в умовах інформатизації; А. Качинський[112] – індикаторів національної безпеки у граничних значеннях метрики; В. Ліпкан[137] – навчального забезпечення національної безпеки України; В. Ліпкан, Ю. Максименко, В. Желіховський[138] – інформаційної безпеки України у процесі євроінтеграції; В. Ліпкан, К. Череповський [139] – імплементації інформаційного законодавства України; Т. Перун[186] – адміністративно-правничі механізми формування інформаційної безпеки в державі; В. Петрик, О. Семченко[187] – забезпечення навчальних видань з інформаційної безпеки держави; Г. Пєвцов, С. Залкін [190] – проблем і методології забезпечення системи інформаційної безпеки у воєнній галузі; А. Тарасюк [225] – *кібербезпеки України в сучасних умовах державотворення*; О. Тихомиров[230] – формування функціоналу інформаційної безпеки сучасної держави; Т. Ткачук[231] – правового регулювання інформаційної безпеки у процесі євроінтеграції України; В. Торічний[234, 233] – інформаційного базису державної безпеки України в умовах соціальної турбулентності; державно-управлінських засад інформаційного базису безпеки держави під час суспільної інформатизації.

Інформаційно-технологічні аспекти формування архітектури інформаційної безпеки для впровадження й удосконалення інформаційно-комунікаційних технологій в освітньому просторі України з метою забезпечення сприятливого інформаційного середовища та відкритої освіти розглядали учені: засоби ІКТ єдиного інформаційного простору освітньо-наукових систем освіти України у колективній монографії за науковою редакцією В. Бикова, авторського колективу – В. Лапінський, А. Пилипчук, М. Шишкіна[100]; методичні системи з новітніми інформаційно-освітніми технологіями забезпечення – Ю. Биков[15]; новітні підходи та принципи розбудови інформаційних порталів – за редакцією В.Бикова, Ю.Жука, авторського колективу (В. Биков, Н. Задорожна, Т.Омельченко)[18]; автоматизовані системи сприятливого інформаційного простору освіти, науки й інноватики, організаційні системи моделей відкритої освіти, хмарні технології, ІКТ-аутсорсинг, ІКТ-функціонал освітніх і наукових інституцій, інноватика перспективного поступу і інформаційно-технологічного потенціалу систем відкритої освіти, методики підготовки фахівців – В.Биков[14, 16, 13, 12]; засоби технічного регулювання інформаційно-комунікаційних компетентностей в системі освіти України, методичні поради – В.Биков, О. Білоус, Ю. Богачков[17]; навчальне видання для педагогів ІКТ в освітньому процесі – Р. Гуревич, Ю. Кадемія[69]; електронний посібник – інноваційні засоби освіти у системі професійної підготовки – А.Гуржій, Л.Карташова[70]; е-освітні ресурси для організації освітнього процесу – А. Гуржій, В. Лапінський[71, 72]; питання стандартизації тезаурусу освітніх ІКТ – К. Кірей, Л. Кірей[115]; інформатизація освітнього простору сучасного університету, підготовка майбутніх фахівців з ІКТ до експертно-аналітичної діяльності освітнього процесу – Л. Панченко[185, 184]; методика застосування ІКТ в освітньому підготовки математиків – О. Співаковський[215]; метрика якості освітніх ІКТ, цифровізація освіти України та перспекииви досліджень оцінювання якості технологічних засобів – О. Спірін[216, 217].

Теоретико-методологічні засади професійної підготовки фахівців з інформаційних технологій та кібербезпеки досліджували науковці: І. Бардус [11] – методологія професійної освіти у галузі інформаційних технологій; В.М. Богуш, В.В. Богуш, В. Бровко, В. Настрадін [24] – навчальне видання про основи кібер-простору, кібербезпеки та кіберзахисту; освітні засоби технічного регулювання підготовки фахівців до формування кібербезпеки, аналіз стану і перспектив підготовки фахівців для сфери кіберзахисту, їх професійний розвиток та кваліфікаційні ознаки компетентності фахівців, тезаурус кіберзагроз в соціально-турбулентному світі – І. Діордіца [83, 86, 81, 82, 84, 85]; теоретико-методичний базис з технічного циклу підготовки майбутніх фахівців з ІКТ – П. Малежик[143, 144]; концептуальні засади плекання компетентностей у фахівців з ІКТ та кіберзахисту, інформаційно-аналітичний органайзер е-освітніх ресурсів забезпечення комп'ютерної графіки у майбутніх фахівців кіберзахисту, методика організації освітнього процесу підготовки ІТ-фахівців – О. Матвійчук-Юдіна [151, 149, 150]; теоретико-методичний супровід забезпечення професійної підготовки фахівців ІКТ – Я. Сікора[213]; забезпечення інформаційного захисту з обмеженим доступом користування, методологічні концепти та методичні основи формування деонтологічних компетенцій фахівців у вищій освіті, у питаннях захисту інформації – В. Артемов[3, 4, 5]; специфіка е-навчання у підготовці та професійного розвитку фахівців ІТ-галузі у ЗВО – А. Васильєв, Ю. Зубань, Ю. Коровайченко, С. Шкарлет[34]; умови забезпечення професійної готовності фахівців інформаційного захисту обмеженого доступу у професійному середовищі – С. Воскобойніков[55]; забезпечення професійно ціннісних якостей майбутніх фахівців з інформаційної безпеки в умовах опанування природничого циклу – Ю. Іванчук[104]; методичний та інформаційно-технологічний інструментарій дотримання кіберзахисту систем за програмованою логікою – О. Ілляшенко[108]; методична система розвиненості інформаційно-цифрових компетентностей у фахівців ІКТ у методичній системі вивчення фізико-технічного циклу – О. Трифонова[235]; сприяння професійній компетентності

майбутніх бакалаврів з інформаційних технологій в освітньому процесі – Л. Зубик[103]; забезпечення професійних компетентностей майбутніх операторів з обробки інформації та програмного забезпечення у професійній підготовці фахівців – М. Газдик[56]; професійна підготовка майбутніх інженерів-програмістів у педагогічних умовах технічного ЗВО – Т. Гончаренко[58]; змістове забезпечення підготовки майбутніх програмістів у політехнічних ЗВО в історичному ракурсі – Г. Лебедь[135].

Аналіз останніх досліджень і публікацій у періодичних виданнях дав змогу виокремити компетентні розвідки дослідників у питаннях щодо: рекомендацій підготовки фахівців для СБУ до кіберзахисту – В.Богуш, М.Хмельницький [23]; встановлення ролі ЗВО у забезпеченні системи інформаційної та кібербезпеки держави – Ю. Борсуковський, В. Бурячок [27]; практичних рекомендацій розбудови профілю навчання «кібернетична безпека» в Україні – В. Бурячок, В. Богуш[30]; розроблення моделі підготовки фахівців галузі інформаційної та кібербезпеки в ЗВО України – В. Бурячок, В. Богуш, Ю. Борсуковський, П. Складанний, В. Борсуковська[32]; навчальні орієнтири фахової підготовки фахівців з кібербезпеки в умовах воєнного стану – В. Горлинський[59]; методологічні аспекти професійної підготовки фахівців сфери кібербезпеки України – Ю.Даник, Ю. Супрунов[76]; практичні настанови розроблення механізмів інформаційної безпеки – Л. Дегтярьова, В. Ляшевський[77]; підготовка кадрів для забезпечення кіберзахисту в умовах цифровізації навчання – О. Дубровін, В. Коваль[94]; специфіка підготовки кадрів для сфери кібербезпеки – О. Євсюкова[95]; концептуалізація навчально-тренувального комплексу підготовки військових спеціалістів інформаційної та кібербезпеки на засадах комп'ютерної гри (гейміфікації) – Л. Козубцова, І. Козубцов, В. Ліщина, С. Штаненко[116]; цифрова обізнаність особистості для розвитку інформатизації суспільства – В. Кудлай[127]; праксеологія навчальних програм з інформаційної безпеки – О. Лаврова[132]; організація фахової підготовки фахівців із кіберзахисту – С. Мельник[153]; аналіз стану та практик підготовки фахівців сфери оборони до інформаційної боротьби – А. Міночкін [160];

підготовка майбутніх кадрів з цифровими компетентностями забезпечення інформаційної безпеки – О. Самойленко[207]; нормативно-правове регулювання фахової підготовки фахівців для галузі кібербезпеки – Ю. Сачук[208]; модель конфлікт-менеджменту взаємодії кіберпростору – В. Семко[209].

Виокремлено особливості формування професійних компетентностей на засадах компетентнісного підходу у ЗВО. Дослідження здійснено фахівцями у профілі педагогічних розвідок: Л. Васіна [35, 36, 37, 39, 38, 40] – інтеграція фахово-математичних знань у підготовці фахівців радіоелектроніки; умови проблемної інтеграції математичних та спеціальних курсів підготовки радіотехніків; специфіка математичного забезпечення професійної підготовки фахівців у неперервній освіті; дидактичні аспекти синергії спеціальної та математичної компонентів знань у професійній підготовці фахівців галузі радіоелектроніки; проблематика прикладного математичного супроводу практики фахової підготовки кадрів радіотехнічного профілю; Т. Гончаренко[57] –професійна підготовка інженерів-програмістів у технічних ЗВО; О. Жарова[96, 97, 98, 99] – сучасні моделі забезпечення інформаційних компетентностей майбутніх радіотехніків в технічних ЗВО у визначених педагогічних умовах; О. Ігнатюк [107]– теоретико-методичні засади підготовки інженерів до професійного розвитку в технічних ЗВО; А. Кокарєва[117, 118] – специфіка професійної підготовки майбутніх фахівців у інженерно-технічній системі освіти; забезпечення професійних якостей майбутніх інженерів; К. Лебедєва[134] – забезпечення професійної компетентності майбутніх інженерів радіотехніки у контексті ресурсного підходу; Г. Луценко [140]– теоретичні та методичні аспекти проєктно-орієнтованого навчання у підготовці майбутніх інженерів; Л. Марцева[146, 147, 148] – особливості фахової підготовки молодших бакалаврів радіотехніки; методичний органайзер підготовки фахівців радіотехнічного профілю в коледжах; В. Петрук[189] – сформованість професійних компетентностей у майбутніх фахівців технічного профілю інтерактивними технологічними засобами; М. Вінник[48] –

забезпечення науково-дослідницьких компетентностей у інженерів-програмістів в ЗВО; О. Гура[68] – фахова підготовка інженерів-програмістів до виконання тестових завдань систем програмування в неформальній освіті; О. Джеджула[80] – графічна підготовка здобувачів інженерного профілю в ЗВО; Ф. Лясова[141] – методики опанування технологій розроблення програмного забезпечення майбутніми інженерами; Л. Сергеєва, Т. Стойчик, К. Мартиненко [210]– організація підготовки фахівців-електротехніків профілю в закладах професійної освіти; К. Стрюк [224]– професійна компетентність молодших спеціалістів з комп'ютерної інженерії у радіотехнічних коледжах; І. Хом'юк[238] – забезпечення базового рівня для професійної мобільності інженерів; В. Татарчук[226, 227, 228, 229] – організація та дидактична специфіка забезпечення графічних компетентностей фахівців з електроніки та телекомунікацій; А. Коломієць[119120] –методологія математичної підготовки майбутніх бакалаврів для сфери електроніки та радіотелекомунікаційних технологій; С. Петрович[188] – забезпечення професійних компетентностей фахівців в галузі обчислювальної техніки; О. Сажієнко [206]– формування фахової компетентності кадрів для застосування інформаційних технологій у системі професійної освіти.

Уточнено практично-корисний зарубіжний досвід професійної підготовки фахівців-інженерів, в тому числі з кібербезпеки: пріоритети професійної підготовки фахівців для сфери безпеки та оборони – Г. Артюшин, К. Тушко[6]; професійна підготовка фахівців з кібербезпеки в університетах США – Б. Бистрова[19]; фахова підготовка інженерів в університетах Великої Британії, змістове наповнення та форми організації навчання бакалаврів інженерії в університетах Великої Британії – Н. Бідюк[21, 22]; професійна освіта магістрів сфери кіберзахисту в університетах Великої Британії – Б. Брайко[28]; фахова підготовка кадрів у галузі електроніки у ЗВО США, професійна та іншомовна освіта фахівців для галузі електроніки; перспективи впровадження досвіду практик США у фахову підготовку фахівців з електроніки в Україні – О. Павленко[180, 181, 182]; пріоритети професійної

підготовки фахівців комп'ютерних наук в ЗВО Японії – І. Пододіменко[193]; кваліфікаційні виміри до набуття спеціальностей для фахівців інформаційних технологій в США, практичний досвід США у підготовці магістрантів з ІКТ в умовах дистанційного навчання для імплементації практик в Україні – Р. Шаран[242, 241]; упровадження практично-корисного досвіду Республіки Польща щодо підготовки фахівців з інформатики в систему педагогічної освіти України – А. Кузьмінський, О. Кучай, О. Біда[129].

Методологічні, інституційні та нормативні та засади розвитку й забезпечення метрологічної діяльності в Україні, що сформували системну основу для підготовки та професійного розвитку висококваліфікованих фахівців у системній єдності метрики, вимірювань, стандартизації ґрунтовно представлені в наукових доробках щодо: історичної ретроспективи всесвітньої історії метрології та забезпечення навчання метрології у закладах освіти України; інституційне регулювання міжнародних і регіональних установ у сфері метрології – О. Величко[41, 42, 43, 44, 45]; аспекти метрології, стандартизації та нагляду у сфері якості – О.Величко, І.Дудич[46]; засади метрологічної діяльності – О.Величко, Л.Коломієць, Т. Гордієнко[47]; історичні трансформації у світовій метрології – Л. Віткін, Ю. Кузьменко[50]; моделювання систем стандартизації України для міжнародної інтеграції економіки – Л.Віткін, Д.Луценко[51]; системне аналізування засобів архітектури технічного регулювання в Україні та можливості її модернізації – Л. Віткін[49]; метрологічна надійність метрики вимірювань – Є. Володарський, І. Потоцький[52]; тезаурус сучасної метрології – Є.Володарський, Л.Кошева[53]; роль академічних шкіл у розбудові галузі приладобудування та технічної електродинаміки – Ф. Гриневич[62]; перспективи наукових напрямів дослідження інформаційних систем та їх метрологічного супроводу в електроенергетиці – Ф.Гриневич, С.Таранов[63]; практики міжнародних установ уповноважених зі стандартизації – Б. Гриньов, Ю. Даниленко, В. Любинський[90]; стандартизація як засіб реалізації інноватики діяльності – Б. Гриньов, Ю. Даниленко, О. Жихарєва, В. Любинський[222]; інформатизація

метрології – В. Ігнаткін, Н.Єфіменко, Ю. Туз[105]; забезпечення відповідності вимірювального інструментарію для застосування європейського підходу в Україні – Ю. Кузьменко, С. Черепков, В.Дуля[128]; менеджмент якості та оцінювання у галузі зв'язку – Л. Коломієць, М. Козаченко, О. Панченко[154]; кваліметрія та метрика вимірювань – В.Мотало, А.Мотало, Б.Стадник[162]; аналізування методики верифікації при калібруванні вимірювального інструментарію – В. Мотало[163].

Визначено, що значну *роль у забезпеченні нарощення когнітивного потенціалу здобувачів освіти* забезпечено авторами посібників та підручників: В. Бабак, С. Бабак, В. Єременко[9] – теоретичні основи інформаційно-вимірюваних систем; Р. Бичківський[20] – метрологія, стандартизація, управління якістю і сертифікація; Л. Боженко [25] – метрологія, стандартизація, сертифікація та акредитація (навчальний посібник); Є. Володарський, В.Кухарчук, В.Поджаренко та Г.Сердюк[54] – метрологічне забезпечення вимірювань і контролю(навчальний посібник); І. Григоренко, С.Кондрашов І. та С.Григоренко [61] – інформаційно-вимірювальні технології та системи (навчальний посібник); А. Гуржій, Л. Возненко, Н.Поворознюк та В.Самсонов [73]– основи інформаційних технологій (навчальний посібник); М. Дорожовець, В.Мотало та Б.Стадник[88] – основи метрології та вимірювальної техніки (підручник); В. Ігнаткін, О.Томашевський та В. Матюшин[106] – основи метрології (навчальний посібник); В. Кухарчук[130] – основи метрології та електричних вимірювань (конспект лекцій); В.Кухарчук, В.Кучерук, Є.Володарський та В.Грабко[131] – основи метрології та електричних вимірювань (підручник); Л.Коломієць, П.Воробієнко та М.Козаченко [155]– метрологія, стандартизація, сертифікація та управління якістю в системах зв'язку (підручник); П. Орнатський [171] – вступ до методології науки про вимірювання; Ю. Павленко та І. Захаров [183] – забезпечення єдності вимірювань (навчальний посібник); В. Поджаренко та В. Кухарчук [191] – вимірювання і комп'ютерно вимірювальна техніка (навчальний посібник); В. Поджаренко, П. Кулаков, О.Ігнатенко та О.Войтович[192] – основи

метрології та вимірювальної техніки (навчальний посібник); Є.Поліщук, М. Дорожовець та В.Яцук [194, 195] – метрологія та вимірювальна техніка (підручник); В. Сиротюк, С. Хімка та С. Сиротюк [212] – віртуальні контрольно-вимірювальні прилади і системи (навчальний посібник); І. Солтис та О.Деревянчук [214] – основи метрології (навчальний посібник); В. Топольник та М. Котляр [232] – метрологія, стандартизація, сертифікація і управління якістю (навчальний посібник); В. Цюцюра та С.Цюцюра [240] – метрологія та основи вимірювань (навчальний посібник); Н.Яворський, В.Теслюк та Є.Литвинова [248] – комп'ютерні методи в інженерії мікроелектромеханічних систем (навчальний посібник).

Здіснено аксіологічний аналіз сучасних досліджень щодо оцінки ефективності освітніх програм професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації дає змогу виокремити чотири взаємопов'язані наукові напрями. *Перший* напрям охоплює дослідження концептуальних засад формування професійних компетентностей майбутніх фахівців до реалізації інформаційної безпеки. Проаналізовано специфіку професійної підготовки фахівців для радіотелекомунікаційних систем з урахуванням структурних вимог до інформаційної безпеки та потреб галузі, що сприяє формуванню узгодженої моделі розвитку компетентностей [142], а також ученими – Н.Рідей, В.Тимошенко, Н. Титова [288] дослідили організацію підготовки фахівців у сфері комунікацій, акцентуючи на інтеграції знань із менеджменту, технічних дисциплін та цифрової безпеки як необхідного елемента сучасної освітньої програми; Р. Преглей Ґарич (R. Preglej Garić), Д.Типурич (D. Tipurić) та А. Алексич (A. Aleksić) [285] підкреслили, що майбутні зміни на ринку праці телекомунікацій вимагають адаптації освітніх стратегій до викликів цифрової трансформації та кіберзагроз; О.Гоян, В. Гоян та Т. Білецька[264] довели, що психосоціальна модель професійного розвитку журналістів може бути ефективно перенесена на підготовку фахівців із безпеки у сфері масових комунікацій із поєднанням технічного й гуманітарного компонентів.

Перспективи подальших досліджень у цьому напрямі полягають у створенні міждисциплінарних навчальних моделей, що поєднують технологічні та комунікаційні компетентності з урахуванням динаміки ринку та особливостей галузевих ризиків.

Другий напрям стосується компетентнісно орієнтованих підходів до структурування змісту освітніх програм: Д. Бендлер (D. Bendler) та М. Фелдерер (M. Felderer) [250] здійснили критичний аналіз наявних моделей компетентностей для фахівців до інформаційної безпеки й запропонували нову структуру, що інтегрує технічні, соціальні, правові й етичні аспекти кібербезпеки; Т. Кузовкова, А. Кузовков, О. Шаравова та І. Шаравов [277] обґрунтували зміну профілю необхідних компетентностей фахівців із радіоелектроніки та зв'язку під впливом цифрових технологій, що зумовлює необхідність гнучкості та системного мислення; Г. Хацівасіліс (G. Hatzivasilis), С. Іоаннідіс (S. Ioannidis), М. Смірліс (M. Smyrlis) [265] довели важливість постійної адаптації навчальних програм до рівня підготовки здобувачів і реальних потреб індустрії шляхом гнучкого коригування модулів; Т. Сенанаяке (T. Senanayake) та С. Фернандо (S.Fernando) [289] звернули увагу на важливу роль базової цифрової грамотності й розуміння ризиків кіберпростору як обов'язкових елементів компетентнісного підходу. Перспективи подальших досліджень у цьому напрямі пов'язані з гармонізацією національних освітніх стандартів із міжнародними рамками компетентностей (з англ. – NICE Framework) або (з англ. – ENISA Skills Framework), а також розробкою інструментів вимірювання результатів навчання в динамічному середовищі.

Третій напрям охоплює впровадження цифрових інструментів та освітніх технологій для забезпечення практичної підготовки здобувачів освіти: М. Мукерджі (M. Mukherjee), Н. Т. Ле (N. T. Le), Ю.-В. Чоу (Y.-W. Chow) та В. Сусіло (W. Susilo) [278] представили аналіз ефективних стратегій навчання кібербезпеки, зокрема через застосування симуляцій, інструментів аналізу ризиків та проєктних підходів до формування навичок; С. Фернандо (S. Fernando) [263] наголошує на важливості адаптації середовища навчання до

умов реального цифрового простору, де користувачі постають перед фішингом, соціальною інженерією та витоками даних; А. Кононенко та І. Смирнова [121] довели ефективність змішаного навчання у підготовці телекомунікаційних та електромеханічних фахівців, що дає змогу поєднувати традиційні курси з інтерактивними тренажерами та кейсами; В. Бурячок та В. Соколов [252] продемонстрували ефективність активного навчання в магістерських програмах через залучення здобувачів освіти до навчальних змагань, гейміфікації та CTF-заходів; А. Алямі (A. Alyami), Д. Семмон (D. Sammon), К. Невілл (K. Neville) та С. Махоні (C. Mahony) [249] здійснили емпіричне дослідження чинників успіху програм щодо освіти, професійної підготовки та підвищення обізнаності з питань безпеки (з англ. – Security Education, Training and Awareness, SETA), серед яких провідне місце займає регулярна практична активність, підтримка керівництва та залучення користувачів. Перспективи подальших досліджень охоплюють створення адаптивних цифрових платформ із функціями персоналізованого контенту, моніторингу динаміки засвоєння знань та вбудованими системами оцінювання.

Четвертий напрям стосується нормативних вимог, стандартів та системної інтеграції освітніх програм у професійне середовище: Г. Бреда (G. Breda) та М. Кісс (M. Kiss) [251]окреслили проблематику стандартизації знань у сфері кібербезпеки для індустрії 4.0, зокрема через аналіз інформаційної безпеки в спеціальних галузях та потреби відповідності міжнародним стандартам, як-от ISO/IEC 27001; П. Орлік (P. Orlik) та Р. Доналд (R. Donald) [284] розкрили питання реформування навчального контенту в телекомунікаційних програмах через упровадження елементів інформаційної безпеки та правової відповідності. Перспективи подальших досліджень у цьому напрямі пов’язані з розробленням універсальних моделей інтеграції академічної підготовки з професійною сертифікацією, а також гармонізацією освітніх стандартів із національними та галузевими вимогами.

Отже, ефективність освітніх програм у сфері інформаційної безпеки радіотелекомунікацій залежить від міждисциплінарної інтеграції, орієнтації на

компетентності, застосування цифрових технологій і відповідності нормативним вимогам. Перспективи подальших досліджень полягають у розробці гнучких адаптивних моделей навчання, що забезпечують стійкість освітнього середовища до технологічних змін та кіберзагроз. Попри значні досягнення щодо організації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки, залишаються нерозв'язаними питання, пов'язані з адаптацією освітніх програм до швидких технологічних змін та вимог кон'юнктури ринку праці. Недостатньо досліджено ефективність практичних інструментів, таких як симуляційні середовища, хмарні лабораторії та засоби моделювання кіберзагроз, що призводить до розриву між теоретичними знаннями та реальними потребами індустрії. Наявні програми нерідко частково ігнорують сучасні стандарти та практики безпеки в контексті 5G-мереж, IoT та автоматизованих систем моніторингу, що обмежує підготовку здобувачів освіти до роботи з комплексними телекомунікаційними інфраструктурами.

Оцінено практичні підходи, зокрема симуляційні платформи та кіберполігони, що дасть змогу розробити концепцію удосконалення підготовки фахівців. Такий підхід поглиблює розуміння основних проблем та окреслює напрями впровадження інноваційних технологій і міжнародних стандартів для підвищення ефективності навчальних курсів. Локальною метою дослідження є оцінювання ефективності сучасних освітніх програм для професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій та визначення шляхів їхнього вдосконалення з урахуванням новітніх технологічних викликів і тенденцій розвитку галузі. Для досягнення цієї мети поставлено локальні завдання дослідження: 1. проаналізувати стан і структуру освітніх програм у сфері електроніки, метрології та радіотелекомунікацій та їх відповідність сучасним стандартам і потребам ринку праці; 2. дослідити методи практичної підготовки та основні компетентності майбутніх фахівців, зокрема застосування симуляційних середовищ, віртуальних лабораторій та моделей кіберзагроз;

3. виокремити обмеження чинних програм, а також розробити науково обґрунтовані рекомендації щодо їхньої модернізації та інтеграції інноваційних технологій.

Здійснено порівняльний аналіз сучасного стану та перспектив удосконалення освітніх програм професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки характеризується тенденцією до інтеграції класичних дисциплін із новітніми цифровими технологіями та підвищеною увагою до практичних аспектів захисту інформації. Розвиток бездротових мереж п'ятого покоління, інтернету речей та критичної інфраструктури зумовлює потребу у фахівцях, здатних працювати з багаторівневими системами безпеки, які охоплюють як технічні, так і організаційні методи протидії кіберзагрозам. Вимоги ринку праці визначають необхідність поєднання фундаментальних знань із криптографії та радіотехніки з практичними навичками застосування сучасних інструментів моніторингу, аналізу трафіку, управління вразливостями та реагування на інциденти. Українські університети активно адаптують свої освітні програми до міжнародних стандартів, таких як ISO/IEC 27001 [271], NIST Cybersecurity Framework [283] та вимог Європейської рамки кваліфікацій EQF [247], проте рівень інтеграції практикоорієнтованих компонентів залишається різним залежно від профілю закладу та наявних ресурсів (табл. 1.1).

Таблиця 1.1

Порівняльна характеристика освітніх програм у сфері електроніка, метрологія та радіотелекомунікацій

Університет	Назва програми	Освітній рівень	Спеціальність та профілізація	Основні акценти програми
Національний університет «Львівська політехніка» [172]	Безпека інформаційних і комунікаційних систем	Магістр	172 «Електронні комунікації та радіотехніка»	Криптографія, аналіз безпеки мереж, захист радіоканалів
Ужгородський національний університет [173]	Безпека інформаційних і комунікаційних систем	Бакалавр	125 «Кібербезпека та захист інформації»	Основи кіберзахисту, практичні курси з управління

Університет	Назва програми	Освітній рівень	Спеціальність та профілізація	Основні акценти програми
				ризиками
Харківський національний університет радіоелектроніки [174]	Безпека інформаційних і комунікаційних систем	Бакалавр	F5 «Кібербезпека та захист інформації»	Мережеві протоколи, захист інформаційних систем, моделювання атак
Київський національний університет імені Тараса Шевченка [175]	Інформаційна безпека телекомунікаційних систем	Бакалавр	172 «Електронні комунікації та радіотехніка»	Захист телекомунікаційних мереж, моніторинг трафіку, реагування на інциденти
Київський політехнічний інститут імені Ігоря Сікорського [178]	Кібербезпека та захист інформації	Бакалавр	125 «Кібербезпека»	Системи управління безпекою, ISO/NIST, реагування на кіберзагрози
Український державний університет імені Михайла Драгоманова [177]	Професійна освіта (Цифрові технології)	Бакалавр	015.39 «Професійна освіта. Цифрові технології»	Підготовка педагогів професійного навчання з IT-компетенціями у цифровій освіті
Тернопільський національний педагогічний університет імені Володимира Гнатюка [176]	Професійна освіта (Комп'ютерні технології)	Магістр	015 «Професійна освіта (Комп'ютерні технології)»	Освіта фахівців у сфері комп'ютерних технологій для професійного навчання та IT-індустрії

Джерело: сформовано на основі [172– 176].

Освітні програми, наведені в табл. 1.1, мають спільну мету: формування комплексних компетентностей у сфері захисту інформаційних та телекомунікаційних систем, проте кожна з них демонструє власні підходи та акценти. Зміст освітньої програми Національного університету «Львівська політехніка» вирізняється глибокою технічною підготовкою з акцентом на радіотехнічні аспекти безпеки, зокрема криптографічні алгоритми для захисту радіоканалів та стійкість бездротових мереж до навмисних завад, що забезпечує високий рівень фундаментальної підготовки та готовність випускників до роботи з інноваційними телекомунікаційними системами [172]. В Ужгородському національному університеті закцентовано на загальних основах

кіберзахисту та управлінні ризиками, що робить освітню програму більш орієнтованою на початковий рівень підготовки з можливістю подальшої спеціалізації у сфері телекомунікацій [173]. Зміст освітньої програми Харківського національного університету радіоелектроніки характеризується інтенсивним практичним складником, зокрема притаманний значний обсяг лабораторних робіт, моделювання реальних атак та аналіз вразливостей, що сприяє формуванню у здобувачів освіти практичний досвід, максимально наближений до професійної діяльності у сфері інформаційної безпеки [174]. У Київському національному університеті імені Тараса Шевченка особливу увагу приділяють питанням моніторингу трафіку та управління інцидентами в телекомунікаційних мережах, що відповідає сучасним вимогам операторів зв'язку та компаній, які працюють із великими потоками даних [175]. В межах освітньої програми Київського політехнічного інституту імені Ігоря Сікорського зінтегровано міжнародні стандарти ISO та NIST з акцентом на формуванні систем управління безпекою та комплексному аналізі ризиків, що дає випускникам можливість працювати не лише в технічному сегменті, але й у сфері аудиту та консалтингу з питань кіберзахисту [178]. Окрему нішу в системі професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки займають освітні програми за спеціальністю 015 «Професійна освіта». Так, в Українському державному університеті імені Михайла Драгоманова реалізується програма «Професійна освіта (Цифрові технології)», яка орієнтована на розвиток ІТ-компетентностей у майбутніх педагогів професійного навчання із поглибленим акцентом на цифрову трансформацію професійної освіти [177]. Натомість у Тернопільському національному педагогічному університеті імені Володимира Гнатюка функціонує магістерська програма «Професійна освіта (Комп'ютерні технології)», що передбачає професійну підготовку фахівців з інтегрованими знаннями у сфері ІКТ, педагогіки й прикладного програмування [176]. Обидві освітні програми формують міждисциплінарну основу для професійної підготовки майбутніх фахівців до впровадження інформаційної безпеки в умовах цифровізації

освітнього і промислового середовища. На практиці всі ці освітні програми функціонують у динамічному середовищі, що потребує регулярного оновлення навчальних планів для відповідності світовим трендам. Наприклад, освітня програма Національного університету «Львівська політехніка» вже впроваджує курси з безпеки мобільних мереж 5G, тоді як Київський політехнічний інститут імені Ігоря Сікорського зосереджується на інтеграції інструментів штучного інтелекту для аналізу інцидентів. Порівняно з Ужгородським національним університетом, який зберігає класичну модель професійної підготовки майбутніх фахівців, Харківський національний університет радіоелектроніки та Київський політехнічний інститут імені Ігоря Сікорського демонструють більшу гнучкість у застосуванні симуляційних платформ і лабораторних стендів, що дає змогу здобувачам освіти набувати практичних навичок, адаптованих до реальних робочих сценаріїв.

Таким чином, хоча всі освітні програми відповідають базовим національним стандартам професійної підготовки майбутніх фахівців, їх практикоорієнтованість, рівень інтеграції новітніх технологій та взаємозв'язок із потребами індустрії різняться, що створює можливості для вдосконалення та гармонізації освітнього контенту на рівні міжуніверситетських ініціатив та партнерств із бізнесом. Практична підготовка здобувачів освіти у сфері електроніки, метрології та радіотелекомунікацій ґрунтується на інтеграції симуляційних середовищ, лабораторних комплексів та систем аналізу загроз, що дає змогу відтворювати реалістичні сценарії кіберінцидентів. Поєднання сучасних наукових теоретичних знань із практичними завданнями сприяє формуванню компетенцій для роботи з високонавантаженими телекомунікаційними системами та захисту критичних каналів зв'язку (табл. 1.2).

Таблиця 1.2

Групи методів практичної підготовки здобувачів освіти з кібербезпеки

Група методів	Зміст та підходи	Очікуваний результат
Симуляційні	Відтворення багаторівневих атак і	Навички оперативного

середовища та кіберполігони	стратегій захисту у віртуалізованому середовищі	реагування та роботи з реалістичними інцидентами
Віртуальні та хмарні лабораторії	Використання хмарних і контейнерних технологій (Docker, OpenStack) для створення навчальних середовищ	Практичний досвід налаштування безпечних мереж і систем
Тестування на проникнення (з англ. – Penetration testing)	Моделювання реальних атак за допомогою інструментів (Kali Linux, Metasploit)	Уміння виявляти та ліквідовувати вразливості
Аналіз мережевого трафіку	Робота з аналізаторами (Wireshark, Zeek), системами IDS/IPS та SIEM	Розвиток навичок моніторингу мережевої активності та виявлення загроз
Командні тренінги (з англ. – Red team vs. blue team)	Практичні вправи з розподілом ролей між командами атакувальних та захисних фахівців	Розвиток командної взаємодії та стратегічного мислення
Кіберзмагання та Capture the Flag (CTF)	Виконання практичних завдань на виявлення вразливостей та захист систем	Формування конкурентних навичок і швидкого аналізу ситуацій

У практичній підготовці майбутніх фахівців вказано методи, які функціонують як взаємодоповнювальна система. Симуляційні середовища, зокрема платформи на зразок CyberRange, дають змогу моделювати складні атаки на телекомунікаційні системи, зокрема DDoS-атаки та загрози для бездротових каналів; функціонують як ізольовані системи для безпечного відпрацювання стратегії протидії загрозам у режимі реального часу. Наприклад, в Харківському національному університеті радіоелектроніки застосовано платформу CyberRange для навчання здобувачів освіти методам тестування на проникнення (з англ. – Penetration testing) та оцінювання рівня безпеки телекомунікаційних мереж [174]. Віртуальні та хмарні лабораторії забезпечують можливість швидкого розгортання освітніх середовищ із використанням таких платформ, як OpenStack, VMware або Docker, що дає змогу імітувати конфігурацію мережевих систем, тестувати захист каналів зв'язку та експериментувати з IDS/IPS. Наприклад, в Ужгородському національному університеті використовують хмарні лабораторії на базі OpenStack, які дають змогу здобувачам освіти налаштовувати захист бездротових мереж відповідно до сучасних стандартів WPA3 [173]. Подібні

віртуалізовані навчальні середовища впроваджуються і в Українському державному університеті імені Михайла Драгоманова, де в межах програми «Професійна освіта (Цифрові технології)» здобувачі освіти оволодівають технологіями контейнеризації та побудови безпечного освітнього цифрового простору [177]. Методи «penetration testing» на практиці реалізуються через популярні інструменти, такі як Kali Linux та Metasploit, що дають змогу моделювати атаки на різних рівнях мережевої інфраструктури. Ці інструменти активно інтегруються в курсах Національного університету «Львівська політехніка», де для глибинного аналізу мережевого трафіку також використовується Wireshark [172]. Командні тренінги та кіберзмагання (з англ. – Capture the Flag) формують навички роботи в умовах тиску та потреби швидкого прийняття рішень; ґрунтуються на принципі розподілу ролей, що дає змогу здобувачам освіти відчути особливості як атакувальних, так і захисних сценаріїв. У Київському національному університеті імені Тараса Шевченка організовує такі заходи у форматі «red team vs. blue team», що доповнюється аналітичними практикумами із застосуванням ELK-stack для збору та аналізу журналів безпеки [175]. Подібні тренінги у формі імітаційних кейсів поступово інтегруються й до педагогічних програм, наприклад у Тернопільському національному педагогічному університеті імені Володимира Гнатюка, де у межах спеціальності «Професійна освіта (Комп'ютерні технології)» застосовуються проєктно-орієнтовані завдання для формування цифрової грамотності, базових навичок кіберзахисту та моделювання ризиків у віртуальному середовищі [176]. В Київському політехнічному інституті імені Ігоря Сікорського реалізовано національний кіберполігон, інтегрований із міжнародними стандартами NIST та ISO/IEC 27001, що дає змогу поєднувати моніторинг безпекових подій за допомогою SIEM-систем із практичними сценаріями захисту критичних інфраструктур [178]. Усі ці методи та інструменти працюють комплексно, створюючи динамічне освітнє середовище, що відповідає реаліям сучасної кібербезпеки. При цьому включення освітніх програм за спеціальністю 015 «Професійна освіта» у ЗВО сприяє підготовці

мультидисциплінарних фахівців, здатних не лише впроваджувати безпекові рішення, а й навчати їм інших у контексті цифрової трансформації. Ключові компетентності для фахівців у сфері захисту інформації в телекомунікаційних системах формуються на основі поєднання базових знань, професійних умінь і здатності адаптуватися до технологічних змін та нових загроз. Сучасні освітні програми структурують ці компетентності на загальні, спеціальні та професійно-практичні групи, що дає змогу цілісно охопити як технічні аспекти, так і організаційні та управлінські навички. Такий підхід гарантує підготовку фахівців, здатних не лише виконувати рутинні завдання захисту даних, але й проєктувати комплексні системи кіберзахисту та брати участь у формуванні політик безпеки (табл. 1.3).

Таблиця 1.3

Групування ключових компетентностей майбутніх фахівців до реалізації інформаційної безпеки

Групування компетентностей	Основні характеристики	Очікуваний результат
Загальні	Критичне та системне мислення, комунікативні навички, здатність до самоосвіти та прийняття рішень	Формування гнучкості мислення, уміння взаємодіяти в команді та адаптуватися до змін
Спеціальні	Розуміння архітектури телекомунікаційних систем, принципів криптографії, управління ризиками та аудит безпеки	Здатність розробляти стратегії захисту та прогнозувати загрози
Професійні	Практичні навички з «penetration testing», налаштування Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS), реагування на кіберінциденти, управління системами моніторингу	Уміння виявляти та усувати вразливості, забезпечувати безперервність захисту
Організаційні	Планування заходів безпеки, знання міжнародних стандартів ISO/IEC 27001 [16], NIST CSF [17], документування політик	Здатність інтегрувати безпекові процеси в корпоративні стратегії
Аналітичні	Аналіз мережевого трафіку, виявлення аномалій, оцінка ризиків, робота з великими даними	Уміння приймати ефективні рішення на основі аналітичних даних
Інноваційні	Застосування штучного інтелекту, автоматизованих систем виявлення загроз, технологій кіберрозвідки	Здатність упроваджувати новітні рішення у сфері кіберзахисту

Підхід до формування компетентностей майбутніх фахівців у сфері захисту інформації в телекомунікаційних системах ґрунтується на поєднанні фундаментальних знань, практичних навичок і стратегічного мислення. В освітніх програмах акцент робиться на формуванні загальних компетентностей, таких як критичне мислення, комунікативні здібності та здатність швидко адаптуватися до нових технологічних викликів, необхідних для ефективної взаємодії в мультидисциплінарних командах. Формування спеціальних компетентностей зорієнтовано на глибоке розуміння архітектури телекомунікаційних систем, принципів криптографії, управління ризиками та побудови комплексних стратегій кіберзахисту. Професійні навички передбачають практичне застосування інструментів для аналізу трафіку, тестування на проникнення, роботу з системами виявлення та реагування на загрози. Аналітичний складник підготовки підсилюється розвитком навичок оцінки кіберризиків, сценарним моделюванням кібератак, що відповідає сучасним вимогам ринку праці у сфері кібербезпеки. Львівська політехніка зосереджується на розвитку спеціальних компетентностей, пов'язаних із безпекою радіоканалів, побудовою систем моніторингу та аудитом інформаційної інфраструктури, що сприяє формуванню здатності у майбутніх фахівців проєктувати політики безпеки та впроваджувати методики контролю загроз у телекомунікаційних системах [172]. Ужгородський національний університет орієнтується на розвиток організаційних та аналітичних компетентностей, особливу увагу приділяючи управлінню ризиками та методам тестування безпеки. Здобувачі освіти вивчають сучасні методики оцінки вразливостей та аудиту систем, що дає їм можливість працювати на перетині технічного та управлінського рівнів кіберзахисту [173]. Харківський національний університет радіоелектроніки акцентує на технічних та професійних компетентностях, зокрема на вмінні створювати захищені мережеві архітектури, конфігурувати системи виявлення вторгнень, здійснювати «penetration testing» та ефективно реагувати на кіберінциденти. Це робить випускників конкурентоспроможними на ринку праці, де цінується

практичний досвід роботи з реалістичними сценаріями атак [174]. В межах освітньої програми Київського національного університету імені Тараса Шевченка здіснюється формування стратегічних компетентностей, зокрема здатність здобувачів освіти щодо – моніторингу телекомунікаційних мереж, прогнозування атак і застосування стандартів безпеки у великих корпоративних середовищах. Приділено увагу роботі з великими масивами даних та аналітичними інструментами, що забезпечує оперативну оцінку загроз і проєктування стратегій захисту [175]. У Київському політехнічному інституті імені Ігоря Сікорського здійснено інтеграцію інноваційних компетентностей, пов'язаних із застосуванням штучного інтелекту (далі – ШІ), автоматизованих систем кібермоніторингу та впровадженням міжнародних стандартів ISO/IEC 27001 [271] та NIST CSF [283], що відповідає сучасним глобальним тенденціям кіберзахисту [178].

Водночас в Українському державному університеті імені Михайла Драгоманова у межах освітньої програми «Професійна освіта (Цифрові технології)» формує міждисциплінарні компетентності на стику педагогіки, цифрових технологій та базового кіберзахисту. Особливу увагу приділено розвитку цифрової грамотності, вмінню моделювати освітнє середовище з підвищеним рівнем інформаційної безпеки, а також використанню віртуалізованих інструментів для контролю ризиків у цифровій освітній інфраструктурі [177]. У Тернопільському національному педагогічному університеті імені Володимира Гнатюка у програмі «Професійна освіта (Комп'ютерні технології)» зорієнтовано на розвиток педагогічно-цифрових і технічних компетентностей, що включають розуміння принципів мережевої безпеки, використання хмарних сервісів, основ криптографії та навичок адаптації навчального контенту до безпечного цифрового простору, що сприяє підготовці майбутніх фахівців, здатних навчати цифровій безпеці інших та проєктувати освітні середовища з урахуванням вимог кібергігієни [176]. Таким чином, у різних освітніх програмах простежується різна спеціалізація: одні заклади акцентують на глибокій технічній підготовці та практичних навичках,

інші – на аналітичних та управлінських аспектах безпеки. Разом це формує комплексну модель компетентностей, необхідних для роботи у сфері телекомунікаційної безпеки, де важливо не лише забезпечити технічну стійкість систем, але й організувати процеси управління ризиками, відповідати міжнародним стандартам та впроваджувати інноваційні технології кіберзахисту. Наявні освітні програми з підготовки фахівців у сфері інформаційної безпеки в телекомунікаційних системах мають низку проблем та обмежень, що знижують їхню ефективність і практичну цінність у сучасних умовах.

Одним з основних недоліків є недостатня інтеграція новітніх технологій, таких як ШІ для аналізу кіберзагроз, блокчейн для захисту даних або автоматизовані системи виявлення атак [250, с. 11; 278, с. 10]. Освітні програми підготовки майбутніх фахівців до реалізації інформаційно безпеки в ЗВО України часто орієнтуються на класичні підходи до захисту інформації, залишаючи поза увагою швидкі темпи розвитку хмарних сервісів, віртуалізації та IoT, що формують нові вектори атак. Це призводить до того, що здобувачі освіти отримують знання, які не завжди відповідають актуальним викликам галузі. Істотною проблемою залишається обмежений доступ до сучасних практичних лабораторій та кіберполігонів, де можна відпрацьовувати навички в умовах, максимально наближених до реальних кіберінцидентів [252, с. 598–600;]. Встановлено, що ЗВО критично не мають належного фінансування для створення освітніх середовищ, які б імітували інфраструктури високого навантаження, 5G-мережі чи захист критичних систем, через що здобувачі освіти отримують переважно теоретичні знання [142, с. 4]. Крім того, низький рівень партнерства з бізнесом і міжнародними компаніями обмежує доступ до актуальних кейсів та реальних прикладів загроз. Застарілий зміст освітніх стандартів та регламентовані навчальні плани не дають змогу оперативно оновлювати зміст курсів відповідно до швидкоплинних змін у сфері кіберзахисту [288, с. 112; 121, с. 55]. Часто недостатньо курсів, присвячених

новітнім стандартам безпеки, управлінню ризиками в мультихмарних середовищах чи аналізу складних багатовекторних атак [251, с. 583; 278, с. 9].

Недостатньо уваги також приділяється розвитку міждисциплінарних компетентностей, таких як юридичні аспекти кібербезпеки, управління інцидентами або бізнес-аналітика в контексті безпеки. Серед проблем варто виокремити також недостатню кількість викладачів-практиків із реальним досвідом роботи в індустрії та проведення сертифікованих тренінгів. Зважаючи на це навчання часто відстає від сучасних вимог і не забезпечує достатнього рівня практичної підготовки [249, с. 60]. Такі обмеження знижують адаптивність програм до реальних викликів, ускладнюючи працевлаштування випускників і їхню готовність ефективно протидіяти актуальним кіберзагрозам. Модернізація навчальних курсів у сфері інформаційної безпеки радіотелекомунікацій має ґрунтуватися на глибокій інтеграції інноваційних технологій та сучасних підходів до практичної підготовки здобувачів освіти. Насамперед доцільно актуалізувати навчальний контент відповідно до глобальних тенденцій кібербезпеки. Це означає, що варто зосередитись, зокрема, на захисті 5G-мереж, IoT-систем та хмарної інфраструктури. Встановлено, що освітні програми мають містити такі елементи, як застосування автоматизованих систем аналізу трафіку, інструментів штучного інтелекту для прогнозування атак та платформ для виявлення Zero-Day вразливостей, що сприятиме формуванню в здобувачів освіти навичок реагування на сучасні загрози, що не завжди охоплюються класичними підходами до кіберзахисту. Важливим кроком є впровадження модульної структури курсів із регулярним оновленням змісту та можливістю швидкого додавання нових тем, що відповідають актуальним викликам індустрії. Також варто збільшити частку практичних занять шляхом створення кіберполігонів, хмарних лабораторій та контейнерних середовищ, де здобувачі освіти можуть моделювати реальні кіберінциденти, здійснювати тестування на проникнення та аналізувати вразливості систем/аккаунтів. Інтеграція міжнародних стандартів безпеки, таких як ISO/IEC 27001, NIST CSF, а також

сертифікаційних практик (CEH, CompTIA Security+, CISSP) сприятиме підготовці випускників до роботи в міжнародних компаніях та підвищить їхню конкурентоспроможність. Необхідно активізувати співпрацю з представниками індустрії, міжнародними кіберцентрами та виробниками програмного забезпечення з метою гарантування інформаційної безпеки, залучаючи їх до розробки практичних кейсів і стажувань на першому робочому місці здобувачів освіти, що сприятиме розвитку у них практико-орієнтованих компетентностей, що відповідають реальним умовам роботи. Важливо розвивати міждисциплінарні напрями, додаючи до курсів аспекти кіберправа, управління бізнес-ризиками та цифрової криміналістики, що є критичним для комплексного підходу до безпеки телекомунікаційних систем. Модернізація освітніх програм також має передбачати застосування технологій штучного інтелекту для персоналізації освітніх траєкторій здобувачів освіти, адаптивного оцінювання та автоматизованого аналізу прогресу. Інтеграція гейміфікаційних платформ, симуляційних сценаріїв та CTF-змагань створить динамічне середовище, де вони зможуть відпрацьовувати навички реагування на складні кіберзагрози в умовах командної взаємодії. Таким чином, модернізовані освітні програми забезпечать баланс між теоретичними знаннями та практичним досвідом, що є важливим чинником підготовки сучасних фахівців до інформаційної безпеки у сфері радіотелекомунікацій.

Отже, дослідження дало змогу встановити, що сучасні освітні програми з підготовки фахівців до інформаційної безпеки у сфері радіотелекомунікацій поступово інтегрують міжнародні стандарти безпеки та орієнтуються на розвиток практичних навичок у сфері кіберзахисту. Водночас з'ясовано, що рівень практичної підготовки та застосування інноваційних технологій істотно різниться між університетами. Основними проблемами залишаються недостатня інтеграція сучасних технологій штучного інтелекту та блокчейн, обмежений доступ до кіберполігонів та віртуальних лабораторій, а також повільна адаптація навчальних планів до швидкоплинних змін у сфері інформаційної безпеки. Рекомендовано модернізувати освітні курси шляхом

упровадження модульної структури, розширення практичного складника та впровадження сучасних інструментів «penetration testing», хмарних лабораторій та систем аналітики на основі ШІ. Важливим є поглиблення співпраці з бізнесом та міжнародними організаціями для створення актуальних кейсів і стажувань. Перспективи подальших досліджень пов'язані з формуванням універсальної моделі компетентностей для фахівців із кібербезпеки в телекомунікаційних системах, а також вивченням можливостей адаптивних платформ і гейміфікованих підходів для підвищення ефективності освітнього процесу.

1.2. Контент-аналіз міжнародного нормативно-правового забезпечення підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій

У сучасних умовах глобалізації та стрімкого розвитку цифрових технологій питання інформаційної безпеки постає як одне з ключових для стабільності держави й суспільства. Від її ефективного функціонування залежить не лише захищеність стратегічних секторів економіки, але й надійність систем державного управління та критичної інфраструктури. Кіберфізичні системи, що вже давно вийшли за межі простих інструментів автоматизації чи комунікації, дедалі більше перетворюються на фундаментальні елементи нової соціально-економічної реальності.

У цій реальності тісно переплітаються технологічний прогрес, економічна безпека та суспільні трансформації. Такий контекст вимагає не лише технічних рішень, а й комплексного підходу до аналізу ризиків та розроблення стратегій захисту інформаційного простору. Згідно результатів наукових досліджень, навіть поодинокі інциденти (порушення цілісності чи доступності даних, витік конфіденційної інформації або цілеспрямовані кібератаки) можуть мати масштабні наслідки. Виникає ризик призупинення виробничих процесів, втрати стратегічних даних і навіть загрозу національній безпеці, що у підсумку може

призвести до дестабілізації суспільної діяльності у цілому [33, 1.a.i.166, 1.a.i.203]. Відповідно стратегічного значення набуває організація процесів у високотехнологічних галузях, зокрема в електроніці, метрології та радіотелекомунікацій, які інтегруються в єдиний інформаційно-телекомунікаційний простір і відповідно стають вразливими до кіберзагроз [1.a.i.136]. У даному контексті інформаційна безпека є ключовою передумовою формування довіри до цифрової архітектури, що забезпечує ефективність функціонування в умовах економіки цифровізації і сприяє захисту прав і свобод громадян, а також спонукає до подальшого розвитку інновацій у пріоритетних високотехнологічних секторах [1.a.i.110].

В умовах цифрової трансформації національного господарства гарантування інформаційної безпеки вимагає не лише технологічних рішень, але й системної підготовки висококваліфікованих фахівців, здатних реалізовувати комплексний підхід у проєктуванні, впровадженні, захисті та експлуатації інформаційних систем. Також зауважено, що формування професійних компетентностей до реалізації інформаційної безпеки потребує чітко структурованої та імплементованої нормативно-правової бази до міжнародних, що б забезпечило гармонійне поєднання міжнародних стандартів, національного законодавства та стратегій освітніх політик [1.a.i.218]. Наразі перед українською системою вищої освіти постає завдання не лише адаптації до глобальних вимог у сфері інформаційної безпеки, але й активного впровадження інституційних механізмів для забезпечення резервів кадрового потенціалу в галузі знань 01 Освіта/Педагогіка (нині – А Освіта). Відтак, актуальність дослідження нормативно-правового забезпечення підготовки майбутніх фахівців визначається не лише безпековими викликами, а й необхідністю методологічного обґрунтування освітніх підходів у компетентнісно-орієнтованій трансформації освітніх стандартів.

Увагу зосереджено на всебічному аналізі джерел нормативного та технічного регулювання, що визначають вимоги до підготовки фахівців, здатних ефективно діяти в умовах підвищеного ризику несанкціонованого

втручання в інформаційні бази (інституційного і персонального характеру), цілеспрямованого спотворення інформації чи її знищення. Увагу приділено стандартам вищої освіти з історичним акцентом галузі знань 01 Освіта/Педагогіка (нині – А Освіта), спеціальністю 015 Професійна освіта (за спеціалізаціями) (нині – А15 Професійна освіта) [1.a.i.219] та галузі знань 12 Інформаційні технології (нині – F Інформаційні технології) спеціальності 125 Кібербезпека (нині – F 5 Кібербезпека та захист інформації) [1.a.i.218], а також компаративному дослідженню міжнародних стандартів серії ISO/IEC 27000 [1.a.i.270], рекомендацій Міжнародного союзу електрозв'язку (з англ. – International Telecommunication Union (далі – ITU)), положень європейських директив загального регламенту про захист даних (з англ. – General Data Protection Regulation (далі – GDPR)) та Директиви безпеки мережевих та інформаційних систем (з англ. – Directive on Security of Network and Information Systems (далі – NIS)), документів Організації Північноатлантичного договору (з англ. – North Atlantic Treaty Organization, далі – НАТО), Організації Об'єднаних Націй (далі –ООН), Європейського Союзу (далі – ЄС) та Організації з безпеки і співробітництва в Європі (з англ. – Organization for Security and Co-operation in Europe, далі –ОБСЄ), що нині забезпечують нормативні вимоги до компетентностей фахівців для формування інформаційної безпеки [1.a.i.261]. Проблема дослідження охоплює процес імплементації міжнародних вимог у національне правове поле та вивчає їх вплив на розроблення освітніх стандартів і програм, що реалізуються вітчизняних закладах вищої освіти. Національний контекст досліджується крізь призму аналізу конституційних положень, профільних Законів України (далі – ЗУ), підзаконних актів та державних стандартів, що забезпечують нормування професійної підготовки фахівців для сфери інформаційної безпеки. Особливе місце в дослідженні має розгляд питань нормативного забезпечення освітньої діяльності, а саме ліцензування, акредитація та регламентація практичної підготовки фахівців, в тому числі формування сприятливих умов для їх неперервного професійного розвитку у галузі.

Теоретичний аналіз правової бази, що унормовує професійну підготовку фахівців для сфери інформаційної безпеки у галузях електроніки, метрології та радіотелекомунікацій, передбачає проєктування її структури, логіки, модернізації змісту та забезпечення ефективності. Аналіз має не лише теоретичне значення для розуміння системних теоретичних і методичних засад професійної підготовки, але й вагоме практичне застосування, зокрема, у забезпеченні дієвих механізмів кадрового та інституційного розвитку у сфері формування інформаційної безпеки, в цілому, та кібербезпеки, зокрема.

У соціально-турбулентних умовах цифрової трансформації та глобальної технологічної конкуренції, забезпечення якості підготовки майбутніх фахівців є запорукою збереження технологічних пріоритетів держави. Отже, удосконалення нормативного регулювання розглядали як стратегічний напрям державної освітньої політики у галузі національної безпеки.

У зв'язку з стрімкою цифровізацією суспільної діяльності та зростання рівня кіберзагроз, що охоплюють як приватні, так і державні інформаційні системи, особливої ваги набуває формування ефективних систем управління інформаційною безпекою. В ускладнених умовах небезпеки кіберсередовища та розгалуження варіації загроз у міжнародному масштабі саме формалізований підхід до стандартизації та забезпечення цілісності, конфіденційності та доступності інформаційних активів сприяє створенню стійких адаптивних моделей безпеки. Серію міжнародних стандартів ISO/IEC 27000 розроблено Міжнародною організацією зі стандартизації (з анг. – International Organization for Standardization (далі – ISO)) спільно з Міжнародною електротехнічною комісією (з анг. – International Electrotechnical Commission (далі – IEC)), відіграє ключову роль у формуванні концептуального та базису забезпечення систем управління інформаційною безпекою (далі – СУІБ) [1.a.i.270]. З метою деталізації розуміння змісту стандартів серії ISO/IEC 27000 та їх функціонального значення в аспектах організації СУІБ розглянуто компаративні характеристики основних нормативних документів (таблиця1.4).

Зауважено, що серія ISO/IEC 27000 включає низку взаємопов'язаних стандартів, що визначають фундаментальні принципи, терміни, процедури та механізми управління інформаційною безпекою.

Таблиця 1.4

Компаративні характеристики стандартів серії ISO/IEC 27000

Стандарти	Основне призначення	Зміст/Компоненти	Значення для СУІБ
ISO/IEC 27001	Визначення вимог до створення, впровадження та вдосконалення СУІБ	Політики та процедури, ризик-орієнтоване управління, сертифікація відповідності	Системний підхід до безпеки, забезпечення підвищення довіри, мінімізація ризиків, відповідність вимогам
ISO/IEC 27002	Рекомендації щодо імплементації нагляду та контролю інформаційної безпеки	14 доменів контролю, практичні заходи, адаптація до ризиків та потреб	Підвищення ефективності, запобігання інцидентам, гнучкість при впровадженні заходів безпеки
Інші стандарти серії	Масштабування напрямів управління інформаційною безпекою	ISO/IEC 27003: впровадження СУІБ; ISO/IEC 27004: оцінка ефективності; ISO/IEC 27005: управління ризиками	Удосконалення компетентностей, вдосконалення безперервності бізнесу, формування професійних навичок

Центральну позицію займає стандарт ISO/IEC 27001, що визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення справочинства СУІБ [1.a.i.272] та унормовує здійснення сертифікації організацій, що прагнуть підтвердити відповідність інституційних безпекових процесів згідно міжнародно визнаних критеріїв. Унікальність стандарту полягає у забезпеченні цілісного, системно-орієнтованого підходу до управління ризиками, пов'язаними з інформаційними ресурсами, і формалізації заходів захисту інформаційних даних у відповідності до їх критичності, значущості та вразливості. Застосування ISO/IEC 27001 є не лише запорукою функціональної стійкості організацій до зовнішніх загроз, але й вагомим елементом довірливого ставлення інтересантів, зокрема клієнтів, партнерів, державних уповноважених органів і міжнародної спільноти. Зазначено, що надзвичайно важливим для дотримання нормативно-правового забезпечення

професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у галузях електроніки, метрології та радіотелекомунікацій, необхідно забезпечити модернізацію сучасних наукових знань та підходів (оскільки стандарти серії ISO/IEC 27000, зокрема ISO/IEC 27001, створюють єдиний понятійний і методологічний абрис, що дозволяє формувати у здобувачів освіти чітке уявлення про сучасні міжнародні норми до інформаційної безпеки, що особливо важливо в технічних сферах, де точність, надійність і конфіденційність інформації мають критичне значення; релевантність і конкурентоздатність (інтеграція вимог ISO/IEC 27001 у підготовку фахівців підвищує їх релевантність професійної відповідності на ринку праці, зокрема в IT-секторі, телекомунікаційних компаніях, метрологічних інституціях, підприємствах військово-оборонного комплексу тощо.

Оволодіння принципами сертифікації СУІБ та корисних практик управління ризиками створює передумови та надає переваги для працевлаштування в міжнародних інституціях і державних установах, що прагнуть дотримуватись стандартів кібербезпеки; системний характер розуміння інформаційної безпеки як сфери охоплення управлінських процесів забезпечує формування у майбутніх фахівців навичок системного управління якістю безпекових процесів та спонукання до проактивного мислення є необхідною умовою для ефективного захисту критичної інформаційної інфраструктури в умовах зростаючих кіберзагроз глобального виміру [1.a.i.165].

Міжнародні рамки кібербезпеки (з англ. – Cybersecurity Framework, далі – CSF) [1.a.i.257] мають рекомендаційний формат з метою запобігання, усунення та реалізації структурованого підходу при реагуванні на виклики у сфері кібербезпеки, які розроблено Національним інститутом стандартів і технологій США (з англ. – National Institute of Standards and Technology, далі – NIST) [1.a.i.256]; структуровано за семантикою – управління, ідентифікація, захист, вияв, реагування та відновлення. Функціонал NIST CSF формує базис для визначення пріоритетних напрямів кібербезпеки, які адаптовано до

виробничого сектору та бізнесу; є взірцем стандартів кібербезпеки, узгоджено зі світовими стандартами ISO/IEC 27001 та IT-стандарт «Контрольні цілі для інформаційних та суміжних технологій» (з англ. – Control Objectives for Information and Related Technology, далі – COBIT).

Відкритий IT-стандарт COBIT, який розроблено Асоціацією з аудиту та контролю інформаційних систем (з англ. – Information Systems Audit and Control Association, далі – ISACA, https://www.isaca.org/) у співпраці з Інститутом управління інформаційними технологіями (з англ. – IT Governance Institute, ITGI, https://www.itgi.org/), містить комплекс стандартів, які зорієнтовано на оптимізацію управління аудитом IT та IT-безпекою.

Впровадження міжнародних стандартів (зокрема ISO/IEC 27001, NIST CSF, COBIT) у освітні програми гармонізує організацію освітнього процесу згідно вимог національної нормативної бази правового і технічного регулювання, а також рекомендацій Національного агентства із забезпечення якості вищої освіти (далі – НАЗЯВО) щодо компетентнісного підходу та інтеграції професійних стандартів [1.a.i.78, 1.a.i.111], а також сприяє імплементації принципів Єдиного цифрового ринку ЄС, підвищенню відповідальності та культури безпеки (усвідомлення важливості дотримання стандартів інформаційної безпеки і формуванню у здобувачів освіти відповідного рівня соціальної відповідальності, правової свідомості, етики та культури доброчесності, роботи з інформацією, що є визначальним в соціально-турбулентних умовах цифровізації) [1.a.i.79, 1.a.i.262, 1.a.i.266]. Таким чином, нормативно-правове забезпечення професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки із урахуванням положень ISO/IEC 27001 дає змогу не лише сформувати якісні освітні соціокультурні форми, орієнтовані на реальні виклики інформатизації суспільної діяльності, але й підвищити національну кіберстійкість як стратегічний пріоритет для технологічно розвиненої України.

Методологічний базис для впровадження ISO/IEC 27001 надає супровідний стандарт ISO/IEC 27002, що реалізує унормовані практики нагляду

і контролю за інформаційною безпекою [1.а.і.273]; документ надає рекомендації щодо вибору, адаптації та впровадження засобів захисту, класифікованих за функціональними доменами безпеки, безпосередньо політику інформаційної безпеки, управління інформаційними ресурсами, контроль доступу, фізичну безпеку, захист від несанкціонованого програмного забезпечення, інцидент-менеджмент, неперервність бізнес-процесів тощо; пропонує установам гнучкий інструментарій, що дозволяє враховувати галузеву специфіку, аналізування типових ризиків та нормативних вимог під час формування власної СУІБ [1.а.і.92]. Таким чином, варто погодитися з дослідниками, які дійшли висновку, що застосування наведених стандартів сприяє інституалізації безпекових процедур, їх інтеграції у внутрішні регламенти організації та підвищенню загальної ефективності менеджменту безпеки.

Приналежно, загальна концепція серії ISO/IEC 27000 передбачає створення єдиної логічно узгодженої системи управління інформаційною безпекою, що забезпечує не лише технічну, а й організаційно-правову та соціальну стійкість [1.а.і.91], а їх значення виявляється в кількох базових вимірах. Узагальнена роль стандартів серії ISO/IEC 27000-ї в управлінні інформаційною безпекою полягає у систематизації ключових переваг та практичної цінності, а саме: забезпечення структурованого базису управління інформаційною безпекою на основі ризиків; дотримання відповідності світовим практикам та сприяння міжнародному визнанню; ефективна ідентифікація, оцінка та мінімізація ризиків; оптимізація процесів безпеки та зниження наслідків інцидентів; дотримання законодавчих і регуляторних вимог; формування професійних компетентностей фахівців сфер критичної інфраструктури та ІТ.

Упровадження міжнародних стандартів ISO/IEC 27000 відіграє системоорганізуючу роль у розбудові ефективної системи управління ризиками; охоплює увесь цикл (від виявлення потенційних загроз до практичної реалізації заходів, спрямованих на мінімізацію їх наслідків на всіх

рівнях організаційного управління); сертифікація згідно стандартів забезпечує міжнародне визнання маркера якості, що не лише підтверджує відповідність інституції вимогам, а й відкриває доступ до міжнародного партнерства. Крім того, застосування стандартів сприяє підвищенню внутрішньої ефективності, зменшує ризик виникнення небажаних інцидентів, що, в свою чергу, дозволяє уникнути фінансових втрат і репутаційних ризиків. Також можна зазначити, що імплементація норм стандартів забезпечує відповідність чинному національному законодавству та міжнародним регуляторним вимогам у сфері захисту інформації, що є необхідною умовою для стабільного інституційного функціонування організацій у цифровому середовищі організації суспільних видів діяльності.

Стандарти серії ISO/IEC 27000-ї серії не лише відіграють роль у контексті функціонування організацій, в тому числі освітніх і наукових, але й здійснюють опосередкований вплив на процеси формування компетентностей майбутніх фахівців у галузях електроніки, метрології та радіотелекомунікацій. Відповідно, їх опанування є невід'ємною частиною освітньої траєкторії майбутнього кадрового резерву, здатного адаптуватися до викликів кіберсередовища, проектувати системи захисту інформації та забезпечувати їх відповідність сучасним нормативним вимогам. Таким чином, включення положень стандартів ISO/IEC 27000 до освітніх програм безпосередньо у питаннях інформаційної безпеки не лише формує у здобувачів освіти навички практичного застосування міжнародних норм технічного регулювання, але й підвищує рівень інтегрованості вітчизняної освітньої наукової системи в глобальний безпековий дискурс, що, у свою чергу, сприяє нарощенню кадрового потенціалу висококваліфікованих фахівців, здатних ефективно впроваджувати підходи стандартизації до реалізації інформаційної безпеки у сферах електроніки, метрології та радіотелекомунікації, де надійність та захищеність інформаційних процесів забезпечує технологічну стабільність, точність вимірювань і функціонування інформаційно-телекомунікаційних систем.

Поряд із загальновизнаними універсальними стандартами серії ISO/IEC, які закладають основу для впровадження системного підходу для забезпечення управління інформаційною безпекою засобами технічного регулювання, важливою складовою розбудови телекомунікаційної інфраструктури є рекомендації ITU [1.a.i.267]. Спеціальний підрозділ ООН ITU здійснює транскордонну координацію діяльності та відіграє провідну роль у активізації процесів стандартизації, розвитку та безпечного функціонування систем інформаційної безпеки. Рекомендації ITU-T слугують технічними орієнтирами для країн-учасниць і галузевих суб'єктів управління безпекою, спрямовуючи розвиток технологій на сумісність, стійкість, зокрема кіберстійкість глобальних комунікаційних мереж [1.a.i.275]. Для узагальнення основних напрямів діяльності ITU у сфері інформаційної безпеки та аналізу технічного змісту (таблиця 1.5) систематизовано ключові рекомендації та ініціативи уповноваженої організації ITU.

Таблиця 1.5

Рекомендації та ініціативи уповноваженої організації ITU

Напрям діяльності ITU	**Зміст та технічні аспекти**	**Практичне значення для телекомунікацій**
Рекомендації ITU-T	Захист мережевої архітектури, криптографія, автентифікація, управління доступом, безпека трафіку	Підвищення кіберстійкості, забезпечення конфіденційності та надійності систем
Безпека унікального числового ідентифікатора в мережі (з англ. – Internet Protocol address (далі – IP) та п'ятого покоління мобільних мереж (з англ. – 5th Generation (далі –5G))	Базові протоколи захисту, специфікації безпеки для мобільного зв'язку нового покоління	Адаптація до нових ризиків і потреб телекомунікаційного середовища
Інтернет речей (з англ. – Internet of Things (далі – IoT)	Вимоги до безпеки IoT-пристроїв і взаємодії в мережах	Захист критичних інфраструктур і уникнення техногенних небезпек
Порядок денний глобальної кібербезпеки (з англ. – Global Cybersecurity Agenda (далі – GCA))	Правові, технічні та організаційні рамки, розвиток людського капіталу	Формування національних стратегій кіберзахисту, вплив на практику застосування технічних стандартів

Варто зазначити, що для сфери забезпечення інформаційної безпеки, рекомендації ITU спрямовано на конфіденційність, цілісність та доступність інформації, що циркулює у телекомунікаційних мережах, а також на захисті власне їх інфраструктури від технологічних і у несанкціонованого характеру загроз. Особливе значення приділено інформаційній безпеці мережевої архітектури, криптографічному захисту даних, управлінню санкціонованим доступом, автентифікації користувачів, обробці інцидентів в сфері безпеки та збереженню надійності сервісів на рівні голосового, відео- і трафіку даних. Системний підхід закладено у рекомендаціях ITU-T і враховує як базові протоколи захисту для IP-мереж і 5G, так і специфічні вимоги до безпеки IoT, які формують нові виклики в контексті інтенсифікації динамічного розвитку інформаційно-телекомунікаційних середовищ, шо обумовлює необхідність інтеграції цих положень у освітні програми професійної підготовки майбутніх фахівців, здатних розробляти та впроваджувати ефективні механізми захисту в умовах швидкозмінних умовах технологізацій, зокрема у таких галузях, як електроніка, метрологія та радіотелекомунікації, де інформаційна безпека є ключовим чинником надійності, точності та функціональної безпеки систем.

Метою функціоналу ITU є втілення Глобального порядку денного кібербезпеки (з англ. – Global Cybersecurity Alliance, далі – GCA) стратегічної дорожньої карти систематичного втілення, що забезпечує розробку та впровадження власних політик кібербезпеки країнам-партнерам [1.a.i.268]. Стратегія включає нормативно-правові, технологічні та організаційно-управлінські положення у механізмах нарощення потенціалу спроможності держав-учасниць. Документ стратегічного характеру підкріплено технічними настановами ITU-T, в яких закріплено добір методів для імплементації безпекових механізмів у телекомунікаційні системи при практичному забезпеченні в реаліях соціальної турбулентності, в свою чергу актуалізує необхідність ознайомлення здобувачів освіти у процесі професійної підготовки, адже на їх базисі майбутні фахівці у сфері електроніки, метрології та радіотелекомунікацій матимуть змогу впевнено застосовувати міжнародні

засоби технічного регулювання безпеки в дійсних телекомунікаційних інфраструктурах, забезпечуючи їх стабільність, надійність та відповідність сучасним викликам цифрової епохи. Таким чином, з огляду необхідності удосконалення професійної підготовки майбутніх фахівців у сферах електроніки, метрології та радіотелекомунікацій, рекомендації ITU відіграють функціональне значення, оскільки визначають галузеві вимоги до структури компетентностей, зокрема щодо захисту інформаційних ланцюгів у мережевому просторі організації з відповідними вимогами до надійності та безпеки.

Володіння знаннями про рекомендації ITU-T, їх класифікації, технічного змісту і практичної реалізації є обов'язковою компонентною для опанування фахівцями, уповноваженими щодо проєктування, впровадження та експлуатації захищених телекомунікаційних систем, особливо у контексті раціоналізації забезпечення критичної інфраструктури. У такий спосіб рекомендації ITU є запорукою відповідності змістового доповнення до універсальних стандартів ISO/IEC, що конкретизують вимоги до забезпечення інформаційної безпеки з урахуванням технічної специфіки глобальних комунікаційних мереж і їх стратегічної ролі в інформаційному просторі держави.

У межах формування нормативного поля інформаційної безпеки в Україні, особливо з огляду на стратегічний курс на європейську інтеграцію, надзвичайного значення набуває імплементація директив ЄС, що регламентують цифрову безпеку та захист персональних даних. Акти вторинного права ЄС встановлюють обов'язкові цілі для держав-членів, які в подальшому мають бути адаптовані у національних системах правових гарантій й захисту. Слід зазначити, що впровадження зазначених актів вимагає суттєвої трансформації освітньої парадигми, насамперед через необхідність переосмислення компетентнісного підходу до підготовки фахівців у галузях, пов'язаних з цифровою інфраструктурою, зокрема в електроніці, метрології та радіотелекомунікацій.

Одним із фундаментальних документів є Загальний регламент про захист даних (з англ. – General Data Protection Regulation, далі – GDPR), який набув чинності у 2018 році та встановив стандарти для обробки персональної інформації в межах ЄС [1.a.i.287], особливість якого полягає в екстериторіальному характері: дія регламенту поширюється на будь-яку організацію, яка обробляє персональні дані громадян ЄС, незалежно від географічної юрисдикції. У системі нормативних координат GDPR визначено ключові принципи, серед яких: законність і добросовісність обробки, цілеспрямованість, мінімізація та точність даних, обмеження строків зберігання, забезпечення конфіденційності та цілісності, а також принцип підзвітності. Технічна реалізація визначених вимог вимагає від майбутніх фахівців компетенцій, які охоплюють управління за згодою суб'єктів даних, впровадження концепцій «захисту за замовчуванням» і «захисту за задумом» (з англ. – Privacy by design and by default), розробку процедур повідомлення про порушення безпеки персональної інформації, а також правову грамотність у сфері захисту прав суб'єктів даних.

Іншим важливим нормативним актом є директива ЄС «Про безпеку мережевих та інформаційних систем» (з англ. – Directive on Security of Network and Information Systems, далі – NIS). Директива NIS актуалізує перші спроби стандартизації підходу до забезпечення кібербезпеки на державному рівні європейських країн-партнерів [1.a.i.259]. Мета директиви NIS полягає в забезпеченні високого рівня кіберстійкості критичних інфраструктур, включаючи операторів основних послуг та постачальників цифрових сервісів. Для досягнення мети кіберстійкості критичних інфраструктур директива NIS запроваджує настанови до впровадження технічних та організаційних заходів управління ризиками, підтримання безперервності сервісів і обов'язкового повідомлення про критичні інциденти уповноваженим державним органам. Зважаючи на те, що сфера електроніки, метрології та радіотелекомунікацій безпосередньо інтегрована до контурів архітектури в національної та міжнародної безпеки, фахівці зазначених напрямів повинні володіти знаннями

щодо політики управління кіберризиками, інструментами виявлення і реагування на інциденти, засобами прєктування стійкості систем та механізмами регуляторної взаємодії.

Для наочного узагальнення нормативного змісту директив GDPR та NIS, а також їх практичного впливу на сферу цифрової безпеки, наведено порівняльну характеристику справочинства у таблиці 1.6.

Гармонізація положень GDPR та NIS до освітніх програм професійної підготовки сприяє формуванню нових компетентностей, необхідних для роботи в середовищі з високими вимогами інформаційної прозорості, правової відповідності та технологічної надійності. Йдеться, зокрема, про інтеграцію у навчальні курси модулів з правового аналізу в галузі цифрового захисту, оцінювання ризиків з урахуванням регуляторних рамок, розроблення та впровадження політик безпеки, а також розвиток міждисциплінарного мислення через синтез технічних і правових знань.

Таблиця 1.6

Компаративістика директив GDPR та NIS

Нормативний документ	**Основна мета**	**Ключові принципи або вимоги**	**Практичні компетенції для фахівців**
GDPR – Деректив загального регламенту про захист даних (з англ. –General Data Protection Regulation)	Захист персональних даних громадян ЄС	Законність, добросовісність, цілеспрямованість, мінімізація, конфіденційність, підзвітність	Управління згодою, концепції «захисту за замовчуванням» і «захисту за задумом» (з англ. – privacy by design/default), реагування на порушення, правова грамотність
NIS Directive - Директиви безпеки мережевих та інформаційних систем (з англ. – Directive on Security of Network and Information Systems)	Кіберстійкість критичних інфраструктур	Управління ризиками, підтримка безперервності послуг, повідомлення про інциденти	Виявлення та реагування на кіберзагрози, побудова стійких систем, знання регуляторної взаємодії

Науковці також справедливо вважають, що особливу увагу слід приділяти практичній підготовці здобувачів освіти шляхом застосування кейс-методів, моделювання реальних інцидентів, аналіз судової та адміністративної практики

щодо порушень у сфері обробки персональних даних, що є актуальним для формування у майбутніх фахівців здатності адекватно реагувати на ризики, пов'язані з витоками даних, несанкціонованим доступом та іншими кібер-інцидентами в галузях електроніки, метрології та радіотелекомунікацій, де обробка персональної та технічної інформації потребує особливо високого рівня захисту та правової обґрунтованості дій [1.а.і.133, 1.а.і.286].

Директиви ЄС, зокрема Загальний регламент про захист даних (GDPR) та «Про безпеку мережевих і інформаційних систем» (NIS), істотно трансформують підходи до професійної підготовки фахівців, що працюють в умовах цифровізації економіки. Оволодіння змістом і принципами нормативних актів технічного регулювання стає необхідною умовою для адаптації освітніх програм до актуальних правових і технологічних викликів, а також для ефективної імплементації міжнародних стандартів у національну освітню практику професійної підготовки фахівців для реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій. Зазначені директиви виконують функцію унормування, а саме з одного боку, формують нормативні рамки для розвитку правочинства у сфері інформаційної безпеки, а з іншого, визначають перелік ключових компетентностей, якими мають оволодіти випускники, для забезпечення їх конкурентоспроможності на ринку праці та здатними до професійної діяльності в умовах цифрової трансформації суспільних видів діяльності (за економічними видами).

Крім нормативно-правових актів ЄС, вагомий вплив на концептуалізацію підходів до формування професійних стандартів у сфері інформаційної безпеки справляють рамкові програми та ініціативи провідних міжнародних організацій – НАТО, ООН та ОБСЄ. Інституції, відповідно до повноважень, послідовно просувають принципи глобальної кіберстійкості, стратегічної співпраці, правової визначеності та забезпечення розвитку людського капіталу у сфері кібербезпеки [1.а.і.158, 1.а.і.159].

У стратегічному вимірі політики НАТО (далі – Альянс) кібербезпека розглядається як одна з ключових складових колективної безпеки в першу

чергу інформаційної [1.a.i.282]. Альянс регулярно здійснює інвестиції у розвиток інституційної спроможності безпеки, зокрема щодо вдосконалення механізмів реагування на кібер-інциденти та впровадження узгоджених стандартів взаємодії між державами-членами і партнерами. Серед провідних ініціатив Альянсу, особливу роль відіграє Центр передових практик досвіду з кібероборони (з англ. – Cooperative Cyebr Defence Centre of Excellence, далі – CCDCOE) у місті Таллінні (Естонія), який забезпечує аналітичну, навчальну та експертну підтримку в галузі кіберзахисту [1.a.i.280]. Високу практичну цінність мають щорічні навчання «Замкнені щити» (з англ. – Locked Shields), що моделюють сценарії багатонаціональної координації та консолідації зусиль у відповідь на масштабні кіберзагрози. Також паралельно НАТО реалізує програми зміцнення кіберспроможностей країн-партнерів (зокрема України), що охоплюють розробку національних стратегій, нормативно-правових засад та інфраструктурної розбудови у сфері кіберзахисту. Отже, для майбутніх фахівців у галузях радіотелекомунікацій, метрології та електроніки (особливо тих, хто працює із захистом критично важливої інфраструктури або в оборонно-промисловому секторі) знання стандартів НАТО, доктрин кібероборони та процедур міжнародної взаємодії є принципово важливим. Оволодіння знань системою з вказаних напрямів не лише забезпечує професійну готовність до роботи в умовах сучасних викликів інформатизації, а й гарантує згуртованість дій згідно із міжнародними протоколами безпеки, що є необхідною передумовою для успішної євроатлантичної інтеграції потенційних кандидатів.

Безпосередньо ООН виконує роль глобальної платформи політичного та правового діалогу з питань інформаційної безпеки. Через механізми Групи урядових експертів (з англ. – Group of Governmental Experts, далі – GGE) та Відкритої робочої групи (з англ. – Open-ended Working Group, далі – OEWG) сприяють виробленню міжнародних норм поведінки держав у кіберпросторі, підтверджує необхідність дотримання принципів міжнародного права та підтримує розробку національних добровільних стандартів відповідальної

поведінки. Окремого значення набувають програми з будови безпеки кіберпотенціалу для країн, що розвиваються, а також діяльність яких, спрямовано на протидію кіберзлочинності. У підсумку просвітницький вплив ООН полягає у формуванні в майбутніх фахівців розуміння міжнародно-правових, етичних і гуманітарних засад інформаційної безпеки, що дозволяє поєднувати технічну компетентність із глобальним усвідомленням соціальної й екологічної відповідальності у цифровому середовищі зайнятості [1.a.i.169, 1.a.i.239].

У свою чергу ОБСЄ розглядає інформаційну безпеку як невід'ємну частину комплексної моделі безпеки. Особливу увагу установа приділяє зміцненню довіри між державами шляхом впровадження Заходи довіри та безпеки (з англ. – Confidence- and Security-Building Measures, далі – CSBMs) у кіберпросторі [1.a.i.29]. У цьому контексті діяльність ОБСЄ охоплює створення платформ для міжнародного обміну інформацією, підтримку розвитку національних інституцій кіберзахисту та забезпечення розлогого розуміння природи кіберзагроз у регіональному вимірі. Тому ознайомлення з відповідними інструментами та методиками функціонального призначення дозволяє мінімізувати ризики ескалації конфліктів, що можуть виникати внаслідок зловживання інформаційно-комунікаційними технологіями. Водночас це формує у фахівців здатність оцінювати інформаційну безпеку не лише з технічної точки зору, а й у безпековому, правовому та геополітичному контексті [1.a.i.198].

Для професійної підготовки майбутніх фахівців для реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій такий міждисциплінарний підхід має принципове значення, оскільки поєднує технічні аспекти захисту інформаційних систем із розумінням міжнародних норм, правових регламентів та конфліктогенних чинників, що супроводжують кіберзагрози. Відповідно у майбутніх фахівців в результаті формується здатність діяти відповідально в інформаційному середовищі, сприяти стабільності та безпеці на міжнародному рівні. Для систематизації основних

положень директив ЄС та міжнародних ініціатив у сфері інформаційної безпеки наведено таблицю 1.7.

Директиви ЄС, стратегічні документи та ініціативи НАТО, ООН і ОБСЄ суттєво впливають на зміст та модернізацію системи професійної підготовки фахівців до реалізації інформаційної безпеки. Опанування знань та процедур справочинства проаналізованих документів забезпечує формування здатності у майбутніх фахівців діяти у міжнародному полі майбутньої професійної зайнятості. Відповідно це створює підґрунтя для підготовки нового покоління професіоналів, які спроможні забезпечити ефективність захисту інформаційного простору професійних середовищ.

Таблиця 1.7

Систематизація основних документів справочинства у сфері інформаційної безпеки

Джерело регулювання	Основний документ/ініціатива	Ключові положення та напрями впливу	Значення для підготовки фахівців
ЄС	Директив загального регламенту про захист даних (з англ. – General Data Protection Regulation)	Захист персональних даних (з англ. – privacy by design/default), права суб'єктів інформаційних даних	Забезпечення формування компетенцій з управління інформаційними даними, правової грамотності, практики запобігання та реагування на втрати інформації
	NIS Directive	Кіберстійкість інфраструктур, управління інформаційними ризиками, національні стратегії інформаційної, кібербезпеки	Формування знань виникнення, передбачення та усунення кіберризиків, інцидент-менеджменту, взаємодія з суб'єктами-регуляторами безпеки
НАТО	CCDCOE – центр передового досвіду з кібероборони (з англ. – Cooperative Cyebr Defence Centre of Excellence), програми партнерства «Замкнені щити» (з англ. – Locked Shields)	Кібероборона, реагування на інциденти, спільні стандарти Альянсу	Орієнтації на забезпечення захисту критичної інфраструктури, участі у кібернавчаннях та долучення до впровадження та дотримання міжнародних стандартів
ООН	GGE – група урядових	Норми правової	Розуміння та дотримання

	експертів (з англ. – Group of Governmental Experts), OEWG – відкриті робочі групи (з англ. – Open-ended Working Group), програми розвитку	поведінки держав-членів, дотримання вимог міжнародного права, заходи протидії кіберзлочинності	глобальних правових засад кібербезпеки, участь у міжнародному діалозі у контексті гарантій безпеки
ОБСЄ	CSBMs – заходи довіри та безпеки (з англ. – Confidence- and Security-Building Measures), платформи обміну інформацією	Забезпечення взаємної довіри в кіберпросторі, розбудова національних потенціалів, аналіз загроз інформаційної безпеки	Інтеграція регіонального виміру безпеки, впровадження підходів до мирного (сталого) використання ІКТ

Інтеграція України до європейського простору та активне залучення до глобальної системи цифрової безпеки передбачає поступову і системну гармонізацію національного нормативно-правового поля у відповідності міжнародних стандартів та рекомендацій [1.a.i.237]. Імплементація їх є необхідною умовою не лише для забезпечення сумісності технічних, управлінських і безпекових підходів, а й для досягнення належного рівня стійкості до кіберзагроз, підвищення технологічного суверенітету держави, а також для розвитку та удосконалення освітньо-наукових систем для професійної підготовки фахівців нового покоління для роботи у сфері електроніки, метрології та радіотелекомунікацій. Оскільки впровадження міжнародних норм в українське законодавство це складний і багаторівневий процес інтеграції [1.a.i.200], то одним із ключових інструментів є ратифікація міжнародних договорів і конвенцій, а саме Будапештської конвенції Ради Європи «Про кіберзлочинність» [1.a.i.29]. Передбачає, що держава бере на зобов'язання узгодження власного законодавства з положеннями відповідних міжнародних документів, що в свою чергу вимагає внесення змін до національних кодексів та розробки й ухвалення нових законів, створення спеціальних механізмів регулювання та оновлення судової практики з урахуванням міжнародних принципів застосування права [1.a.i.156]. Наступним кроком до впровадження міжнародних норм в українське законодавство, є імплементація пов'язана з адаптацією законодавства до правового доробку ЄС

надбання спільноти (з франц. – acquis communautaire). Сукупність законодавчих актів є невід'ємною частиною виконання зобов'язань, зафіксованих в Угоді про асоціацію між Україною та ЄС [1.a.i.236]. В умовах цифрової трансформації особливу увагу зосереджено на реалізації положень Загального регламенту про захист даних (GDPR) [1.a.i.287] і Директиви про безпеку мережевих та інформаційних систем (NIS Directive) [1.a.i.259]. Адаптація полягає у трансляції нормативного змісту цих документів у національне законодавство шляхом прийняття спеціалізованих законів і підзаконних актів. Зокрема, Закону України «Про захист персональних даних» [1.a.i.198], що стало кроком поступу до нормативного наближення до стандартів GDPR, проте повна гармонізація ще потребує розширення термінологічного апарату, механізмів захисту прав суб'єктів даних, санкційної політики та процедур моніторингу [1.a.i.236]. Імплементація положень NIS2 Directive [1.a.i.258], у свою чергу, вимагає формування інституційної архітектури національної системи кібербезпеки, зокрема визначення органів уповноваженого нагляду та контролю, створення національного регулювання обміну інформацією щодо кіберінцидентів та встановлення критеріїв для визначення операторів критичної інфраструктури [1.a.i.145].

Наступним важливим напрямом є впровадження міжнародних технічних стандартів. Серія ISO/IEC 27000 і рекомендації ITU, повинні бути взяті як базис технічної регламентації для розробки національних стандартів [1.a.i.152]. Незважаючи на те, що зазначені стандарти не мають прямої юридичної обов'язковості, вони де-факто регулюють галузеві практики і застосовуються як еталони при формуванні регуляторних політик. Національні органи стандартизації, зокрема ДП «УкрНДНЦ», уповноважені щодо гармонізації міжнародних стандартів і можуть адаптувати їх у вигляді ідентичних або модифікованих національних стандартів [1.a.i.254]. Сприяння інтеграції вітчизняної нормативної системи до єдиного міжнародного простору технічного регулювання, забезпечує уніфіковані підходи до розбудови системи управління інформаційною безпекою та створює умови для участі українських

інституцій у глобальних мережах безпекових процесів. Не дивлячись на те, що рекомендації міжнародних організацій (НАТО, ООН та ОБСЄ) [1.а.і.243] мають радше рекомендаційний, ніж обов'язковий характер, Україна враховує їх для визначення стратегічних цілей і принципів у галузях інформаційної та кібербезпеки, як складової стратегії раціональної безпеки.

Нині Україна активно долучається до спільних ініціатив модернізації освітніх програм професійної підготовки майбутніх фахівців, проєктів з забезпечення нарощення кібер-потенціалу та отримує консультативну підтримку в межах співпраці з міжнародними організаціями. Їх рекомендації враховують під час розробки національних стратегій і концепцій національної безпеки та кібероборони, планів реагування на кібер-інциденти, а також при визначенні вимог до професійної підготовки майбутніх фахівців у сфері радіотелекомунікацій, кіберінженерії та захисту критично важливої інфраструктури забезпечення інформаційних ресурсів. Врахування Україною рекомендацій міжнародних міжурядових організацій, зокрема НАТО, ООН та ОБСЄ, у сфері інформаційної безпеки має принципове значення для формування компетентнісної моделі професійної підготовки майбутніх фахівців у сфері електроніки, метрології та радіотелекомунікацій, оскільки зазначені інституції акумулюють найкращі світові практики, стандарти й методології у протидії кіберзагрозам, інтеграції їх положень у національну освітню політику забезпечення професійної підготовки висококваліфікованих кадрів, здатних діяти в уніфікованому міжнародному правовому, технічному та організаційному полі зайнятості. Міжнародні рекомендації також сприяють гармонізації освітніх програм згідно сучасних вимог глобального ринку праці та з урахуванням актуальних викликів інформатизації суспільної діяльності, зокрема у розвитку кіберсистем та безпекових процедур справочинства у критичній інфраструктурі, забезпечують формування у майбутніх фахівців комплексного розуміння не лише технічних аспектів захисту інформації, а й правових, організаційних та етичних принципів і норм регулювання ефективної діяльності у сфері інформаційної безпеки. У результаті впровадження

зазначених рекомендацій професійна підготовка фахівців у сфері електроніки, метрології та радіотелекомунікацій набуває системного та інтегрованого характеру, забезпечуючи здатність випускників не лише впроваджувати сучасні управлінські та технологічні рішення, а й ефективно діяти в умовах глобального виміру стандартизації інформаційних середовищ професійної зайнятості.

Для узагальнення основних напрямів імплементації міжнародних норм у національне законодавство України наведено таблицю 1.8, що відображає ключові механізми, нормативні джерела та їх практичне значення.

Таблиця 1.8

Систематизація напрямів імплементації міжнародних норм правочинства та технічного регулювання

Напрям імплементації	**Джерело/Ініціатива**	**Практична реалізація**	**Вплив на професійну підготовку**
Ратифікація міжнародних угод	Будапештська конвенція	Узгодження законодавства, оновлення судової практики	Забезпечення формування навичок правозастосування, розуміння та дотримання вимог міжнародного правочинства
Адаптація до директив надбання (з франц. – acquis) ЄС	Директив загального регламенту про захист даних ((з англ. – General Data Protection Regulation, GDPR), Директиви безпеки мережевих та інформаційних систем (з англ. – Directive on Security of Network and Information Systems, NIS Directive), Угода про асоціацію	Закони України, Комп'ютерна група реагування на надзвичайні ситуації (з англ. - Computer Emergency Response Team, CERT), регуляторні механізми	Юридичні та технічні компетенції в кібербезпеці, політики захисту інформаційних даних
Гармонізація та адаптація до технічних стандартів	ISO/IEC 27000, ITU, адаптація у ДСТУ	Розробка, гармонізація та застосування національних стандартів	Знання міжнародних еталонів технічного регулювання, здатність до професійної діяльності в єдиному просторі технічного регулювання
Орієнтація на дотримання рекомендацій	НАТО, ООН, ОБСЄ	Стратегії, концепції кібероборони,	Міжнародна консолідація, участь у спільних ініціативах,

міжнародних інституцій		програми підтримки інформаційної безпеки	інформаційно-аналітичні та інтеграційні навички та компетенції

Актуалізовано необхідність узгодження міжнародних і національних правових норм, які іноді відрізняються за змістом чи процедурами. Додатково ускладнює ситуацію й те, що ресурси, які потрібні для забезпечення якості імплементації стандартів (кадри, фінанси, матеріально-технічна база), часто обмежені в Україні. Ухвалені рішення не завжди реалізуються повною мірою. Особливої уваги заслуговує питання забезпечення кадрового потенціалу, адже ефективна імплементація передбачає наявність фахівців нової формації, здатних працювати у перетині технічної регулятивної, правочинної та адміністративної управлінської площин. Освітньо-наукові системи мають реагувати на виклики інформатизації через запровадження спеціалізованих освітніх програм, міждисциплінарних курсів, дуальних форм навчання, забезпечення підвищення кваліфікації, професійної підготовки та перепідготовки фахівців, що обумовлює ефективність працевлаштування майбутніх фахівців для реалізації комплексних завдань інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій, де стрімкий розвиток ІКТ вимагає постійного оновлення знань, формування гнучких освітніх траєкторій і забезпечення тісного зв'язку між теорією, методикою, практикою та актуальними вимогами ринку професійної зайнятості.

Отже, впровадження міжнародних стандартів і практик корисного досвіду у сфері інформаційної безпеки в українське законодавство, це складний і стратегічно важливий процес інтеграції України з метою зміцнення національної безпеки та кіберстійкості, при підготовці фахівців здатних працювати у глобальному цифровому середовищі, легітимне правочинство відіграє вирішальне значення.

1.3 Формально-логічний та компаративний аналіз нормативно-правового забезпечення професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації

Водночас можна відмітити, що технології змінюються швидше, ніж встигають ухвалюватися нові закони. Отже виникає відставання нормативної правової та технічної баз регулювання, слабке реагування на виклики інформатизації, такі, як ШІ, квантові обчислення, блокчейн тощо. З метою погодження міжнародних і національних вимог потрібна повна юридична відповідність, імплементованість та системна координація між законодавчими інстанціями. Однією з проблем, як чинник обмеження, є дефіцит фінансових, правових і матеріально-технічних ресурсів, необхідних для ефективного правового та інституційного забезпечення ефективності впровадження заходів технічного регулювання (стандартів). Таким чином, в академічних колах неодноразово наголошено на приділенні особливої уваги кадровому потенціалу: вкрай необхідними є фахівці, які поєднують інформаційно-аналітичні здатності моніторингу, управління та експертизи інформаційної безпеки інституційної й професійної діяльності з ґрунтовними знаннями міжнародного права та нормативного дизайну забезпечення якості й безпеки.

Удосконалення нормативно-правової бази регулювання інформаційної безпеки потребує системної діагностики та узгодження національного законодавства з європейськими й міжнародними стандартами, що має забезпечити відповідність правових норм сучасним викликам цифрової трансформації, динаміці технологічного розвитку сфери електроніки, метрології та радіотелекомунікацій та вимог у співпраці з міжнародними партнерами. Початковим етапом є компаративний аналіз чинних нормативних актів України з міжнародними стандартами та директивами ЄС, що дозволяє виявити застарілі положення, дублювання чи суперечності, а також визначити чинні норми, що не враховують специфіку застосування новітніх технологій. Ключове значення має оцінка рівня імплементації директив GDPR NIS,

стандартів ISO/IEC 27000 і рекомендацій ITU, а також аналіз їх практичної ефективності в умовах соціальної турбулентності. Дослідники відзначають, що формальне ухвалення норм зачасту не супроводжується в повній мері дієвими підзаконними актами, процедурами та механізмами контролю, що знищує бажану їх результативність. Особливої уваги потребує вплив впровадження інноваційних технологій у професійну діяльність майбутніх фахівців сфери електроніки, метрології та радіотелекомунікацій на правочинство. Встановлено, що ШІ, значні масиви інформаційних даних, автоматичні системи контролю та управління, мережі 5G та новітні системи комунікації радикально змінюють характер та інтенсивність потенційних кіберризиків і методів їх подолання, що зумовлює потреби регульованого оновлення нормативної правової бази. Регулювання професійної підготовки фахівців, пошук оптимальних шляхів гармонізації передбачає, з одного боку, активну імплементацію надбання спільноти (з франц. – Acquis communautaire) з урахуванням європейського досвіду та національної специфіки, а з іншого, ухвалення нових і модернізацію чинних актів, як у сфері освіти, науки й інноватики, так і у професійних середовищах зайнятості. Водночас важливим завданням є формування гнучкої системи моніторингу та адаптації законодавства до змін у інформаційному, зокрема кіберпросторі, динаміці технологічного поступу й міжнародному правочинстві. Також необхідною умовою забезпечення ефективності правового та технічного регулювання є оптимізація міжвідомчої координації між державними інституціями, за уповноваженими зі формування та контролю інформаційної безпеки, органами стандартизації та сертифікації, регуляторами в сфері електроніки, мерології та радіотелекомунікацій й телекомунікаційного сектора, а також активна взаємодія з академічною спільнотою, бізнесом та приватним сектором професійного втілення [1.a.i.26]. Водночас варто інвестувати в розвиток людського капіталу через створення програм професійної підготовки, перепідготовки та підвищення кваліфікації фахівців, здатних розробляти, оцінювати та реалізовувати законодавчі вимоги стратегії інформаційної безпеки держави у майбутній професійній зайнятості.

Наведено таблицю 1.9, в якій узагальнено можливості імплементації міжнародних норм в Україні у сфері інформаційної безпеки.

Забезпечення ефективного функціонування системи інформаційної безпеки у сучасному глобалізованому середовищі потребує наявності висококваліфікованих фахівців, компетентність яких має відповідати не лише національним, а й міжнародним стандартам. Формування їх професійних спроможностей обумовлюється не лише вимогами роботодавців або регуляторних органів управління підготовкою й професійною зайнятістю, а й закріплюється у міжнародних нормативно-методичних документах, стандартах, директивах та ініціативах стратегічного розвитку, які окреслюють рамки, зміст і забезпечення професійної підготовки майбутніх фахівців. У цьому контексті визначення комплексу знань, умінь і навичок, необхідних фахівцям до реалізації інформаційної безпеки, є одним із пріоритетних завдань на етапі оновлення освітніх, освітньо-професійних програм та розбудова й забезпечення відповідності національних рамок кваліфікацій до міжнародних, зокрема освітніх і професійних.

Таблиця 1.9

Імплементація міжнародних норм в Україні у сфері інформаційної безпеки

Категорія	Зміст	Потенційні рішення
Технологічна динаміка	Відставання нормативної бази, гальмівні бар'єри реагування на новітні загрози (ШІ, IoT, блокчейн)	Постійне оновлення нормативних актів, створення гнучких механізмів адаптації до національних реалій
Юридична сумісність	Невідповідності між міжнародними та національними нормами, термінологічні проблеми установленого тезаурусу	Розробка узгоджених положень правочинства, консультації з міжнародними експертами щодо їх гармонізації
Обмежені ресурси	Дефіцит кадрового забезпечення, фінансування, матеріально-технічних засобів	Інвестування в освіту, науку й інноватику, розвиток державного і приватного партнерства, активізації підвищення кваліфікації фахівців за цільовим призначенням професійних середовищ зайнятості
Прогалини в законодавстві	Застарілі правові акти, відсутність механізмів ефективної реалізації,	Модернізація чинного законодавства, інформаційно-

	дублювання нормативів правового й технічного регулювання	аналітичне оцінювання, прийняття нових нормативних актів
Вплив інноваційних технологій	Відсутність регулювання автономних систем, та автоматизованих систем управління та контролю квантових обчислень, 5G, значних масивів даних	Оцінка ризиків та небезпек, правова діагностика та аналітика, інтеграція технічних стандартів
Кадровий потенціал	Недостатнє фахівцями нових формацій забезпечення із технічно-правовими компетенціями регулювання	Створення міжгалузевих програм підготовки міждисциплінарних, підтримка курсів дуальності освіти, перепідготовка та підвищення кваліфікації кадрів
Інституційна координація	Слабка взаємодія органів, фрагментарність забезпечення й підтримки регуляторного поля	Посилення міжвідомчої координації, розробка спільних стратегій і планів

Міжнародна серія стандартів ISO/IEC 27000, хоча формально не містить безпосереднього опису освітніх або професійних кваліфікацій, все ж визначає компетентнісне ядро складових компонентів їх компетентності, необхідне для впровадження та підтримки ефективної СУІБ. Тож, стандарт ISO/IEC 27001 передбачає створення інтегрованої структури управління ризиками, в разі застосування якої фахівець повинен володіти навичками системного аналізу та ідентифікації загроз, встановлення рівня вразливостей системи, оцінки ризиків, розроблення та реалізації наглядових заходів, а також моніторингу відповідності політик безпеки, зокрема інформаційної [1.a.i.272]. ISO/IEC 27002 доповнює ці вимоги практичними рекомендаціями щодо реалізації системи контролю, що вимагає від профільних фахівців, як технічної компетентності (знання щодо організації та управління мережевої системи безпеки, криптографії, безпеки мобільних застосунків), так і організаційної (впровадження політик, стратегії управління активами, навчання та управління персоналом) [1.a.i.273]. Зрозуміло, що юридичний контекст також не може бути ігнорованим, оскільки ефективна система управління інформаційною безпекою має забезпечувати відповідність національним і міжнародним нормам.

У рекомендаціях Міжнародного союзу електрозв'язку (ITU) докладно описано вимоги для фахівців відповідної сфери; виокремлено питання захисту мереж і послуг (від архітектури безпеки й автентифікації користувачів до

застосування криптографії та реагування на кіберінциденти) [1.a.i.276]. Майбутні фахівці мають розбиратися та брати участь у проєктуванні мережевих систем організації і справочинності протоколів передачі інформаційних даних, розуміти принципи роботи розподілених систем та вміти забезпечувати захист сучасних технологій (5G і IOT), що вимагає від фахівців сучасних наукових знань та інженерних навичок з уміннями системно аналізувати архітектурно складні загрози в інфраструктурі систем інформаційної безпеки.

У правовому та техніко-регуляторному вимірі ключову роль відіграють директиви ЄС, GDPR та NIS. Вимоги Загального регламенту про захист даних формують набір компетентностей, які виходять за межі технічної спеціалізації: це розуміння принципів «захисту за замовчуванням» (з англ. – Privacy by default) та захисту за задумом (з англ. – Privacy by design), проведення оцінки впливу на захист даних (з англ. – Data Protection Impact Assessment, DPIA), розробка політик захисту приватності, управління згодою, а також вміння комунікувати з регуляторними установами та уповноваженими органами. Директивою NIS зосереджено увагу на ризик-менеджменті критичної інфраструктури, що вимагає навичок управління інцидентами, планування регулярності сервісів, системного аналізу вразливості, системи інформаційної безпеки, а також організації міжвідомчої координації зусиль згуртованості [1.a.i.113, 1.a.i.205]. Зважаючи на те, що директиви прямо чи опосередковано впливають на зміст національних нормативно-правових актів, вони визначають професійні вимоги і до майбутніх вітчизняних фахівців, які матимуть професійне працевлаштування у дотичних галузях – від електроніки, метрології до цифрової організації комунікацій за призначенням.

Вагомий вплив на структуру фахових компетентностей мають також рамкові ініціативи визначених міжнародних інституцій: НАТО, ООН та ОБСЄ. Зокрема, спеціальні програми НАТО у сфері кіберзахисту обумовлюють необхідність формування здатностей для співпраці та міждержавного партнерства, системного аналізу інформаційних загроз у провадженні

державної політики, спільного стратегічного планування кібероперацій, участі в міжнародних навчаннях та відпрацювання процедур колективного реагування у питаннях забезпечення кібербезпеки згідно міжнародно правових рамок захисту даних. Згідно узгоджених ініціатив ООН та ОБСЄ особливу увагу приділяється дотриманню норм міжнародного права, етиці роботи в кіберпросторі, формуванню взаємної довіри між країнами-партнерами відповідальність за дотримання, що також покладає спеціальні вимоги до фахівців щодо їх системно-аналітичного, критичного й креаційного мислення, здатності до міжгалузевої комунікації та стратегічного планування систем (інформаційної безпеки й управління нею) [1.a.i.114].

На додаток до нормативних джерел, міжнародна професійна спільнота розробила й ухвалила низку галузевих рамок компетентностей, що застосовуються у якості орієнтирів для розробки й ефективного впровадження освітніх програм професійної підготовки майбутніх фахівців та їх сертифікації. Найбільш відомими серед них є – Структура кадрової бази кібербезпеки США (з англ. – NICE Cybersecurity Workforce Framework), Міжнародний консорціум з сертифікації в галузі безпеки інформаційних систем (з англ. – The International Information System Security Certification Consortium, далі – ISC2), Сертифікований професіонал з безпеки інформаційних систем (з англ. – Certified Information Systems Security Professional, далі – CISSP), курси з безпеки – CompTIA Security+, EC-Council сертифікований хакер з етики (з англ. – certified ethical hacker, далі – CEH) та інші [1.a.i.253, 1.a.i.260, 1.a.i.269].

Систематизують і класифікують спеціалізації у сфері інформаційної безпеки зазначені установи за функціональними доменами (аналітика загроз, адміністрування безпеки, цифрова криміналістика, захист інфраструктури тощо) і конкретизують очікувані знання, уміння, навички (далі – ЗУН) згідно обраної кар'єрної траєкторії. Хоча визначені рамки не мають статусу міжнародного нормативного акту, проте їх розглядають як результат консенсусу рекомендації експертної групи та активно застосовують при формуванні стандартів професійної освіти. Для стислої систематизації

міжнародних вимог до компетентностей фахівців у питаннях формування інформаційної безпеки, в таблиці 1.10 наведено порівняльну характеристику ключових джерел щодо очікуваних ЗУН та їх практичного значення для професійної підготовки майбутніх фахівців.

Сучасні вимоги до підготовки фахівців у галузі інформаційної безпеки не обмежуються когнітивним потенціалом технічних знань. Нині від майбутніх фахівців очікують розуміння нормативно-правових і техніко-регламентуючих засад та володіння організаційно-управлінськими навичками й уміннями. Лише синергія зазначених складових уможливлює сформування професіоналів, здатних до роботи у складних умовах соціальної турбулентності цифровізації доби, до конкурентноспроможності на міжнародному ринку зайнятості зі спроможністю адаптації до викликів глобального виміру.

Таблиця 1.10

Порівняльна характеристика ключових джерел щодо ЗУН та їх практичного значення для професійної підготовки майбутніх фахівців

Джерело стандарту / ініціативи	Основні вимоги до компетентностей	Очікувані ЗУН	Значення для професійної підготовки
ISO/IEC 27001/27002	Управління ризиками, впровадження системи й засобів контролю	Системного аналіз загроз, технічні та організаційні навички, відповідність нормативним вимогам	Основне компетентносте ядро для СУІБ
ITU-T	Безпека мереж, криптографія, захист новітніх технологій	Проектування інформаційних систем електрозв'язку, робота з протоколами, інтеграція захисту у 5G, IoT	Інженерна підготовка у сфері радіотелекомунікацій
GDPR (ЄС)	Захист персональних даних, конфіденційність за замовчуванням (з англ. – privacy by design/default)	Оцінка впливу на захист даних (з англ. – Data Protection Impact Assessment, DPIA), розробка політик інформаційної безпеки, управління згодою, правове і технічного регулювання	Юридична і управлінська компетентність
NIS Directive (ЄС)	Управління кіберризиками, критичною інфраструктурою	Інцидент-менеджмент, планування безперервності, системний аналіз вразливостей і небезпеки	Компетенції з забезпечення кіберстійкості систем
Ініціативи НАТО /	Кіберзахист, міжнародне	Участь у міжнародних навчаннях, міждисциплінарні	Орієнтація на глобальне

ООН / ОБСЄ	правове, регулювання етика, стратегічне планування	комунікації, інформаційно правове аналітичне забезпечення	співробітництво та колективну безпеку
Галузеві професійні рамки (NICE, CISSP, CEH)	Функціональні домени (аналітика загроз, інфраструктура, цифрова криміналістика)	Технічні знання, сертифікація, стандарти, відповідність обов'язком ролям і кар'єрним траєкторіям	Стандартизація змісту освітніх програм, підготовка до сертифікації

З огляду на практичний досвід традиційної професійної освіти, вузька інженерно-технічна підготовка не забезпечує в повній мірі готовності до виконання професійних завдань в сучасних реаліях фахівці компетентні в реалізації інформаційної безпеки мають поєднувати технічно-аналітичну діяльність експертно з правовою грамотністю, умінням організовувати та забезпечувати процеси, заходи безпеки, прогнозувати, моделювати й керувати інформаційними ризиками та мислити стратегічно. Особливо актуальним визнано у галузях електроніки, метрології та радіотелекомунікацій інформаційна безпека, як ключового чинника ефективного функціонування критичної інфраструктури.

Відтак освітні програми мають виходити за межі традиційної інженерно-технічної підготовки. Йдеться про поступове впровадження міжнародних стандартів, врахування акредитаційних критеріїв і компетентнісних моделей, які орієнтують майбутніх фахівців не лише на вирішення суто технічних завдань, а й на роботу в умовах жорсткого техніко-регуляторного, правового й професійно етичного контролю за соціальною й екологічною відповідальністю у професійному колі зайнятості.

Аналіз зарубіжного досвіду підтверджує: підготовка кадрів для реалізації інформаційної безпеки повинна бути комплексного зорганізованою на засадах й системного підходів; включати не лише інженерно-технічні та цифрові навички, а й організаційно-управлінського уміння працювати з ризиками, забезпечувати неперервність мережевих процесів, захищати критичну інфраструктуру від інформаційних небезпек кіберзагроз та дотримуватися

принципів цифрової етики. Зазначені аспекти нині залишаються відносно слабо забезпечені в національних освітніх програмах, що свідчить про необхідність їх подальшої модернізації та вдосконалення.

Окремою проблемою є обмежена увага до новітніх технологій. Теми інтернету речей, мобільного зв'язку п'ятого та шостого покоління, граничні або периферійні обчислення (з англ. – Edge computing), штучного інтелекту й методів кіберзахисту майже не представлено у навчальних дисциплінах. Створює протиріччя між очікуваннями ринку праці та релевантними результатами підготовки майбутніх фахівців, які змушені самостійно надолужувати сучасні наукові знання для інтеграції у високотехнологічне середовище цифровізації економічних видів діяльності [1.a.i.111, 1.a.i.255].

Значною мірою недовпрорядкованою залишається міждисциплінарність та міжгалузевість змістового наповнення, які нині є запорукою сучасних моделей інформаційної та кібербезпеки мережевих систем. Інформаційна безпека як галузь знань нині не може обмежуватися лише інженерно-технічними дисциплінами та потребує глибокого правового аналізу змісту навчання та забезпечення, розуміння норм міжнародного соціального права та стратегій інформаційної безпеки, володіння етичними принципами цифрової поведінки, здатності до критичного стратегічного мислення для безпеки комунікації у міжнародному середовищі праці [1.a.i.239]. Міжнародні підходи, сформульовані у програмах НАТО, ООН, ОБСЄ, а також у положеннях GDPR і NIS, передбачають масштабування рамок компетентностей з врахуванням складових дипломатії, міжнародного врегулювання кіберінцидентів та транскордонного управління інформаційною безпекою [1.a.i.280].

Брак інституційних механізмів є одним із бар'єрів інтеграції освітньо наукових систем сертифікації майбутніх знань, навичок та умінь поряд зі комплексом готовності, здатності й компетентності за міжнародними моделями кваліфікацій сучасних рамок. Відсутність системного залучення до організації освітнього процесу таких орієнтирів, як NICE Framework або ISC2 CBK, не дозволяє гарантувати оперативність відгуку майбутніх фахівців соціально

турбулентним умовам глобального виміру професійної зайнятості [1.a.i.269, 1.a.i.279]. Що, в свою чергу, формує залежність від для дипломної освіти, яка забезпечується поза межами університетів, і призводить до подовження циклів професійної адаптації [1.a.i.274].

Зокрема, міжнародний стандарт від NIST, який надає універсальний словник для класифікації завдань, знань, умінь та навичок (KSA) у сфері кібербезпеки (з англ. – NICE Cybersecurity Workforce Framework), розроблено процедуру Національним інститутом стандартів і технологій США, що визначає понад 50 кваліфікаційних рамок у сфері кібербезпеки, класифікованих за категоріями, спеціалізаціями та наборами компетентностей. ISC2 CBK, у свою чергу, є глобальним еталоном компетентностей і знань, що охоплює ключові домени галузі організації й забезпечення інформаційної безпеки, включно з управлінням ризиками й небезпеками систем, безпекою програмного забезпечення, криптографією, правовими аспектами реагування на інциденти [1.a.i.269].

В Україні окремі навчальні центри, такі як Партнери з безпеки інформаційних систем (з англ. – Informations System Security Partners) ISSP Training Center, вже пропонують курси за міжнародними стандартами (CISSP, CEH, CHFI, CSA), однак ці ініціативи залишаються фрагментарно впровадженими у професійну підготовку майбутніх фахівців, не інтегрованими в стратегію державної освітньої політики [1.a.i.274]. Наведено таблицю 1.11, що унаочнює і показує узагальнення основних відмінностей між міжнародними вимогами та стандартами вищої освіти України щодо підготовки фахівців для реалізації інформаційної безпеки.

Водночас, серйозним недоліком є недостатньо приділена увага до практичних методів професійної підготовки майбутніх фахівців. В українських освітніх програмах майже не використовуються симуляційні моделі, кейс-методи, воркшопи, тренінги, які імітують реальні умови реагування на інформаційні ризики та кібер-інциденти. Хоча в міжнародній практиці перелічений навчальний інструментарій є визначеним практично орієнтовним

компонентом професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки.

Встановлено, що вказані методи сприяють майбутнім фахівцям швидко адаптуватися у ситуаціях професійної невизначеності інформаційних систем, корпоративної взаємодії в команді під час виникнення й подолання кризових подій, дотримуватися професійної та цифрової етики в умовах конфлікту інтересів та всебічної співпраці у проєктах багаторівневої організації.

Таблиця 1.11

Відмінності між міжнародними вимогами та стандартами вищої освіти України щодо підготовки фахівців для реалізації інформаційної безпеки

Критерій порівняння	**Міжнародні підходи**	**Національні професійні стандарти освіти України**	**Ідентифіковані розбіжності**
Компетентнісна структура	Інтеграція технічних, правових, управлінських, етичних знань і компетенцій	Переважно інженерно-технічна спрямованість	Недостатня міждисциплінарність та міжгалузевість функціонального призначення
Управління ризиками	Системний аналіз і моніторинг загроз, оцінювання ризиків і небезпек, необхідність нагляду та контролю	Часткове охоплення, фрагментарне представлення	Відсутність системного підходів та комплексного
Інформаційний захист критичної інфраструктури	Регламентовано процедурами NIS, ITU, НАТО	Загальні положеннях, без конкретних моделей	Недостатньо деталізоване висвітлення корисних практик застосування
Інноваційні технології	5G/6G, IoT, AI, квантова криптографія — включень до освітніх програм і кваліфікаційних рамок компетентностей	Епізодичне або відсутнє врахування	Неузгодженість із інформаційно-технологічними трендами сфер призначення
Міжнародне право і етика	Загальний регламент про захист даних (з англ. – General Data Protection Regulation, GDPR), Робоча група відкритого складу (з англ. – Open-ended Working Group, OEWG), Загальна сукупність знань (з англ. – Common Body of	Загальні гуманітарні курси, не інтегровано з огляду кібербезпекового контексту	Відсутність практичної юридичної, управлінської підготовки

Критерій порівняння	Міжнародні підходи	Національні професійні стандарти освіти України	Ідентифіковані розбіжності
	Knowledge, CBK) акцент на правовій грамотності, етичній поведінці		
М'які навички та симуляції	Хакатони, змагання з кібербезпеки, в якому учасники шукають (секретні дані) «прапори» (з англ. – Capture The Flag), що ховаються в уразливостях програм та систем, а потім «захоплюють» їх, щоб отримати бали, командна взаємодія, стратегічна комунікація	Обмежено врахування, не є системною складовою навчальних планів підготовки	Недостатня практична орієнтація та навички оперативного антикризового реагування
Сертифікаційні орієнтири	Національна ініціатива США з освіти в галузі кібербезпеки (з англ. – National Initiative for Cybersecurity Education, NICE), ISC2, CEH, Міжнародна асоціація, що встановлює IT-стандарти та пропонує універсальні сертифікації та стандартизація програм і курсів у системі професійної освіти	Відсутність формалізації інтеграції	Ризики невідповідностей майбутніх фахівців вимогам реалізацій інформаційної безпеки за сферами призначення

Натомість в українських стандартах вищої освіти недостатньо чітко регламентовано вимоги до формування так званих м'яких навичок, які для реалізації інформаційної безпеки є не менш важливими, ніж інженерно-технічна та цифрова обізнаність. Уміння вести конструктивний діалог з уповноваженими органами технічного регулювання, визначати стратегії захисту інформаційних даних в умовах модернізації нормативної бази, координувати дії з іншими учасниками соціосистеми інформаційної та кібербезпеки, як структурні компоненти освітнього середовища професійної підготовки майбутніх фахівців [1.a.i.78, 1.a.i.111].

Узагальнюючи викладене, слід закцентувати увагу на необхідності багатовекторного оновлення українських моделей освітніх наукових систем,

підготовку кадрів. У даному контексті потрібно забезпечити впровадження таких змістових блоків навчання, що інтегрують інженерно-технічні знання з правовими, управлінськими та етичними аспектами, формуючи єдину логіку модернізації й удосконалення майбутніх фахівців. Важливим доповненням регламентовано створення механізмів постійного оновлення змісту освітніх програм відповідно з динамікою міжнародної безпеки інформаційно-технологічних середовищ електроніки, метрології та радіотелекомунікацій. Адаптацію можна здійснити лише за умов залучення різних стейкхолдерів (представників уповноважених державних органів, органів самоврядування бізнесу, державних інституцій, нагляду й контролю міжнародних партнерів і громадських установ), що покликані до спільного формування й забезпечення відповідності професійним стандартам освіти.

Результати компаративного аналізу дають підстави вважати, що гармонізація українських стандартів вищої освіти із вимогами соціальної турбулентності глобального виміру, має розглядатися не як ініціатива факультативного навчання, а як обов'язковий компонент державної стратегії освітньої політики, інформаційної й кібербезпеки, мобільність і конкурентоспроможність фахівців на міжнародному ринку праці й сприятиме зміцненню інституційної стійкості України перед сучасними викликами цифровізації суспільної діяльності.

Формування національної системи інформаційної безпеки неможливе без втілення міжнародно імплементованого підґрунтя правочинства, що визначає пріоритети державної політики захисту інформаційного простору зайнятості. Важливою передумовою є конституційно закріплені гарантії: окреслюють обсяг прав і свобод громадян, визначають відповідальність держави щодо захисту персональних інформаційних даних, підтримання кіберстійкості та охорони критичної інформаційної інфраструктури. Інтеграція положень Конституції в освітню політику, орієнтовану на підготовку майбутніх фахівців у галузі електроніки, метрології та радіотелекомунікацій набуває актуального значення.

Конституцією України обумовлено ідеологічний та правовий каркас для подальшої регламентації питань інформаційної безпеки, видів економічної/професійної й соціальної діяльності; регламентує норми гарантій прав і свобод громадян на інформаційну безпеку, встановлюють допустимі межі її реалізації в умовах загроз національному суверенітету, громадському порядку чи правам інших осіб. Зокрема, положення про недопустимість втручання в особисте життя (ст. 32), вимоги щодо конфіденційності інформації, право на доступ до публічної інформації (ст. 34), а також визначення інформаційної безпеки як складової національної безпеки (ст. 17) є право засадничими для формування галузевого законодавства [1.a.i.122]. Для майбутніх фахівців важливо усвідомлювати, що правовий статус інформації, включаючи персональні, технічні або службові дані, визначається не лише інформаційно-технологічними умовами її зберігання або передачі, але й конституційно гарантованими механізмами правового захисту та соціальних гарантій безпеки. Розуміння зазначеного дозволяє уникати технологічного редукціонізму – спрощеного сприйняття безпеки як виключно технічного завдання, позбавленого правових і гуманітарних вимірів в умовах соціальної турбулентності. Ключовим для організації освітньої, наукової й інноваційної діяльності є закріплення правочинних положень, що забезпечують баланс між правом на інформаційну свободу та необхідністю її обмеження в інтересах національної безпеки та стратегії інформаційної безпеки, стратегії інформаційної безпеки зокрема. Таким чином формується компетентнісний базис для професійної підготовки майбутніх фахівців, які повинні не лише оволодіти техніко-регуляторними засобами захисту, але й діяти у відповідності до конституційних принципів реалізації інформаційної безпеки. Поняття «інформаційна безпека» в національному правовому полі (як і згідно міжнародних підходів), охоплює ширший спектр безпекових питань етичної відповідальності, захист інформаційного суверенітету, дотримання прав людини в цифровому середовищі [1.a.i.123]. Отже, національне законодавство у сфері інформаційної безпеки має не лише інструментальне, але й ціннісне

значення для професійної підготовки висококваліфікованих фахівців; визначає ієрархію норм, відповідно до якої формуються освітні модулі, компетентнісні орієнтири стандартів професійної діяльності [1.a.i.109]. Інтеграція положень Конституції до вимог освітньої діяльності не має обмежуватися декларативним ознайомленням здобувачів освіти зі змістом, а має реалізовуватися шляхом включення до навчальних дисциплін кейсів правозастосування та технічного реалізування, аналізу професійних спорів у сфері захисту інформації, вивчення практики судочинства, а також компаративного аналізу відповідальності міжнародним нормам [1.a.i.164]. Лише за умови усвідомлення ролі конституційно-правових механізмів інформаційного захисту можливо сформувати покоління фахівців, здатних не лише впроваджувати інформаційно-комунікаційні й соціокультурні технології, але й забезпечувати відповідність професійної діяльності демократичним принципам безпеки, прав людини та вимогам управління безпекою інформаційних процесів суспільної діяльності. Саме в цьому полягає системоутворююча роль конституційного регулювання в освітній моделі, орієнтованій на підготовку висококваліфікованих кадрів, спроможних забезпечувати стійкість і безпеку інформаційного середовища держави на засадах права, гуманізму та професійної компетентності для забезпечення сталості розвитку.

Національне законодавство України, становить складну та багаторівневу систему нормативних актів, що визначають правові, організаційні та технічні засади захисту інформаційного простору держави [1.a.i.202]. Нормативно-правовий базис є важливим чинником і ресурсом для формування змістового наповнення освітніх програм, спрямованих на підготовку фахівців для реалізації інформаційної безпеки в галузі електроніки, метрології та радіотелекомунікацій [1.a.i.223]. Одним із базових правових актів, які встановлюють стратегічні орієнтири розвитку національної безпеки, де інформаційна безпека визначається як її невід'ємна складова законодавчого забезпечення, що формує рамки для оцінки ризиків, пов'язаних із цифровими загрозами, а також встановлює пріоритетні напрями державної політики в

умовах інформаційно-технологічної трансформації в умовах цифровізації суспільної діяльності [1.а.і.201].

Важливе значення має законодавче регулювання інформаційних відносин, яке охоплює визначення видів інформації, принципів доступу, захисту та обігу даних. Правове розмежування відкритої інформації та інформації з обмеженим доступом є критичним для формування у здобувачів освіти уявлення про режими конфіденційності та засоби правового реагування на порушення в цій сфері [1.а.і.199].

При проєктуванні інформаційно-телекомунікаційних систем із вбудованими механізмами дотримання норм правового й технічного регулювання, особливу увагу варто приділити законам, що регламентують їх функціонування, підлягає правовому захисту. Нормативні вимоги до створення і функціонування комплексних систем захисту інформації, а також механізми їх сертифікації й атестації становлять підґрунтя їх практики в галузі кіберзахисту об'єктів критичної інфраструктури [1.а.і.197]. Освітній процес професійної підготовки фахівців та аналітиків інформаційних баз має враховувати практичні компоненти, орієнтовані на оволодіння нормативними процедурами правочинства та технічної врегульованості.

Нині сучасний стан українського законодавства (у сфері інформаційної та зокрема кібербезпеки), відображає потреби оперативного реагування на глобальні загрози та зростаюче масштабування та складність інформаційних систем/мереж у цифровому середовища. Нормативні акти, що визначають порядок захисту критичної інфраструктури, розподіл повноважень між суб'єктами кібербезпеки та механізми реагування на інциденти, формують цілісну систему правил і стратегію інформаційної безпеки в Україні, що вимагає від фахівців не лише професійної інженерно-технічної підготовки, а й правової обізнаності. Тому освітні програми повинні поєднувати у змістовому наповненні інженерні знання з елементами правової аналітики. Майбутні фахівці повинні інтерпретувати повноваження й обов'язки держави, бізнесу та

громадян у сфері захисту інформації й реалізації стратегії політики інформаційної безпеки.

Законодавство суміжних галузей, а саме, електронних соціокультурних, інформаційно-телекомунікаційних, радіотелекомунікацій, метрології стандартизації й сертифікації ліцензування й акредитації, моніторингу, аудиту, експертизи та захисту персональних даних не менш вагоме. Вимоги до достовірності вимірювань у метрології, збереження цілісності переданих даних у телекомунікаціях, вони передбачають не лише технічні рішення, а й правові гарантії захисту в системі знань, тому повинні бути інтегровані в навчальні плани професійної підготовки майбутніх адміністраторів інформаційних систем, розробників і фахівців із контролю якості.

Варто виокремити закони, що регулюють режим доступу до конфіденційної інформації. Так, Закон України «Про державну таємницю» визначає процедури втаємничення – засекречення та розсекречення, а також правил роботи з інформаційними масивами даних для експертно – аналітичних завдань стратегічного значення для безпеки держави [1.а.і.196]. Знання правничих положень є обов'язковим для майбутніх фахівців, які працюватимуть з об'єктами обробки втаємничених даних, оскільки ті несуть безпосередню юридичну та соціальну відповідальність за реалізацію інформаційної безпеки.

Важливе значення Закону України «Про захист персональних даних», який встановлює правила обробки інформації, та дозволяє ідентифікувати особу [1.а.і.198]; регламентує порядок отримання згоди, доступу, зберігання та передачі персональних даних. Для фахівців, які працюють із базами інформаційних даних, інформаційними системами/мережами чи займаються аналітикою у сфері охорони здоров'я, фінансів або освіти, науки й інноватики дотримання норм захисту персональних даних є професійною необхідністю їх компетентності. Тому під час організації освітнього процесу, потрібно не лише навчити здобувачів освіти правилам роботи з конфіденційною інформацією, а й сформувати етичне ставлення до її захисту та розуміння юридичних наслідків

щодо її порушень. Актуальні практичні заняття, які враховують змодельовані ситуації витоку інформаційних даних, несанкціонованого доступу чи порушення режиму секретності з подальшим аналізом правових наслідків.

Для узагальнення основних положень законодавчих актів, що регулюють інформаційну безпеку та суміжні сфери, у роботі наведено в таблиці 1.12 характеристики її предмету регулювання та значення їх врахування у змісті та забезпеченні для професійної підготовки.

Інтеграція вищерозглянутих нормативних засад у архітектуру освітньо-наукової діяльності є запорукою для формування цілісної професійної ідентичності майбутніх фахівців.

Таблиця 1.12

Основні характеристики та значення інформаційної безпеки для професійної підготовки майбутніх фахівців у контексті Законів України

Закони України	Визначено предмет регулювання	Значення для професійної підготовки майбутніх фахівців
Про основи національної безпеки України	Визнання інформаційної безпеки як складової національної безпеки	Розуміння стратегічних викликів, усвідомлення ролі інформаційної безпеки у державному управлінні
Про інформацію	Класифікація видів інформації, доступ, обіг, обмеження доступу	Формування знань про режими конфіденційності, правову та соціальну відповідальність
Про захист інформації в інформаційно-телекомунікаційних системах	Технічні та правові вимоги до захисту інформації в ІТК-системах	Практичні навички та уміння щодо проєктування захищених систем, сертифікації та атестації
Про кібербезпеку України	Захист критичної інфраструктури, визначення суб'єктів кібербезпеки	Розуміння організації кіберсередовища, забезпечення й підтримка сервісів, взаємодія та управління інцидентами згідно нормативних вимог
Про електронні комунікації	Регулювання телекомунікаційних мереж, безперебійність зв'язку	Технічна та інформаційна компетентність у розбудові та захисті комунікаційних систем/мереж
Про метрологію та метрологічну діяльність	Вимоги до достовірності вимірювань та збереження цілісності й об'єктивності даних	Забезпечення точності та надійності даних у критичних точках середовищ та експертного оцінювання складових кризових ситуацій
Про захист персональних даних	Правовий режим обробки та захисту персональної інформації	Юридична грамотність у сфері конфіденційності, дотримання принципів GDPR

Про державну таємницю	Визначення категорій засекреченої інформації та порядку доступу	Формування професійної етики, роботи з обмеженим доступом, соціальна й правова відповідальність

Законодавчий базис виступає не лише джерелом унормування й правочинства обов'язкових вимог, але й як орієнтир для критичного креаційного мислення здобувачів освіти, що сприяє адаптації до трансформацій правового поля, впровадженню безпекових механізмів, законів й інструментів – також згідно до правових норм, і підтримці рівня правової культури у професійних середовищах зайнятості. Роль законодавства як інтегрального елементу системи підготовки компетентних, відповідальних та соціально свідомих фахівців для сфери інформаційної безпеки є беззаперечною [1.а.і.202].

У системі національного правового та технічного регулювання інформаційної безпеки важливе місце належить підзаконним нормативно-правовим актам, що визначають положення, закріплені в Законах України, і фактично є нормативно-правовими механізмами втілення державної політики національної безпеки та стратегій її складових (соціальної, інформаційної, екологічної, економічної, тощо); а також щодо питань захисту даних. Водночас зазначені документи здійснюють безпосередній вплив на організацію освітнього процесу, оскільки задають функціональні пріоритети в стандартизації підготовки майбутніх фахівців у галузі електроніки, метрології та радіотелекомунікацій [1.а.і.123].

Укази Президента України є інструментом утвердження державних стратегій і концепцій у сфері національної, загалом, та інформаційної безпеки, зокрема. У змісті указів визначено пріоритети державної політики щодо формування базові векторів розвитку кіберзахисту та окреслено роль відповідних суб'єктів, зокрема сфери освіти, науки й інноватики. Особливої уваги заслуговують укази, що вводять у дію рішення Ради національної безпеки і оборони України, оскільки вони мають обов'язкову силу впливу та стратегічне значення для формування освітньо-наукового змісту сучасних

наукових знань у контексті підготовки майбутніх і задіяних фахівців, здатних забезпечувати інформаційну стійкість і безпеку держави [1.а.і.223].

Постанови Кабінету Міністрів України відіграють системоутворюючу роль у нормативному правових механізмам реалізації інформаційної та кібербезпеки в державі та визначають правила практичного втілення заходів захисту інформації в державному секторі, регулюють процедури створення мереж систем захисту інформації, унормовують положення щодо забезпечення діяльності урядових уповноважених органів регулювання, визначають вимоги до формування й забезпечення безпекових завдань захисту й оборони критичної інфраструктури та механізми державного контролю та нагляду [1.а.і.197]. Правове й технічне справочинство регулює формування нормативної відповідності середовища, підготовки та зайнятості фахівців, і спонукає до набуття та розвитку в них компетентностей, які мають бути сформовані у змісті освітніх програм навчальних планів та окремих курсів і освітніх модулів.

Параметри ефективності організації освітнього процесу підготовки та розвитку фахівців визначає Міністерство освіти і науки України, що затверджує стандарти вищої освіти, кваліфікаційні вимоги та зміст і забезпечення освітніх програм для задоволення потреб згуртування інформаційної безпеки професійних і соціального середовищ зайнятості, ухвалено наказом [1.а.і.221], окреслюють коло повноважень органів державного регулювання процесу формування професійних компетентностей майбутніх фахівців.

Державна служба спеціального зв'язку та захисту інформації України, що розробляє технічні нормативи з питань криптографічного й технічного захисту інформації, здійснює атестацію забезпечення об'єктів, затверджує методики та порядки створення Комплексної системи захисту інформації (далі – КСЗІ) [1.а.і.168], її нормотворчі акти формують базис нарощення потенціалу спеціалізованих знань у сфері кіберзахисту.

Міністерство оборони України, Міністерство цифрової трансформації, а також інші органи виконавчої влади здійснюють справочинство регулювання функціональної специфіки формування інформаційної безпеки у відповідних

секторах економіки, опанування змісту регламентів забезпечує міжгалузеве бачення у майбутніх задіяних фахівців, що сприяє розвитку системного мислення при опануванні конкретно науковими знаннями. У контексті державного регулювання питання інформаційної безпеки регламентуються низкою нормативних актів, що розробляються та оприлюднюються ключовими інституціями, зокрема Міністерством оборони України, Міністерством цифрової трансформації, а також іншими уповноваженими органами виконавчої влади; зміст документів включає специфіку функціонування відповідних секторів економіки, визначає принципи, механізми та стандарти захисту інформаційного простору суспільної діяльності; ознайомлення з нормативними матеріалами усіх учасників освітнього процесу сприяє формуванню у майбутніх фахівців системного, міждисциплінарного підходу до системного аналізу безпекових викликів, активізує розвиток пізнавально-інтегративної діяльності здобувачів освіти та забезпечує гармонізацію й синергію взаємозв'язків між технологічними, правовими та організаційними аспектами забезпечення захисту інформації [1.а.і.157].

Для узагальнення та контент-аналізу ключових підзаконних актів у сфері інформаційної безпеки та розкриття їх в організації освітнього процесу професійної підготовки та розвитку майбутніх і задіяних фахівців, сформовано таблицю 1.13, для систематизації джерел регулювання та встановлення їх функціонального призначення та впливу на професійну підготовку кваліфікованих кадрів.

Визначальну нормотворчу роль технічного регулювання відіграють національні стандарти України – державні стандарти технічного управління (далі – ДСТУ), також у формуванні забезпеченні інформаційної безпеки; базуються на міжнародних нормах (зокрема ISO/IEC 27000) і забезпечують уніфікацію підходів до проєктування, впровадження та аудиту систем захисту даних; утверджують вимоги щодо оцінювання ризиків, розробки політик безпеки, застосування криптографічних засобів та процедур реагування на інциденти; застосування стандартів у організації освітнього процесу дає

підстави здобувати освіти, набути практичні навички та уміння й орієнтування на передові практики забезпечення.

Крім того, впровадження положень підзаконних актів в структуру освітніх програм дозволяє сформувати у здобувачів освіти цілісне розуміння вимог національного регулювання, що забезпечує відповідність здобутих компетентностей потребам держави й ринку праці.

Таблиця 1.13

Систематизація джерел регулювання та встановлення їх функціонального призначення і впливу на професійну підготовку фахівців для реалізації інформаційної безпеки

Джерело регулювання	Характеристика функціонального призначення	Роль у організації освітньо-наукової діяльності
Укази Президента України	Затвердження стратегій, введення в дію рішень Ради національної безпеки і оборони України	Орієнтація на пріоритети державної політики, формування стратегічного бачення у майбутніх і задіяних фахівців
Постанови Кабінету Міністрів України	Правила захисту інформації, вимоги до КСЗІ, регулювання захисту критичної інфраструктури	Формування нормативного регулювання поля професійної діяльності, практична орієнтація освітнього процесу
Накази МОН України	Стандарти освіти, кваліфікаційні вимоги до компетентності	Архітектура системи компетентностей, визначення змісту освітніх програм
Нормативні документи Держспецзв'язку	Технічні регламенти, методики, порядок створення КСЗІ	Забезпечення опанування та поглиблення професійних знань у сфері криптографії та технічного захисту
Документи Міністерства оборони України, Міністерства цифрової трансформації України тощо	Спеціальні вимоги до безпеки в секторах оборони, цифрової трансформації у державі	Формування міжгалузевого бачення, орієнтація на специфіку здійснення професійної діяльності
ДСТУ у сфері інформаційної безпеки	Адаптація ISO/IEC, вимоги до ризик-менеджменту, політик безпеки, аудиту	Прикладна професійна підготовка, імплементація міжнародних практик корисного досвіду стандартизації

Нині, нажаль, вплив законодавства України (у сфері кібербезпеки) на формування вимог до змісту й модернізації освітніх програм (та як наслідок на підготовку кадрів) потребує критичного оцінювання його ефективності. Адже в

умовах зростання кіберзагроз та інтенсивної цифрової трансформації, важливим є не стільки факт розроблення і формування при впровадженні законодавчих вимог, скільки їх уможливлення оперативного реагування на нові виклики цифровізації в умовах соціальної турбулентності. Тому актуальним завданням є системний аналіз чинної нормативної бази та її відповідності вимогам сучасного ринку праці та динамічного розвитку сфери електроніки, метрології та радіотелекомунікацій. Попри розробленість значного масиву нормативно-правових актів, виявляються невідповідності, що ускладнюють ефективну імплементацію їх положень у сферу вищої освіти, зокрема, та освіти, науки й інноватики, загалом. До основних чинників дисбалансу належать: гальмування оновлення регуляторного базису згідно поступу технологічного розвитку; фрагментованості правових обрисів забезпечення галузевих секторів економіки; відсутність в новій мері нормативної деталізації, необхідної для міждисциплінарної підготовки кадрів. Важливим завданням (як вже було вказано) є гармонізація українського законодавства згідно європейських аналогів правового регулювання стандартів, що сприяє повноцінній інтеграції України в цифровий простір ЄС.

Водночас чинна нормативна база відіграє позитивну роль: закладає у освітніх програмах змістове наповнення для формування базових знань про правові основи захисту даних, структуру кіберзагроз і вимоги до безпеки інформаційних мереж і систем. Проте, оновлення стандартів уповільнено, а регуляторні механізми залишаються обмежено лабільними. Тому заклади освіти втрачають темпи оперативної адаптації освітніх програм до нових реалій соціальної турбулентності. Якісна трансформація системи правочинства організації освітнього процесу потребує оновлення законодавчих засад регулювання. Варто забезпечити взаємодію між державними структурами, університетами, органами громадського самоврядування та бізнесом. Лише спільними зусиллями можливо сформувати безпечний освітній простір, який буде відповідати сучасним викликам інформаційної безпеки та сприятиме зміцненню технологічної стійкості держави. У галузі електроніки, метрології та

радіотелекомунікацій актуальність питань нормативно-правового забезпечення постає гостро, адже галузь знань безпосередньо пов'язана зі забезпеченням кадрами потреб формування критичною інфраструктури. Тому якість підготовки кадрів має означати не лише академічну успішність здобувачів освіти, а й реальні гарантії спроможності кадрового потенціалу забезпечення кіберстійкості та національної безпеки держави.

У межах спеціальності 015 «Професійна освіта (за спеціалізаціями)» згідно Стандарту вищої освіти перший (бакалаврський) рівень, галузь знань 01 «Освіта / Педагогіка», затвердженого наказом Міністерства освіти і науки України від 21.11.2019 р. № 1460 [1.a.i.220] є спеціалізації 015.39«Цифрові технології» та 015.32 «Електроніка, метрологія та радіотелекомунікації», які орієнтовано на професійну підготовку майбутніх педагогів професійного навчання для закладів професійної (професійно-технічної освіти) з орієнтиром на застосування сучасних ІКТ під час організації освітнього процесу та організаційно-управлінської діяльності.

До прикладу, спеціальності галузі 12 «Інформаційні технології», зокрема 125 «Кібербезпека та захист інформації» та 126 «Інформаційні системи і технології», згідно стандартів вищої освіти передбачають поглиблену підготовку майбутніх фахівців у питаннях захисту інформації, застосування криптографічних методів шифрування та дешифрування, управління ризиками та небезпеками, аудитів здійснення інформаційної безпеки, технічного і правового забезпечення кіберзахисту усіх видів економічної діяльності, вимоги, що логічно корелюють із міжнародними нормативами, такими як ISO/IEC 27001, а також з європейськими рамками компетентностей у сфері інформаційної безпеки.

У структурі освітніх стандартів акцентовано увагу на переліку компетентностей, які мають бути сформовані у випускників. Йдеться не лише про загальні когнітивні, соціальні чи аналітичні якості, але й про фахові компетентності, які, в ідеалі, мають включати вміння розпізнавати, моделювати та нейтралізувати інформаційні ризики в контексті спеціалізованих

інформаційно-технічних систем і мереж. Для фахівців галузі знань електроніки це може означати здатність до створення безпечної архітектури системи процесно-апаратного забезпечення, обладнання пристроїв, для радіотелекомунікацій – уміння гарантувати стійкість каналів передачі даних до несанкціонованого втручання, а для метрології – захист точності та достовірності параметральної метрики оцінювання інформації від несанкціонованих впливів, які порушують її цілісність, а для майбутніх фахівців сфери освіта/педагогіка –сформованість професійної компетентності до реалізації інформаційної безпеки у професійних середовищах зайнятості.

Запорукою досягнення орієнтирів якості освітніх програм та їх релевантності у контексті реалізації інформаційної безпеки є інтенсивність динаміки національних стандартів узгодження з міжнародними директивами NICE Cybersecurity Workforce Framework (з англ. – інструкції, розроблені, щоб допомогти організаціям оцінити та покращити , здатність запобігати, виявляти та реагувати на ризики кібербезпеки) рекомендацій Міжнародного союзу електрозв'язку (ITU) [1.a.i.275, 1.a.i.276]. Компаративістика рамок, уможливлює оцінювання, наскільки система підготовки фахівців в Україні відповідає вимогам глобального виміру, що дозволяє виявленню сильних та слабких сторін національних моделей і розуміння потреб випускників чи отримують ті знання, вміння та навички, які забезпечують їм конкурентну перевагу на міжнародному ринку праці для реалізації інформаційної безпеки в галузі електроніки, метрології та радіотелекомуцікацій.

Особливої ваги набуває зміст необхідність удосконалення навчальних планів, включення курсів, що охоплюють правові техніко-регулятивні, організаційно-управлінські аспекти захисту персональних даних, управління ризиками, принципи безпечного програмування та проектування алгоритмів реагування на кібер-інциденти, що свідчить про прагнення закладів освіти не лише слідувати трендам, а й забезпечувати модернізацію систем професій на її підготовки фахівців, здатних діяти в складно, динамічному організованому цифровому середовищі, завдяки інженерно технічній компетентності,

розумінню етичних, правових і стратегічних викликів, що постають перед сучасними професіоналами для реалізації інформаційної безпеки.

Аналіз навчальних планів демонструє, що більшість спеціальностей інженерно-педагогічного профілю хоч і мають дисципліни з елементами в модулях інформаційної безпеки, проте їх зміст за часту лімітується розлогим оглядом проблематики для ознайомлення здобувачів освіти. Необхідно в першу чергу системно актуалізувати тактику пріоритетних напрямів присвячену глобальним загрозам соціальної турбулентності. Практичні освітні модулі здебільшого не демонструють реальних сценаріїв та механізмів передбачення, запобігання та усунення кібератак чи прикладів невідповідностей та ризиків вразливості технічних систем. У метрології, зокрема, ще відсутні практичні заходи, які регламентують цифровий аудит вимірювального обладнання, його верифікації та розроблення механізмів перевірки, валідації та достовірності інформаційних даних у цифровому середовищі.

Практична складова підготовки майбутніх фахівців для реалізації інформаційної безпеки стикається з низкою бар'єрів системних обмежень, які суттєво впливають на якість організації освітнього процесу. Однією з визначних проблем залишається недостатня повноцінність, відповідність стандартам матеріально-технічного та інформаційно-технологічного оснащення закладів освіти: сучасне обладнання, необхідне для моделювання реальних кіберзагроз і відпрацювання сценаріїв прогностики, моделювання та управління. За часту застаріло, або відсутнє у апробованих процедурах адміністрування. Крім того, бракує міждисциплінарного освітнього технічно обґрунтованого базису, що б дозволило інтегрувати інженерно-технічні, правові, технологічні та організаційно-управлінські засоби кібербезпеки в єдину освітню програму професійної підготовки майбутніх фахівців галузі електроніки, метрології та радіотелекомунікацій. Відсутність симуляційних моделей кіберінфраструктур, наближених до реальних умов, обмежує

можливості реалізації інформаційної безпеки формування практичних навичок та вмінь у здобувачів освіти, необхідних у професійній діяльності.

Окремої уваги заслуговує питання формування кадрового резерву для забезпечення викладання в галузі знань (електроніки, метрології та радіотелекомунікацій), що потребує залучення фахівців, які володіють не лише сучасними науковими знаннями, а й мають практичний досвід роботи з ІТ-системами, захисту аудиту та організації забезпечення адміністрування інформаційної безпеки з оперативним реагуванням на інциденти. Проте визнаних професіоналів складно інтегрувати в освітній процес підготовки майбутніх фахівцівбез створення належних умов — зокрема, кадрової ротації з систематичним підвищенням кваліфікації, налагодження партнерства із бізнесом, а також впровадження дуальної моделі освіти, яка поєднує академічне навчання з практикою в установах та на підприємствах відповідних середовищ інформаційної зайнятості.

Нормативно-правова та техніко-регулятивна база в Україні хоча формально і передбачає можливості модернізації підготовки кадрів для організації забезпечення кібербезпеки, її практична реалізація потребує модернізації та удосконалення змісту освітніх програм. Йдеться не лише про розроблення та впровадження спеціалізованих курсів для різних рівнів навчання, а й про забезпечення їх міждисциплінарності – зокрема, між інженерно-технічними, інформаційно-технологічними правовими дисциплінами та аспектами захисту даних та їх адміністрування, регулювання цифрових невідповідностей у ризиках і забезпечення цифрової етики в кіберпросторі. Важливо також адаптувати моделі, підготовки та професійного розвитку фахівців до реалій цифровізації, як середовища навчання, так і зайнятості де інтенсивність змін і складність викликів вимагають гнучкості, та оперативності практичної орієнтації у забезпеченні відповідності вимогам якості й безпеки.

Для систематизації ключових характеристик освітніх програм у контексті реалізації інформаційної безпеки майбутніми фахівцями для галузі електроніки,

метрології та радіотелекомунікацій представлено узагальнені дані (таблиця 1.14), що відображають основні нормативні орієнтири та акценти компетентностей в тому числі практичні виклики, що постають перед установами освіти в процесі професійної підготовки майбутніх фахівців.

Нормативно встановлено вимоги до освітніх програм і релевантних результатів компетентностей майбутніх фахівців у галузі електроніки, метрології та радіотелекомунікацій, інтегровані зі складовими компонентами реалізації інформаційної безпеки у професійних середовищах, визначають стратегічний інструментарій для формування забезпечення потенціалу систем вищої освіти адекватно відповідати викликам цифровізації епохи суспільних видів діяльності.

Таблиця 1.14

Контент-аналіз освітніх програм у контексті реалізації інформаційної безпеки майбутніми фахівцями для галузі електроніки, метрології та радіотелекомунікацій

Спеціальність/освітня програма/спеціалізація	Компетентнісні складові	Ідентифіковані виклики
Професійна освіта (Цифрові технології)	Використання ІКТ, спеціалізоване програмного забезпечення з метою інтеграції в освітнє середовище	Обмежений контекст реалізації інформаційної безпеки, потреба у міждисциплінарній інтеграції компонентів інформаційної безпеки
Кібербезпека	Управління ризиками, криптографія, аудит, правове регулювання	Недостатня міждисциплінарність, кадрові та технічні обмеження
Електроніка	Створення безпечної архітектури пристроїв, надійність апаратних компонентів	Потреба в інтеграції компонентів інформаційної безпеки, слабка практична підготовка
Телекомунікації та радіотехніка	Захист каналів передачі, стійкість мереж, протоколи безпеки	Відсутність актуалізованих дисциплін з інформаційної безпеки, брак інфраструктури для практик
Метрологія та вимірювальна техніка	Цифровий аудит, автентифікація даних, верифікація точності у цифрових системах	Низька інтеграція з кібербезпекою, обмежена експертиза
Інформаційні системи і технології	Проєктування ІТ-систем з вбудованими засобами	Оглядовий характер дисциплін у контексті інформаційної безпеки,

	безпеки	нестача фахівців зі змішаними/ перехресними компетенціями

Деталізовано освітні цілі, навчальні результати, в тому числі набір загальних спеціальних та міждисциплінарних компетентностей, які покликана забезпечити професійна підготовка майбутніх фахівців галузі, здатних до фахових дій в умовах багатофакторної інформаційної загрози.

Отже, зміст освітніх програм, орієнтовано на зазначені складові галузі знань, має включати структуровану сукупність дисциплін, що охоплюють як фундаментальні основи інформаційної безпеки, так і спеціалізовані галузеві напрями її забезпечення. Формування теоретичного підґрунтя забезпечується через вивчення основ криптографії, системної безпеки, моделювання загроз, а також проектування й управління в архітектурі захищену інформаційно-комунікаційних та радіотелекомунікаційних систем. Теоретичний компонент підготовки має бути тісно пов'язаний із поглибленим опрацюванням аспектів кіберзахисту, релевантних до семантики складових галузі зокрема: для електроніки — безпека процесно-апаратного забезпечення, для метрології — захист даних параметральної метрики вимірювань якості й безпеки, для радіотелекомунікацій –безпека передавання та обробки сигналу сприйнятного користувачами формату з врахування особливостей категорії сфери соціального захисту.

Засвоєння нормативно-правових засад для реалізації інформаційної безпеки є важливим елементом сучасних освітніх програм. Здобувачі освіти мають не лише ознайомитися з національним законодавством України (законами про кібербезпеку, захист персональних даних, проектування функціонування, прогнозування й моделювання стану й розвитку інформаційних систем і мереж),а й розуміти міжнародний контекст інтеграції у питаннях організації й забезпечення інформаційної безпеки. Йдеться про регламенти та директиви ЄС (зокрема GDPR і NIS Directive), міжнародні стандарти ISO/IEC 27000-ї серії, а також рекомендації Міжнародного союзу електрозв'язку (ITU). Завдяки цьому формується цілісне уявлення системи

вимог до організації систем безпеки даних та принципи технічного регулювання на основі безперервної й стійкої роботи за цільовим призначенням потреб споживачів.

Пріоритетною складовою є практика; що має не обмежуватися теоретичним відтворенням професійних знань, умінь та навичок, а й бути максимально наближеною до реальних умов професійної й соціальної зайнятості. Здобувачі освіти під час лабораторних занять в інституційних умовах ЗВО та у професійних/ виробничих умовах опановують здатності до створення та тестування захисту систем, беруть участь в аудитах, готують курсові й дипломні роботи/проєкти з інтеграцією засобів безпеки в прикладні інженерно-технологічні рішення. Виробнича практика на підприємствах, де організовано захист професійних інформаційних середовищ, уможливлює апробацію небезпеки і фахове становлення майбутніх фахівців за практичним застосуванням набутих знань та досвіду реагування на конкретні ризики.

У результаті майбутні фахівці повинні не лише орієнтуватися в законодавчих нормах і технічних стандартах регулювання галузі знань та професійної сфери, мають вміти визначати інформаційні й інші загрози безпеці, аналізувати чинники впливу їх причини, проектувати механізми та системи захисту й забезпечувати їх відповідність (систем) чинним вимогам, що забезпечить їх готовність до реальних умов професійної зайнятості в майбутньому. Особлива увага приділяється формуванню комплексу вмінь працювати із процесно-апаратними засобами інформаційно й криптографічного захисту, системами, мережами нагляду за доступом, регламентами процедур управління безпекою, а також досягненню здатності до оперативного реагування на інциденти, аналізу кіберподій і реалізації заходів безпеки щодо відновлення порушених функціоналу систем і мереж в галузі електроніки метрології та радіотелекомунікації. Складовим компонентом професійного профілю є сформованість правової, цифрової, інформаційної та управлінської грамотності в контексті дотримання норм національного та міжнародного регулювання якості й безпеки. Випускники ЗВО, мають не лише оволодіти

вимогами відповідних актів, а й уміти їх інтерпретувати та застосовувати на практиці у професійній діяльності згідно посадових обов'язків, зокрема при оцінюванні ризиків зламу, розробці стратегій і планів політики інформаційної безпеки, а також у процесах ліцензування сертифікації послуг. Важливим є формування здатності до системного аналізу якості й безпеки складових і систем/мереж зв'язку й комунікацій – інтегрування технічного, організаційного та правових гарантій соціального виміру безпеки в умовах єдиної управлінської концепції та стратегії реалізації.

Комунікативна компонента, критичне, аналітичне та креаційне мислення, здатність до прийняття відповідальних організаційно-управлінських рішень у організації підготовки та неперервного професійного розвитку визначаються як ключові надфахові складові професійної компетентності, які забезпечують майбутніх фахівців не лише ефективну командну взаємодію, але й готовність, адаптації в умовах інтенсивної технологічної динаміки процесів у розбудові архітектури систем/мереж для реалізації інформаційної безпеки у галузі електроніки, метрології та радіотелекомунікацій, змін законодавства, появи нових типів загроз в умовах соціальної турбулентності. Система професійної підготовки має передбачати розвиток навичок шляхом залучення здобувачів освіти до міждисциплінарних проєктів дослідництва, соціальної згуртованості та інноватики, кейс-стаді, дипломатії дебатів і дискурсів симуляційних вправ, тренінгів що моделюють передбачення, усунення та запобігання кібер-інцидентів .

Відповідно до вищезазначених вимог до компетентностей, логічним продовженням є структурно-логічна та структурно-функціональна організація освітнього процесу професійної підготовки майбутніх фахівців на основі навчальних планів та освітньо-професійних програм, що системно інтегрують міжгалузеві та спеціальні знання з інформаційної безпеки у системі неперервної освіти здобувачів. У цьому контексті навчальні плани є інструментом нормативного структурування освітнього процесу, задаючи обсяг, послідовність і логіку формування знань, умінь та навичок, а також

врегульовують баланс між теоретичним вивченням, практичною підготовкою та науковим опрацюванням проблем реалізації інформаційної безпеки в Україні та світі.

Особливе значення має нарощення методологічного забезпечення нормативних дисциплін, що формують базис професійної підготовки майбутніх фахівців для реалізації інформаційної безпеки у професійних середовищах зайнятості за призначенням галузі та охоплюють теоретичні знання щодо принципів захисту даних, інформаційних та криптографічних методів, мережеві протоколи процедур організації й адміністрування безпеки, моделі антикризового управління ризиками та технології проєктування систем реалізації інформаційної безпеки. В тому числі мають бути розроблено галузевоорієнтовані спеціальні курси згідно потреб захисту критично важливих інформаційних об'єктів у галузі електроніки, метрології та радіотелекомунікацій, з урахуванням інженерно-технічної специфіки та чинників загроз, притаманних відповідним секторам економіки за видами професійної діяльності майбутніх фахівців.

Встановлено, що сучасні освітні програми повинні мати модульну оструктуреність, що дає змогу поєднувати обов'язкові та вибіркові освітні компоненти, поглиблюючи індивідуальні освітні траєкторії підготовки здобувачів освіти. З огляду на це, програми кожної дисципліни мають бути концептуально узгодженими зі стандартами вищої освіти, інтегрувати положення вітчизняного законодавства, а також міжнародних нормативних актів, що регулюють інформаційну безпеку, кіберзахист та захист персональних даних. Приналежно, акцент на практичну складову освітнього процесу передбачає включення лабораторних модулів, тренінгових занять, участі у розробленні командних проєктів, воркшопів та навчальних симуляцій і тренінгів, які дають змогу здобувачам освіти не лише теоретично засвоїти матеріал, а й відпрацювати алгоритми прийняття організаційно-управлінських рішень у проблемних ситуаціях передбачення, усунення й запобігання інцидентів інформаційної безпеки, системного аналізу вразливостей і

невідповідностей у забезпеченні кіберстійкості систем. Вбачається, що завдяки системному адмініструванню впровадження стратегії інформаційної безпеки досягається формування інтегрованої спроможності об'єктів інформаційного захисту при дотриманні відповідності нормам правового й технічного регулювання в умовах міжгалузевої взаємодії.

Ефективність реалізації навчальних планів і освітніх програм, орієнтованих на сферу інформаційної безпеки неможлива без постійного оновлення науково-методичного супроводу інформаційно-технологічного забезпечення, що мають узгоджуватися з актуальними змінами у нормативно-правовому базисі та перспектив і тенденцій прогнозування й моделювання науково-технічного розвитку суспільства в умовах цифровізації. Освітній процес потребує не лише формального дотримання стандартів, а й гнучкої адаптації до нових викликів, що виникають у цифровому середовищі в умовах модернізації освітньо-наукових систем та міжнародної імплементації правочинства. Саме тому особливої ваги набуває залучення до організації освітнього процесу фахівців-практиків, методологів-дослідників, бізнесменів та політиків, які мають практично-корисний досвід роботи з реальними кіберзагрозами на рівнях організації та управління якістю й безпекою систем у напрямах функціоналу семантики, володіють сучасними інструментами системного аналізу ризиків та здатні передати студентам не лише знання, а й професійну інтуїцію і сформувати їх спроможність.

Інтеграція міждисциплінарних кейсів, що поєднують технічні, правові та управлінські аспекти, а також впровадження мобільного проєктного навчання (м-навчання), створюють умови для формування майбутніх фахівців, здатних діяти в умовах соціальної турбулентності та невизначеності, оперативно адаптуватися до змін цифровізації суспільної діяльності і відповідати принципам і вимогам професійного розвитку та стійкості у проблемних і складних ситуаціях, в разі майже щоденного еволюціонування кіберзагроз. Такий підхід дає змогу не лише розвивати технічні навички, а й формувати

стратегічне мислення, здатність до командної роботи, критичного аналізу та прийняття рішень у динамічно плинних цифрових середовищах зайнятості.

У цьому контексті навчальні плани та дисципліни, що мають забезпечити на формування комплексної професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у галузі електроніки, мерології та радіотелекомунікацій. Модернізація професійної підготовки забезпечує готовність до розв'язання складних завдань у сфері захисту інформації, де технічна грамотність має доповнюватися розумінням правових норм, етичних принципів і стратегічних підходів до управління ризиками в умовах постійної інформаційно-технологічної динаміки суспільної діяльності.

Система ліцензування та акредитації освітньої, науково-технічної та науково-дослідницької, інноваційної видів діяльності в Україні є інструментом державного технічного регулювання якості й безпеки вищої освіти, що спрямовано на забезпечення відповідності організації освітнього процесу встановленим стандартам і критеріям параметральної метрики вимірювань їх рівня забезпечення у системах (управління, підготовки, розвитку як у закладах освіти й науки, так і в уповноважених інституцій). Її значущість особливо зростає у контексті підготовки майбутніх фахівців у галузях, що потребують високого рівня забезпечення формування інженерно-технічної, організаційно-управлінської, адміністративної, інформаційно-аналітичної, моніторингової цифрової, кваліталогічної й безпекової складових професійної компетентності, зокрема для реалізації інформаційної безпеки у галузі електроніки, метрології та радіотелекомунікацій. Ефективність забезпечення механізмів ліцензування та акредитації, стандартизації та сертифікації є запорукою підготовки висококваліфікованих і конкурентоспроможних кадрів, здатних відповідати на виклики цифрової доби та інформаційно-технологічного розвитку суспільства. Згідно процедур технічного регулювання ЗВО зобов'язані дотримуватися низки вимог, які охоплюють ключові складові навчально-науково-пізнавальної учасників освітнього процесу, зокрема, важливого значення набуває кадрове забезпечення, що передбачає дотримання відповідності кваліфікаційних

характеристик науково-педагогічного персоналу, наявність наукових ступенів і вчених звань, а також відповідність міжнародним рамкам кваліфікації фахівців і викладачів професійним стандартам у набутому практичному досвіді, особливо для реалізації інформаційної безпеки систем і мереж як у професійній підготовці та розвитку майбутніх і задіяних фахівців, так і в архітектоніці сфер, галузей професійної й соціальної зайнятості.

Панівні позиції практиків-професіоналів актуалізують важливість матеріально-технічної бази, що охоплює цілісність інформаційно-технологічного забезпечення інфраструктуру освітнього процесу, а наявність спеціалізованих проблемних навчальних, науково-дослідних, науково-виробничих випробувальних лабораторій, сучасного технічного й вимірювального обладнання, а також доступ до ліцензованого програмного супроводу, що відповідає профілю освітньої програми, зокрема осцилографи, генератори сигналів, калібрувальна апаратура, засоби для криптографічного захисту та стенди для моделювання кібератак, а запорукою формування практичних навичок майбутніх фахівців, здатних ефективно працювати у професійному середовищі зайнятості та запобігати ризикам інформаційної безпеки.

Складовою системної організації та управління якістю постає навчально-методичний органайзер освітнього процесу, що включає розробку і впровадження актуальних навчальних планів та освітніх програм, адаптованих до сучасних вимог ринку праці та інноваційних змін відповідної галузі знань та сфер працевлаштування. Відповідний рівень методичної підтримки (наявність підручників, посібників, вказівок до практичних і лабораторних занять, підготовки курсових і дипломних робіт/проєктів) сприяє формуванню цілісності, наступності й неперервності освітнього простору, завдяки яким здобувачі освіти опановують вимоги як теоретичної, так і практичної підготовки, а функціонування внутрішніх систем управління якістю й безпекою освітнього простору дозволяє здійснювати об’єктивний контроль за

релевантністю навчання й оперативно коригувати виявлені невідповідності вимогам стандартів.

Формування професійної спроможності здобувачів вищої освіти неможливе без організації системної практичної підготовки, що є не лише етапом закріплення теоретичних знань, а й механізмом інтеграції, адаптації та становлення цифровізації суспільної діяльності в реальних умовах функціонування об'єктів і суб'єктів в реалізації інформаційної безпеки у професійних середовищах. У сучасних умовах це досягається через стратегічне партнерство міжінституційної співпраці університетів та виробничими галузевими структурами, органами влади й самоврядування, що забезпечують організацію виробничих, навчальних, технологічних та переддипломних практиктичного навчання здобувачів. Міжінституційна співпраця дозволяє студентам не просто ознайомитися з івиробничими, метрологічними, радіотелекомунікаційними, інформаційними процесами, а й набути компетенцій, релевантних до актуальних викликів інформаційної безпеки в умовах цифровізації суспільної діяльності.

Особливої ваги у формуванні майбутніх фахівців набуває практична підготовка у реалізації інформаційної безпеки у професійній діяльності, де ефективність працівників визначається здатністю до аналітичного та критичного мислення, прогнозування ризиків та спроможністю з розробки превентивних заходів протидії кіберзагрозам. Поєднання опанування когнітивним потенціалом академічної бази з практичним досвідом індустрії у галузі електроніки, метрології та радіотелекомунікацій забезпечують сформованість у компетентних професіоналів, здатностей діяти в умовах високої технологічної та соціальної турбулентності.

У цьому контексті акредитація освітніх програм, що підтверджується Національним агентством із забезпечення якості вищої освіти, виконує не лише наглядову регуляторну функцію, а й слугує індикатором довіри до якості й безпеки організації освітнього процесу, а також підтверджує відповідність програм державним стандартам, легітимізує освітню діяльність і підвищує

рівень переконаності здобувачів освіти та роботодавців щодо якості підготовки майбутніх фахівців. Залучення незалежних експертів до процесу визначення відповідності забезпечення об'єктивність оцінювання та сприяє глибокому аналізу змісту програм з метою модернізації та удосконалення у закладах освіти. Оприлюднення результатів акредитації посилює прозорість освітньо-наукових систем ЗВО, формує механізми громадського нагляду та академічної підзвітності.

Водночас ліцензування та акредитація враховують запити ринку праці, що дозволяють коригувати навчальні плани та освітні програми до реальних соціально-економічних і інформаційно-технологічних потреб, що особливо актуально у контексті забезпечення кібербезпеки як критичного чинника стратегії національної безпеки в умовах воєнного стану. Зростання системності інформаційних загроз та необхідність убезпечення критичної інфраструктури життєзабезпечення суспільної діяльності вимагають від освітніх програм оперативної гнучкості, портативності та здатності до ефективного реагування.

Таким чином, система ліцензування та акредитації відіграє багатофункціональну роль: синергії державного регулювання, академічної відповідальності і професійної релевантності у створенні базису для інтеграції вищої освіти України у глобальний і європейський освітній простір, що забезпечує її здатність до ефективної адаптації в умовах цифровізації суспільної діяльності (табл.1.15).

Регламентація освітньо-наукової та інноваційної діяльності спирається на чинні національні правові акти, насамперед на Положення про проведення практики студентів закладів вищої освіти України, що ухвалено Міністерством освіти і науки України, а також на внутрішні установчі та адміністративні документи університетів, які враховують галузеву специфіку та особливості впровадження сучасних освітніх програм.

Організація практичного навчання передбачає класифікацію за її видами (навчальні, виробничі, технологічні, переддипломна, та стажування), визначення змістових і часових складових у навантаженні, постановку цілей і

завдань, а також механізми контролю й оцінювання релевантності набутих активів. Для реалізації інформаційної безпеки у професійному середовищі під час виробничої та переддипломної практики студенти мають змогу апробувати здатності роботи з інформаційними системами/мережами, вивчати методики та процедури виявлення та усунення вразливостей, застосовувати методи та засоби захисту, брати участь у реагуванні на кібер-інциденти. Програми практик формуються з урахуванням фахових/професійних компетентностей, затверджених у відповідних освітніх стандартах, та згідно тенденцій ринку праці, що дозволяє забезпечити релевантність практичної підготовки та сприяти професійній адаптації та становленню майбутніх фахівців.

Таблиця 1.15

Критерії забезпечення якості освітніх програм у контексті реалізації інформаційної безпеки та їх значення для підготовки фахівців

Критерій	Змістовне наповнення	Значення для підготовки фахівців
Кадрове забезпечення	Кваліфікація викладачів, наявність ступенів, вчених звань та їх міжнародна сертифікація (CISSP, CEH тощо)	Гарантії відповідного рівня якості викладання, дотримання сучасних стандартів інформаційної безпеки
Матеріально-технічна база	Лабораторне та полігонне забезпечення, криптографічне та вимірювальне процесно-апаратне та випробувальне обладнання, устаткування кіберстендів, програмне забезпечення	Формування практичних навичок, умінь, здатностей, змодельоване середовище проблемних і складних ситуацій, виникнення, усунення та запобігання кібер-інцидентів
Науково- та навчально-методичне забезпечення	Навчальні плани, освітні програми, актуальні дисципліни, підручники, методичні вказівки	Системність, неперервність, наскрізність підготовки, відповідність потребам якості та безпеки цифровізації ринків праці
Практична складова навчання	Партнерство з державними, уповноваженими й громадськими органами реалізації інформаційної безпеки, бізнес-структурами, підприємствами, технологічні виробничі практики	Індустріально-технологічна орієнтація становлення, набуття досвіду в реальному безпековому контексті професійної соціальної зайнятості
Внутрішні системи управління якістю	Контроль результатів, корекція освітнього процесу, план поліпшення як відповідь на	Підвищення ефективності освітньої траєкторії, адаптивність до викликів

й безпекою систем/мереж	виявлені недоліки	
Акредитація освітніх програм	Зовнішнє оцінювання, участь незалежних експертів, оприлюднення результатів, доступ громадськості	Підвищення прозорості, довіра здобувачів освіти та працедавців, відповідність державним і міжнародним стандартам

Вимоги до організації та забезпечення баз практик визначаються не лише формальними ознаками відповідності профілю підготовки, а й інституційною здатністю зі забезпечення відповідного рівня управлінської технічної та соціальної підтримки освітнього процесу. До баз практики висуваються кваліфікаційні критерії, серед яких наявність відповідної матеріально-технічної інформаційно-технологічної, моніторингової інфраструктури, сучасного програмного забезпечення, доступу до наявних інформаційних систем/мереж з високим рівнем захисту, а також досвід практичної реалізації інформаційної безпеки у галузі електроніки, метрології та радіотелекомунікацій. Важливою запорукою є кваліфікований склад кадрового потенціалу підприємств та установ: наявність фахівців і професіоналів відповідної галузі, здатних виконувати функції наставників, тренерів, коучів зі набуття професійного зростання і здійснювати на практиці консалтингово-дорадчу діяльність для студентів, забезпечувати безпечні умови праці та дотримувати конфіденційності, формувати практичні навички організації та адміністрування доступом, що також входять до обов'язкових умов наставництва.

Ефективність практичної підготовки значною мірою залежить від якості взаємодії між закладами освіти, установами та підприємствами-замовниками кадрів. Співпраця реалізується шляхом укладання офіційних угод, що регламентують права й обов'язки сторін, а також узгодження програм практик, що мають бути змістовно інтегрованими до виробничого контексту. Аксіологічне значення має залучення практиків до організації та забезпечення освітнього процесу неперервної підготовки фахівців згідно соціального замовлення через участь у розробці навчальних матеріалів, проведення гостьових лекцій, наставництво при виконанні курсових та дипломних

робіт/проєктів, що дозволяє не лише покращити прикладне спрямування підготовки, а й сформувати у здобувачів освіти реалістичне уявлення щодо власної відповідності вимогам професійного середовища та очікуванням працедавців.

Систематичний зворотний зв'язок від установ і підприємств-партнерів є індикатором ефективності організації практичної підготовки майбутніх фахівців. Оцінювання рівня сформованості професійної компетентності до реалізації інформаційної безпеки при підготовці майбутніх фахівців під час практики дозволяє ЗВО оперативно коригувати змістове наповнення і методику організації викладання, адаптувати освітні програми до змін професійних середовищ, мінімізувати розрив між академічною освітою, наукою та інноватикою та реальними умовами й вимогами професійної зайнятості в галузі електроніки, метрології та радіотелекомунікацій.

Поряд із регламентацією загальних принципів до визначених завдань вагомим вважаємо наповнення програм підвищення кваліфікації перекваліфікації та здобуття дотичних, перехресних кваліфікацій актуального змісту, відповідали б сучасним викликам інформаційної безпеки систем/мереж та інтенсивним технологічним змінам у профільних секторах економіки. Післядипломна освіта має виходити за межі простого оновлення базових наукових знань, орієнтуватись на оволодіння сучасними інформаційними, комунікаційними, соціокультурними технологіями, засобами системного аналізу кібер-інцидентів та методами забезпечення стійкості критичних об'єктів інфраструктури у галузі електроніки, метрології та радіотелекомунікацій. Дедалі більшого значення набувають гнучкі освітні формати організації освітнього процесу. Короткострокові курси та модулі інтенсивної підготовки, мобільного, дистанційного чи змішаного навчання, дозволяють охопити розлогий спектр різночинних категорій слухачів (від новачків до досвідчених інженерів, науковців, педагогів і представників державного сектору). Важливо, щоб програми не обмежувалися передачею знань, а й забезпечували формування архітектури здатностей у професійній

компетентності майбутніх і задіяних фахівців, в тому числі викладачів, і бажання до самостійного професійного розвитку, оцінки ризиків та ухвалення організаційно-управлінських інституційних рішень ЗВО у ситуаціях невизначеності.

Окремої уваги потребує впровадження незалежних механізмів оцінки якості підвищення кваліфікації та перепідготовки. Йдеться про зовнішню сертифікацію результатів навчання, практичне тестування набутих компетентностей і прозору систему надання права на діяльність ліцензування та встановлення відповідності в акредитації суб'єктів освітньо-наукової діяльності. Застосування зазначеного інструментарію підвищує довіру до системи професійного розвитку, сприяють соціальній і академічній мобільності кадрів і забезпечують доступ до міжнародного ринку праці.

Встановлено, що у галузі електроніки, метрології та радіотелекомунікацій, де цифровізація безпосередньо поєднана з вимогами інформаційної безпеки та кіберстійкості, адже забезпечення якості у системі неперервної підготовки та підвищення кваліфікації фахівців сфери освіти, науки й інноватики стає ключовим механізмом адаптації, становлення та професійного зростання фахівців. Інституційна спроможність професійних середовищ можлива лише за умов реалізації послідовної державної політики, що спирається на міцну нормативно-правову базу та міжгалузеву співпрацю міжсекторального управління якістю й безпекою систем/мереж. Нормативне регулювання удосконалення процесів підвищення кваліфікації й перепідготовки фахівців є невід'ємним і необхідним складником забезпечення національної безпеки держави та інформаційної кібербезпеки, зокрема.

Для систематизації пріоритетної проблематики і можливих рішень наведено рисунок 1.1, що узагальнює юрисдикцію міжнародних стандартів, національних законодавчих актів у освітніх регуляціях та демонструє їх взаємозв'язок і вплив на формування професійних компетентностей з реалізації інформаційної безпеки у сфері зайнятості.

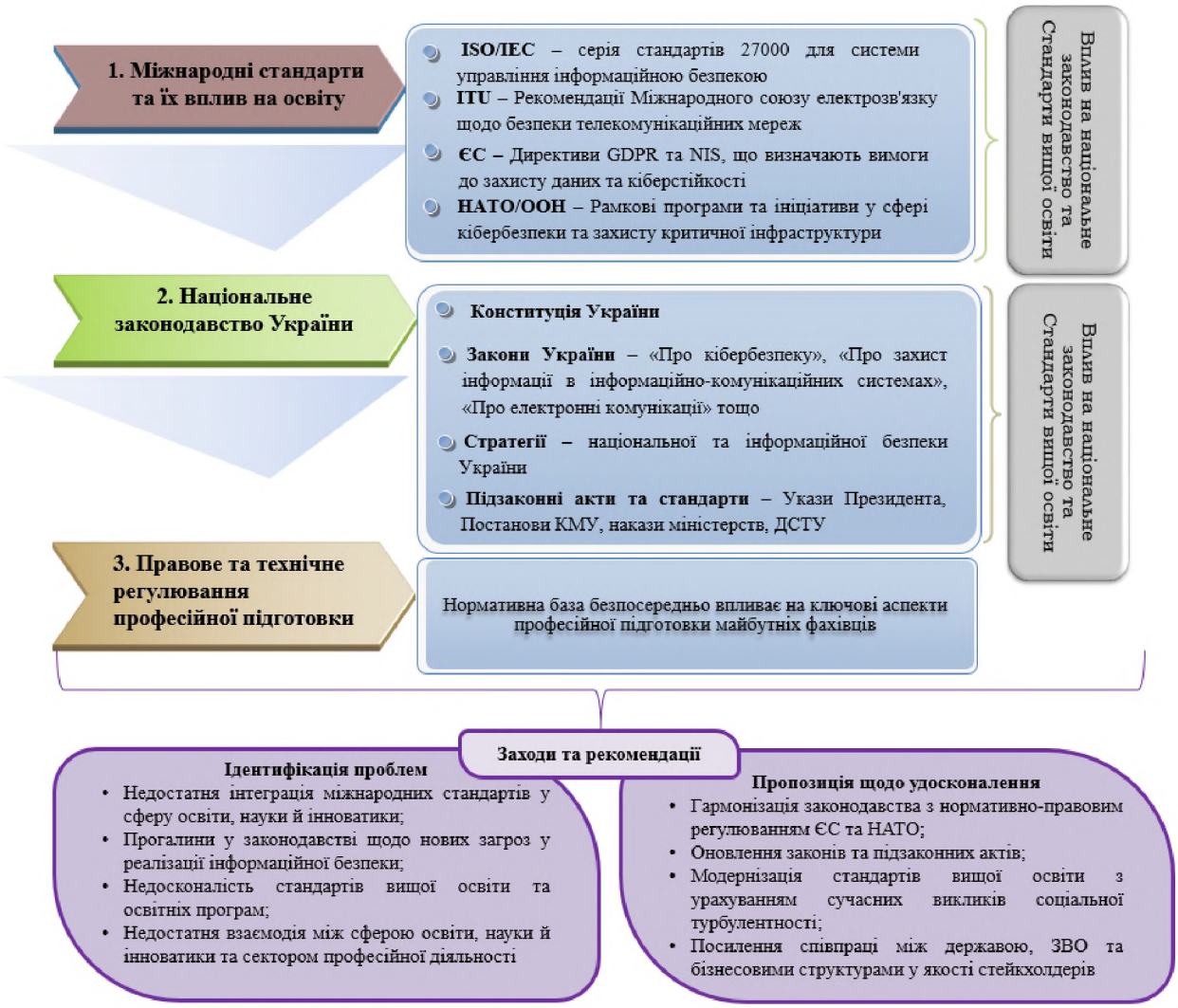

Рис.1.1 Нормативно правове забезпечення підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій

Удосконалення професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері радіотелекомунікацій на тлі стрімкого зростання кіберзагроз, хмарних сервісів, мобільних мереж та інтернету речей потребує теоретичного і і методологічного обгрунтування.

Висновки до першого розділу

Виявлено, що наявні освітні програми лише частково відповідають сучасним технологічним викликам і потребам ринку праці, що забезпечує не в повній мірі сформованість професійної компететності випускників до реальної

роботи з захистом телекомунікаційних систем. Оцінювання ефективності сучасних освітніх програм із підготовки майбутніх фахівців до релазіації інформаційної безпеки у сфері електроніки, меторологі та радіотелекомунікацій та визначення шляхів удосконалення з урахуванням новітніх технологій і міжнародних тенденцій розвитку галузі. Методологія дослідження передбачає застосування порівняльного аналізу навчальних планів і структур освітніх програм провідних українських університетів, аналіз змісту програмних результатів навчання та систематизацію компетентностей здобувачів освіти. Застосовано метод аксіологічного та порівняльного аналізу для узагальнення основних підходів і виокремлення прогалин у змісті професійної підготовки майбутніх фахівців для реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій. Результати дослідження показали, що більшість програм містять базові дисципліни з криптографії, управління ризиками та адміністрування мереж, але недостатньо враховують актуальні аспекти кіберзахисту 5G-мереж, IoT-систем та автоматизацію моніторингу загроз. Встановлено, що практичний аспект підготовки залишається обмеженим, що ускладнює підготовку випускників до роботи у високонавантажених телекомунікаційних середовищах. Наукова новизна полягає у визначенні основних недоліків чинних програм і формуванні рекомендацій щодо їхнього оновлення шляхом застосування сучасних методів практичної підготовки, хмарних лабораторій та симуляційних середовищ. Модернізація освітніх програм повинна передбачати регулярне оновлення навчального контенту, посилення практикоорієнтованих компонентів та інтеграцію міжнародних стандартів інформаційної безпеки.

Здійснено контент-аналіз, що засвідчив про відповідність не в повній мірі нормативно-правової бази та освітніх стандартів для реалізації інформаційної безпеки майбутніми та задіяними фахівцями. Насамперед йдеться про недостатнє врахування міжнародних норм: навіть там, де окремі положення GDPR чи директиви NIS уже формально імплементовано, їх практичне застосування у організації освітнього процесу зачасту має радше

декларативний, ніж дієвий характер, а також безпосередньо обмежує можливості формування у здобувачів освіти професійних компетентностей до реалізації інформаційної безпеки, які реально затребувані національними та міжнародними ринками зайнятості.

Проблемною залишається відірваність змістового наповнення освітніх програм та їх матеріально-технічного й інформаційно-технологічного забезпечення від практики. Брак науково- та навчально-методичного супроводу кейсів, прикладних лабораторних і випробувальних освітніх модулів і партнерства з працедавцями призводить до того, що навіть добре структуровані програми підготовлені фахівцями «на папері», не завжди відповідають вимогам забезпечення праці в умовах реальної соціальної турбулентності та кіберзагроз воєнного стану. Вихід вбачається у гнучкішій взаємодії між державою, ЗВО, галузевими установами та підприємствами, що дозволить оновлювати навчальні плани та освітні програми, забезпечити їх зміст максимально наближеним до практики.

Таким чином, подальший розвиток системи професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки потребує не тільки вдосконалення законодавчої бази, а й активної інтеграції сфери освіти, науки й інноватики з професійними середовищами, що забезпечить підготовку кадрів, здатних діяти ефективно у складному й мінливому просторі цифровізації суспільної діяльності.

Список використаної літератури до першого розділу:

лексєєва Т. І. Міжнародні організації: сучасні пріоритети та нові виклики в системі міжнародної інформаційної безпеки. *Збірник наукових праць «Проблеми міжнародних відносин»*. 2020. № 34. С. 12–21.

2. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. Київ: Право України, 2013. 184 с.

3. Артемов В. Ю. Організація захисту інформації з обмеженим доступом: підручник/ за заг. ред. Є. Д. Скулиша. К.: Вид-во: НА СБ України, 2011.– 378 с.

4. Артемов В. Ю. Теоретико-концептуальні засади формування деонтологічної компетенції фахівців у системі вищої освіти: монографія. Київ: Наук.-вид. центр Національного авіаційного університету: ПВП «Задруга», 2015. 298 с.

5. Артемов В. Ю. Теоретичні та методичні основи формування деонтологічної компетентності фахівців із організації захисту інформації з обмеженим доступом: дис. ... д. пед. наук: 13.00.04 – теорія і методика професійної освіти. Київ, 2015. 43 с.

6. Артюшин Г., Тушко К. Сучасні тенденції професійної підготовки фахівців сектору безпеки та оборони у країнах, що розвиваються. Збірник наукових праць Національної академії державної прикордонної служби України. СЕРІЯ: Педагогічні науки. № 2 (21). 2020. С. 5-17.

7. Архипов О.Є., Муратов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія. Київ: Наук.-вид. відділ Національної академії Служби безпеки України, 2011. 193 с.

8. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір: автореф. дис. ... канд. філософських наук: спец.: 09.00.03. Київ, 2012. 16 с.

9. Бабак В.П., Бабак С.В., Єременко В.С. та ін. Теоретичні основи інформаційно-вимірювальних систем: підручник/ за ред. В.П. Бабака. Київ: Університет новітніх технологій. НАУ, 2017. 496 с.

10. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.

11. Бардус І О. Фундаменталізація професійної підготовки майбутніх фахівців у галузі інформаційних технологій до продуктивної діяльності: монографія. Харків: ПромАрт, 2018. 393 с.

12. Биков В. Ю. Інноваційний розвиток засобів і технологій систем відкритої освіти. Сучасні інформаційні технології та інноваційні методики у підготовці фахівців: методологія, теорія, досвід, проблеми : зб. наук. пр. Київ-Вінниця, 2012. Вип. 29. С. 32–40.

13. Биков В. Ю. Хмарні технології, ІКТ-аутсорсинг і нові функції ІКТ підрозділів освітніх і наукових установ. *Інформаційні технології в освіті*. 2011. № 10. С. 8–23.

14. Биков В.Ю. Автоматизовані інформаційні системи єдиного інформаційного простору освіти і науки. *Збірка наукових праць Уманського державного педагогічного університету ім. Павла Тичини*. 2008. Ч. 2. С. 47–56.

15. Биков В.Ю. Методичні системи сучасних інформаційно-освітніх технологій. *Проблеми та перспективи формування національної гуманітарно-технічної еліти : зб. наук. пр.*: за ред. Л. Л. Товажнянського, О. Г. Романовського. Харків, 2002. Вип. 3. С. 73–83.

16. Биков В.Ю. Моделі організаційних систем відкритої освіти: монографія. Київ: Атіка, 2008. 684 с.

17. Биков В.Ю., Білоус О. В., Богачков Ю. М. Основи стандартизації інформаційно-комунікаційних компетентностей в системі освіти України: метод. реком.; за заг. ред. В. Ю. Бикова, О. М. Спіріна, О. В. Овчарук. Київ: Атіка, 2010. 88 с.

18. Биков В.Ю., Задорожна Н. Т., Омельченко Т. Г. Сучасні підходи та принципи побудови порталів. *Засоби і технології єдиного інформаційного*

освітнього простору: зб. наук. пр. Інституту засобів навчання АПН України [ред. В. Ю. Бикова, Ю. О. Жука]. Київ, 2004. С. 17–44.

19. Бистрова Б.В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США. автореф. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Київ, 2018. 20с.

20. Бичківський Р.В. та ін. Метрологія, стандартизація, управління якістю і сертифікація. Львів: Видавництво Національного університету «Львівська політехніка», 2002. 560 с.

21. Бідюк Н.М. Підготовка майбутніх інженерів в університетах Великої Британії /ред. Н.Г. Ничкало. Хмельницький: ХДУ, 2004. 306 с.

22. Бідюк Н.М. Розвиток змісту та форм організації підготовки бакалаврів інженерії в університетах Великої Британії: автореф. дис. … канд. пед. н. : 13.00.04 «Теорія і методика професійної освіти». Тернопіль, 2000. 20 с.

23. Богуш В., Хмельницький М. Пропозиції щодо системної підготовки фахівців для служби безпеки україни до діяльності в кіберпросторі. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (37). С. 60–81.

24. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кібер-простору, кібербезпеки та кіберзахисту: навч альний посібник/ під ред. В. М. Богуша. Київ: Ліра-К, 2020. 552 с.

25. Боженко Л.І. Метрологія, стандартизація, сертифікація та акредитація: навчальний посібник. Львів: Афіша, 2006. 324 с.

ондаренко Л.М. Міжвідомча координація у забезпеченні інформаційної безпеки: роль держави та приватного сектору. *Державне будівництво*. 2023. № 3 (99). С. 170–177.

27. Борсуковський Ю.В., Бурячок В.Л. Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України. *Сучасний захист інформації*. 2017. №1. с. 34–40.

28. Брайко Б.В. Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії: автореф. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Хмельницький, 2020.

удапештська конвенція про кіберзлочинність: аналіз імплементації в Україні: монографія / за ред. В. Д. Іванова. Київ: Юрінком Інтер, 2023. 312 с.

30. Бурячок В. Л., Богуш В. М. Рекомендації щодо розробки та запровадження профілю навчання "Кібернетична безпека" в Україні. *Безпека інформації*. 2014. Т. 20, № 2. С. 126–131.

31. Бурячок В.Л. Рекомендації щодо побудови тазапровадження профілю навчання «кібернетична безпека» в Україні / В. Л. Бурячок, В. М. Богуш / Безпека інформації. 2014. Т. 20. С. 126–131

32. Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М., Борсуковська В.Ю. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання*, 2018, Том 67, №5. С. 277-290.

алюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2021. № 1. С. 45–52.

34. Васильєв А.В., Зубань Ю.О., Коровайченко Ю.М., Шкарлет С.М. Застосування електронного навчання для підготовки й підвищення кваліфікації фахівців ІТ-галузі у вищих навчальних закладах: монографія. Суми: Сумський державний університет, 2013. 138 с.

35. Васіна Л. С. Інтеграція професійних та математичних знань у підготовці фахівців радіоелектронного профілю. Проблеми інтеграції у сучасній професійній освіті: методологія, теорія, практика: монографія / за ред. І. Козловської, Я. Кміта. Львів: Сполом, 2004. С. 126–133.

36. Васіна Л. С. Обґрунтування умов інтеграції математичних та спеціальних дисциплін у підготовці радіотехніків. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців:*

методологія, теорія, досвід: зб. наук. пр. Вінниця: ТОВ фірма «Планер», 2005. Вип. 7. С. 138–142.

37. Васіна Л. С. Обґрунтування умов інтеграції математичних та спеціальних дисциплін у підготовці радіотехніків. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід: зб. наук. пр.* Вінниця: ТОВ фірма «Планер», 2005. Вип. 7. С. 138–142.

38. Васіна Л.С. Дидактичні умови інтеграції спеціальних та математичних знань у професійній підготовці фахівців радіоелектронного профілю. *Наукові записки Тернопільського державного педагогічного університету ім. В. Гнатюка. Серія: Педагогіка*. 2004. Вип. 5. С. 65–69. 410

39. Васіна Л.С. Прикладне математичне забезпечення професійної підготовки фахівців в умовах ступеневої освіти. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми*: зб. наук. пр. Вінниця, 2004. Вип. 6. С. 83–189.

40. Васіна Л.С. Проблема прикладного математичного забезпечення професійно-практичної підготовки фахівців радіотехнічного профілю. *Педагогіка і психологія професійної освіти*. 2003. № 6. С. 84–91.

41. Величко О. Всесвітня історія метрології: від давнини до кінця XIX століття. Київ: «Основа», 2006. 424 с.

42. Величко О.М. Викладання метрології у навчальних закладах України. Український метрологічний журнал. 1998. № 3. С. 11 – 15.

43. Величко О.М. Всесвітня історія метрології: від давнини до Метричної конвенції: монографія. Херсон: Олді-Плюс, 2020. 527 с.

44. Величко О.М. Діяльність міжнародних і регіональних організацій з питань метрології. Український метрологічний журнал. 1997. № 2. С. 51 – 57.

45. Величко О.М. З історії розвитку метрології в Україні: із середини XX століття до сучасності. Український метрологічний журнал. 1997. № 1. С. 27 – 30.

46. Величко О.М., Дудич І.І. Основи метрології, стандартизації та контролю якості. Ужгород: Видавничий центр УжДУ, 1998. 284 с.

47. Величко О.М., Коломієць Л.В., Гордієнко Т.Б. Основи метрології та метрологічна діяльність. Херсон: Олді-Плюс. 2021. 576 с.

48. Вінник М.О. Формування науково-дослідницької компетентності майбутніх інженерів-програмістів в умовах освітнього середовища вищого навчального закладу: автореф. дис. … канд. пед. наук : 13.00.04 – теорія і методика професійної освіти. Херсон, 2016. 20 с.

49. Віткін Л. Аналіз системи технічного регулювання, стандартизації, метрології в Україні та заходи щодо її удосконалення на 2017 рік. *Метрологія та прилади*. 2017. № 1. С. 3-8.

50. Віткін Л., Кузьменко Ю. Історичні зміни у світовій метрології - почесний виклик для України у новому статусі. *Метрологія та прилади*. 2019. № 1. С. 3-6.

51. Віткін Л., Луценко Д. Модель реформування системи стандартизації України в контексті міжнародних зобов'язань та необхідності модернізації економіки. *Стандартизація, сертифікація, якість*. 2013. № 3. С. 3–12.

52. Володарський Є., Потоцький І. Забезпечення метрологічної надійності вимірювань. *Вимірювальна техніка та метрологія*. 2019. №80, Вип.3. С. 5-9.

53. Володарський Є.Т., Кошева Л.О. Понятійно-термінологічні аспекти сучасної метрології. Український метрологічний журнал. 2012. № 1. С. 3 – 10.

54. Володарський Є.Т., Кухарчук В.В., Поджаренко В.О., Сердюк Г.Б. Метрологічне забезпечення вимірювань і контролю: навч. посіб. Вінниця: Вінницький державний технічний університет, 2001. 244 с.

55. Воскобойніков С.О. Воскобойніков С.О. Педагогічні умови формування професійної готовності майбутніх фахівців інформаційної безпеки до захисту інформації з обмеженим доступом. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Полтава, 2015. 290 с.

56. Газдик М.М. Формування професійної компетентності майбутніх операторів з обробки інформації та програмного забезпечення у процесі фахової підготовки: дис. … д-ра філософії : 01 Освіта/Педагогіка, спец. 015 Професійна освіта (за спеціалізаціями). Мукачево, 2024. 304 с.

57. Гончаренко Т. Є. Педагогічні умови професійної підготовки майбутніх інженерів-програмістів у технічному університеті: автореф. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Харків, 2018. 20 с.

58. Гончаренко Т.Є. Педагогічні умови професійної підготовки майбутніх інженерів-програмістів у технічному університеті: автореф. дис. ... канд. пед. наук : спец. 13.00.04 теорія і методика професійної освіти. Харків. 2018. 20 с.

59. Горлинський В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі Information Technology and Security. 2024. Vol. 12, Iss. 2 (23). pp. 268-282.

60. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: підручник. Київ: Видавнича група BHV, 2009. 608 с.

61. Григоренко І.В., Кондрашов С.І., Григоренко С.М. Інформаційно-вимірювальні технології та системи: навчальний посібник. НТУ «ХПІ», 2023. 254 с.

62. Гриневич Ф.Б. Визначний внесок наукових шкіл в галузі приладобудування. Технічна електродинаміка. 1995. № 5. С. 74 – 76.

63. Гриневич Ф.Б., Таранов С.Г. Розвиток досліджень в науковому напрямку «Інформаційно-вимірювальні системи та метрологічне забезпечення в електроенергетиці». Технічна електродинаміка. Вип 4. 2007. С. 3 – 20.

64. Гуз А. М. Сучасні проблеми Європейської безпеки: навчальний посібник. Київ, Вид-во НА СБ України 2013. 316 с.

65. Гуз А.М. Державно-правовий механізм реалізації інформаційної політики. *Інформаційна безпека людини, суспільства, держави. Науково-практичний журнал.* 2013. №1(11). С. 18-24.

66. Гуз А.М. Еволюція світових стандартів інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави. Науково-практичний журнал.* 2013. №2(12). С. 5-9.

67. Гуз А.М. Становлення та розвиток світових стандартів інформаційної безпеки. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 18. Економіка і право.* Випуск 21. 2013. С. 154-159.

68. Гура О.О. Підготовка майбутніх інженерів-програмістів до тестування програмного забезпечення в умовах неформальної освіти: дис. … канд. пед. наук : 015 Професійна освіта (за спеціалізаціями). Запоріжжя. 2021. 344 с.

69. Гуревич Р. С., Кадемія Ю. В. Інформаційно-комунікаційні технології в навчальному процесі: посібник для пед. працівників і студ. пед. вищ. навч. закл. ; Ін-т педагогіки і психології проф. освіти АПН України, ВДПУ ім. М. Коцюбинського. Вінниця, 2002. 116 с.

70. Гуржій А. М., Карташова Л. А. Електронний посібник :інноваційний засіб навчання у системі професійної освіти. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми.* 2014. № 37. С. 16–22.

71. Гуржій А. М., Лапінський В. В. Електронні освітні ресурси – від теорії до практики. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми.* 2014. № 38. С. 3–11.

72. Гуржій А. М., Лапінський В. В. Електронні освітні ресурси як основа сучасного навчального середовища загальноосвітніх навчальних закладів. *Інформаційні технології в освіті : зб. наук. пр.* 2013. Вип. 15. С. 30–37.

73. Гуржій А.М., Возненко Л.І., Поворознюк Н.І., Самсонов В.В. Основи інформаційних технологій: навч. посіб. для здобувачів професійної (професійно-технічної) освіти. Київ: Літера ЛТД, 2023. 288 с.

74. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. ... канд. юрид. наук: 25.00.02. Київ, 2004. 22 с.

75. Гурковський В.І. Деякі організаційно-правові питання взаємовідносин органів державної влади в сфері інформаційної безпеки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2002. Вип. 5. С. 87.

76. Даник Ю.Г., Супрунов Ю.М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. *Збірник наукових праць ЖВІ НАУ «Інформаційні системи»*. 2011, Вип.5, С. 5–22.

77. Дегтярьова Л. М., Ляшевський В. Г. Практичні прийоми та керівні принципи розробки комплексів інформаційної безпеки. *Системи управління, навігації та зв'язку*. 2017. Випуск 2 (42). С. 94–97.

ержавна служба спеціального зв'язку та захисту інформації України. Оновлення освітніх програм у сфері кібербезпеки згідно з новими профстандартами: д

ержавний науково-дослідний інститут технологій кібербезпеки та захисту інформації. Орган з сертифікації систем менеджменту. URL: (дата звернення: 22.08.2024).

і 80. Джеджула О.М. Теорія і методика графічної підготовки студентів інженерних спеціальностей вищих навчальних закладів : автореф. дис. … д-ра пед. наук: 13.00.04 – теорія і методика професійної освіти. Тернопіль, 2007. 42 с.

а 81. Діордіца І.В. Кваліфікаційні вимоги до компетенцій фахівців з кібербезпеки. *Інформаційне право*. 2017. № 2. С. 215–219.

п 82. Діордіца І.В. Напрями підготовки та підвищення кваліфікації фахівців з кібербезпеки. *Інформаційне право*. 2017. № 3. С. 199–202.

а 83. Діордіца І.В. Освітні стандарти підготовки фахівців із кібербезпеки. н *Національний юридичний журнал: теорія і практика*, 2017. Вип. 1, С. 50-53.

и 84. Діордіца І.В. Освітні стандарти підготовки фахівців із кібербезпеки. (дата звернення: 22.08.2024). *Національний юридичний журнал: теорія і практика*. 2017. № 1(23). С. 50–53.

85. Діордіца І.В. Поняття та зміст кіберзагроз у сучасних умовах. *Інформаційне право*. 2017. № 1. С. 44–48.

86. Діордіца І.В. Стан підготовки фахівців у сфері кібербезпеки. *Visegrad Journal on Human Rights*. 2016. № 6(1). С. 53–68.

87. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ: НАПрН України, НДІІП, НАН України, Національна бібліотека України імені В.І. Вернадського, 2015. 388 с.

88. Дорожовець М.М., Мотало В.П., Стадник Б.І. та ін. Основи метрології та вимірювальної техніки: підручник у 2 т. Т. 1. Основи метрології; за ред. Б. Стадника. Львів: НУ «Львівська політехніка», 2005. 532 с.; Т. 2. Вимірювальна техніка; за ред. Б. Стадника. Львів: НУ «Львівська політехніка», 2005. 656 с.

89. Доронін І. М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження: дис. …д-ра юрид. наук: 12.00.01. Київ, 2020. 539 с.

90. Досвід роботи міжнародних організацій зі стандартизації / Б. Гриньов, Ю. Даниленко, В. Любинський // Стандартизація, сертифікація, якість. 2014. № 5. С. 11 – 13.

СТУ ISO/IEC 27000:2024. Інформаційні технології. Методи та засоби забезпечення безпеки. Системи управління інформаційною безпекою. Огляд і термінологія. Київ: Держспоживстандарт України, 2024. 44 с.

92. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT). Київ: ДП «УкрНДНЦ», 2023. 112 с.

93. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 190 с.

94. Дубровін О. С., Коваль В. М. Підготовка фахівців з кібербезпеки в умовах цифровізації освіти. *Інформаційна безпека*. 2021. No 4. С. 12–19.

95. Євсюкова О.В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. *Державне управління: удосконалення та розвиток*. 2021. № 2. ORCID: 0000-0002-1299-6955.

96. Жарова О. В. Модель формування інформаційної компетентності майбутніх радіотехніків в технічному університеті. *Наукові записки. Серія: Педагогічні науки: зб. наук. пр*. 2014. Вип. 19 (119). С. 83–89.

97. Жарова О. В. Педагогічні умови формування інформаційної компетентності майбутніх радіотехніків. *Вища освіта України у контексті інтеграції до європейського освітнього простору*. 2014. № 5. С. 56–61.

98. Жарова О. В. Проблеми формування інформаційної компетентності майбутніх фахівців радіотехніків у технічних університетах. Наукові записки Вінницького Державного педагогічного університету ім. М. Коцюбинського. Серія: Педагогіка і психологія: зб. наук. пр. 2014. Вип. 42. С. 107–110.

99. Жарова О.В. Формування інформаційної компетентності майбутніх радіотехніків у процесі професійної підготовки в технічному університеті: дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Київ, 2015. 228 с.

100. Засоби інформаційно-комунікаційних технологій єдиного інформаційного простору системи освіти України: монографія/ за наук. ред. В. Ю. Бикова; Ін-т інформ. технологій і засобів навч. НАПН України. Київ: Педагогічна думка, 2010. 160 с.

101. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. … д-ра пол. наук : 23.00.02. Львів, 2021. 35 с.

102. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: АртЕк, 2018. 445 с.

103. Зубик Л.В. Формування професійних компетентностей майбутніх бакалаврів з інформаційних технологій у процесі вивчення фахових дисциплін. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Рівне, 2016. 331 с.

104. Іванчук Ю.Б. Формування професійно значущих якостей майбутніх фахівців з інформаційної безпеки в процесі вивчення науково-природничих дисциплін: автореф. дис. ... канд. пед. наук: 13.00.04 – теорія і методика професійної освіти. Київ, 2013. 20 с.

105. Ігнаткін В.У., Єфіменко Н.А., Туз Ю.М. та ін. Інформація, інформатика та метрологія / за ред. В.У. Ігнаткіна. Дніпро: ПП Видавництво «Нова ідеологія», 2021. 450 с.

106. Ігнаткін В.У., Томашевський О.В., Матюшин В. М. Основи метрології: [Електронний ресурс]: навч. посіб. / Запоріжжя: Запорізький національний технічний університет, 2017. 1 електрон. опт. диск (DVD-ROM);

107. Ігнатюк О.В. Теоретичні та методичні основи підготовки майбутнього інженера до професійного самовдосконалення в умовах технічного університету: автореф. дис. ... д-ра пед. наук : 13.00.04 – теорія і методика професійної освіти. Харків, 2010. 44 с.

108. Ілляшенко О. О. Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці: автореф. дис. ... канд. техн. наук : спец. 05.13.05 – комп'ютерні системи та компоненти. Харків, 2018. 24 с.

афедра інформаційного, господарського та адміністративного права. Робоча програма навчальної дисципліни «Інформаційна безпека» / КПІ ім. Ігоря Сікорського. 2023. URL: https://matan.kpi.ua/media/onp-ta-opp/bak/syll-n/ЗО07_Інформаційна_безпека.pdf (дата звернення: 22.08.2024).

афедра інформаційної безпеки КПІ ім. Ігоря Сікорського. Теоретична та п

афедра кібербезпеки та захисту інформації КНУ. Оновлення освітніх програм у ифері кібербезпеки згідно з новими професійними стандартами. 2023. URL: к

л 112. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень монографія. К.: НІСД, 2013, 104 с.

ібербезпека на міжнародному рівні: виклики та можливості NIS2 для н

а

українських компаній. *Міжнародна асоціація аудиту, комплаєнсу та етики*. (дата звернення: 22.08.2024).

ібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних. *Вісник юридичного факультету УжНУ*. 2025. № 3. С. 39–47.

115. Кірей К. О., Кірей Л. О. До проблеми стандартизації термінології освітніх інформаційно-телекомунікаційних технологій. *Вісник Черкаського університету. Серія : Педагогічні науки*. Черкаси, 2009. Вип. 146. С. 27–29.

116. Козубцова Л.М., Козубцов І.М., Ліщина В.О., Штаненко С.С. Концепція навчально-тренувального комплексу підготовки військових спеціалістів інформаційної та кібербезпеки на засадах комп'ютерної гри (гейміфікації). *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2022. № *2*(18), 49–60.

117. Кокарєва А.М. Особливості професійної підготовки майбутніх фахівців у системі інженерно-технічної освіти України. *Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: збірник наук. пр.* Київ: Вид-во Нац. авіац. ун-ту „НАУ-друк", 2018. Вип. 12(1). С. 65–69.

118. Кокарєва А.М. Формування професійно значущих якостей майбутніх інженерів у процесі фахової підготовки в технічному університеті. *Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: збірник наук. праць*. Київ: Вид-во Нац. авіац. ун-ту „НАУ-друк", 2016. Вип. 2(9). С. 78–82.

119. Коломієць А. А. Фундаменталізація математичної підготовки майбутніх бакалаврів галузі електроніки та телекомунікацій: монографія / за наук. ред. В.І. Клочка. Вінниця: ТВОРИ, 2021. 360 с.

120. Коломієць А.А. Теорія і практика фундаменталізації математичної підготовки майбутніх бакалаврів галузі знань «електроніка та телекомунікації». дис. д-ра. пед. наук: 13.00.04 – теорія і методика професійної освіти. Рівне, 2023. 628 с.

121. Кононенко А., Смирнова І. Реалізація технологій змішаного навчання майбутніх фахівців телекомунікацій та електромеханіків: порівняльний аналіз. *Науковий вісник Вінницької академії безперервної освіти. Серія «Педагогіка. Психологія».* 2023. Вип. 4. С. 53– 58.

онституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 22.08.2024).

онцепція інформаційної безпеки України. Організація з безпеки і співробітництва в Європі (ОБСЄ). 2015. URL:

124. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібн. Київ: Кондор, 2008. 382 с.

125. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

126. Корченко О.Г. Системи захисту інформації: монография. Київ: НАУ, 2004. 264с.

127. Кудлай В.О. Цифрова грамотність особистості в контексті розвитку інформаційного суспільства. *Вісник Маріупольського державного університету*. 2015. Вип. 10. С. 97–104.

128. Кузьменко Ю., Черепков С., Дуля В. Оцінка відповідності засобів вимірювальної техніки – реалізація в Україні європейських підходів (принципів). *Метрологія та прилади*. 2018. № 1. С. 11-17.

129. Кузьмінський А.І., Кучай О.В., Біда О.А. Використання польського досвіду підготовки фахівців з інформатики в системі педагогічної освіти України. *Інформаційні технології і засоби навчання*. 2018. Том 68, № 6. С. 206–217.

130. Кухарчук В.В. Основи метрології та електричних вимірювань. Частина І : конспект лекцій. Вінниця: ВНТУ, 2020. 148 с

131. Кухарчук В.В., Кучерук В.Ю., Володарський Є.Т., Грабко В.В. Основи метрології та електричних вимірювань: підручник. Херсон: Олді–плюс, 2020.

132. Лаврова О. Ефективність навчальних програм з інформаційної безпеки. Актуальні питання освіти. 2018. № 3. С. 53–59.

ахно В. А., Касаткін Д. Ю., Сагун А. В. Методичні вказівки з навчальної практики «Проєктування систем кібербезпеки». Київ: НУБіП України, 2022. 58 с.

134. Лебедєва К.О. Формування професійної компетентності майбутніх інженерів радіотехнічних спеціальностей на засадах ресурсного підходу: дис. … д-ра філософії: 015 – Професійна освіта. Харків, 2020. 378 с.

135. Лебедь Г. М. Ґенеза змісту фахової підготовки майбутніх програмістів у політехнічних навчальних закладах України (кінець XX початок XXI століття): дис. ... канд. пед. наук : 13.00.01 - загальна педагогіка та історія педагогіки: 01-освіта/педагогіка. Херсон ; Тернопіль. 2018. 265 с.

ізунов С. І., Костенко В. О. Методологія наукових досліджень для спеціальностей «Кібербезпека», «Телекомунікації та радіотехніка»: конспект лекцій. Запоріжжя: ЗНТУ, 2023. 84 с.

137. Ліпкан В. А. Національна безпека України: навч. посіб. Київ: КНТ, 2009. 576 с.

138. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ: КНТ, 2006. 280 с

139. Ліпкан В.А., Череповський К.П. Інкорпорація інформаційного законодавства України: монографія/за заг. ред. В.А. Ліпкана. К.: О.С. Ліпкан, 2014. 408 с.

140. Луценко Г.В. Теоретико-методичні засади професійної підготовки майбутніх інженерів в умовах проектно орієнтованого навчання», дис. ... д. пед. н: 13.00.04 – теорія і методика професійної освіти. Глухів 2019. с.

141. Лясова Ф.С. Методика навчання технології розробки програмного забезпечення майбутніх інженерів програмістів: автореф. дис. … канд. пед. наук : 13.00.02. Київ, 2014. 20 с.

142. Магілевський В. В. Формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах. *Педагогічна академія: наукові записки*. 2025. Вип. 14. DOI: https://doi.org/10.5281/zenodo.14723771.

143. Малежик П.М. Теоретичні й методичні засади технічної підготовки майбутніх фахівців з інформаційних технологій: дис. ... д. пед. наук: 13.00.02 – теорія та методика навчання (технічні дисципліни). Київ, 2020. 487 с.

144. Малежик П.М. Технічна підготовка майбутніх фахівців з інформаційних технологій: монографія. Київ: Вид-во НПУ імені М.П. Драгоманова, 2020. 337 с.

алиновський В. Я. Міжнародні договори в системі національного права України. Київ: Алерта, 2022. 240 с.

146. Марцева Л. А. Професійна підготовка молодших спеціалістів радіотехнічного профілю в технічних коледжах: монографія. Вінниця: Тезис, 2015. 633 с.

147. Марцева Л.А. Організаційно-методичні засади оптимізації підготовки майбутніх фахівців радіотехнічного профілю в коледжах: посібник. Вінниця: Тезис, 2015. 128 с.

148. Марцева Л.А. Теоретичні та методичні основи професійної підготовки молодших спеціалістів радіотехнічного профілю: дис. ... д. пед. наук: 13.00.04 – теорія і методика професійної освіти. Львів, 2015. 459 с.

149. Матвійчук-Юдіна О. В. Інформаційно-аналітичний метод підтримки навчального процесу підготовки ІТ-фахівців. *Проблеми інженерно-педагогічної освіти: зб. наук, праць*. 2015. № 48–49. С. 268–277.

150. Матвійчук-Юдіна О.В. Комплекс електронних освітніх ресурсів навчання комп'ютерної графіки майбутніх бакалаврів кібербезпеки: автореф.

дис. … канд. пед. наук: 13.00.10 – інформаційно-комунікаційні технології в освіті. Київ, 2018. 23 с.

151. Матвійчук-Юдіна О.В. Концепція формування професійних компетентностей фахівців з інформаційних технологій та кібербезпеки. *Наукоємні технології*, 2019. Вип. 3(43). С. 330-342.

ельник І. С. Кібербезпека в Україні: стан імплементації міжнародних норм. *Держава та право*. 2023. № 81. С. 132–138.

153. Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*. 2016. № 10. С. 79-88.

154. Метрологія у галузі зв'язку: монографія. Одеса: Видавничий Дім «СтандартЪ», 2006. Кн. 1: Метрологія, стандартизація, менеджмент якості та оцінка відповідності / Л.В. Коломієць, М. Т. Козаченко, О. А. Панченко [та ін.] ; за ред. Л. В. Коломійця. 242 с.

155. Метрологія, стандартизація, сертифікація та управління якістю в системах зв'язку: підручник / Л.В. Коломієць, П. П. Воробієнко, М. Т. Козаченко [та ін.]; за заг. ред. Л. В. Коломійця. Одеса : ВМВ, 2009. 376 с.

іжнародна фундація виборчих систем (IFES). Правова база кібербезпеки в Україні: загальний огляд і аналіз. 2021. URL: https://ifesukraine.org/wp-

іністерство оборони затвердило основні засад інформаційної та кібербезпеки. (дата звернення: 22.11.2024).

іністерство оборони України. Впровадження міжнародних стандартів та підходів НАТО з кібербезпеки. 2024. URL: (дата звернення: 22.08.2024).

іністерство оборони України. Основні засади кібербезпеки в інформаційно-комунікаційних системах: впровадження практик НАТО. 2024. URL: (дата звернення: 22.11.2024).

160. Міночкін А.І. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців. Оборонний вісник. *К., Центр воєнної політики та політики безпеки.* 2011. №2. С. 12–14.

161. Молодецька-Гринчук К. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах: автореф. дис. … д-ра технічних наук: 21.05.01. Київ, 2018. 42 с.

162. Мотало В., Мотало А., Стадник Б. Метрологія, кваліметрія та кваліметричні вимірювання: теорія і практика. *Вимірювальна техніка та метрологія*. 2014. № 76. С. 5-21.

163. Мотало В.П. Аналіз методик верифікації та калібрування засобів вимірювальної техніки. *Вимірювальна техніка та метрологія*. 2019. №80(1). С. 51-66.

аціональне агентство України з питань державної служби. Загальна короткострокова програма «Інформаційна безпека» НАДС. 2024. URL: дата звернення: 22.11.2024).

аціональний інститут стратегічних досліджень. Розвиток освітніх програм у сфері захисту критичної інфраструктури (КІ). 2024. URL: (дата звернення: 22.08.2024).

аціональний кластер кібербезпеки. Найактуальніші дослідження у сфері кібербезпеки України та світу – 2020–2021. CRDF Global, НКЦК, USAID. 2021. (дата звернення: 22.08.2024).

167. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.

Д ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в ІТС. Київ: ДССЗЗІ України, 2005.

лійник К. М., Войціховський А. В. Кібербезпека як напрям діяльності ООН. *Актуальні питання протидії кіберзлочинності та торгівлі людьми: збірник матеріалів Всеукраїнський науково-практичний конференції* (Харків, 15.11.2017

р.) / МВС України, Харк. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2017. С. 200–202.

170. Олійник О. В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України: монографія. К., Вид. підпр-во «Український пріоритет», 2012. 400 с.

171. Орнатський П.П. Вступ до методології науки про вимірювання. К.: ІСДО, 1994. 246 с.

172. Освітня програма Безпека інформаційних і комунікаційних систем (спеціальність 172 «Електронні комунікації та радіотехніка», магістерський рівень). Львівська політехніка: вебсайт. 2019. URL: https://directory.lpnu.ua/majors/ikta/8.125.00.01/19/2024/ua/full (дата звернення: 29.07.2025).

173. Освітня програма Безпека інформаційних і комунікаційних систем (спеціальність 125, бакалаврський рівень). Ужгородський національний університет: вебсайт. 2024. URL: https://vstup.osvita.ua/y2024/r8/207/1329920/ (дата звернення: 29.07.2025)

174. Освітня програма Безпека інформаційних і комунікаційних систем (спеціальність F5 «Кібербезпека та захист інформації», бакалавр). ХНУРЕ: вебсайт. 2025. URL: https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-f5-kiberbezpeka-tazakhyst-informatsii/bakalavr-f5-kiberbezpeka-ta-zakhyst-informatsii/bezpeka-informatsijnykh-ikomunikatsijnykh-system?utm_source=chatgpt.com (дата звернення: 29.07.2025)

175. Освітня програма Інформаційна безпека телекомунікаційних систем і мереж (спеціальність 172 «Електронні комунікації та радіотехніка», бакалавр). КНУ ім. Тараса Шевченка: вебсайт. 2019–2025. URL: https://rex.knu.ua/informational-security-of-telecommunca tion-systems-and-networks/ (дата звернення: 29.07.2025)

176. Освітня програма Професійна освіта (Комп'ютерні технології) (спеціальність 015). Тернопільський національний педагогічний університет імені Володимира Гнатюка. 2025. URL:

https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/2023/Vido mosti_015.39.pdf (дата звернення: 29.07.2025)

177. Освітня програма Професійна освіта (Цифрові технології) (спеціальність 015.39). Український державний університет імені Михайла Драгоманова: Вступ.OSVITA.UA. 2025. URL: https://vstup.osvita.ua/y2025/r27/6704/1502852/ (дата звернення: 29.07.2025)

178. Освітня професійна програма Кібербезпека та захист інформації (спеціальність 125 «Кібербезпека») – КПІ ім. Ігоря Сікорського: вебсайт. 2025. URL: https://osvita.kpi.ua/125 (дата звернення: 29.07.2025)

179. Основи інформаційного та соціально-правового моделювання: навч. посіб. / Ланде Д.В., Фурашев В.М., Юдкова К.В. К.: НТУУ "КПІ", 2014. 220 с.

180. Павленко О. В. Професійна підготовка фахівців з електроніки у закладах вищої освіти США: дис. … канд. пед. наук : 13.00.04 – теорія і методика професійної освіти. Київ. 2021. 296 с.

181. Павленко О.В. Перспективні напрями застосування досвіду США до професійної підготовки фахівців з електроніки в Україні: методичні рекомендації. Київ: КПІ ім. Ігоря Сікорського, 2020. 35 с.

182. Павленко О.В. Професійна та іншомовна підготовка фахівців з електроніки: досвід США: методичні рекомендації. Київ: КПІ ім. Ігоря Сікорського, 2020. 39 с.

183. Павленко Ю. Ф. Забезпечення єдності вимірювань: навчальний посібник. Частина 1 / Ю. Ф. Павленко, І. П. Захаров. Харків: ТОВ «Оберіг», 2023. 172 с.

184. Панченко Л. Ф. Підготовка майбутніх фахівців з інформаційних технологій до здійснення навчальної аналітики. *Вісник Кременчуцького національного університету імені Михайла Остроградського. Серія : Педагогічні науки.* 2015. Вип. 1 (2). С. 89–96

185. Панченко Л.Ф. Інформаційно-освітнє середовище сучасного університету: монографія. Луганськ : ДЗ «ЛНУ імені Тараса Шевченка», 2010. 280 с.

186. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: спец.: 12.00.07. Львів, 2019. 268 с.

187. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник; за заг. ред. О. А. Семченка та В. М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

188. Петрович С.Д. Формування професійної компетентності у майбутніх фахівців з обчислювальної техніки в процесі вивчення спеціальних дисциплін в технічних коледжах: автореф. дис. … канд. пед. наук : 13.00.04 – теорія і методика професійної освіти. Вінниця. 2011. 20 с.

189. Петрук В. А. Формування базового рівня професійної компетентності у майбутніх фахівців технічних спеціальностей засобами інтерактивних технологій: монографія. Вінниця: ВНТУ, 2011. 285 с.

190. Пєвцов Г. В., Залкін С. В. та ін. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення : монографія. Харків : ХНУПС ім. Івана Кожедуба, 2014. 332 с.

191. Поджаренко В.О. Кухарчук В.В. Вимірювання і комп’ютерно вимірювальна техніка: навчальний посібник. К.: УМК ВО, 1991. 239 с.

192. Поджаренко В.О., Кулаков П.І., Ігнатенко О.Г., Войтович О.П. Основи метрології та вимірювальної техніки: навчальний посібник. Вінниця: ВНТУ, 2006. 151 с.

193. Пододіменко І. І. Сучасні тенденції професійної підготовки фахівців з комп'ютерних наук в університетах Японії. *Порівняльна професійна педагогіка*. 2013. № 1. С. 315-322.

194. Поліщук Є.С., Дорожовець М.М., Яцук В.О. та ін. Метрологія та вимірювальна техніка: підручник. Львів : «Бескид-Біт», 2003. 544 с.

195. Поліщук Є.С., Дорожовець М.М., Яцук В.О. та ін.; Метрологія та вимірювальна техніка : підручник/ за ред. Є.С. Поліщука. Львів: Вид-во Львівської політехніки, 2012. 544 с.

ро державну таємницю: Закон України від 21 січня 1994 р. № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93. URL:

ро затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ від 19.06.2019 № 518. Офіційний вісник України. 2019. № 51. Ст. 1723. URL: (дата звернення: 22.08.2024).

ро захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 22.08.2024).

ро інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL:

ро міжнародні договори України: Закон України (Відомості Верховної Ради України (ВВР), 2004, № 50, ст.540) URL: https://zakon.rada.gov.ua/laws/show/1906-15#Text (дата звернення: 22.08.2024).

ро національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241. URL:

ро основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

ада національної безпеки і оборони України. Стратегія кібербезпеки України: проєкт документа. 2021. URL: (дата звернення: 22.08.2024).

204. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Київ: Видавництво НАВС, 2012. 104 с.

авчук С.О. Виклики гармонізації законодавства ЄС в галузі кібербезпеки для У

к 206. Сажієнко О.П. Формування фахової компетентності бакалаврів рфери комп'ютерних технологій у процесі професійної підготовки: дис. … докт. філос.: 015 – професійна освіта. Умань, 2020. 272 с.

ї 207. Самойленко О. Формування цифрової компетентності у майбутніх фахівців з інформаційної безпеки. *Актуальні питання гуманітарних наук.* Вип. 60, том 4, 2023. С. 157-161.

. 208. Сачук Ю. Нормативно-правові засади забезпечення професійної підготовкифахівців із кібербезпеки та захисту інформації. *Молодь і ринок.* № 12 (167), 2018. С. 45-50

л 209. Семко В.В. Модель конфлікту взаємодії об'єктів кібернетичного простору. *Збірник наукових праць Національного авіаційного університету «Проблеми інформатизації та управління».* 2012. № 2(38). С. 88-92

т 210. Сергеєва Л.М., Стойчик Т.І., Мартиненко К.В. Організація рофесійної підготовки фахівців електротехнічного профілю в навчально-практичних центрах закладів професійної (професійно- технічної) освіти. *Наукові записки малої академії наук України*. 2022. № 3(25), С. 145–154.

н 211. Сердюк І.А. Організаційні засади публічного управління інформаційною безпекою суспільства в умовах загроз ментальному здоров'ю: дис. … канд. наук з держ. упр.: 25.00.05 – державне управління у сфері ержавної безпеки та охорони громадського порядку. Київ, 2023. 256 с.

о 212. Сиротюк В.М., Хімка С.М., Сиротюк С.В. Віртуальні контрольно-имірювальні прилади і системи: навчальний посібник. Львів: «Магнолія 2006», 2024. 128 с.

л 213. Сікора Я.Б. Теоретико-методичні засади адаптивної системи рофесійної підготовки майбутніх фахівців з інформаційних технологій в в

а

умовах цифровізації. дис. ... д. пед. наук: 13.00.04 – теорія і методика професійної освіти. Житомир, 2025. 709с.

214. Солтис І.В., Деревянчук О.В. Основи метрології: навчальний посібник. Чернівці: Чернівецький нац. унтет, 2021, 152 с.

215. Співаковський О.В. Теорія і практика використання інформаційних технологій у процесі підготовки студентів математичних спеціальностей: монографія. Херсон: Айлант, 2003. 250 с.

216. Спірін О. М. Критерії і показники якості інформаційно-комунікаційних технологій навчання. *Інформаційні технології і засоби навчання.* 2013. № 1 (33). URL: http://journal.iitta.gov.ua.

217. Спірін О. М. Проблеми інформатизації освіти України в контексті розвитку досліджень оцінювання якості засобів ІКТ. *Інформаційні технології і засоби навчання.* 2012. № 1 (27). URL: http://journal.iitta.gov.ua/index.php/itlt/article/view/632/483.

218. Стандарт вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти: наказ Міністерства освіти і науки України від 04.10.2018 № 1074 (зі змінами – наказ Міністерства освіти і науки України від 29.10.2024 № 1547). URL: https://zakon.rada.gov.ua/laws/show/243/2021 (дата звернення: 22.08.2024).
тандарт вищої освіти України перший (бакалаврський) рівень, галузь знань 01 – «Освіта / Педагогіка», спеціальність 015 – «Професійна освіта (за спеціалізаціями)»: наказ Міністерства освіти і науки України від 21.11.2019 р. № 1460. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/07/28/015-Profosvita-bakalavr.pdf (дата звернення: 22.08.2024).

220. Стандарт вищої освіти України перший (бакалаврський) рівень, галузь знань 01 «Освіта / Педагогіка», спеціальність 015 «Професійна освіта (за спеціалізаціями)»: наказ Міністерства освіти і науки України від 21.11.2019 р. № 1460. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-

osvita/zatverdzeni%20standarty/2021/07/28/015-Profosvita-bakalavr.pdf (дата звернення: 22.08.2025).

тандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека» / Затв. наказом Міністерства освіти і науки України від 18 березня 2021 р. № 332. Київ: МОН України, 2021. URL: https://osvita.ua/legislation/Vishya_osvita/81973/ (дата звернення: 22.08.2024).

222. Стандартизація як інструмент забезпечення інноваційної діяльності / Б. Гриньов, Ю. Даниленко, О. Жихарєва, В. Любинський // Стандартизація, сертифікація, якість. 2013. № 3. С. 13 – 16.

тратегія кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. Офіційний вісник Президента України. 2021. URL: (дата звернення: 22.08.2024).

224. Стрюк К.М. Формування професійної компетентності молодших спеціалістів з комп'ютерної інженерії у радіотехнічних коледжах: дис.канд. пед. наук : 13.00.04 – теорія і методика професійної освіти. Харків. 2020. 334 с.

225. Тарасюк А.*В.* Кібербезпека України на сучасному етапі державотворення*:* теоретико-правові основи*:* монографія. Одеса: Фенікс,. 2020. 404 с.

226. Татарчук В. В. Організаційні та дидактичні особливості формування графічної компетентності майбутніх фахівців у галузі електроніки та телекомунікацій. *Педагогіка безпеки*, 2022. № 7(1-2), С. 1–07

227. Татарчук В. В. Професійна підготовка фахівців у галузі електроніки та телекомунікацій як педагогічна проблема. *Наукові інновації та передові технології*. 2023. № 11(25). С. 612-625.

228. Татарчук В. В. Формування графічної компетентності майбутніх фахівців у галузі електроніки та телекомунікацій. *Наука і техніка сьогодні*. 2023. № 11(25). С. 580-593.

229. Татарчук В.В. Формування графічної компетентності майбутніх фахівців у галузі електроніки та телекомунікацій із застосуванням цифрових технологій у закладах вищої освіти: дис. ... д-ра філ.: 015 Професійна освіта. Вінниця, 2025. 262 с.

230. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави. Київ: Видавництво НА СБ України, 2014. 196 с.

231. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук: спец.: 12.00.07. Ужгород, 2019. 487 с.

232. Топольник В.Г., Котляр М.А. Метрологія, стандартизація, сертифікація і управління якістю: навчальний посібник. Львів: Магнолія, 2009. 212 с.

233. Торічний В.О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.

234. Торічний В.О. Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз: дис. ... док. пед. наук: 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Харків, 2020. 368 с.

235. Трифонова О.М. Методична система розвитку інформаційно-цифрової компетентності майбутніх фахівців комп'ютерних технологій у навчанні фізики і технічних дисциплін: дис. … д-ра пед. наук : 13.00.02, 13.00.04 / ЦДПУ ім. В. Винниченка. Кропивницький, 2020. 595 с.

года про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, від 27.06.2014. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 22.08.2024).

повноважений Верховної Ради України з прав людини. Цифрова безпека українців: рухаємося за європейськими стандартами. 2025. URL:

(дата звернення: 22.06.2025).

238. Хом'юк І.В. Теоретико-методичні засади формування базового рівня професійної мобільності майбутніх інженерів. Вінниця: ВНТУ, 2012, 379 с.

ебенко С. Б. Міжнародні та європейські гарантії забезпечення прав людини в кіберпросторі. *Юридичний науковий електронний журнал*. 2022. № 5. С. 161–

240. Цюцюра В.Д., Цюцюра С.В .Метрологія та основи вимірювань: навчальний посібник. К.: Знання-Прес, 2003. 80 с.

241. Шаран Р. Досвід США з підготовки магістрів інформаційних технологій в системі дистанційної освіти та можливості його впровадження в Україні. Порівняльно-педагогічні студії. 2010.№ 1-2, С. 29-35.

242. Шаран Р. Кваліфікаційні напрями підготовки фахівців інформаційних технологій в США. *Вища освіта України.* Педагогіка вищої школи: методологія, теорія, технології. 2009. № 3(1), С. 611-614.

евчук О. П. Врахування рекомендацій міжнародних організацій (НАТО, ООН, ОБСЄ) при формуванні кіберполітики України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. № 82. С. 110–116.

244. Шемчук В. В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз: монографія. Київ: Видавництво Ліра-К, 2020. 352 с.

245. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / за заг. ред. К. І. Бєлякова. Київ: КВІЦ, 2019. 344 с.

246. Юридична відповідальність за правопорушення в інформаційній сфері: теорія і практика: монографія / за заг. ред. К. І. Бєлякова. Київ: 2016. 293 с.

247. яEuropean qualifications framework (EQF). Cedefop. 2012–2025. URL: https://www. cedefop.europa.eu/en/projects/european-qualifications-framework-eqf 27001 (date of access: 30.07.2025)

248. Яворський Н.Б., Теслюк В.М., Литвинова Є.І. Комп'ютерні методи в інженерії мікроелектромеханічних систем: навчальний посібник. Львів: Вид-во Львів. політехніки, 2016. 304 с.

249. яяAlyami A., Sammon D., Neville K., Mahony C. Critical success factors for security education, training and awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. *Information & Computer Security*. 2024. Vol. 32, № 1. pp. 53–73.

250. яяBendler D., Felderer M. Competency models for information security and cybersecurity professionals: analysis of existing work and a new model. ACM Transactions on Computing Education. 2023. Vol. 23, № 2. pp. 1–33.

251. яяBreda G., Kiss M. Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. *Procedia Manufacturing*. 2020. Vol. 46. pp. 580– 590.

252. яяBuriachok V., Sokolov V. Implementation of active learning in the master's program on cybersecurity. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing. Vol. 938. Springer, Cham. 2020. pp. 598–607.

яCompTIA. Security+ (SY0-601) Certification Exam Objectives. – CompTIA, 2024. – URL: https://www.comptia.org/en-us/certifications/security

яCouncil of Europe. Convention on Cybercrime (ETS No. 185) [Електронний ресурс]. 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 22.08.2025).

яCSIRT Держспецзв'язку. Оновлення освітніх програм у сфері кібербезпеки згідно з новими профстандартами: досвід та плани. – 2023. – URL:

я

(дата звернення: 22.08.2025).

яCybersecurity Framework. *NIST*. URL: https://www.nist.gov/cyberframework (дата звернення: 22.08.2025).

яDeloitte Ukraine. Вплив Директиви NIS2 на підприємства критичної інфраструктури України в межах інтеграції до ЄС [Електронний ресурс]. 2024. URL: https://www.deloitte.com/ua/uk/services/consulting/perspectives/impact-of-nis2-directive-on-ukraine-critical-infrastructure-enterprises-eu-integration.html (дата звернення: 22.08.2025).

259. яяDirective (EU) 2016/1148 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 (NIS Directive). *Official Journal of the European Union*. 2016. L 194. C. 1–30.

260. яяEC-Council. CEH Candidate Handbook v4.0. – EC-Council, 2023. – URL: https://www.eccouncil.org/wp-content/uploads/2023/02/CEH-Handbook-v4.0.pdf (дата звернення: 22.08.2025).

261. яяEuropean Union Agency for Cybersecurity (ENISA). NIS 2 Directive: Key provisions and implementation challenges. 2023. URL: https://www.enisa.europa.eu/ (дата звернення: 22.08.2025).

262. яяEY Україна. Оцінка відповідності та впровадження системи управління інформаційною безпекою за стандартом ISO 27001. URL: https://www.ey.com/uk_ua/services/consulting/compliance-assessment-and-implementation-of-the-information-security-management-system (дата звернення: 22.08.2025).

263. яяFernando S. The Different Aspects of Information Security Education. Research Anthology on Advancements in Cybersecurity Education. 2022. pp. 50–72.

264. яяGoian O., Goian V., Biletska T., Bessarab A., Zykun N. Communicative strategies of professional development of a TV and radio journalist: psychotypology and social model. Academic Journal of Interdisciplinary Studies. 2020. Vol. 9, № 5. pp. 147–157.

265. яяHatzivasilis G., Ioannidis S., Smyrlis M., Spanoudakis G., Frati F., Goeke L., Hildebrandt T., Tsakirakis G., Oikonomou F., Leftheriotis G., Koshutanski

H. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*. 2020. Vol. 10, № 16. Article 5702. URL: https://www.academia.edu/73709685/Modern_Aspects_of_Cyber_Security_Training_and_Continuous_Adaptation_of_Programmes_to_Trainees (date of access: 14.07.2025).

266. яяIMS Cert. ISO 27001 – система менеджменту інформаційної безпеки. URL: https://ims-cert.com/mezhdunarodnaya-sertifikacziya-ua/iso/iec-27001-ua.html (дата звернення: 22.08.2025).

яInternational Telecommunication Union (ITU). About ITU: Bridging the digital divide. 2023. URL: https://www.itu.int/ (дата звернення: 22.08.2024).

яInternational Telecommunication Union (ITU). Global Cybersecurity Agenda https://www.itu.int/en/action/cybersecurity/pages/gca.aspx (дата звернення:

яISC². CISSP Certification Overview. – International Information System Security Certification Consortium, 2024. – URL: https://www.isc2.org/Certifications/CISSP

270. яяISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO, 2018. 44 p.

271. яяISO/IEC 27001 – Information security management systems: Requirements. International Organization for Standardization. 2022. URL: https://www.iso.org/standard/27001 (30.07.2025)

яISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International

яISO/IEC 27002:2022. Information security, cybersecurity and privacy protection –

274. яяISSP Training Center. Сертифікація з кібербезпеки: курси, програми, вендори. 2025. URL: https://www.issp.training (дата звернення: 22.08.2025).

яITU-T Recommendation X.1205. Overview of cybersecurity. Geneva: ITU, 2008. 48 p. URL: https://www.itu.int/rec/T-REC-X.1205-200804-I (дата звернення:

яITU-T X.805. Security architecture for systems providing end-to-end

277. яяKuzovkova T. A., Kuzovkov A. D., Sharavova O. I., Sharavov I. M. The impact of technological progress on the competencies of electronics, radio engineering, communications and Журнал «Наукові інновації та передові технології» № 9(49) 2025 (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»). pp. 1–6.

278. яяMukherjee M., Le N. T., Chow Y.-W., Susilo W. Strategic approaches to cybersecurity learning: a study of educational models and outcomes. *Information*. 2024. Vol. 15, № 2. DOI: https://doi.org/10.3390/info15020117.

яNational Institute of Standards and Technology. Workforce Framework for

яNATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). About us. 2024. URL: https://ccdcoe.org/about-us/ (дата звернення: 22.08.2025).

яNATO Cooperative Cyber Defence Centre of Excellence. Cybersecurity Education

яNATO. NATO's approach to cyber defence [Електронний ресурс]. 2024. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 22.08.2025).

283. яяNIST Cybersecurity Framework (CSF). National Institute of Standards and Technology: вебсайт. 2024. URL: https://www.nist.gov/cyberframework 27001 (date of access: 30.07.2025)

284. яяOrlik P., Donald R. Telecommunications programs. In: Media Education Assessment Handbook. Routledge. 2020. pp. 55–78.

285. яяPreglej Garić R., Tipurić D., Aleksić A. Future of work in telecommunication sector: challenges for education and training. ICERI2022 Proceedings. 2022. pp. 6079–6086.

286. яяPrometheus. Безпека в інтернеті під час війни: практичний курс. 2022. URL: https://prometheus.org.ua/prometheus-free/cybersecurity-during-war-practical/ (дата звернення: 22.08.2025).

яRegulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Електронний ресурс]. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 22.08.2025).

288. яяRidei N., Tymoshenko V., Tytova N., Khodunova V., Biletska A. Organization of professional training of communication management and communications specialists. *Journal of Education, Technology and Computer Science*. 2022. Vol. 33, № 3. pp. 109–117.

289. яяSenanayake T., Fernando S. Information security education: watching your steps in cyberspace. The Online Journal of Science and Technology. 2018. Vol. 8, № 2. URL: https://tojsat.net/journals/tojsat/articles/v08i02/v08i02-16.pdf (date of access: 05.05.2025).

РОЗДІЛ 2.
ОБГРУНТУВАННЯ ТА РОЗРОБЛЕННЯ МОДЕЛІ ОРГАНІЗАЦІЇ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ФАХІВЦІВ ДО РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ЕЛЕКТРОНІКИ, МЕТРОЛОГІЇ ТА РАДІОТЕЛЕКОМУНІКАЦІЙ

2.1 Проєктування моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій

Забезпечення пізнання об'єкту/оригіналу дослідження (процес професійної підготовки майбутніх фахівців) здійснено завдяки проєктуванню моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій (далі – Модель) в якості аналогу/копії, яка візуалізує об'єкт і його семантику (функціонал), характерні особливості процесу професійної підготовки майбутніх фахівців спеціальності А5 Професійна освіта (спеціалізацій – Цифрові технології та Електроніка, метрологія та радіотелекомунікації) з освітньою кваліфікацією – бакалавр професійної освіти (рис.2.1).

Актуалізує необхідність розроблення й обґрунтування Моделі стратегічна мета інформаційної безпеки України (щодо нарощення потенціалу спроможностей з її забезпечення (безпеки держави), зокрема середовищ професійної зайнятості в умовах цифровізації, надання інформаційно-технологічної підтримки ресурсозабезпечення та інструментних засобів сервісу національних стратегій соціальної та інформаційної політики для гарантій стабільного захисту, обґрунтованості державного суверенітету України, її територіальної цілісності, розвитку демократичного культур-потенціалу, соціально-правового гарантування захисту громадян, в цілому, і кожного, зокрема) і мета організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців-бакалаврів професійної

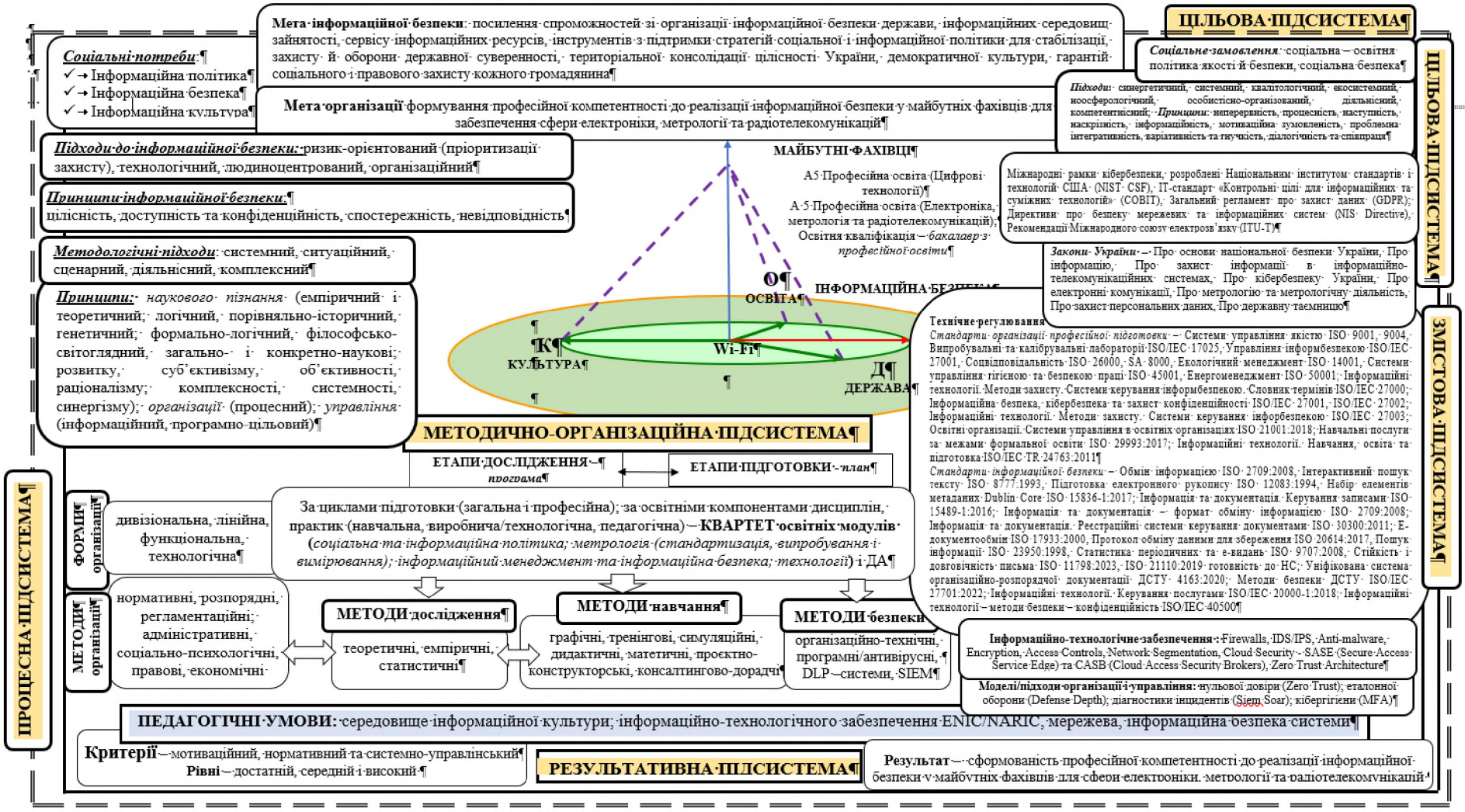

Рис. 2.1 Модель організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій

освіти для забезпечення їх професійної зайнятості у сфері електроніки, метрології та радіотелекомунікації ((безпекових спроможностей – цифрового простору державних безпекових гарантій захисту української громадянської ідентичності, медіа-здатностей, медіа- та інформаційної культури, правничих компетенцій доступу до інформації та її захисту; готовності до інформаційної реінтеграції різночинних категорій здобувачів освіти та професійно й соціально задіяних громадян України (в тому числі на захоплених агресором територіях), безпекових спроможностей забезпечення систем стратегічних комунікацій та суспільної інформатизації формування інформаційної культури, міжкультурного діалогу, компетентностей інформатизації у сферах екологічної, енергетичної, економічної, соціально-гуманітарної, національної, кібербезпеки – інформаційної, галузевої, регіональної, інституційної безпеки), здатностей персональної безпеки).

Визначення раніше невиокремлених педагогічних аспектів обумовило виділення й укомплектування *цільової підсистеми* Моделі з врахуванням цільових соціальних – потреб інформаційної політики, безпеки і культури в Україні та замовлення на висококваліфіковаинх кадрів з реалізації суспільної інформаційної безпеки засобами освітньої політики якості й безпеки життєдіяльності. Здійснено добір підходів (ризик-орієнтований (пріоритизації захисту), технологічний, людиноцентрований, організаційний) і принципів інформаційної безпеки (цілісність, доступність та конфіденційність, спостережність, невідповідність), підходів (синергетичний, системний, квалітологічний, екосистемний, ноосферологічний) і принципів (неперервність, процесність, наступність, наскрізність, інформаційність) соціальної політики та методологічних підходів (системний, ситуаційний, сценарний, діяльнісний, комплексний) і принципів (наукового пізнання (емпіричний і теоретичний; логічний, порівняльно-історичний, генетичний; формально-логічний, філософсько-світоглядний, загально- і конкретно-наукові; розвитку, суб'єктивізму, об'єктивності, раціоналізму; комплексності, системності, синергізму); організації (процесний); управління (інформаційний, програмно-

цільовий)) для досягнення синергії (методологічної) як стратегічної, так і цільової мети дослідження (розробка, теоретичне обґрунтування та експериментальна перевірка Моделі), впровадження Моделі як абрису системи і процесу професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки (у сфері електроніки, метрології та радіотелекомунікацій) та стратегічного бачення триадної єдності *КОДу*, де *К* – культура, *О* – освіта, *Д* – держава при реалізації та нарощенні культур-потенціалу інформаційної безпеки майбутнього кадрового забезпечення сфер – електрорадіотелекомунікацій, її метрології та стандартизації; освіти, науки й інноватики; культури і мистецтва) майбутніми фахівцями з професійною компетентністю до реалізації інформаційної безпеки.

Методично-організаційна підсистема Моделі та умови забезпечення – середовище інформаційної культури, інформаційно-технологічне забезпечення та сервісна підтримка освітньо-наукової діяльності ЗВО, мережева інформаційна безпека системи/процесу професійної підготовки майбутніх фахівців (сфери електроніки, метрології, радіотелекомунікацій) забезпечують вияв і ефективність діяльності учасників освітнього процесу (процесу професійної підготовки), процесної та змістової – модернізації його активів – освітніх ресурсів та *змістової підсистеми* Моделі як у етапах процесів дослідження – (камерального, мотиваційного, констатувального, формувального та праксеологічного), так і професійної підготовки (профорієнтаційного, навчально-пізнавального – загального, професійно-орієнтованого, спеціального, технологічного, релевантного).

Розроблено та сформовано методичний органайзер комплексу методів (організації, дослідження, навчання, безпеки), форм (організації, системи/процесу), засобів/інструментів (технічного регулювання організації професійної підготовки (*стандарти організації професійної підготовки* – Системи управління якістю ISO 9001, 9004, Випробувальні та калібрувальні лабораторії ISO/IEC 17025, Управління інформбезпекою ISO/IEC 27001, Соцвідповідальність ISO 26000, SA 8000, Екологічний менеджмент ISO 14001,

Системи управління гігієною та безпекою праці ISO 45001, Енергоменеджмент ISO 50001; Інформаційні технології. Методи захисту. Системи керування інформбезпекою. Словник термінів ISO/IEC 27000; Інформаційна безпека, кібербезпека та захист конфіденційності ISO/IEC 27001, ISO/IEC 27002; Інформаційні технології. Методи захисту. Системи керування інфорбезпекою ISO/IEC 27003; Освітні організації. Системи управління в освітніх організаціях ISO 21001:2018; Навчальні послуги за межами формальної освіти ISO 29993:2017; Інформаційні технології. Навчання, освіта та підготовка ISO/IEC TR 24763:2011; *Стандарти інформаційної безпеки* – Обмін інформацією ISO 2709:2008, Інтерактивний пошук тексту ISO 8777:1993, Підготовка електронного рукопису ISO 12083:1994, Набір елементів метаданих Dublin Core ISO 15836-1:2017; Інформація та документація. Керування записами ISO 15489-1:2016; Інформація та документація – формат обміну інформацією ISO 2709:2008; Інформація та документація. Реєстраційні системи керування документами ISO 30300:2011; Е-документообмін ISO 17933:2000, Протокол обміну даними для збереження ISO 20614:2017, Пошук інформації ISO 23950:1998, Статистика періодичних та е-видань ISO 9707:2008, Стійкість і довговічність письма ISO 11798:2023, ISO 21110:2019 готовність до НС; Уніфікована система організаційно-розпорядчої документації ДСТУ 4163:2020; Методи безпеки ДСТУ ISO/IEC 27701:2022; Інформаційні технології. Керування послугами ISO/IEC 20000-1:2018; Інформаційні технології – методи безпеки – конфіденційність ISO/IEC 40500), міжнародної інформаційної діяльності/безпеки, інформаційно-технологічного забезпечення (Firewalls, IDS/IPS, Anti-malware, Encryption, Access Controls, Network Segmentation, Cloud Security - SASE (Secure Access Service Edge) та CASB (Cloud Access Securit Міжнародні рамки кібербезпеки, розроблені Національним інститутом стандартів і технологій США (NIST CSF), IT-стандарт «Контрольні цілі для інформаційних та суміжних технологій» (COBIT), Загальний регламент про захист даних (GDPR); Директиви про безпеку мережевих та інформаційних систем (NIS Directive), Рекомендації Міжнародного союзу електрозв'язку (з

англ. – ITU-T) у Brokers), Zero Trust Architecture), а також моделей/підходів до організації та управління (нульової довіри (з англ. – Zero Trust); еталонної оборони (з англ. – Defense Depth); діагностики інцидентів (з англ. – Siem Soar); кібергігієни (з англ. – Multi-Factor Authentication, MFA))).

Забезпечення реалізації принципів неперервності, процесності, наступності, наскрізності та інформаційності у змістовому наповненні *процесу професійної підготовки (освітнього процесу)* майбутніх фахівців реалізовано завдяки розробленню і впровадженню *змістової підсистеми* Моделі, сформованої відповідно за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах дисциплін і практик апробованого КВАРТЕТУ освітніх модулів – 1. Соціальна та інформаційна політика**;** 2.Метрологія(стандартизація, випробування і вимірювання); 3. Інформаційний менеджмент та інформаційна безпека та 4.Технології з виокремленими освітніми компонентами (для *спеціалізації «Цифрові технології»* – відповідно 1. *Соціальна та інформаційна політика* – теоретико-правові основи освіти та вступ до спеціальності; безпека життєдіяльності та основи охорони праці; 2.*Метрологія(стандартизація, випробування і вимірювання)* – стандартизація та технічні вимірювання, контроль, діагностика та ремонт персональних комп'ютерів; 3. *Інформаційний менеджмент та інформаційна безпека* – теорія автоматичного управління, комп'ютерні мережі та захист даних, основи кібербезпеки, автоматизовані системи організаційного управління та управління базами даних, їх проєктування та експлуатація; 4.*Технології* – технології навчання, інформаційні технології (мережеві) та технології програмування в сфері освіти, науки й інноватики, конфліктологія в професійній діяльності, науково-технічна творчість, комп'ютерне документоведення; для *спеціалізації «Електроніка, метрологія та радіотелеомунікації»* – відповідно 1. *Соціальна та інформаційна політика* – громадянська освіта та основи демократії, академічна культура, теоретико-правові основи професійної (професійно-технічної) освіти; 2. *Метрологія(стандартизація, випробування і вимірювання)* – нормативно-

методична база у сфері метрології, основи метрології та метрологічного забезпечення, технічного регулювання, сертифікація продукції, послуг та персоналу, квалітологія і системи управління якістю; 3. *Інформаційний менеджмент та інформаційна безпека* – вступ до фаху, інформаційна безпека та захист інформації, інформаційний менеджмент, інформаційно-комунікаційні мережі та платформи; 4. *Технології* – цифрові освітні та комунікативні технології в галузі, аналітико-синтетична переробка інформації, документознавство, нормативно-технічний та електронний документообіг) дивізіональної/лінійної, функціональної, технологічної форм організації процесу і релевантності навчальних досягнень у здобувачів освіти під час державної атестації).

Синергію *процесної і змістової підсистем* як у етапах дослідження (мотиваційного, констатувального, формувального і праксеологічного), так і професійної підготовки (профорієнтаційного, навчально-пізнавального, релевантного) забезпечено комплексом методів – організації (нормативні, розпорядні, регламентаційні, адміністративні, соціально-психологічні, правові, економічні), дослідження (теоретичні, емпіричні, статистичні), навчання (графічні, тренінгові, симуляційні, дидактичні, матетичні, проєктно-конструкторські, консалтингово-дорадчі), безпеки (організаційно-технічні, програмні/антивірусні, DLP – системи, SIEM) у ЗВО експериментальної площадки (Український державний університет імені Михайла Драгоманова, Бердянський державний педагогічний університет і Харківський національний автомобільно-дорожній університет).

Методи організації забезпечують супровід – *адміністрований* через організаційно-розпорядчі, які керуються виконавською дисципліною та відповідальністю (соціальною, екологічною, правовою) у координаційно-субординаційній взаємодії – організаційно-управлінських процедур директивного характеру з наступним наглядом їх виконання; *регулятивний* через регламентуючі методи забезпечення функціоналу (цільового призначення за видами та на рівнях організації діяльності) згідно статутних положень і

визначених положень структурно-організаційних підрозділів і чинних посадових інструкцій для усіх учасників освітнього процесу; *нормативний* – керуються застосуванням визначених засобів технічного регулювання стандартів (ДСТУ, ISO), часового унормування видів діяльності, передбачених трудовим договором, правилами внутрішнього розпорядку, графіком робочого часу, посадовими інструкціями; *розпорядчий* – поточно-розпорядчі методи застосовуються для подолання оперативних проблем, перешкод, ситуацій, завдань та передбачають форми наказу (обов'язкові до виконання), розпорядження – вузько спрямованого призначення для окремих груп, допоміжні вказівки для полегшення виконання завдань/уточнення деталізації; *соціально-економічний* – економічні методи матеріального заохочення виконання завдань (преміювання та надбавки за складність, напруження та досягнення високих показників, також матеріальної відповідальності за виявлені невідповідності нормативам при виконанні задач); госпрозрахункові структурні підрозділи працюють в умовах фінансової самостійності; *ментальний* – соціально-психологічні методи, способи впливу на особисту свідомість працівників через їх соціальні запити/морально-етичний стан колективу (соціальні – для поліпшення умов праці, формування корпоративної культури, соціального захисту (компенсації, страховки); психологічно-мотиваційні спонукання співробітників засобами визнання їх здобутків, формування сприятливого клімату, зв'язків з громадськістю); *правничий* – правові методи застосування законодавчих актів для забезпечення регулювання міжособистісних взаємин у колективі (трудове, адміністративне, цивільне, господарське, земельне, екологічне право), внутрішніх актів (наказів, розпоряджень, доручень). У Додатку А наведено характеристику методів організаці, специфіку базису та характер вплиув на організаційно-управлінські, структурно-оргнізаційні та організаційно-методичні процедури забезпечення ефективності Моделі.

Виокремлено методи дослідження – теоретичні (задля здійснення аксіологічного, функціонального, формально-логічного, порівняльного аналізу), емпіричні та методи матетиматичної статистики.

Системоутворююче значення у підсистемних взаєминах їх структурних складових поряд із формами та методами організації відіграють *методи формування безпекового середовища освіти*, такі як організаційно-технічні, програмні/антивірусні, DLP, SIEM для підготовки майбутніх фахівців згідно законодавчих галузевих, інституційних і персональних вимог щодо права на діяльність ЗВО: методи – *організаційно-технічні* забезпечують безпековий базис політики якості й безпеки життєдіяльності соціокультурних форм організації в університетах-партнерах (поряд з організаційними передбачено дотримання відповідності технічним регламентам усіх видів діяльності в ЗВО видам безпеки освітнього середовища – соціальної, екологічної, інформаційної, економічної, інституційної, академічної, персональної, національної (в тому числі оборонної)); *програмні/антивірусні методи* (з англ. – Endpoint Security) модернізації компонентів підготовки від демонстрації базових інсталяцій програмного забезпечення до системного навчально-наукового пізнання, досліджень та моніторингу ризиків і небезпек при формуванні антивірусних систем з технологіями сигнатурного аналізування, евристики та просунутого поведінкового аналізу у межах систем (з англ. – Endpoint Detection and Response EDR); інформаційно-комп'ютерної безпеки (з англ. – Sandboxing) моніторингу невизначених обєктів у віртуальних комірках криптографічних процедур шифрування в протоколах даних та захисту у трафіках(VPN та TLS); *методик попередження витоку даних* (з англ. – Data Loss Prevention, DPL) у процесі передавання сучасних наукових знань у процесі опрацювання контентів за призначенням класифікаційних ознак функціонування даних, оволодіння компетенцій їх диференціації на рівнях доступу конфіденційності даних (відкриті, втаємничені); методи нагляду (АСК) за процесами і параметрами через аналітичний інструментарій трафіків (поштових сервісів, зовнішніх носіїв/месенджерів та хмарних сервісів); діджитал-сліди / числові відбитки (з

англ. – Data Fingerprinting) шляхом генерування ідентифікаторів цінних паперів – DPL-системам розпізнавання несанкціонованих копій – фрагментів контентів; *управління інцидентами* (з англ. – Security Information and Event Management, SIEM) – моніторингу безпекових центрів (з англ. – SOC Engine) інфраструктури для встановлення загроз і розроблення прогнозних сценаріїв деактивації атак, стану безпеки в реальному часі; централізації – розбудови архітектури процесів (логів) від антивірусних агентів на серверних потужностях для аналізування інцидентів. У Додатку Б наведено характеристику методів формування безпеки у підготовці майбутніх фахівців, визначено їх роль у освітньому процесі на виокремлено ключові навички та уміння майбутніх фахівців.

Запропоновано методи навчання у професійній підготовці майбутніх фахівців до реалізації інформаційної безпеки для забезпечення освітніх матеріалів ефективності:

- графічні з використанням графічних діаграмних інфографічних ілюстрацій складних проблемних концептів, систем і процесів у галузі інформаційної безпеки для забезпечення сприйняття;

- тренінгові практичної організації семінарів, вебінарів, майстеркласів, воркшопів, на яких здобувачі освіти опаановують практичні навички та уміння у реальних умовах професійної адаптації, опрацьовуючи процедури реагування на інценденти безпеки;

- симуляційні зі прогнзуванням сценаріїв, реальними загрозами кібератак для тренування майбутніх фахівців у питаннях виявлення, усунення та запобігання ризикам їх виконання;

- дидактичні з використанням класичних освітніх ресурсів (лекцій, підручників та ммедіа) для опануваннятеоретичних основ формування інформаційної безпеки;

- матетичні зі застосуванням науково-пізнаваьних підходів аналізу та моделювання ризиків і небезпек, що сприяє фахівцям у прийняття доцільних управлінських безпекових рішень;

- проєктно-конструкторські зі розроблення і реалізації проєктів, що дають змогу здобувачам освіти опанувати спеціальні аспекти реалізації інформаціної безпеки при взаємодії в проєктних групах;

- консалтингово-дорадчі зі залученням експертів (аналітиків, практиктиків, науковців) в галузі інформаційної безпеки для здійснення експертних процедур консультаційних сесій, коли здобувачі освіти опановують навички консалтингу, дорадництва у співпраці з визначними авторитетами.

Моделі та підходи організації й управління, такі як нульова довіра, еталонна оборона, діагностика інцидентів і кібергігієна відіграють важливу роль у забезпеченні інформаційної безпеки, зокрема кібербезпеки. Здійснено їх добір, а саме:

- нульової довіри як підхід, що забезпечує умови, коли жоден користувач або пристрій не вважається верифікованим в незалежності від місця дислокації по відношенню до корпоративних мереж (покликання на доступ до інформаційних ресурсів перевіряються, а режим доступу надається лише після аутентифікації та авторизації споживачів інформаційних сервісів);

- еталонної оборони як стратегії зі розроблення складнорівневого захисного механізму для захисту від несанкціонованих атак, що включає ідентифікацію зламів брандмауерів, кодифікацію даних та заходів забезпечення системного захисту;

- діагностики інцидентів як процес ідентифікації, аналізування та відгуку на інциденти порушення захисту систем безпеки: моніторинг систем, протоколи подій, встановлення джерел атак для оперативного реагування й запобігання в майбутньому;

- кібергігієни як органайзеру заходів, які користувачі використовують для власного обладнання та персоналізації даних; включає регулярне оновлення програмного забезпечення, застосування складних дискрипоторів, опарцювання ситуацій з потенційними ризиками та небезпеками фішингу і дотримання безпекових процедур при роботі з Інтернетом.

Виокремлено *ефективні форми організації навчання* фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій – дивізіональна, лінійна, функціональна та таехнологічна; згідно Закону України «Про вищу освіту» [1] форми навчання у ЗВО встановлено як очна (денна, вечірня), заочна (дистанційна з розміщенням курсів від Google, Cisco або Microsoft на Coursera та Дія.Освіта), комбінова; форми організації освітнього процесу – навчальні заняття, самостійна робота, практична підготовка та контрольні заходи вхідного, проміжного, кінцевого нагляду, державної атестації та міжнародної атестації (професійного визнання, процедур сертифікації) у короткострокових програмах «Під керівництвом інструктора або самостійне навчання» (з англ. – Instructor-Led або Self-Study) для набуття визнаного статусу – етичний хакінг засвідчується сертифікатом Етичного хакера (з англ. – Certified Ethical Hacker, CEH), безпекового керування з сертифікатами фахівця з безпеки інформаційних систем (з англ. – Certified Information System Security Professional, CISSP) та сертифікат менеджера з інформаційної безпеки (з англ. – Certified Information Security Manager, CISM), а також аудитора ризиків – офіційного представника міжнародного органу сертифікації (з англ. – Professional Evaluation and Certification Board, PECB Group Inc.) в Україні з сертифікацію (ISO 27001, Lead Implementer).

Соціальний та інформаційний вектори політичної діяльності є тісно переплетеними напрямами державної стратегії національної безпеки: перший – соціальний сфокусовано на підтримці добробуту, покращенні життєвих стандартів та гарантуванні соціальних прав громадян, захисту України; другий – регулює діяльність інформаційних мереж від генерації до розповсюдження інформаційних даних, забезпечує гарантії питань кібербезпеки для розбудови цифрового простору держави.

Стратегічні вектори соціальної політики передбачають:

– соціальний захист та модернізацію механізмів соціальної підтримки, також удосконалення системи соціального страхування;

– сфери зайнятості зі стимулюванням соціальних відносин, професійної й соціальної зайнятості населення;

– гармонізацію суспільних взаємин Людини – Природи – Суспільства – професійного середовища щодо формування сприятливих умов для самореалізації особистості та правового й технічного регулювання соціальних гарантій і захисту у суспільних відносинах.

Визначено ключові складові інформаційної політики:

– менеджмент інформаційних ресурсів: система адміністрування процесів накопичення, систематизації та поширення інформаційних даних; стратегічне планування, маркетинг в цифровому та медіапросторі;

– кібербезпека захисту національного інформаційного поля зайнятості, забезпечення цілісності та безперебійності у роботі інформаційних систем/мереж/процесів;

– інформаційне суспільство: діджиталізація, гейміфікація, транспарентність, забезпечення доступу до надійних джерел інформації за призначенням аналітичного пошуку користувачів, впровадження новітніх ІТ-технологій.

Виокремлено ключові компоненти взаємозв'язку, а саме: соціальна інформація (сучасні наукові знання, інформаційні дані, історична ретроспектива суспільного розвитку) застосовується у регулюванні соціальних відносин, механізмів, у реалізації інформаційної політики і забезпечення соціальної стабільності розвитку суспільства. Державна інформаційна політика сприяє задоволенню потреб населення та гармонійному поєднанню правочинства та засобів технічного регулювання з суспільним /соціальним вектором цивілізаційного розвитку.

У галузі електроніки, метрології та радіотелекомунікацій професійна підготовка майбутніх фахівців ґрунтується на синтезі технічних регламентів та гуманітарних чинників/механізмів державної політики.

Розкрито значення соціальної політики у професійній підготовці майбутніх фахівців та її структурні складові. Так, соціальний компонент

державної політики відіграє роль гаранта громадянського добробуту та є морально-етичним імперативом регулювання безпеки й професійної етики у роботі з технологіями в галузі.

Соціальна інженерія забезпечує аналізування механізмів/способів маніпуляції, мотивації та психолого-педагогічного впливу для нейтралізації загроз інформаційної безпеки, які виникають завдяки вразливості людської психіки.

Професійна етика та відповідальність для формування цілісного розуміння, недосконаліть метрологічного забезпечення та метрики їх оцінювання або збою в інфокомунікаційній інфраструктурі є джерелами ризиків і небезпек для безпеки життєдіяльності громадян.

Цифрова інклюзія та адаптація до викликів інформаційного суспільства забезпечується шляхом формування стійкості інфраструктури та демократизації доступу до цифрових ресурсів для різночинних категорій верств населення.

Інформаційна політика у підготовці майбутніх фахівців галузі визначає правові та стратегічні плани у майбутній професійній діяльності фахівців.

Нормативно-правову базу врегульовує застосування в сфері освіти, науки й інноватики та опанування в освітньому процесі Закону України «Про основні засади забезпечення кібербезпеки України» [2] та міжнародних стандартів, таких як ISO/IEC 27001.

Завдяки Державній стратегії національної безпеки забезпечується усвідомлення важливості її складових, а саме Стратегії інформаційної безпеки держави, зокрема у питаннях протидії дезінформації та захисту критичної інфраструктури України.

Політика антикризового менеджменту забезпечує алгоритми координації з державними органами (наприклад CERT-UA) у разі цифрової агресії на метрологічне устаткування.

Уточнено структуру професійного змісту у галузевому контексті – галузі АОсвіта, спеціальності А15 Професійна освіта (за спеціалізаціями – Цифрові

технології; Електроніка метрологія та радіотелекомунікації) структура змістових складових підготовки, якої включає:

✓ електроніка – забезпечення технічної витривалості, міцності програмно-апаратного забезпечення, комплексів електрокомунікацій, верифікація мікросхем керування щодо відсутності шкідливого функціоналу («апаратних троянів») та гарантії захисту вбудованих обчислювальних платформ;

✓ метрологія – забезпечення точності метрики вимірювання та валідності верифікації метрологічних показників, також кіберзахисту інтелектуальних мереж вимірювання (зокрема Smart Grids) від маніпуляцій із даними та зовнішнього спотворення результатів (оцінювання, аналізу);

✓ радіотелекомунікації – криптографічний захист процесів/мереж/інформаційних потоків даних у радіоканалах, аудит протоколів бездротової передачі (5G/Wi-Fi), блокування несанкціонованого доступу в мережеві вузли.

Здійснено добір змістових компонентів для модернізації структури і змісту навчання майбутніх фахівців у освітніх компонентах:

1) нормативно-правового інформаційного базису політики держави у контексті опанування законодавчого поля та нормативних актів Держспецзв'язку стосовно безпеки об'єктів критичної інфраструктури; вивчення регламентів ліцензування та сертифікації радіотелекомунікаційних засобів та високоточного інструментарію;

2) метрологічної стійкості інформаційної безпеки – розробка та застосування методик верифікації достовірної доведеності результатів вимірювань; захист інтелектуальних сенсорів та датчиків від зовнішнього втручання та спробам запобігання дезінформації системи («від метрологічного тероризму»);

3) безпека електронних комунікацій та радіотехнологій – впровадження процедурно-регламентованих криптографічних протоколів у структурних сегментах бездротової передачі інформаційних даних; нейтралізація каналів

несанкціонованої втрати даних, що виникають внаслідок побічних (нелігітимних) електромагнітних випромінювань та наведень;

4) соціально-психологічні аспекти кібербезпеки у протидії соціальній інженерії в професійно технічному ком'юніті; дотримання морально-етичних стандартів під час роботи з персональними даними в системах зв'язку.

Виокремлено особливості сертифікації та вимоги до встановлення відповідності кадрового резерву. Для забезпечення відповідності у роботі в галузі інформаційної безпеки майбутні фахівці повинні мати такі кваліфікаційні характеристики: бути обізнаним та застосовувати на практиці знання стандартів ДСТУ ISO/IEC серії 27001 та галузевих вимог до комплексних систем захисту інформації (далі – КСЗІ); мати відповідний професійний рівень, підтвердженям міжнародними сертифікатами, таких як CompTIA Security+ або Cisco Certified Support Technician (CCST) Cybersecurity, які визнано на ринку зайнятості у галузі; володіти здатністю до реалізації політики інформаційної безпеки, що є гарантом оперативного налагодження безперебійного функціонування радіотелекомунікацій (передачі даних); забезпечувати достовірність засобами метрології даних за цільовим призначенням для економіки згідно потреб у видах економічної діяльності; розробляти та регулювати роботу захищених електронних баз.

У межах парадигми безпеки життєдіяльності та охорони праці фокус у підготовці майбутніх фахівців як професійно компетентних з інформаційної безпеки, трансформується з абстрактного захисту інформаційних масивів даних на фокус-убезпечення матеріальних об'єктів через інформаційні канали при забезпеченні функціоналу систем професійної зайнятості управління інформаційного безпекою в галузі.

Систематизовано та запропоновано практичні рекомендації змістових конструктів, імплементованих у структуру загальної, професійної та спеціальної підготовки майбутніх фахівців в галузі у розрізі освітніх компонентів, відповідно:

«Соціальна політика», яка зважаючи на специфіку людського чинника та цифрову етику, соціальна складова полягає у реалізації права персоналу на безпечні умови праці та захист населення від наслідків техногенних ризиків і небезпек (аварій, катастроф); забезпечення психологічної стійкості передбачає формування готовності фахівців до оперативного прийняття організаційно-управлінських рішень у складних кризових ситуаціях (в умовах фіксованих кібератак на об'єктах критичної інфраструктури), яку вбачаємо невід'ємною частиною культури безпеки праці, інформаційної, академічної й корпоративної культури стейкхолдерів. Етика соціальної (правової, екологічної) відповідальності та цифрова етика – усвідомлення, що компрометація систем управління (радіовежами або енргомережами) трансформується з цифрової проблеми у прямі ризики та загрози життєдіяльності людей.

«Соціальне страхування, санітарія та гігієна праці» – дотримання регламентів професійної праці з високочастотними випромінюваннями (мереж, радіотелекомунікацій) з високою напругою.

«Інформаційна політика» – технічне регулювання та інформаційна безпека систем/мереж/процесів. Інформаційна політика передбачає упорядкування оповіщення населення , зокрема щодо передачі сигналів тривоги та забезпечення управління безпекою систем моніторингу та охорони праці. Активність сигналів сповіщення передбачається у політичних стратегіях державних вимог у вимогах безперебійності та захищеності каналів екстреного зв'язку (сигнали цивільної оборони, системи 112). Захист інформаційних даних щодо стану здоров'я населення передбачає захист даних біометричного моніторингу та показників метрології зі стану здоров'я персоналу та активів рекреаційного потенціалу.

«Кібер-фізична безпека» – стандартизація засобів технічного регулювання щодо захисту автоматики з метою запобігання несанкціонованого відключення систем життєзабезпечення робочої зони (вентиляції, освітлення, протипожежних систем) .

3. Структура і змістове наповнення підготовки щодо безпеки життєдіяльності, охорони праці і інформаційної безпеки – інтеграційний контент. Для майбутніх фахівціводо реалізації інормаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій синергізовано складові електробезбеки та технічного захисту інформації, безпеки електромагнітних процесів.

Електробезпека та технічний захист інформації передбачає поєднання методів захисту від ураження струмом із технологіями технічного захисту інформації в разі втрати в ланцюгах живлення.

Безпека електромагнітних процесів: вивчення санітарно-гігієнічних норм Міністерства охорони здоров'я щодо гранично допустимих рівнів випромінювання передавальних пристроїв як засобів унормування працеохоронних заходів для інженерів зв'язківців. Забезпечення метрологічної надійності систем захисту інформації, навчання майбутніх фахівців щодо надійності датчиків газу, радіації чи тиску.

Підсумкові зведення полягають у формулюванні умовиводу, що інформаційна безпека є запорукою/градієнтом фізичної здатності виживання людини у галузі електроніки та зв'язку. Визначені вразливі у протоколах невідповідності або помилки програмного забезпечення систем управління/підготовки автоматично порушують умови праці (працеохоронний) та підвищують потенційний ризик життєдіяльності.

Атестація працівників та сертифікація їх робочих місць у галузях електроніки, метрології та радіотелекомунікацій потребує дотримання технічних стандартів інформаційної безпеки, так і вимог охорони праці, що є обов'язковим чинником гарантій допуску до середовища професійної зайнятості із високочастотним обладнанням, засобами криптозахисту та на об'єктах критичної інфраструктури.

Уточнено та конкретизовано сертифікаційні регламенти та спеціальні вимоги для галузі електроніки у сфері зв'язку щодо нормативного базису

процесу сертифікації робочих місць; визначено, що робочі місця фахівців повинні відповідати певним критеріям:

– законодавчим вимогам Законів України – «Про охорону праці» [3], «Про соціальні послуги» [4], «Про статус і соціальний захист громадян, які постраждали внаслідок Чорнобильської катастрофи» [5], «Про основні засади соціального захисту ветеранів праці та інших громадян похилого віку в Україні» [6], «Про соціальний і правовий захист військовослужбовців та членів їх сімей» [7], «Про соціальний захист та підтримку дітей, які постраждали внаслідок збройної агресії Російської Федерації проти України, та внесення змін до деяких законодавчих актів України щодо впорядкування надання соціальних послуг та виплат» [8] щодо загальних умов безпеки (освітлення, економіка, мікроклімат праці);

– спеціальним вимогам НПАОП 0.00-1.28-10 – правилам експлуатації електронно-обчислювальних машин [9];

– засобам стандартизації ДСТУ ISO/IEC 27001 – стандартам фізичної безпеки середовищ обробки інформації обмеженого доступу користування.

Для фахівців для реалізації інформаційної безпеки сертифікацією робочих місць передбачено дотримання спеціальних вимог для галузі електроніки, а саме – електромагнітної гігієни середовища праці, нагляду за електромагнітним фоном, унормованого МОЗ, що одночасно мінімізує фізичний вплив/забруднення середовища праці та убезпечує інформаційний обіг даних у системі побічних електромагнітних випромінювань та наведень щодо інформацію безпеки; електробезпеки – роботи з електроустаткуванням електроустановки, що монтуються за нормативами правил налаштування електроустановок, повинні мати заземлення. У контексті технічного захисту інформації сприяє запобіганню, передбаченню, виникнення та усунення шкідливих сигналів у мережах живлення.

Специфіка захисту шляхом екранування роботи з конфіденційними електронними засобами, робочий екран підлягає сертифікації як «екранована робоча комірка – зона приміщення» від дистанційних втрат інформації:

4.Інструментальне забезпечення технічного оснащення щодо організації робочих місць інженерів, що підлягають сертифікації та забезпечуються: метрологічно верифікованим обладнанням: приладів спектроаналізування, осцилографування та метрики напруги полів, які сертифіковані державною повіркою (Держспоживстандарту), що засвідчує достовірність вимірювання параметрів; убезпеченими каналами зв'язків зі використанням сертифікованих програм програмного забезпечення та процесно-апаратного ключа – токена, VPN з позитивним експертним підтвердженням (Держспецзв'язку).

5. Преференції відповідальності та соціально-правового захисту включають інструкції для фахівців після підтвердження інструктажів з техніки безпеки та працеохорони з електроапаратними комплексами та з режимом конфіденційності щодо доступу даних; врахування професійних ризиків у діяльності, що враховуються у трудових договорах на зразок роботи з високим оптико-сенсорним та психолого-емоційним напруженням, яке властиво при здійсненні моніторингових процедур розгляду кіберінцидентів).

Система професійної підготовки майбутніх фахівців галузі електроніки, метрології та радіотелекомунікацій ґрунтується на метрологічному базисі верифікації метрики даних. У разі визначення скомпрометованих джерел (кібератаки або заміни еталонів), архітектура інформаційної безпеки в цілому втрачає кіберспроможність захисту.

Виокремлено змістові компоненти метрологічного наповнення у фахівців – законодавчі акти з метрології та стандартизації – Закони України «Про метрологію та метрологічну діяльність» [10]; міжнародних засобів стандартизації ISO/IEC 17025 (нормативні регламенти для випробувальних та калібрувальних лабораторій); особливу увагу приділяють настановам Європейського співробітництва в законодавстві щодо метрології (з англ. – European Cooperation in Legal Metrology, далі – WELMEC, https://www.welmec.org/) щодо регулювання захисту програмного забезпечення систем вимірювальної метрики.

Техніко-регулятивні методи безпеки метрики оцінювання, застосування методів криптографічної повірки та підтвердження автентичності сигналів безпосередньо в сегментах вимірювань інтелектуальних датчиків верефікації безпеки перехоплення – впровадження методів кодифікації сигналу у радіотелекомунікаційній метриці вимірювань мережевих систем комунікацій; забезпечення розвиненості навичок розпізнавання «метрологічних фантомів» – штучно згенерованих даних, що винулюють штатну роботу процесно-апаратного обладнання.

Забезпечення інформаційного захисту в метрології шляхом верифікації та валідації програмного забезпечення для технічних засобів вимірювальної метрики, зокрема інтегрованих до хмарних мереж.

6. Ієрархічна архітектура системи підготовки майбутніх фахівців включає структурні компоненти освітнього процесу з врахуванням необхідності формування професійних компетенцій з інформаційної безпеки у сфері електроніки, радіотелекомунікацій, інформаційного захисту і менеджменту підтримки та забезпечення, не лише як фізичних явищ: рівнів – фізичного сигналу володіння методами прецизійного перетворення фізичних параметрів та захисту сенсорного обладнання від апаратного маніпулювання; передачі знань при опануванні процедур спеціалізованих протоколів передачі даних (з англ. – LoRaWAN, Wireless, M-Bus) у контексті забезпечення стійкості у ході заглушення сигналів (з англ. – jamming); опрацювання та зберігання інформації, оцінювання відповідності як системи метрологічним нормативам, так і аудиту процедур перевірки даних, валідації програмного забезпечення; забезпечення вимог стандартизації у професійній підготовці майбутніх фахівців, адже стандартизація дозволяє фахівцям оперувати прийнятною єдиною мовою опанування змісту і процедур технічного регулювання засобів інформаційної безпеки, а саме: інструментарієм менеджменту інформаційних ризиків (ISO/IEC 27002); нормами безпеки промислових систем автоматизації (ДСТУ 8393).

Засоби технічного регламентування слугують чинником правових гарантій допуску безпечного обладнання до роботи у професійних середовища; гарантом безпеки життя персоналу. У контексті охорони праці майбутні фахівці несуть відповідальність за параметри безпеки робочої зони персоналу, тому здобувачі освіти опановують методами прогнозування, запобігання та усунення складних і критичних ситуацій для убезпечення роботи в галузі.

Запропоновано тематичну рубрику практикумів, які забезпечують системність навичок і умінь з інформаційної безпеки та охорони праці у метрології, електроніки та радіотелекомунікацій .

Тема 1 «Метрологічний кейс надійності та захисту програмного забезпечення» передбачає вивчення – аудиту витривалості програмного забезпечення вимірювального програмно-апаратного комплексу приладів щодо застосування криптографічного шифрування у верифікації прошиття осцилографів або аналізаторів спектрів встановлення модифікаційних кодів; валідації протоколів опрацювання даних з експериментальною обробкою перевірки стійкості інтелектуальних систем до вкиду фальшованих даних (з англ. – False Data Injection, далі – FDI) та маніпуляційних змін метрологічних звітів; захист інтерфейсів калібрування при забезпеченні багаторівневих входів та автентифікації для низькорівневих сервісних портів (UART, JTAG) електронних модулів за для блокування несанкціонованих перепрошивок.

Тема 2 «Інформаційна безпека в радіотелекомунікуванні та електроніці» передбачає – аналізування технічних потоків витоку інформаційних даних за побічних електромагнітних випромінювань та наведень при застосуванні вимірювальних приймачів діагностики сигналів, випромінювання кабелів передачі; пошук способів безбар'єрності для цифрових каналів зв'язку зі моделюванням процедур протидії навмисним радіобар'єрам «глушіння» (з англ. – Jamming) та аналіз достовірності передачі метрологічних показників за умов посилення перешкод; аналізування параметрів безпеки бездротових сенсорних систем процесів (з англ. – LoRaWan/ZigBee); шифрування

інформаційних масивів даних моніторингу системи працеохорони в умовах виробничих середовищ.

Тема 3 «Безпека життєдіяльності та метрологічний контроль» передбачає метрологічну діагностику безпеки при верифікації газоаналізаторів або дозиметрів та робочого середовища (газових, радіаційних) з моделюванням напрямів та інтенсивності кібератак у реальних умовах; оцінювання електромагнітної безпеки робочої зони – інструментальний нагляд випромінювання від антенофідерних пристроїв та порівняння з гранично допустимими нормами Державних санітарних норм і правил; моделювання зламів системи захисту електроустановок при врахуванні причин і наслідків критичних невідповідностей у процесах захисту засобів автоматизації та упередження щодо небезпеки ураження струмом або пошкодження процесно-апаратних комплексів.

Визначено прилади та матеріали для організації занять, а саме: цифрові осцилографи з аналітичною функцією протоколювання; програмно-апаратні радіосистеми (з англ. – Software Defined radio, SDR) типу HackRF для забезпечення генерадіоефірів; еталонні джерела сигналів з повіреною діагностикою параметральної метрики електромагнітних полів.

Інформаційний менеджмент в галузі передбачає стратегічне керування інформаційно-технологічними циклами метрології та передачі у мережах телекомунікацій електронними засобами забезпечення.

Сформовано змістове забезпечення інформаційного менеджменту (з англ. – Data Governance), що присвячено управлінню життєвими циклами інформаційних потоків даних у технологічних системних комплексах, включає компоненти: управління активами (з англ. – Asset Management) ведення протоколів реєстрації процесно-апаратних засобів вимірювання як технічного обладнання, так і ліцензованого програмного забезпечення – згідно з вимог засобів технічних регламентів (ISO/SES 27001); менеджмент моделювання – контроль трансформацій налаштування мережевих систем і процесно-апаратного обладнання, маршруту даних і прошиття мікроконтролерів та

корекцією присвоєння калібрувальних коефіцієнтів у приладах вимірювання; організація унормованого документообігу шляхом стандартизації процедур технічних документів (паспортизація), протоколів та сертифікатів встановлення відповідності засобів радіозв'язку.

Розкрито архітектуру організації підготовки забезпечення навколо безпеки (з англ. – Secbrity Framwork) майбутніми фахівцями на базисі стандартизації цілісності непорушності і доступу у складових: апаратної безпеки (з англ. – Hardware Security), а саме специфіки захисту від впливу ураження апаратних троянів мікросхем та керування фізичним доступом до телекомунікаційних комірок сховищ; метрологічна безпека, менеджмент ризиків і небезпек фальшифування – замін вимірювальних показників (з англ. – Data Integrity), а саме опанування знань і особливостей застосування стандартів ДСТУ ISO 10012 щодо систем менеджменту вимірювань; менеджмент інцидентів з оформленням формулярів відновлення каналів зв'язку та проведення моніторингових систем після блокування мереж зв'язку або масового атакування на управління радіокомунікаціями.

Специфіка галузевого змісту триади – Електроніка, Метрологія, Радіотелекомунікації у освітніх програмах підготовки майбутніх фахівців (педагогів професійного навчання) передбачено інтеграцію питань менеджменту у технічні освітні компоненти: щодо електроніки – управління каналами постачання для запобігання втручання контрафактних та шпигунських мікросистем у процесно-апаратні комплекси; щодо метрології – організація системи метрики і верифікації «метрологічного сліду» у довірчих ланцюгах від діагностики робочих датчиків до забезпечення відповідності державним еталонам в середовищі цифровізації професійної зайнятості майбутніх фахівців; щодо радіотелекомунікацій – системне адміністрування радіочастотних спектрів та дотримання безпекових протоколів передачі даних (SDN, NFV).

У таблиці 2.1 представлено модель матриці типового процесу метрологічної метрики керування телекомунікацій та у Додатку В вказано розподіл функціоналу майбутніх фахівців.

Таблиця 2.1

Матриця RACI – Менеджмент безпеки та метрології

Процеси/значення	**Повноваження фахівця-метролога**
Неопрошивка вимірювального обладнання	A (Затвердження відповідальним за результат процесу)
Валідація та перевірка достовірності датчиків	R/A (Виконавець/ відповідальна особа)
Реакції на кіберінцедент у процесах зв'язку	C (оцінювання впливів на день), експерт, консультант
Нагляд за електромагнітним фоном	C (організація діагностики приладів)
Резервне копіювання метрологічних звітів	C (визначення термінів/поінформування)

Зв'язки безпеки життєдіяльності та працеохорони забезпечує інформаційний менеджмент через підтримку безпекових рішень щодо: діджиталізації систем управління працеохорони – модернізація автоматизованого моніторингу стану готовності майбутніх фахівців і задіяного персоналу та організація електронних протоколів інструктажів з охорони праці; антикризовий менеджмент – розбудова архітектури трафіку, що у разі аварійних ситуацій оперативно забезпечує активність сигналів екстрених служб над звичайним трафіком у мережах; матриці «Виконавець, відповідальний, експерт, інформований» (з англ. – Responsible, Accountable, Consulted, Informed, далі – RACI), що сприяють визначенню обов'язків функціоналу між технічними фахівцями та менеджментом системних адміністраторів за для реалізації інформаційної безпеки згідно метрологічної точності метрики вимірювання показників (допустимих, надійності).

2.2 Педагогічні умови реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій

Виокремлено та обґрунтовано з практичними рекомендаціями педагогічні умови забезпечення впровадження Моделі, а саме – формування сприятливого середовища плекання інформаційної культури; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу та мережева інформаційна безпека системи.

Простір формування інформаційної культури – це комплекс ресурсів: технічних, інформаційних, програмних засобів, а також соціокультурних та правових умов, що сприяють ефективній діяльності людини в інформаційному суспільстві; охоплює навички пошуку, критичної оцінки, безпечного використання та створення нової інформації, генеруючи етичні та технологічні аспекти.

Компонентами й складовими потенціалу інформаційної культури є:

технічний та програмний базис, що включає комп'ютерні мережі (інтернет), автоматизовані системи – сховищ та аналізу опрацювання даних, а також контролю (АСК).

інформаційні ресурси електронних баз інформації, цифрових бібліотек та архівів правового та технічного регулювання;

індивідуальна\особистісна культура включає уміння – застосування цифрової та правової грамотності, креаційного, аналітичного, критичного мислення, формулювання запитів та етичного використання контентів;

соціокультурні умови правових норм гарантій соціального захисту, інформаційної безпеки та кіберзахисту, а також академічної, цифрової та професійної етики поведінки в мережах.

Простір інформаційної культури розбудовує архітектуру як у освітньому, професійному, так і у соціально-побутовому середовищах в умовах рівноважної взаємодії Людини – Природи – професійної сфери з інформаційними масивами і потоками даних.

Формування середовища сприяння інформаційної культури як педагогічної умови полягає у забезпеченні цілісної неперервної системи підготовки та організації освітнього процесу із формату трансляції знань у простір активної навчально-пізнавальної взаємодії усіх учасників освітнього процесу згідно потреб у цільовій інформації за призначенням користувачів.

Розглянуто механізми нарощення потенціалу інформаційної культури:

розробка проєкту змістового наповнення циклів і структури навчання, інтеграція освітніх завдань для здобувачів і споживачів послуг на навчально-науково-пізнавальну діяльність та пошук, критичне аналізування та етичне використання інформаційних даних, а не лише в інформаційні модулі;

формування цифрового освітнього простору зі впровадженням хмарних технологій, мультимедійних засобів та віртуальних бібліотек, що забезпечує неперервний доступ до якісних освітніх ресурсів;

запровадження інтерактивних методів навчання зі застосуванням веб-квестів, гейміфікації/ігровізації та проєктної діяльності для формування практичних навичок і умінь з інформаційної діяльності за призначенням середовищ майбутньої професійної зайнятості;

зростання потенціалу інформаційної культури педагогічних працівників, надавачів послуг як модераторів інформаційних масивів даних сучасних наукових знань галузі з відповідним рівнем цифрової, економічної, екологічної та медіаграмотності та технологічної компетентності;

мотиваційне забезпечення для розвитку у здобувачів освіти усталеної внутрішньої потреби в неперервному оновленні сучасних наукових знань і самостійної науково-пошуковій діяльності з метою самовдосконалення через самоосвіту, самоменеджмент і професійне зростання.

Інформаційний принцип у організації освітнього процесу сприяє переходу від рівня «комп'ютерної обізнаності» до сформованого потенціалу інформаційної культури здобувачів освіти, свідомого існування в умовах цифровізації суспільства.

Технічні та програмні інструменти формування середовища інформаційної культури в ЗВО задля забезпечення його функціонування як педагогічної умови передбачає інтеграцію ключових засобів інструментарію, а саме:

– системи керування навчанням (LMS) – Google Classroom, Moodle, Canvas;

– хмарні сервіси для корпоративної співпраці – Google Workspace (Docs, Sheets), Miro, Padlet;

– інструментарій візуалізації та креативності, а також проєктування, моделювання, дизайну – Canva, Genially, Prezi;

– засоби нагляду та самоперевірки – Kahoot!, Quizizz, Plagiarisma (Turnitin);

– електронні бібліотеки, архіви та освітні інформаційно-телекомунікаційні платформи й науково-метричні бази – Scopus, Web of sience, Google Scholar, Coursera, EdEra.

Виокремлено критерії та показники метрики вимірювання рівня сформованості інформаційної культури у здобувачів освіти. З метою оцінювання ефективності функціоналу освітнього середовища в умовах цифровізації, надавачі послуг спираються на систему взаємоузгодженого критеріального апарату скринінгового стану дослідження відповідності педагогічних умов потребам організації освітнього процесу:

когнітивний критерій – передбачає усвідомлення учасниками освітнього процесу механізмів роботи пошукових алгоритмів/систем, обізнаність щодо авторського права, інтелектуальної власності та правил академічного цитування, академічної етики та доброчесності, керівних принципів інформаційної та кібербезпеки й особливостей функціонування середовища навчання, дослідництва й інноватики в умовах цифровізації;

діяльнісний критерій – визначає пошукову активність учасників освітнього процесу (здатність оперативно ідентифікувати релевантні дані з різних джерел походження, технологічну адаптивність у доборі та

укомплектуванні освітніх, інформаційних і соціокультурних технологій, а також сформованість цифрової, зокрема медіаграмотності, яка виявляється в умінні виокремлювати достовірну інформацію та уникати маніпулятивний чи фейковий контент;

ціннісно-етичний критерій – визначає відповідність вимогам щодо дотримання норм мережевого/цифрового етикету, соціально та екологічно відповідального ставлення до захисту персональних даних усіх учасників освітнього процесу (особливо здоровязбереження і впливу на них стану надзвичайних ситуацій), сприяння розвитку у них критичного, аналітичного та креаційного мислення у опрацюванні споживаного контенту та неприйнятності плагіату.

Оптимальним шляхом практичної реалізації зазначеної педагогічної умови є переорієнтація під час організації/модернізації освітнього процесу з пасивного засвоєння відомостей («інформування щодо інформаційних даних») на активну навчально-науково-пізнавальну діяльність у цифровому освітньому просторі. До прикладу, замість традиційного реферату, що зачасту передбачає механічне копіювання, доцільно запропонувати здобувачам освіти розроблення колективної Wiki-сторінки (онлайн-сторінки web-ресурсів) або аналітичного огляду. У межах навчального завдання кожен учасник має здійснити пошук щонайменше п’яти першоджерел, перевірити їх достовірність та оформити бібліографічне посилання згідно вимог у відповідності до встановлених стандартів.

У забезпеченні праксеології сприяння формування простору інформаційної культури як педагогічної умови навчальні завдання проєктують за принципом «від споживання до продукування». Розроблено адаптивну модель навчального проєкту, запропонованого здобувачам освіти згідно змісту обраного освітнього компоненту.

Назва проєкту – «Інформаційна розвідка: від ланцюгів пошуку даних до визначення їх достовірності» з метою опанування змісту теми обраної проблематики цільового призначення та оволодіння процедурами верифікації

інформаційних даних щодо вимог академічної етики та доброчесності й апробації з інструментарієм візуального оприлюднення результатів навчальних досягнень здобувачів освіти за для параметральної оцінки якості інформаційних масивів даних з метою вирішення складних і критичних ситуацій щодо інформаційної безпеки системи.

Виокремлено етапи алгоритму підготовки навчального проєкту, а саме: перший етап «Формування завдання як замовлення на розробку (когнітивний аспект)», другий етап «Фільтрація, концентрація, визначення та критичний аналіз (аналітичний аспект)», третій етап «Співпраця та академічна етика (ціннісний аспект)» та четвертий етап «Креаційне опрацювання (організаційно-діяльнісний аспект)».

Завдання першого етапу полягає у формулюванні щонайменше трьох функціональних пошукових запитів з використанням логічних сервісів (лапки для конкретизації формулювань, оператор «–» для вилучення невідповідностей як результатів пошуку тощо); інструментарій: Google Scholar, інші пошукові системи; очікувані результати: укомплектування набору із п'яти істотних у змістовому сенсі джерел, а саме – наукові статті, монографії, дисертації, проєкти, відеоматеріали, підкасти контентів).

Завдання другого етапу «Фільтрація, концентрація, визначення та критичний аналіз (аналітичний аспект)» – провадити оцінювання виокремлених інформаційних джерел за допомогою CRAAP-тесту:

актуальність (з англ. – currency) – дата оприлюднення та відповідність сучасному стану проблеми дослідження;

релевантність (з англ. – relevance) – відповідність визначеній меті дослідження;

авторитетність (з англ. – authority) – професійна компетентність авторів, їх репутаційне реноме;

точність (з англ. – accuracy) – наявність доказової доведеності та коректних посилань на першоджерела;

мета (з англ. – purpose) з англ. – інформування, комерційний вплив чи пропагандистський, популіський, просвітницький характер доробку.

Очікуваний результат – здійснено добір не менше трьох достовірних та науково визнаних джерел у пануючих теоріях і переконаннях академічної спільноти.

Завдання третього етапу «Співпраця та академічна етика (ціннісний аспект)»: створення спільної ментальної карти (з англ. – Mind Map) або інтерактивного оголошення, де кожен учасник презентує одну ключову тезу зі свого джерела з обов'язковою активізацією гіперпосилань на першоджерела; застосування інструментарію – Miro, Padlet, Google Jamboard.

Окремі визначено вимоги щодо уникнення прямого цитування без належних посилань при подачі змістових контентів у форміаті коректних перефразувань з дотриманням принципів академічної доброчесності.

Завдання четвертого етапу «Креаційне опрацювання (діяльнісний аспект)» передбачає узагальнення змістового навчання контенту матеріалів і розробку освітнього продукту у якості ресурсу для апробації та верифікації. Приклади освітніх продуктів – проєктування аналітичної інфографіки (засобами Canva); розробка навчальних відеопрезентацій у форматі призначення соціальних мереж (Tik-Tok/Reels стилістики); інтерактивний цифровий пост/плакат/модель, оформлений засобами інструментарію (створений у Genially).

Обґрунтовано критерії оцінювання навчального проєкту:

релевантність переліку джерел (2 бали): використання розлогого спектра інформаційних ресурсів (статті, відео-контенти, авторські курси, наукові праці тощо) з верифікацією їх достовірної надійності;

дотримання визначеної політики ЗВО академічної етики і доброчесності (2 бали): коректне оформлення згідно вимог стандартів бібліографічних покликань, відсутність ознак плагіату;

технічна операційність (2 бали): обґрунтовано доцільність добору цифрового інструментарію, забезпечення структурованості та візуальної сприйнятності їх презентації.

рівень критичного мислення (4 бали): здобувач освіти аргументує обґрунтованість причин відхилення невідповідностей окремих джерел як недостовірних або нерелевантних для досягнення цільової мети дослідження обраної проблеми.

Інформаційно-технологічне забезпечення та сервіс у системі освітньо-наукової діяльності ЗВО це не лише усукупнення окремих програмних продуктів, а й цілісна єдність функціональної орієнтації сервісної системи, що забезпечує автоматизацію управління, моніторингу ефективності та нагляду за організацією освітнього процесу, підтримку академічних шкіл наукових досліджень та ефективніх комунікацій (соціокультурні, інформаційні тощо) між усіма суб'єктами освітнього середовища.

У контексті сприяння формуванню простору інформаційної культури, цифровий інформаційно-технологічний сервіс повинен мати ознаки транспарентності (прозорості, доступності, відкритості), партисипатії (взаємодії в управлінні) інтерфейсу, що забезпечує користувачів змістовим наповненням діяльності, а не лише у зв'язку з подоланням технічних перешкод.

Окреслено структуру сучасного інформаційно-технологічного забезпечення та сервісу у ЗВО:

освітній сегмент (з англ. – learning management) – системи освітнього менеджменту (Moodle, Google Classroom, Canvas), які здійснюють функції інформаційно-технологічного парку/хабу для розміщення навчальних і наукових продуктів/ресурсів та методик оцінювання; електронний розклад та персональні кабінети здобувачів/викладачів – забезпечують автоматизований облік і контроль за результатами навчальних досягнень, моніторинг якості управління; платформи для воркшопів, майстер-класів, вебінарів – інтеграція сервісів Zoom/Teams/Meet безпосередньо в структуру освітніх програм та практичної підготовки;

науково-дослідницький компонент/архітектура (з англ. – Research infrastructure) – інституційний репозитарій (відкрите електронне архівоване сховище наукових доробків учених, викладачів та здобувачів освіти (зокрема на базі DSpace тощо); наукометричний інструментарій як авторизований доступ до інформаційних баз даних (Scopus, Web of Science, ScienceDirect); системи діагностики текстових контентів на плагіат і ШІ, основні інструменти відповідності вимогам академічної етики та доброчесності (StrikePlagiarism, Unicheck); координатори керування бібліографією (підтримка роботи з Mendeley, Zotero, EndNote для систематизації джерельної бази);

адміністративно-комунікаційний компонент – електронний документообіг (цифровізація управлінських процедур) і мінімізація паперових носіїв справочинства (заяви, накази, звітність); корпоративна електронна пошта та хмарні технології/сховища зберігання (зокрема Microsoft 365 та Google Workspace), що формують уніфікований простір для збереження й обміну інформацією.

Виокремлено статус інформаційно-технологічного забезпечення та сервісу як чинника забезпечення розбудови середовища інформаційної культури, адже інформаційно-технологічне забезпечення і сервіс як педагогічна умова не обмежується функціональним призначенням, а сприяє формуванню відповідних практик професійної поведінки у учасників освітнього процесу:

дотримання принципу єдиного входу (з англ. –«Single Sign-On») передбачає використання одного облікового запису для доступу до ресурсів, що забезпечує відповідальне ставлення до захисту персональних даних (власних та інших осіб);

2) персоналізація – можливість адаптації цифрового середовища відповідно до індивідуальних освітніх і дослідницьких потреб користувачів;

3) мобільність – забезпечення мобільних застосунків і сервіс формату m-learning, що забезпечує неперервність навчання у соціально-турбулентних умовах.

У таблиці 2.2. представлено алгоритм практичного впровадження інформаційно-технологічного забезпечення та сервісу в якості організаційної процедури адміністрування в ЗВО.

Таблиця 2.2

Матриця впровадження інформаційно-технологічного забезпечення та сервісу для ЗВО

№ етапу	Дія сервісу	Результат культури
Доступність	Надання Wi-Fi та доступу до хмарних сервісів 24/7	Уміння працювати з будь-якою інформацією
Навігатор	Створення єдиного порталу сервісів (Dashboard)	Здатність структурувати власну цифрову робочу зону
Облік і контроль	Автоматична перевірка доробків на плагіат і ШІ	Усвідомлення аксіологічної цінності захисту авторства, інтелектуальної власності та оригінальності
Зворотній зв'язок	Електронні опитування (Quality Assurance)	Менеджмент удосконалення/модернізації освітнього середовища

Встановлено проблеми та ризики невідповідностей у проєктуванні інформаційно-технологічного забезпечення та сервісу, які принципово необхідно уникати/мінімізувати ризики виникнення «цифрового бар'єру», за наявності яких надмірна складність інтерфейсу сервісу перетворюється на чинник – невідповідності умовам якості й безпеки організації освітнього процесу. У зв'язку з цим необхідним компонентом системи є Help Desk та постійні воркшопи/тренінги/методичні семінари для викладачів (з англ. – Digital Literacy Training).

Інтеграція наукометричного інструментарію у професійну підготовку здобувачів освіти, що сприяє їх становленню зі статусу пасивних споживачів теоретичних знань на активних суб'єктів навчально-науково-пізнавальної діяльності та набуття рівноправної позиції учасників/управлінців у

академічному співтоваристві, що, в свою чергу, у подальшому забезпечить базис формування інформаційної культури навчання та дослідництва.

Запропоновано абриси Моделі застосування наукометричних сервісів в освітній процес складається з :

лабораторної роботи «Науково-метричний цифровий профіль дослідника», під час якої здобувачам пропонується сформувати власний цифровий науковий профіль ідентичності; завдання – створення власного профілю в Google Scholar з метою набуття навичок управління персональною науковою репутацією та представлення/презентації/апробації наукових результатів; свідоме критичне ставлення до власної наукової діяльності як публічної категорії та оприлюднення процесу верифікованої ідентифікації статусу дослідника;

практичної роботи на кшталт пошуково-аналітичного практикуму інформаційного пошуку у наукометричних базах, що передбачає не лише оволодіння інформацією, а й метрику оцінювання валідованих наукових результатів і продуктів; завдання – виокремити не менше п'яти найцитованіші доробки, опубліковані за проблематикою дослідження за останні три роки; інструментарій (наукометричні платформи Scopus, Web of Science для академічних комунікацій у системі ResearchGate); мета педагогічної аналітики – визначення провідних науковців, авторів і рейтингових видань у відповідній галузі науки й знань, що формує здатність у здобувачів освіти орієнтуватися у структурі світового академічного простору;

самостійної роботи – використання бібліографічних керівних застосунків як інструментів автоматизації та нагляду; завдання – автоматизація формування переліків використаних інформаційних джерел для підготовки теоретичного обґрунтування досліджень у курсових і випускових роботах; інструментарій (Zotero або Mendeley); прогнозований результат – оптимізація часових витрат на технічне опрацювання покликань і аналітичне узагальнення та синтез інноваційних/креаційних ідей;

самостійної роботи – оцінювання якості наукових доробків інформаційних джерел (зокрема Journal Metrics) з метою навчання диференціації провідних наукових видань, публіцистичних та просвітницьких; завдання – визначення приналежності до класифікації квартилів (Q1-Q4) журналів за показниками рейтингу журналу Scimago (з англ. – Scimago Journal Rank, далі – SJR) з метою формування критичного аналітичного ставлення до добору наукових, довідкових, навчальних джерел та свідомого вибору фахових науково-метричних платформ для публікації наукових результатів досліджень.

У таблиці 2.3 наведено практичний алгоритм у етапах практичної схеми інтеграції до освітнього компоненту.

Таблиця 2.3

Практична схема інтеграції в освітні компоненти

Етап	Алгоритм для здобувачів	Результат
Інформаційного пошуку	Використання операторів Boolean у Scopus	Відповідна релевантність очікувань щодо призначення переліку джерел
Зберігання даних	Імпорт метаданих у Zotero	Власна цифрова бібліотека
Аналізування	Порівняння індексів Хірша провідних науковців	Визнання наукових трендів, пріоритетів, напрямів досліджень
Публікації	Перевірка журналу в переліку фахових видань МОН України/ Scopus/ WoS	Академічна етика та політика безпеки

Формат практичного заходу воркшоп «Наукове письмо, наукометрія» для поетапного опрацювання текстових контентів та їх інвентаризації у виданнях встановленого науково-метричного формату з інструментарію метрики оцінювання визнання наукових результатів.

Запропоновано зміст і структуру освітнього компонента «Цифрове забезпечення та інформаційна культура у наукових дослідженнях у модулях», що має на меті – формування компетенцій автоматизації науково-дослідної роботи. Модуль 1. «Стратегія пошуку» передбачає навігацію по міжнародним наукометричним платформам (Scopus та Web of Science); професійна майстерність щодо ранжування класифікаційних ознак у хронології, типах публікацій та у галузях наук і знань. Модуль 2. «Керування джерельністю

інформаційних баз) передбачає – роботу із Zotero (налаштування інтеграції з браузерами та текстовими редакторами); формування персональних когнітивних профілів як банкінгу сучасних наукових знань. Модуль 3. «Академічна етика і доброчесність, ідентифікація» передбачає створення профілів в ORCID та ResearchGate; правові та етичні аспекти соціальної й академічної відповідальності. Модуль 4. «Аналітичне оцінювання й експертиза якості журналів» має на меті оцінювання авторитетності видань за допомогою аналітичної платформи SJR.

Виокремлено покрокова міні-інструкція для здобувачів освіти :

алгоритм пошуку еталонних публікацій – відкрийте Google Scholar; для отримання доступу до повнотекстових матеріалів додайте оператор filetype:pdf; оберіть інструмент «Цитувати», для швидкого створення покликання за стандартом APA або ДСТУ; збережіть знахідки у персональному кабінеті за допомогою функції «Моя бібліотека»;

процес автоматизації списку літератури (Zotero) – завантажте Zotero Connector для Chrome/Firefox; під час перегляду публікації на порталі видавництва, натисніть на піктограму розширення (метадані статті будуть автоматично імпортовані до персональної бази); у тексті роботи (MS Word) скористайтесь вкладкою «Add/Edit Citation», оберіть потрібне джерело і система автоматично сформує коректні покликання та фінальний бібліографічний список;

перевірка академічної доброчесності журналу – випишіть найменування видання або його код ISSN; знайдіть сторінку часопису на ресурсі SJR; встановіть – наявність маркерів якості (приналежність видань до квартилів Q1 або Q2, стабільну позитивну динаміку графіків як підтвердження їх високої репутації).

Окреслено необхідні ресурси для педагогів, науковців, а саме платформ – Coursera: Genealogies of Knowledge, що спрямована на концептуальний аналіз генезису та еволюції наукових текстів; офіційні ресурси від Clarivate як україномовні вебінари, які присвячено методології роботи з міжнародною

базою даних Web of Science; Prometheus з комплексом спеціалізованих курсів з питань дотримання академічної етики і доброчесності.

Для трансформації інформаційно-технологічного забезпечення та сервісу із допоміжного інструментарію в сприятливу педагогічну умову необхідно забезпечити його інтеграцію в освітній простір як середовище, що детермінує оновлення методик і методів навчання. Алгоритм реалізації педагогічної умови як організаційну процедуру рекомендовано для ЗВО у етапах впровадження:

– технологічний етап – сервісно-орієнтована архітектура інформаційно-технологічного забезпечення та сервісу має бути безшовною, що забезпечується через упровадження єдиної комірки доступу (SSO) для уніфікованого входу до LMS Moodle, репозитаріїв та наукометричних баз, а також застосування хмарної мобільності (Google Workspace for Education або Microsoft 365), що надає змогу забезпечити синхронне партнерство корпоративної взаємодії;

– методичний етап – створення цифрового освітнього контенту з інтерактивним змістом можливостей мікронавчання (з англ. – Microlearning), а саме розбивка матеріалів на лаконічні відео-контенти, інтерактивні тести в H5P та презентації-симуляції; адаптивність налаштування сервісів пропонує здобувачам освіти додаткові матеріали в залежності від персоналізації траєкторії та навчальних досягнень;

– суб'єктний етап – технологічна підтримка суб'єктів щодо мінімізації «технологічного стресу" службами підтримки HelpDesk (чат-боти, інструкції, рекоменації) та впровадження цифрового наставництва через практичні воркшопи з цифрової грамотності (Zotero);

– діагностичний етап – моніторинг та фітбек як сервіс, який забезпечує автоматичний збір даних про активність користувачів, зокрема навчальної аналітики (з англ. – Learning Analytics) – педагоги бачать через панель керування LMS, на якому етапі здобувачі освіти «гальмують», і оперативно коригують завдання; цифрове портфоліо – сервіс, що забезпечує

автоматичне накопичення досягнень здобувачів (сертифікати Coursera, Prometheus тощо, наукові публікації).

Приклад практичного кейсу викладачі надають за допомогою покликання (зокрема на інтерактивну дошку Padlet) зі інтегрованими пошуковими запитами в Scopus; шаблони для редагування Google Docs; перелік автоматизованих систем/перевірок на плагіат та ШІ, що забезпечує здобувачам освіти алгоритм дослідницьких дій інформаційно-технологічного забезпечення та сервісу.

Мережева інформаційна безпека (далі – МІБ) у організації професійної підготовки в ЗВО вбачається не лише як технічний контекст зі захисту інформаційних даних, а як інформаційно-безпековий базис формування професійної підготовки майбутніх фахівців в цифровому освітньому просторі та убезпечує організацію освітнього процесу. Забезпечення МІБ у професійній підготовці майбутніх фахівців реалізується на трьох взаємопов'язаних рівнях:

технологічний рівень (інфраструктура), на якому створюється безпечне середовище для здобувачів освіти та надавачів послуг з автентифікацією та доступом при впровадженні двофакторної автентифікації (2FA) для входу в LMS (Moodle) і корпоративну пошту; захист у мережі каналів зв'язку при використанні VPN для доступу до академічних ресурсів ЗВО та шифрування даних (SSL/TLS); фільтрація контентів з налаштуванням мережевих екранів (з англ. – Firewalls) для блокування небезпечних ресурсів у внутрішній мережі університету;

освітньо-методичний рівень (змістове наповнення навчання) , на якому МІБ необхідно інтегрувати в освітні програми як наскрізну компетенцію кібергігієни для навчання протидії фішингу, реалізації проєктів соціальної інженерії та захисту персональних даних, а також академічної безпеки (захисту авторських прав, інтелектуальної власності використання ліцензій Creative Commons); формування навичок, умінь, здатностей до управління «цифровим слідом» забезпечення, розуміння причинно-наслідкових зв'язків активності у мережах нині та впливу на їх (учасників освітнього процесу) майбутню професійну репутацію (з англ. – Personal branding security).

етико-правовий рівень (інформаційна культура), на якому реалізується дотримання корпоративних стандартів поведінки майбутніми фахівцями шляхом упровадження Політики прийнятного використання (з англ. – Acceptable Use Policy, далі – AUP). Розвиток критичного мислення для верифікації інформації, протидії фейкам та маніпуляціям у професійній сфері; захищеність партнерської співпраці у розробках зі хмарними сервісами (таких як Google Workspace, Teams). У таблиці 2.4 візуалізовао педагогічний вплив мережевої інформаційної безпеки як умови забезпечення ефективності Моделі.

Таблиця 2.4

Забезпечення МІБ як педагогічної умови

Компоненти	Педагогічна дія	Результати
Превентивний	Тренінги з кібербезпеки для абітурієнтів, слухачів і здобувачів III і IV курсів	Мінімізація ризиків втрати інформаційних даних
Навчально-науково-діяльнісний	Моделювання кіберзагроз у професійній сфері	Навички та уміння операційного реагування на інциденти невідповідностей
Наглядовий	Моніторинг дотримання правил етики мережевої безпеки	Формування професійної компетентності та відповідальності

Практичну роботу «Кібер-майданчик» для здобувачів вищої освіти доцільно впроваджувати з віртуальними симуляціями для вирішення професійних завдань в умовах імітації кібератак або дотримання обмеженого доступу, що сприятиме пізнавальній трансформації теоретичних знань у професійні здатності та компетентності на практиці.

Система мережевої безпеки у ЗВО забезпечує виконання функції захисту цифрового освітнього середовища та є інструментарієм гарантій академічної свободи.

Розроблено інтенсив-спецкурс «Кібербезпека в сфері освіти, науки й інноватики: від навчання до компетентності» у форматі циклу 3 вебінарів (по 60 хвилин) з практичним тренінгом: 1) гігієна кібербезпеки облікових даних –

підбір надійних паролів та використання керівних застосунків (Bitwarden, LastPass); налаштування 2FA в Google Workspace та Moodle; практичний тренінг з перевірки власної електронної пошти на несанкціоновані витоки через сайт (Have I Been Pwned, https://haveibeenpwned.com/); 2) захист мережевих комунікацій та хмарних сервісів – диференціація рівнів доступу в Google Docs, запобігання Zoom-бомбінгу, ідентифікація фішингових розсилок в академічному просторі; 3) академічна мережева безпека та інтелектуальна власність – методики захисту та маркування авторських доробків з використанням Creative Commons.

Запропоновано пам'ятку зі кібергігієни для здобувачів освіти за концепцією «Друкуй і використовуй»(з англ. – Print&Use): 1) забезпечуйте унікальність паролів, створюйте ексклюзивну комбінацію для кожного сайту, аби уникнути несанкціонованих зламів, періодично оновлюйте паролі раз на кілька місяців і уникайте дублювання коду для декількох сайтів; 2) дотримуйтеся подвійного захисту (2FA) – вмикайте двофакторну автентифікацію під час роботи з корпоративною поштою та при відвідуванні університетських платформ; 3) здійснюйте перевірку покликань, адже перед завантаженням файли варто уточнити адресу посилань; 4) дотримуйтеся безпеки підключень, уникай використання вікритих мереж з незахищеним Wi-Fi без VPN при роботі з конфіденційною інформацією; 5) пам'ятайте про цифровий слід, адже порушення інформаційної етики та неусвідомлення будь-якої публічної активності в мережі призводить до персональної та інституційної уразлиовтсі інформаційної безпеки; 6) здійснюйте системну актуалізацію з регулярним оновленням програмного забезпечення гаджетів, що допомагає подолати критичні ураження інформаційної безпеки системи в цілому.

Запропоновано засоби ресурсної підтримки для поглиблення знань за допомогою віртуального глосарію Бібліотеки посилань (з англ. – Link Library) для надавачів освітніх послуг – курс «IT-безпека: захист від цифрового кібершахрайства» від Google на платформі Coursera

(https://www.coursera.org/learn/it-security-ua); для здобувачів освіти – участь у інтерактивній грі «Interland» (https://beinternetawesome.withgoogle.com/uk_ua/interland) від Google для навчання інформаційній безпеці з використанням освітніх серіалів з кібергігієни на порталі Дія.Освіта.

Мережева інформаційна безпека реалізується як педагогічна умова при впровадженні переходу від технічного захисту до створення безпекової системи та передбачає кроки стратегії: формування «Довірчого цифрового середовища» (інфраструктури)»; сервіси, якими користуються здобувачі освіти є еталонно безпечними – інтеграція технології автентифікації (з англ. – Single Sign-On, далі – SSO) з використанням єдиного корпоративного облікового запису (наприклад, Google Workspace for Education), що передбачає обов'язкову двофакторну автентифікацією; сегментація мережі – навчальні проблемні лабораторії повинні мати ізольовані комірки у мережі, де здобувачі вищої освіти мають змогу експериментувати з програмним забезпеченням без ризику для мереж ЗВО; використання VPN-сервісів ЗВО для доступу до внутрішніх академічних сховищ даних та репозитаріїв, що привчає до необхідності захисту каналів зв'язку; впровадження «Наскрізної кібергігієни» як методичний крок, в разі коли безпека є частиною навчальних занять, а не лише окремим курсом зі застосуванням підходу «Безпека за розробкою» (з англ. – Safe by Design), оскільки будь-яке завдання (чи то створення сайту, бази даних, написання коду) оцінюється не лише за функціональність, а й за рівень безпеки захисту даних; застосування практикумів верифікації з використанням інструментарію діагностики джерел (наприклад, Who.is для перевірки документів або VirusTotal для аналізу файлів) перед їх використанням у науково-дослідницькій роботі; академічна етика та доброчесність як запорука безпеки мереж – робота з Unicheck або у інших системах антиплагіату та перевірки на ШІ як спосіб захисту власного інтелектуального надбання; забезпечення формування корпоративної культури «Цифрового імунітету» як реалізація суб'єкт-суб'єктних відносин у вихованні внутрішнього контролю здобувачів освіти та

надавачів освітніх послуг під час навчання засобами симуляції при проведенні запланованих «фішингових атак» від Центру моніторингу забезпечення якості освіти; розробка «Кодексу цифрової поведінки» у співпраці зі здобувачами для впровадження правил взаємодії в мережах (етика чатів, захист персональних даних усіх учасників освітнього процесу); сприяння розвитку медіаграмотності, а саме навчання розпізнаванню маніпуляцій та інформаційно-психологічної операції (далі – ІПСО), що є критичним для інформаційної безпеки мереж майбутніх та інституційних професійних середовищ; забезпечення функціонування систем моніторингу та сертифікації (нагляд), а саме цифровий статус у впровадженні системи сертифікації (наприклад, після проходження тесту на Skills for All від Cisco), що підтверджує готовність і здатністьздобувачів освіти до роботи з конфіденційною інформацією; контроль безпеки цифрового простору через періодичне опитування щодо доступності та зручності безпекових сервісів підтримки з метою встановлення прихованих (небезпечних) методів передачі даних серед учасників освітнього процесу.

У результаті здобувачі не лише опановують професію, а й набувають здатностей професійно діяти в умовах кіберзагроз, забезпечувати захист навчальних здобутків, академічних надбань, репутації персональної та інституційної (ЗВО).

Висновки до другого розділу

Розроблено і обґрунтовано проєктування моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій для галузі А Освіта, спеціальності А5 Професійна освіта (спеціалізацій – Цифрові технології та Електроніка, метрологія та радіотелекомунікації) з освітньою кваліфікацією – бакалавр професійної освіти. Визначено її підсистеми у синергетичній єдності, а саме: цільова, змістова, методично-організаційна, процесна та результативна. У цільовій підсистемі визначено мету інформаційної безпеки та мету організації; враховано цільові соціальні потреби

інформаційної політики, безпеки і культури в Україні та соціальне замовлення на реалізацію освітньої політики якості й безпеки, соціальної безпеки, а також комплекс підходів і принципів інформаційної безпеки, підходів і принципів соціальної політики та методологічних підходів і принципів наукового пізнання, організації та управління, що сприяло формуванню триадної єдності *КОДу*, де *К* – культура, *О* – освіта, *Д* – держава при реалізації та нарощенні культур-потенціалу інформаційної безпеки майбутнього кадрового забезпечення сфери електроніка, метрологія та радіотелекомунікацій та цифрових технологій.

Реалізовано у етапах процесів дослідження і професійної підготовки конгломерацію підсистем моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій – методично-організаційну, змістову та процесну підсистеми, що дало змогу розробити та упровадити – КВАРТЕТ освітніх модулів (соціальна та інформаційна політика, метрологія (стандартизація, випробування і вимірювання), інформаційний менеджмент та інформаційна безпека та технології) з виокремленими освітніми компонентами. Розроблено та сформовано методичний органайзер комплексу методів (організації, дослідження, навчання, безпеки), форм (організації, системи/процесу), засобів/інструментів технічного регулювання (міжнародних інституцій, Закони України, технічне регулювання організації професійної підготовки), інформаційно-технологічне забезпечення та моделі/підходи організації управління.

Виокремлено та обґрунтовано педагогічні умови реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій та представлено критеріальний апарат оцінювання рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій за критеріями (мотиваційний, нормативний та системно-управлінський) та на рівнях (достатній, середній і високий) у

результативній підсистемі моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Список використаної літератури до другого розділу:

1. Про вищу освіту: Закон України (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004). URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text (дата звернення 25.09.2025).

2. Про основні засади забезпечення кібербезпеки України: Закон України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 25.09.2025).

3. Про охорону праці: Закон України (Відомості Верховної Ради України (ВВР), 1992, № 49, ст.668). URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення 25.09.2025).

4. Про соціальні послуги: Закон України (Відомості Верховної Ради (ВВР), 2019, № 18, ст.73) URL: https://zakon.rada.gov.ua/laws/show/2671-19#Text (дата звернення 25.09.2025).

5. Про статус і соціальний захист громадян, які постраждали внаслідок Чорнобильської катастрофи: Закон України (Відомості Верховної Ради УРСР (ВВР), 1991, № 16, ст.200). URL: https://zakon.rada.gov.ua/laws/show/796-12#Text (дата звернення 25.09.2025).

6. Про основні засади соціального захисту ветеранів праці та інших громадян похилого віку в Україні: Закон України (Відомості Верховної Ради України (ВВР), 1994, № 4, ст.18). URL: https://zakon.rada.gov.ua/laws/show/3721-12#Text (дата звернення 25.09.2025).

7. Про соціальний і правовий захист військовослужбовців та членів їх сімей: Закон України (Відомості Верховної Ради України (ВВР), 1992, № 15, ст.190). URL: https://zakon.rada.gov.ua/laws/show/2011-12#Text (дата звернення 25.09.2025).

8. Про соціальний захист та підтримку дітей, які постраждали внаслідок збройної агресії Російської Федерації проти України, та внесення змін до деяких законодавчих актів України щодо впорядкування надання соціальних послуг та виплат: Закон України (Відомості Верховної Ради (ВВР), 2025, № 10,

ст.24). URL: https://zakon.rada.gov.ua/laws/show/3999-20#Text (дата звернення 25.09.2025).

9. Про затвердження Правил охорони праці під час роботи з інструментом та пристроями: Наказ Міністерства енергетики та вугільної промисловості України № 966 від 19.12.2013. URL: https://zakon.rada.gov.ua/laws/show/z0327-14#Text (дата звернення 25.09.2025).

10. Про метрологію та метрологічну діяльність: Закон України (Відомості Верховної Ради (ВВР), 2014, № 30, ст.1008). URL: https://zakon.rada.gov.ua/laws/show/1314-18#Text (дата звернення 25.09.2025).

11.

РОЗДІЛ 3.
ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА МОДЕЛІ ОРГАНІЗАЦІЇ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ДО РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МАЙБУТНІХ ФАХІВЦІВ ДЛЯ СФЕРИ ЕЛЕКТРОНІКИ, МЕТРОЛОГІЇ ТА РАДІОТЕЛЕКОМУНІКАЦІЙ

3.1 Критеріальний апарат діагностики рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій

Здійснено добір та удосконалено зміст освітніх компонентів, в межах яких обґрунтовано програмні результати навчання та загальні та спеціальні (фахові) компетентності відповідно за циклами загальної і професійної підготовки майбутніх фахівців галузі А Освіта, спеціальності А15 Професійна освіта (Електроніка, метрологія та радіотелекомунікації) для першого (бакалаврського) рівня вищої ступеня відповідно обґрунтовано навчально-методичне забезпечення практичної підготовки за видами практик (навчальна, виробнича/технологічна, педагогічна) і представлено у дослідженні як **КВАРТЕТ освітніх модулів –** *соціальна та інформаційна політика; метрологія* (стандартизація, випробування і вимірювання); *інформаційний менеджмент та інформаційна безпека; технології*, які структуровано і викладено нижче.

І. Освітній модуль «*Соціальна та інформаційна політика*» забезпечено освітніми компонентами циклу загальної підготовки здобувачів вищої освіти– «Громадянська освіта та основи демократії», «Академічна культура» та професійної підготовки – «Теоретико-правові основи професійної (професійно-технічної) освіти».

Встановлено, що освітній компонент «*Громадянська освіта та основи демократії*» має на меті формування у здобувачів освіти свідомого розуміння принципів функціонування демократичної держави та готовності захищати

права людини на засадах верховенства права, гуманізму та демократії; відповідно формування компетентностей як-то здатностей: до реалізації прав і обов'язків у статусі суб'єкта суспільних відносин; рефлексія фундаментальних цінностей відкритого демократичного суспільства; розуміння детермінант сталого розвитку, принципів правової держави, а також безумовного пріоритету прав і свобод людини в національному контексті України; академічної культури усного та письмового володіння державною мовою як інструментом професійної комунікації та соціальної інтеграції; до прийняття верифікованих та аксіологічно обґрунтованих рішень у складних соціальних контекстах; свідомої реалізації принципів рівних можливостей та врахування гендерної специфіки суспільних процесів у професійній та громадській діяльності; цілеспрямованої трансляції та впровадження принципів демократії співжиття в освітній процес.

Забезпечення *програмних результатів навчання* здобувачів освіти**:** уміння реалізувати принципи демократичної правової держави у професійному та суспільно-політичному дискурсі; обґрунтовано застосовувати стратегії прийняття рішень на засадах релевантної інформації та усталеної системи аксіологічних (ціннісних) орієнтирів; критичне аналізування суспільно-значимих проблем життідіяльності; усвідомлення онтологічної цінності державного суверенітету, територіальної цілісності та сталого розвитку демократичних інституцій України як гарантів національної безпеки; уміння емпатійно взаємодіяти та конструктивно комунікувати; готовність нести персональну соціальну відповідальність за результати діяльності в межах функціональних повноважень; неухильно дотримуватися норм професійної та академічної етики; інтегрувати міжнародні правові стандарти та позитивні національні практики у структуру професійної діяльності для забезпечення її відповідності глобальним та локальним вимогам якості; сприяти формуванню інклюзивного середовища та впровадження принципів гендерного мейнстримінгу й паритетності як фундаментальних засад сучасної корпоративної та суспільної культури.

Освітній компонент циклу загальної підготовки «*Академічна культура*» має на меті засвоєння здобувачами освіти цінностей академічної етики та доброчесності, розвиток культурпотенціалу навичок наукового письма та етики взаємодії в освітньому середовищі; відповідно сприяє формуванню *компетентностей* як-то здатностей: до кумуляції та трансляції морально-етичних, соціокультурних, академічних і наукових надбань людства; системного розуміння генезису та еволюційних закономірностей обраної предметної галузі, її епістемологічного статусу в загальній структурі наукового знання, а також її ролі у прогресі соціотехнічних і технологічних систем; дотримання принципів мультикультуралізму, толерантності та глибокій повазі до різноманітності світоглядних систем; до забезпечення професійної діяльності згідно імперативів чинного законодавства, державних освітніх стандартів та інституційно нормативно-правової бази ЗВО; до системної агрегації, критичної експлікації та верифікованої інтерпретації емпіричних даних відповідно до профілю спеціалізації. Виокремлено *програмні результати навчання*: застосовувати механізми демократичної правової держави у фаховій практиці та соціальних ініціативах; опанувати методологічно обґрунтовані рішення на основі релевантної інформації та ієрархічно вибудуваної системи ціннісних орієнтирів; системний аналіз антропологічних та соціально значущих світоглядних парадигм; інтелектуальна рефлексія щодо значення суверенітету, територіальної цілісності та архітектури демократичного устрою України як фундаментальних засад національного буття; опановувати культурпотенціал взаємодії, емпатії та конструктивного діалогу в академічному середовищі; бути відповідальним за результати інтелектуальної та професійної діяльності в межах функціональної компетенції; неухильно дотримуватися стандартів академічної етики та доброчесності; компаративний аналіз та практичне впровадження міжнародних стандартів, нормативних вимог і передових вітчизняних практик у власну професійну діяльність з метою належної конкурентоспроможності.

Освітній компонент циклу професійної підготовки «Теоретико-правові основи професійної (професійно-технічної) освіти» має не меті опанування теоретичних аспектів та нормативно-правових засад забезпечення та управління системою професійної освіти; формування *компетентностей* як-то здатностей: до реалізації громадянсько-правової суб'єктності як активного суб'єкта правовідносин; аксіологічного осмислення засад транспарентності демократичного суспільства, імперативів сталого розвитку та доктрини верховенства права як фундаментальних гарантів захисту прав і свобод людини в національному правовому полі України; до системної імплементації класичних та новітніх освітніх теорій, а також науково обґрунтованих методологій у практичну площину освітнього процесу для досягнення прогнозованих результатів навчання; забезпечення високого рівня правової культури педагогів професійного навчання, що виявляється у провадженні діяльності в межах правового поля, визначеного чинним законодавством України, державними стандартами професійної освіти та локальними актами інституційного регулювання; до інтеграції та практичного застосування тезаурусу, методологічного інструментарію та фундаментальних принципів природничих і соціально-гуманітарних наук у розв'язанні прикладних завдань професійної освіти; до проєктування та реалізації механізмів забезпечення якості освітнього процесу, здійснення функцій управління структурами закладів професійної освіти на основі принципів стратегічного, антикризового та конфлікт-менеджменту.

Сформульовано *програмні результати навчання*: оволодіння архітектурою нормативно-правової бази, галузевим законодавством та державними стандартами, що регламентують професійну діяльність в закладах професійної освіти (а також установах і підприємствах); уміння актуалізувати правові норми у контексті поточного виробничого навчання; опанувати концептуальні засади психології, педагогіки, а також тезаурусу фундаментальних і прикладних наук на рівні, достатньому для забезпечення цілісності освітнього процесу та досягнення дескрипторів навчання,

визначених освітньою програмою; навички упровадження сучасних дидактичних парадигм та методичних засад у практику викладання навчальних дисциплін; здатність до стратегічного вибору та адаптації інноваційних освітніх технологій і методик навчання з метою забезпечення якості освітнього процесу; усвідомлено володіти діалектикою динамічних соціально-економічних процесів у вимірі глобальної турбулентності; оволодіння методологічним інструментарієм ефективного господарювання та раціонального природокористування на засадах сталого розвитку; оволодіння методологією управління людським капіталом та матеріальними ресурсами; опанування навичками стратегічного планування, моніторингу, аудиту та верифікації звітності на підприємствах і в установах галузевої спрямованості; уміння реалізувати умови інклюзивного професійного середовища на основі дотримання принципів гендерного паритету, рівноправності та недискримінації.

ІІ. Освітній модуль *«Метрологія (стандартизація, випробування і вимірювання)»* представлено у контексті освітніх компонентів циклу професійної підготовки здобувачів вищої освіти – «Нормативно-методична база у сфері метрології», «Основи метрології та метрологічного забезпечення, технічного регулювання», «Сертифікація продукції, послуг та персоналу» та «Квалітологія і системи управління якістю».

Освітній компонент **«***Нормативно-методична база у сфері метрології***»** має на меті формування у здобувачів освіти комплексу наукових знань про нормативні імперативи, методичне забезпечення функціоналу метрології, правові засади метрологічної діяльності та системи нормативних документів, що забезпечують цілісну єдність методики вимірювань; *формування компетентностей* як-то здатностей: до розв'язання багатокритеріальних завдань та імплементації прикладних алгоритмів у сфері професійної освіти; синтез фундаментальних педагогічних теорій та галузевих методик (зокрема метрологічного забезпечення) в умовах глобальної турбулентності суспільства та нелінійності соціально-технічних процесів; у якості спроможності до

прийняття валідованих та аксіологічно обґрунтованих рішень на основі метрологічної точності, достовірності даних та нормативно-правової відповідності; як когнітивної адаптивності та професійного розвитку під час саморегульованого навчання та освоєння інноваційного інструментарію в динамічному середовищі високих технологій та стандартів; до проєктування індивідуальних освітніх траєкторій здобувачів освіти, спрямованих на покращення їх результативності, фахове зростання та досягнення цільових індикаторів успіху; здійснювати математичне моделювання та обчислення параметрів технологічних процесів; володіння алгоритмами метрологічного контролю та технічного розрахунку відповідно до специфікацій галузі; до агрегації, експлікації та метрологічної інтерпретації даних (як-то системний збір, критичний аналіз та інтерпретація емпіричної інформації (результатів вимірювань, випробувань та моніторингу) з метою забезпечення статистичної значущості та об'єктивності висновків у межах обраної спеціалізації.

Уточнено *програмні результати навчання*: вміння забезпечувати експертно-правову релевантність у сфері метрології; володіння чинною нормативно-правовою базою (Закон України «Про метрологію та метрологічну діяльність», підзаконних актів, технічних регламентів та галузевих стандартів (ДСТУ, ISO/IEC)); імплементувати нормативні вимоги у процеси технічного контролю, верифікації та забезпечення цілісної єдності системи вимірювань у виробничих та інституційних структурах; упроваджувати сучасні методологічні підходи під час викладання спеціалізованих дисциплін; здійснювати стратегічний вибір та адаптувати інноваційні технології, методи імітаційного моделювання вимірювальних процесів та проблемно-орієнтованого навчання при застосуванні засобів технічного регулювання в метрологічних метриках.

Освітній компонент «*Основи метрології та метрологічного забезпечення, технічного регулювання*» має на меті опанування здобувачами вищої освіти фізико-технічних основ вимірювань та принципів усунення технічних бар'єрів через технічне регулювання; системних наукових знань та практичних умінь щодо забезпечення системності метрики вимірювань,

функціонування національної та міжнародної метрологічних систем, а також опанування нормативно-правових засад технічного регулювання як фундаментальної бази забезпечення якості та безпеки (продукції, процесів і послуг) та безпеки життєдіяльності соціокультурних форм; *формування компетентностей* як-то здатностей до: систематичного опанування інноваційних методів вимірювань, чинних стандартів і регламентів технічного регулювання у сфері метрології та метрологічного забезпечення; стимуляції та мотивації здобувачів освіти на досягнення високих стандартів точності та впровадження передових метрологічних практик; імплементації сучасних інформаційних систем та спеціалізованого програмного забезпечення для автоматизації вимірювань та обробки результатів лабораторних інформаційних менеджмент-систем (з англ. – Laboratory Information Management System, LIMS) під час організації освітнього процесу; диференціації оцінювання на основі критеріїв верифікації (компетенції розробляти, обґрунтовувати та упроваджувати діагностичні стратегії метрологічного забезпечення); експертизи та аналітичного оцінювання засобів вимірювальної техніки; системного аналізу, вибору та ефективної експлуатації вимірювального обладнання з метою мінімізації похибок та забезпечення відповідності вимогам технічних регламентів; ефективного використання спеціалізованого програмного забезпечення, інструментарія для розрахунку невизначеності вимірювань, калібрування засобів вимірювальної техніки та статистичного управління технологічними процесами моніторингу та контролю якості продукції (з англ. – Statistical Process Control); інтеграції законів фундаментальних наук та загальної теорії вимірювань у ході вирішення складних прикладних завдань метрологічного забезпечення; метрологічного супроводу розрахунків параметрів технологічних процесів із врахуванням впливу зовнішніх чинників на точність результату; аналізування та інтерпретації результатів вимірювань, а саме валідації первинних даних, їх статистичного оброблення та формування обґрунтованих висновків щодо відповідності об'єкта встановленим допускам; забезпечення функціонування

системи менеджменту якості в освітній установі згідно зі стандартами серії ISO 9001/17025 та метрологічного менеджменту в освіті.

Конкретизовано *програмні результати навчання* обґрунтовано як вміння до: забезпечення метрологічної та технічної інтероперабельності вимірювальних систем у межах інформаційного освітнього простору у галузі електроніки, метрології та радіотелекомунікацій; ідентифікації, аналізування та верифікації технічних й метрологічних ризиків у галузі електроніки, метрології та радіотелекомунікацій; реалізувати метрологічний консалтинг та забезпечувати ризик-орієнтований менеджмент щодо реалізації інформаційної безпеки; розробляти та упроваджувати стратегічне планування, прогнозування та операційний менеджмент освітніх і виробничих процесів із дотриманням принципів метрологічної етики та формування культурпотенціалу забезпечення якості; цифровізації та верифікації метрологічних даних (пошуку, критичного аналізу та статистичної обробки професійної інформації із застосуванням спеціалізованого програмного забезпечення та ІКТ); аналітико-синтетичної діяльності з метою виконання складних підрахунків невизначеності вимірювань, параметрів технологічних режимів та показників надійності технічних систем; розв'язувати складні задачі метрологічного спрямування з проєктування об'єктів та вибору матеріалів, спираючись на методи технічного нормування, розрахункові допуски та вимоги взаємозамінності; здійснювати науково виважений підбір еталонної бази методів вимірювань та контрольного устаткування для розв'язання складних технічних завдань згідно з критеріями точності; управління кадровим ресурсом і матеріальними активами, навичками стратегічного планування, внутрішнього аудиту та формування метрологічної звітності відповідно до вимог стандартів серії ISO.

Освітній компонент «*Сертифікація продукції, послуг та персоналу*» має на меті опанування процедурами підтвердження відповідності об'єктів/процесів вимогам акредитації/сертифікації продукції, послуг та персоналу; *формування компетентностей* як-то здатностей до: аналітичного оцінювання вимог технічного регулювання і процедур сертифікації продукції, послуг та персоналу

з метою прийняття ефективних організаційно-управлінських рішень у майбутній професійній діяльності щодо забезпечення відповідності вимог до якості; застосовування ІКТ та програмного забезпечення під час оброблення інформаційних даних, е-документообігу та комунікування у сфері сертифікаційної діяльності; неперервного професійного розвитку, систематичного оновлення знань щодо міжнародних і національних стандартів, процедур сертифікації, систем управління якістю та сучасних технологій оцінювання її відповідності; ефективно взаємодіяти у міждисциплінарних і професійних колективах під час проведення процедур сертифікації, аудиту, інспекційного контролю та підготовки експертних висновків; прояву професійної ініціативи у впровадженні сучасних підходів до оцінювання відповідності, удосконалення процедур сертифікації, розвитку систем управління якістю та оптимізації організаційних процесів у сфері стандартизації; планування, організація та координації освітніх й професійних проєктів, спрямованих на підвищення рівня компетентності у сфері стандартизації, сертифікації та забезпечення якості; формування мотиваційного освітнє середовище, орієнтованого на розвиток професійних компетентностей здобувачів освіти у сфері стандартизації, сертифікації та управління якістю, стимулюючи їх до досягнення високих результатів у професійній діяльності; комплексного аналізу технічних та організаційних рішень щодо вибору, експлуатації та модернізації технологічного обладнання з урахуванням вимог стандартів, технічних регламентів і процедур сертифікації; застосовування спеціалізованих програмних комплексів, інформаційних систем управління якістю та цифрових платформ для підготовки, оброблення й аналізу даних у процесі проведення процедур сертифікації та оцінювання відповідності вимогам якості й безпеки; реалізації професійної діяльності у сфері сертифікації продукції, послуг і персоналу відповідно до чинного законодавства, міжнародних і національних стандартів, технічних регламентів та внутрішніх нормативних документів закладів освіти й організацій; організації професійної діяльності і виробничих процесів з урахуванням

принципів екологічної безпеки, ресурсо- та енергозбереження, охорони праці, гігієни праці та безпеки життєдіяльності, забезпечуючи відповідність умов праці сучасним стандартам і нормативам соціальної та екологічної відповідальності, стандартам до випробувальних лабораторій та інформаційно-технологічних систем.

Сформульовано *програмні результати навчання* обґрунтовано як вміння до: оперувати системою чинних нормативно-правових актів, національних і міжнародних стандартів, галузевих регламентів; аналізувати та оцінювати ризики, ідентифікувати проблемні ситуації у професійній діяльності, обґрунтовувати та обирати ефективні стратегії їх розв'язання з урахуванням вимог стандартів і процедур сертифікації; проєктувати та впроваджувати освітні й професійно орієнтовані проєкти, спрямовані на підвищення якості підготовки фахівців та удосконалення професійних компетентностей; діагностувати та прогнозувати результативність освітнього процесу, забезпечувати його ефективність шляхом коригування змісту, форм і методів навчання для досягнення визначених програмних результатів та підтримки реалізації індивідуальних освітніх траєкторій здобувачів освіти; виконувати розрахунки у сфері стандартизації та сертифікації, а також застосовувати відповідні методики оцінювання показників якості продукції, послуг і професійної діяльності персоналу; розв'язувати типові спеціалізовані завдання у професійній сфері; застосовувати у професійній практиці національні та міжнародні стандарти, регламенти і процедури, що забезпечують якість, безпечність та відповідність стандартам продукції, послуг і персоналу встановленим вимогам; здійснювати планування, організацію, контроль та підготовку звітної документації в установах, організаціях і на підприємствах; дотримуватися принципів рівності можливостей, гендерної збалансованості та недискримінації у професійній діяльності, сприяючи формуванню інклюзивного та етичного професійного середовища.

Освітній компонент «*Квалітологія і системи управління якістю*» має на меті формування у здобувачів освіти системного підходу до управління якістю

на підприємстві/організації/установі/закладі на основі міжнародних стандартів серії ISO 9000; опанування методами контролю та аналізу якості; формування *компетентностей* як-то здатностей до: розв'язання складних профільних завдань практичного спрямування у контексті міждисциплінарності визначеного спеціалітету, застосування теоретичних і методологічних основ педагогіки і методики професійного навчання, основних положень квалітології; ефективного управління освітніми ресурсами на засадах забезпечення якості освіти та наукових досліджень, моніторингу результативності освітніх процесів із використанням ІКТ; неперервного навчання щодо опанування сучасними науковими знаннями за для забезпечення якості освіти; планування, реалізації та оцінювання результатів освітньої діяльності та згідно визначеного спеціалітету; інтеграції сучасних ІКТ та програмного забезпечення під час організації освітнього процесу/виробничих процесів; реалізації стратегій та принципів (транспарентності, об'єктивності та валідності) оцінювання результатів (освітніх, виробничих); забезпечення професійної діяльності згідно чинних вимог законодавства України; упровадження ефективних методів організації праці з дотриманням вимог інформаційної, соціальної, екологічної безпеки, безпеки життєдіяльності, охорони та гігієни праці, енерго- і ресурсозбереження.

Програмні результати навчання обґрунтовано як вміння: оволодіння нормативно-правовою базою, галузевими стандартам та регламентами, що визначають вимоги до організації діяльності установ/підприємств/організацій/закладів освіти у сфері електроніки, метрології та радіотелекомунікацій; діяти свідомо і прагнути до соціальної відповідальності у контексті демократичних принципів і цінностей як складових національної системи сталого розвитку України; забезпечувати ефективну комунікацію у професійній взаємодії та співпраці, зокрема на міжкультурному та міжнаціональному рівнях з дотриманням принципів академічної етики і доброчесності, толерантності та гендерної рівності; ідентифікувати, аналізувати та оцінювати проблемні ситуації; застосовувати

алгоритми ризик-менеджменту та інструментарій систем управління якістю для вибору оптимальних організаційно-управлінських рішень; використовувати підходи стандартизації, сертифікації та забезпечення якості; аналізувати соціально-економічні процеси та тенденції розвитку суспільства, що впливають на функціонування організацій та систем управління, застосовуючи економічні та управлінські підходи до ефективного використання ресурсів; планувати, здійснювати організацію та моніторинг, нагляд та аудит діяльності установ/підприємств/організацій/закладів освіти з урахуванням принципів управління якістю та ефективності організаційних процесів.

ІІІ. Освітній модуль «*Інформаційний менеджмент та інформаційна безпека*» забезпечено освітніми компонентами циклу професійної підготовки здобувачів вищої освіти– «Вступ до фаху», «Інформаційна безпека та захист інформації» та «Інформаційний менеджмент, інформаційно-комунікаційні мережі та платформи».

Освітній компонент «*Вступ до фаху*» має на меті формування у здобувачів освіти пропедевтичного усвідомлення абрисів майбутньої професійної діяльності, опанування тезаурусу професійного спрямування, принципів та методів організації на першому робочому місці у сфері електроніки, метрології та радіотелекомунікацій; формування *компетентностей* як-то здатностей до: формування аксіологічного світобачення майбутнього фахівця; усвідомлення ролі та значення розвитку професійної освіти у контексті соціальної турбулентності суспільства; опанування наукових академічних здобутків у поєднанні з дотриманням принципів транспарентності та партисипатії; ефективної оперативності в цифровому освітньому середовищі з використанням сучасних ІКТ; оволодіння стратегіями неперервної самоосвіти (з англ. – Life-long learning) та здатність до інтенсивної когнітивної адаптації, конструктивної колаборації у професійних спільнотах для досягнення спільних стратегічних цілей; імплементації методологічного понятійно-категоріального апарату, методологічних і концептуальних основ фундаментальних і прикладних наук у практичну

площину професійно-педагогічної діяльності; оволодіння аналітико-синтетичним інструментарієм опрацювання емпіричних і теоретичних даних; верифікації та релевантної інтерпретації фахової інформації з метою прийняття обґрунтованих професійних рішень.

Програмні результати навчання обґрунтовано як вміння: використовувати наукові знання з фундаментальних, психолого-педагогічних, соціо-гуманітарних та фахових дисциплін для розв'язання професійних завдань; планувати й організовувати власну професійну діяльність; емпатійно взаємодіяти, дотримуючись стандартів професійної та корпоративної етики; оперувати програмним забезпеченням ІКТ.

Освітній компонент «*Інформаційна безпека та захист інформації*» має на меті засвоєння теорії і методики забезпечення конфіденційності, цілісності та доступності інформації; опанування архітектури комплексних систем захисту інформації; опанування методики криптографічного та технічного захисту інформації; аналізу вразливості та оцінювати ризиків у сфері електроніки, метрології та радіотелекомунікацій; формування *компетентностей* як-то здатностей: приймати обґрунтовані організаційно-управлінських рішення щодо забезпечення інформаційної безпеки та захисту інформації на основі системного аналізу ризиків в умовах соціальної турбулентності; використання інструментарію ІКТ з метою забезпечення конфіденційності обміну даними та захисту інформації; до оволодіння сучасними науковими знаннями у процесі неперервного професійного розвитку з моніторинговим аудитом інформаційних загроз і небезпек (зокрема кібератак); до ефективної корпоративної взаємодії, координації, прогнозування, запобігання та усунення кіберіцендентів; спрямовувати здобувачів освіти на прогрес і досягнення; стимулювання інновацій діяльності майбутніх фахівців до реалізації інформаційної безпеки; використовувати ІКТ та спеціалізоване програмне забезпечення інформаційного освітнього середовища (криптографічного захисту, систем виявлення вторгнень та антивірусних комплексів, тестування на проникнення, проведення аудиту безпеки та

комп'ютерно-технічної експертизи (з англ. – Digital Forensics); забезпечувати ергономіку робочих місць майбутніх фахівців у сфері електроніки, метрології та радіотелекомунікацій; збирати, аналізувати та інтерпретувати інформаційні дані у сфері електроніки, метрології та радіотелекомунікацій; Здатність до агрегації та інтелектуального аналізу великих масивів даних (з англ. – Big Data Analytics) для ідентифікації та оцінювання вразливостей та прогнозування станів захищеності систем.

Програмні результати навчання обґрунтовано як вміння як-то: реалізації безпечної роботи в комп'ютерних мережах; аргументувати та обґрунтовувати вибір програмних та технічних засобів захисту (антивіруси, криптографія); аналізувати та оцінювати стан інформаційної безпеки та забезпечувати інформаційну безпеку, обираючи ефективні шляхи вирішення складних і проблемних завдань; застосовувати у майбутній професійній діяльності інновації ІКТ.

Освітній компонент «*Інформаційний менеджмент та інформаційно-комунікаційні мережі та платформи*» має на меті формування у здобувачів світи ефективно управляти інформаційними мережами/платформами/системами та кадровим складом (персоналом), враховуючи вимоги інформаційної безпеки на засадах міжнародних стандартів управління (ISO 27001, COBIT), стратегій управління інформаційною безпекою у сфері електроніки, метрології та радіотелекомунікацій; формування *компетентностей* як здатностей: оперувати сучасним комплексом ІКТ для автоматизації управлінських процесів та забезпечення інформаційної безпеки; до ефективної взаємодії/колаборації від час проєктування та експлуатації інформаційних систем/мереж/засобів для реалізації інформаційної безпеки; до ініціативної та підприємливої діяльності; до оцінювання ризиків/зисків щодо удосконалення інформаційної інфраструктури закладу/організації/установи/підприємства; формування цифрової та медіа-грамотності, культури інфо- та кібербезпеки; опанування складного аналітичного інструментарію за стандартами інформаційної безпеки

(кібербезпеки); до реалізації стратегій тріади Центрального розвідувального управління уряду США (з англ. – Central Intelligence Agency, CIA) – конфіденційність, цілісність, доступність захисту інформації; організації безпечного ергономічного середовища при роботі з IT-інфраструктурою, дотримання регламентів техногенної та екологічної безпеки серверних систем; застосовувати алгоритми антикризового менеджменту для реалізації інформаційної безпеки, стратегічного управління IT-проєктами та забезпечення неперервного професійного росту персоналу; до моніторингу, верифікації та інтерпретації великих масивів даних (з англ. – Big Data) для прийняття виважених управлінських рішень; забезпечувати якість освітніх процесів, інформаційних потоків і управління діяльністю закладів освіти у сфері електроніки, метрології та радіотелекомунікацій.

Програмні результати навчання обґрунтовано як вміння: здійснювати аудит інформаційної діяльності організації/підприємства/закладу освіти у сфері електроніки, метрології та радіотелекомунікацій; оволодіння методологією застосування міжнародних та національних стандартів (ISO/IEC, NIST) щодо реалізації інформаційної безпеки (також кібербезпеки), нормативно-правового регулювання е-документовпорядження; усвідомлення специфіки цифрової комунікації в умовах глобальної турбулентності суспільства; реалізації корпоративної взаємодії на принципах фасилітації у професійній взаємодії з урахуванням соціокультурного потенціалу організації інформаційного менеджменту на засадах соціального захисту і правових гарантій якості й безпеки систем/мереж/платформ/ процесів; оволодіння інструментарієм стратегічного комунікативного менеджменту; забезпечення адаптивних моделей взаємодії на основі аналізу цільових аудиторій (з англ. – Stakeholder analysis) та використання верифікованих каналів передачі даних для забезпечення високої якості інформаційного обміну; ідентифікації та мінімізації інформаційних ризиків (з англ. – IT Risk Management); до системного аналізу кризових/ проблемних ситуацій у професійному середовищі; планування робочих процесів (з англ. – Workload management) із

використанням систем автоматизації управління інформаційними проєктами, що спрямовано на цифрову трансформацію освітньої чи виробничої системи; оволодіння психолого-педагогічним інструментарієм у поєднанні з персоналізованими технологіями навчання (з англ. – Adaptive Learning); проєктування та стимуляції цифрового контенту з використанням аналітики навчання (з англ. – Learning Analytics); до профорієнтаційного самовизначення суб'єктів освітнього процесу.

IV. Освітній модуль «*Технології*» забезпечено освітніми компонентами циклу професійної підготовки здобувачів вищої освіти– «Цифрові освітні та комунікативні технології в галузі», «Аналітико-синтетична переробка інформації», «Документознавство» та «Нормативно-технічний та електронний документообіг».

Освітній компонент «*Цифрові освітні та комунікативні технології в галузі*» має на меті опанування здобувачами освіти інструментарію цифрової трансформації професійної діяльності, створення ефективного освітнього контенту; вивчення трендів цифровізації в системі професійної освіти, характеристику архітектури сучасних систем управління навчанням (LMS-платформ – Moodle, Google Classroom, Canvas, Microsoft Teams); розробляти інтерактивний мультимедійний/візуальний контент (Canva, Genially, Prezi) на принципах корпоративної та академічної етики та інформаційної безпеки; формування *компетентностей* як-то здатностей: збереження та пропагування аксіологічних соціокультурних цінностей під час застосування засобів ІКТ; усвідомлення і дотримання етичних норм цифрового гуманізму та підтримкою психофізичного благополуччя в умовах цифровізації; до прийняття ефективних організаційно-управлінських рішень на основі аналізу великих даних (з англ. – Data-driven decision making); до неперервного професійного саморозвитку та оволодіння методологією корпоративної взаємодії/колаборації у реальному/віртуальному/дистанційному середовищі; експертизи ІКТ-інфраструктури, спеціалізованого програмного забезпечення у сфері електроніка, метрологія та радіотелекомунікації як дидактичний конфігуратор

освітнього інформаційного середовища для оптимізації комунікаційних процесів; забезпечувати інклюзивність та мережеву етику (з франц. – Netiquette) у мультикультурному цифровому просторі; до реалізації інноваційних освітніх стартапів/проєктів/воркшопів/тренінгів на засадах гендерної рівності, цифрової транспарентності та партисипатії; проєктування індивідуальних освітніх траєкторій здобувачів освіти засобами адаптивних технологій з використанням ШІ; оволодіння методикою цифрового оцінювання та зворотного фідбеку на основі критеріального підходу для стимулювання академічного прогресу в електронному освітньому середовищі.

Програмні результати навчання обґрунтовано як вміння: здійснювати управління проблемними ситуаціями, проєктами, практиками з використанням ІКТ; застосовувати програмне забезпечення з використанням технологій електронного навчання (з англ. – E-learning) та дистанційного/змішаного формату навчання; обґрунтовувати принципи кроскультурної цифровізації та мережевої взаємодії/колаборації в умовах глобальної турбулентності суспільства для реалізації інформаційної безпеки; моделювати адаптивні стратегії цифрової комунікації на засадах академічної етики і доброчесності в умовах дистанційного/змішаного формату організації освітнього процесу; здійснювати системний аналіз, верифікацію професійних ризиків у цифровому освітньому середовищі, прогнозування, передбачення та подолання кризових професійних ситуацій для реалізації інформаційної безпеки; проєктувати освітні траєкторії (індивідуальної та групової комплектації) щодо забезпечення професійного розвитку майбутніх фахівців сфери електроніки, метрології та радіотелекомунікацій; оперувати методиками пошуку, критичного та системного аналізу, інтерпретації інформації засобами ІКТ та ШІ з використанням спеціалізованого програмного забезпечення; використовувати психолого-педагогічний інструментарій та методологію управління інноваційними проєктами у сфері електроніки, метрології та радіотелекомунікацій.

Освітній компонент «*Аналітико-синтетична переробка інформації*» має на меті опанувати здобувачами освіти методики і методи інтелектуальної обробки первинних документів для створення вторинних інформаційних продуктів (анотацій, рефератів, оглядів) з дотриманням принципів інформаційної безпеки; методики бібліографічного індексування, класифікації інформації, предметизації та дескрипторного аналізу текстів; методики реферування та анотування інформації; *формування компетентностей* як здатностей: до прийняття організаційно-управлінських рішень, семантичного аналізу та критичного оцінювання вхідних інформаційних потоків; опанування інновацій у контексті забезпечення методологій інтелектуального аналізу даних (з англ. – Data Mining); оволодіння інструментарієм автоматизованих систем аналітико-синтетичної переробки інформації; до імплементації цифровізації систем управління контентом в систему професійної освіти у сфері електроніки, метрології та радіотелекомунікації; до забезпечення релевантності освітнього процесу за допомогою формалізованих критеріїв оцінювання інформаційної компетентності; здійснення експертизи та оптимізації архітектури інформаційних систем/платформ/мереж для реалізації інформаційної безпеки; до алгоритмізації робочих/виробничих процесів на засадах ергономіки та інформаційної; безпеки застосування фундаментальних методів системного аналізу, моделювання та математичної статистики для формалізації та розрахунку параметрів складних технологічних процесів у галузі електроніки, метрології та радіотелекомунікацій; до моніторингу, прогнозування, запобігання ризиків і небезпек задля проєктування систем управління та забезпечення якості і безпеки освітнього процесу професійної підготовки майбутніх фахівців у сфері електроніки, метрології та радіотелекомунікацій.

Програмні результати навчання обґрунтовано як вміння: здійснювати моніторинг та аналітико-синтетичну обробку нормативно-правової бази та галузевих стандартів; здійснювати системний та критичний аналіз проблемних ситуацій; обґрунтовувати стратегії, підходи і принципи інформаційної безпеки

шляхом критичного оцінювання інформаційної кон'юнктури галузі електроніки, метрології та радіотелекомунікації; здійснювати повний цикл аналітико-синтетичної переробки інформації із застосуванням ІКТ; проєктувати та імплементувати освітній контент на основі первинних наукових джерел для створення методичних комплексів та інноваційних розвивальних проєктів; володіти підходами та принципами функціонування апаратного забезпечення аналітико-синтетичної переробки інформації; на засадах системного аналізу оцінювати ефективність експлуатаційних параметрів програмного забезпечення/ устаткування в галузі електроніки, метрології та радіотелекомунікації; обробляти науково-технічну документації з дотриманням міжнародних та національних стандартів (ISO, ДСТУ) при формуванні інформаційних запитів, індексуванні та створенні вторинних документів.

Освітній компонент «*Документознавство*» має на меті вивчення теоретичних засад створення, функціоналу та особливостей зберігання документів як джерел інформації та юридичних доказів; опануванні і володіння типологізацією/класифікацією документів; *формування компетентностей* як-то здатностей: до прийняття організаційно-управлінських рішень на основі системного аналізу релевантної документаційної бази; оволодіння методикою та методами оцінювання достовірності та повноти інформації з дотриманням принципів інформаційної безпеки; оперування інструментарієм систем е-документообігу засобами ІКТ; використання спеціалізованого програмного забезпечення для автоматизації життєвого циклу документа та створення цифрового освітнього контенту; до застосування інновацій у контексті цифровізації документознавства та архівознавства; адаптації наукових знань у практичну професійну діяльність з метою генерування та реалізації стартап-проєктів у сфері інформаційного сервісу та документаційного забезпечення управління; до адміністрування проєктів з реінжинірингу документних процесів та впровадження безпаперових технологій; до фасилітації освітнього процесу через проєктування раціональних інформаційних зв’язків; формування професійної майстерності з інформаційної культури, забезпечення

інформаційної безпеки під час оперування документаційними процесами у сфері електроніки, метрології та радіотелекомунікації; дотримання регламентів захисту інформації з обмеженим доступом.

Програмні результати навчання обґрунтовано як вміння: здійснювати професійну діяльність на засадах стратегії інформаційної безпеки; володіти та застосовувати національні стандарти (зокрема ДСТУ 4163:2020) та міжнародні регламенти (ISO 15489) щодо створення, уніфікації та зберігання документів у сфері електроніки, метрології та радіотелекомунікацій; ідентифікувати та мінімізувати документні ризики (втрата інформації, витік даних, фальсифікація); оперувати аналітичним інструментарієм оцінювання ефективності документопотоків та розроблення стратегій антикризового управління інформаційними ресурсами; оперувати документною інформацією із залученням систем е-документообігу; експертного відбору інструментальних засобів обробки та довготривалого зберігання цифрового контенту відповідно до параметрів інформаційної безпеки; реалізувати освітні проєкти, спрямовані на підвищення рівня цифрової грамотності та розвиток інформаційної культури; моделювати структури е-документів та формулювання вимог до носіїв інформації; оволодіння методами формалізації та розрахунку параметрів систем документаційного забезпечення для оптимізації проектування технічних об'єктів галузі електроніки, метрології та радіотелекомунікації; упровадження антикризового менеджменту, стратегічного планування та прогнозування, моніторингу та верифікації звітності в організаціях; адміністрування інформаційних процесів делегування повноважень через систему розпорядчої документації.

Освітній компонент «*Нормативно-технічний та електронний документообіг*» має на меті опанувати – нормативно-правовими нормами е-документообігу; технологіями класичного та е-діловодства; функціоналу системи електронного документообігу (зокрема з використанням електронного цифрового підпису) на принципах інформаційної безпеки; *формування компетентностей* як-то здатностей до: прийняття релевантних рішень на

основі аналізу нормативно-технічної документації та експертизи оцінювання е-документів; володіння методологією корпоративної взаємодії при забезпеченні е-документообігу; оволодіння інструментарієм систем е-документообігу та засобами криптографічного захисту інформації; інтеграції спеціалізованих програмних комплексів у цифровий освітній простір для автоматизації документопотоків та управління контентом; моніторингу та імплементації інновацій стандартів у сфері цифрової трансформації документообігу; адаптивного засвоєння нових протоколів передачі даних зі забезпеченням інформаційної безпеки; до організації освітніх проєктів з реінжинірингу документно-інформаційних процесів; системного та критичного аналізу та аудиту ефективності впровадження системи е-документообігу; обґрунтовувати проєктні рішення щодо модернізації ІТ-інфраструктури та вибору апаратного забезпечення для забезпечення життєвого циклу нормативно-технічного документообігу; здійснення професійної діяльності у відповідності до регламентів державних стандартів, вимог технічного регулювання та чинного законодавства у сфері електронних довірчих послуг і захисту персональних даних.

Програмні результати навчання обґрунтовано як вміння: здійснювати документний супровід згідно нормативно-правової бази та галузевих стандартів (ДСТУ, ISO); оперувати методологією верифікації е-документів та технічної документації у професійній діяльності; ідентифікувати та мінімізувати ризики і небезпеки у системах е-документообігу; володіти повним циклом оперування інформаційними активами із використанням спеціалізованого програмного забезпечення для архівації, криптографічного захисту електронного підпису та довготривалого зберігання цифрових даних; стратегічного планування та адміністрування документопотоків; управління персоналом та ресурсами через автоматизовані системи контролю виконання (з англ. – Workflow) та формування регламентованої звітності; проєктування та імплементації цифрових освітніх екосистем (LMS/LXP); володіння методами розробки навчально-методичного супроводу для дистанційного/змішаної організації

освітнього процесу із інтеграцією інструментів електронного документообігу; упроваджувати принципи функціонування апаратної інфраструктури для забезпечення безперебійного технічного документообігу; виконувати спеціалізовані розрахунки та моделювати життєвий цикл технічних об'єктів у межах інтегрованих систем проектування; визначати роль цифрової трансформації та електронного урядування (з англ. – E-Government) у глобальних соціально-економічних процесах; ефективно оперувати інформаційними ресурсами задля забезпечення інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій.

3.2 Педгогічний експеримент

Педагогічний експеримент включав етапи дослідження – камеральний, мотиваційний, констатувальний, формувальногоий та праксеологічний.

Експериментальною площадкою виступили провідні ЗВО – Український державний університет імені Михайла Драгоманова, Бердянський державний педагогічний університет і Харківський національний автомобільно-дорожній університет, в яких здійснюється професійна підготовка здобувачів освіти галузі знань А Освіта, спеціальності А15 Професійна освіта за спеціалізаціями – Цифрові технології; Електроніка, метрологія і радіотелекомунікації освітнього ступеня «Бакалавр». Загалом вибірка респондентів становила 239 осіб, з них 120 особи віднесено до контрольної групи (далі – КГ), а 119 – до експериментальної групи (далі – ЕГ).

На камеральному етапі експерименту обґрунтовано програмні результати навчання, загальні та спеціальні (фахові) компетентності відповідно за циклами загальної і професійної підготовки майбутніх фахівців галузі А Освіта, спеціальності А15 Професійна освіта (Електроніка, метрологія та радіотелекомунікації) для першого (бакалаврського) рівня вищої ступеня задля формування критеріальног апарату діагностики рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

На мотиваційному етапі експерименту діагностовано рівень мотивації до формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців.

На констатувальному етапі встановлено фактичний стан сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій, а на формувальному – здійснено апробацію розробленої моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій та методики організації процесу професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації.

На праксеологічному етапі дослідження здійсено узагальнення результатів.

Розроблено формуляр аудиторської діагностики (табл.3.1.), згідно якого здійснено оцінювання складових професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій за формуляром аудиторської діагностики.

Таблиця 3.1

Складові професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій за формуляром аудиторської діагностики

Рівні / **Складові компетентості**	**Достатній (С)**	**Середній (В)**	**Високий (А)**
Інтегральна			
здатність до розв'язання складних спеціалізованих завдань і практичних проблем у професійно-педагогічній діяльності; використання теоретико- методологічних засад педагогіки, а також			

Складові компетентості / Рівні	Достатній (С)	Середній (В)	Високий (А)
положень суміжних галузей знань			
здатність до комплексних, варіативного використання міждисциплінарних підходів, до аналітичного мислення та здатності до прийняття обґрунтованих організаційно-управлінських рішень			
Загальні			
здатність реалізовувати громадянські права та обов'язки, усвідомлювати цінності демократичного суспільства, принципи верховенства права, повагу до прав і свобод людини та необхідність забезпечення сталого розвитку держави і суспільства			
усвідомлення культурно-історичної спадщини суспільства, здатність зберігати та примножувати морально-етичні, культурні, наукові та академічні цінності, а також розуміння закономірностей розвитку відповідної предметної галузі, її ролі у системі наукових знань та впливу на розвиток науки, техніки і технологій			
здатність підтримувати здоровий спосіб життя шляхом використання різних форм рухової активності			
здатність до формування комунікативної культури, оволодіння державною мовою в усній та письмовій формах			
здатність здійснювати професійну комунікацію іноземною мовою здатність до прийняття обґрунтованих організаційно-управлінських рішень, навички використання сучасних ІКТ			
готовність до неперервного навчання та саморозвитку, а також уміння ефективно працювати в команді			
усвідомлення цінності культурного різноманіття, повага до принципів мультикультурності, толерантність у міжкультурній взаємодії			
готовність виявляти ініціативність, підприємливість і соціальну активність			
усвідомлення принципів гендерної рівності та рівних можливостей як важливою умови формування демократичного освітнього середовища			
Спеціальні			
здатність застосовувати сучасні освітні теорії, концепції та методологічні підходи у професійно-педагогічній діяльності. забезпечуючи ефективну організацію освітнього процесу			
спроможність формувати у здобувачів освіти громадянські та демократичні цінності, сприяти їх соціальній відповідальності та активній громадянській позиції			
здатність організовувати та реалізовувати навчальні й розвивальні проєкти, а також спрямовувати освітню діяльність здобувачів освіти на досягнення високих результатів і професійного зростання			
інтеграція сучасних інформаційних технологій та спеціалізованого програмного забезпечення в освітнє середовище, що забезпечує інноваційність освітнього процесу та підвищує його ефективність методами об'єктивного оцінювання навчальних досягнень, застосовувати сучасні освітні стратегії та критерії оцінювання			

Складові компетентості / Рівні	Достатній (С)	Середній (В)	Високий (А)
результатів навчальної діяльності			
здатність аналізувати ефективність проєктних і технологічних рішень, пов'язаних із добором, експлуатацією, модернізацією та вдосконаленням технологічного обладнання відповідної галузі використання спеціалізованого програмного забезпечення для розв'язання фахових завдань, а також здійснення педагогічної діяльності з дотриманням вимог чинного законодавства, освітніх стандартів і внутрішніх нормативних документів закладу освіти організація безпечних умов праці, що включає дотримання вимог екологічної безпеки, охорони праці, безпеки життєдіяльності та виробничої гігієни			
здатність застосовувати фундаментальні та прикладні наукові знання у професійній діяльності, виконувати необхідні технологічні розрахунки у відповідній галузі та здійснювати аналітичну обробку інформації			
здатність управляти складними процесами та проєктами, приймати управлінські рішення в умовах невизначеності, нести відповідальність за результати діяльності та сприяти професійному розвитку здобувачів освіти			
здатність забезпечувати якість освітнього процесу та ефективно організовувати управління діяльністю закладу освіти, відповідає сучасним вимогам розвитку системи професійної освіти			

Обробка результатів здійснено шляхом підрахунку балів та присвоєння за європейського шкалою оцінювання (ЄКТС) значення, де достатній «С» - майже добре (60-79 балів), середній «В» - достатньо добре (80-89 балів), високий «А» - відмінно (90-100 балів).

У ході констатувального експерименту діагностовано складові рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій за аудиторською діагностикою, яку представлено у таблиці 3.2. та рис.3.1.

Таблиця 3.2

Показники сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ на констатувальному етапі експерименту

Рівні	Критерії											
	мотиваційний				нормативний				системно-управлінський			
	ЕГ		КГ		ЕГ		КГ		ЕГ		КГ	
	к-сть	%	к-сть	%	к-сть	%	к-сть	%	к-сть	%	к-сть	%
Високий	28	23,5	28	23,4	21	17,7	21	17,5	13	10,9	14	11,7
Середній	49	41,2	50	41,4	50	42,0	50	41,7	48	40,3	49	40,8
Достатній	42	35,3	42	35,2	48	40,3	49	40,8	58	48,8	57	47,5
Всього	119	100	120	100	119	100	120	100	119	100	120	100

У таблиці 3.2 та на рисунку 3.1 представлено результати констатувального етпу педагогічннго експкриментy – показники рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ відповідно:

- ✓ достатній (за мотиваційним критерієм – 35,3 і 35,2 %, за нормативним – 40,3 і 40,8%, за системно-управлінським – 48,8 і 47,5%);
- ✓ середній (за мотиваційним критерієм – 41,2 і 41,4 7%, за нормативним – 42,0 і 41,7%, за системно-управлінським – 40,3 і 40,8%);
- ✓ високий (за мотиваційним критерієм – 23,5 і 23,4 %, за нормативним – 17 7 і 17,5 %, за системно-упавлінським – 10,9 і 11,7%).

Під час формувального експерименту професійна підготовка здобувачів освіти ЕГ була організована за спеціально розробленою програмою упровадження моделі організації формування професійної компететності реалізації інформацйної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій; «КВАРТЕТу» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах дисциплін і практик професійної підготовки майбутніх фахівців для галузі

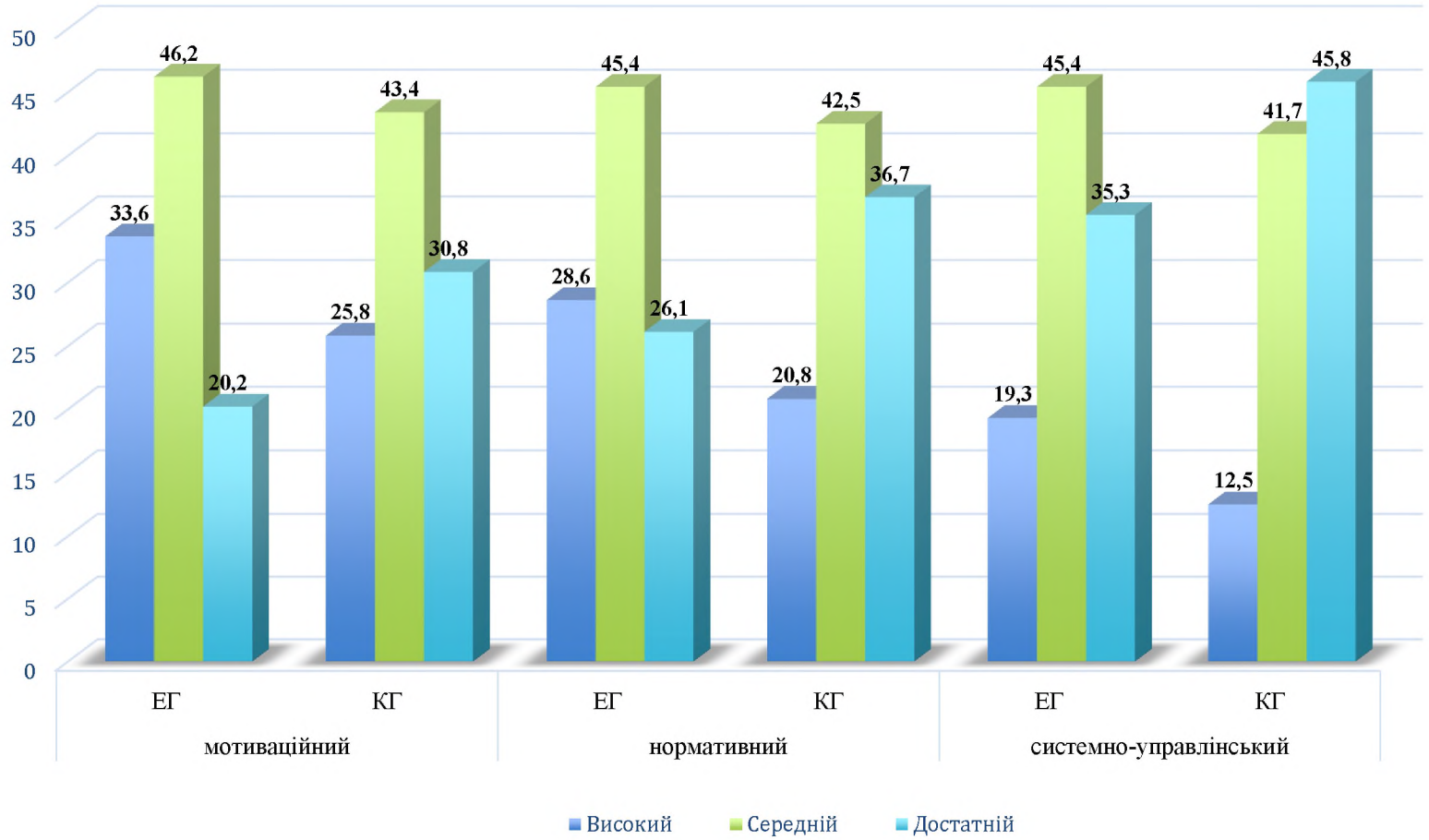

Рис. 3.1 Показники сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ на констатувальному етапі експерименту

знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелеомунікації» – соціальна та інформаційна політика, метрологія, інформаційні менеджмент та безпека, технології; педагогічних умов забезпечення впровадження Моделі, а саме – формування сприятливого середовища плекання інформаційної культури; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу та мережева інформаційна безпека системи, у КГ – за традиційною.

Формувальний етап експерименту організовано у нативних умовах освітнього процесу варіабельно, що передбачає цілеспрямовану варіативність в цільових групах респондентів з однаковими вихідними умовами окремих параметрів дослідження у порівнянні з вихідними/кінцевими результатами.

Проведене аналізування результатів формує підгрунтя для оцінювання ефективності теоретичних та методичних засад педагогічної проблеми професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій, методичного інструментарію, розробленої моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Анкету щодо діагностики рівня сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій (таблиця 3.3) розроблено з модифікацією на основі навчального посібника «Інформаційна безпека та кібербезпека держави» за загальною редакцією М. Присяжнюка [2].

Таблиця 3.3

Анкета оцінювання ефективності когнітивного потенціалу у складових професійної компетентностей до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій

№ п/п	Рівні / Складові компетентності	Достатній (С)	Середній (В)	Високий (А)
1	***Оцінювання ефективності когнітивного потенціалу у здобувачів освіти загальних та ключових компетенцій інформаційної безпека та кібербезпеки в системі національної безпеки України***			
1.1	Встановлення місця і ролі інформаційної безпеки (також кібербезпеки) в системі державної безпеки			
1.2	Визначення змісту тезаурусу інформаційної безпеки та кібербезпеки, застосування на практиці			
1.3	Встановлення, дотримання та збереження специфіки пріоритетів національних інтересів України у питаннях інформаційної безпеки (також кібербезпеки)			
1.4	Визначення векторів перспектив та стратегій забезпечення інформаційної безпеки (також кібербезпеки)			
2	***Оцінювання сформованості практичних компетенцій моніторингу, прогнозування ризиків та небезпек національній безпеці України у сфері інформаційної безпеки (також кібербезпеки)***			
2.1	Визначення імовірних і прогнозованих потенційних ризиків загроз національним інтересам України у сферах інформаційної безпеки (також кібербезпеки)			
2.2	Оперування класифікацією тезаурусу загроз безпеці держави (кіберпростору)			
2.3	Розуміння необхідності визначення основних об'єктів кіберзахисту України			
2.4	Виявлення та запобігання комп'ютерній злочинності та кібертероризму			
3	***Діагностування загрози інформаційній сфері та персональній безпеці***			
3.1	Встановлення інформаційних впливів та їх різновидностей			
3.2	Визначення об'єктів інформаційного впливу			
3.3	Оперування тезаурусом маніпулювання свідомістю Людини			
3.4	Застосування механізмів технологій маніпулювання свідомістю Людини			
3.5	Характеризування специфіки персональної інформаційно-психологічної безпека			
4	***Оцінювання інформаційно-технологічних компетенцій, застосування медіа-засобів у забезпечені інформаційної безпеки держави***			
4.1	Розрізняти та здійснювати професійну медіа-діяльність в контексті інформаційної безпеки на основі правового регулювання			

4.2	Визначати ризики та зиски комунікацій в епоху інформаційного безладу			
4.3	Діагностувати за допомогою ІКТ загрози інформаційній безпеці, що здійснюються через медіа-засоби			
4.4	Запобігання штучним вкидам інформації в інформаційному протистоянні			
5	***Оцінювання компетенцій інформаційної журналістської практики, протидії пропаганді та ІПСО***			
5.1	Запобігання російським інформаційним наративам проти України та встановлення специфіка їх викриття			
5.2	Визначення деструктивних впливів на свідомість аудиторій			
5.3	Застосування фактчекінгу, як інструменту протидії в гібридній війні			
6	***Оцінювання компетенцій психологічної стійкості протидії маніпулятивному впливу медіа***			
6.1	Характеризування технологій масового маніпулятивного впливу			
6.2	Реалізація сугестивних технологій маніпуляції			
6.3	Реалізація технологій маніпулювання в аудіовізуальних медіа			
6.4	Визначення впливу на медіа-діяльність			
6.5	Реалізація технологій маніпулювання в онлайн-медіа			

Розглянемо рівні сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій КГ та ЕГ під час формувального етапу експерименту (таблиця 3.4).

Таблиця 3.4

Показники рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ на формувальному етапі експерименту

Рівні	Критерії											
	мотиваційний				нормативний				системно-управлінський			
	ЕГ		КГ		ЕГ		КГ		ЕГ		КГ	
	к-сть	%	к-сть	%	к-сть	%	к-сть	%	к-сть	%	к-сть	%
Високий	40	33,6	31	25,8	34	28,6	25	20,8	23	19,3	15	12,5
Середній	55	46,2	52	43,4	54	45,4	51	42,5	54	45,4	50	41,7
Достатній	24	20,2	37	30,8	31	26,1	44	36,7	42	35,3	55	45,8
Всього	119	100	120	100	119	100	120	100	119	100	120	100

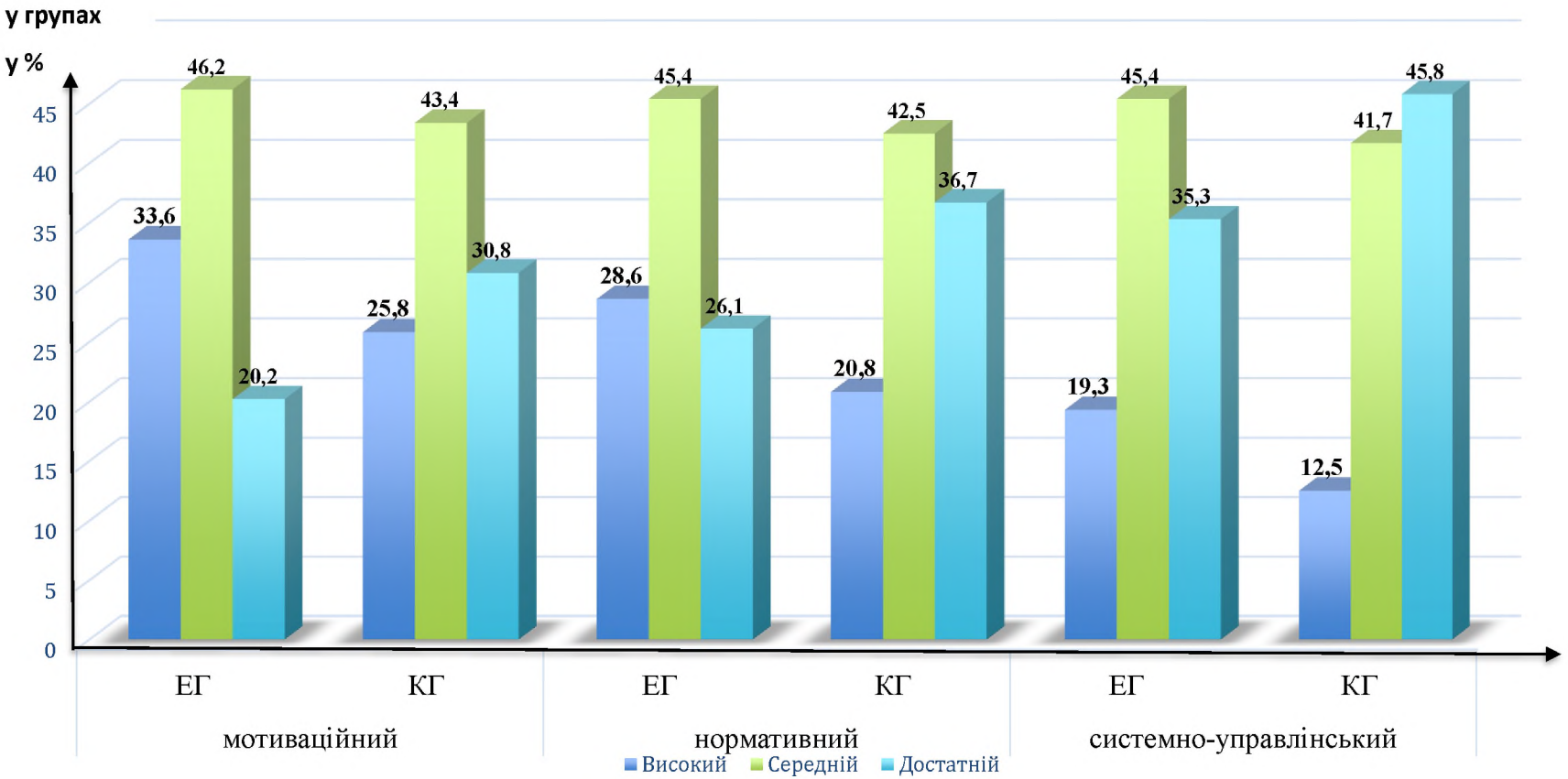

Рис. 3.2 Показники рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ на формувальному етапі експерименту, у %

Динаміка рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій після застосування розроблених у ЕГ – моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій; «КВАРТЕТу» освітніх модулів за циклами загальної, професійної та спеціальної підготовки в освітніх компонентах дисциплін і практик професійної підготовки майбутніх фахівців для галузі знань А Освіта, спеціальності А Професійна освіта, спеціалізації «Цифрові технології» та «Електроніка, метрологія та радіотелеомунікації» – соціальна та інформаційна політика**,** метрологія, інформаційні менеджмент та безпека, технології; педагогічних умов реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій; структури професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій та критеріального апарату діагностики сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у критеріях (мотиваційний, нормативний та системно-управлінський) представлено в таблиці 3.5.

Таблиця 3.5

Порівняльний аналіз рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій до і після педагогічного експерименту, у %

Рівні	Критерії											
	мотиваційний				нормативний				системно-управлінський			
	ЕГ		КГ		ЕГ		КГ		ЕГ		КГ	
	До	*Після*	*До*	*Після*	*До*	*Після*	*До*	*Після*	*До*	*Після*	*До*	*Після*
Високий	23,5	33,6	23,4	25,8	17,7	28,6	17,5	20,8	10,9	19,3	11,7	12,5
Середній	41,2	46,2	41,4	43,4	42,0	45,4	41,7	42,5	40,3	45,4	40,8	41,7
Достатній	35,3	20,2	35,2	30,8	40,3	26,1	40,8	36,7	48,8	35,3	47,5	45,8
Всього	100	100	100	100	100	100	100	100	100	100	100	100

Порівняльний аналіз рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здобувачів освіти ЕГ і КГ під час констатувального та формувального етапів проведення експерименту візуалізовано на рисунку 3.3.

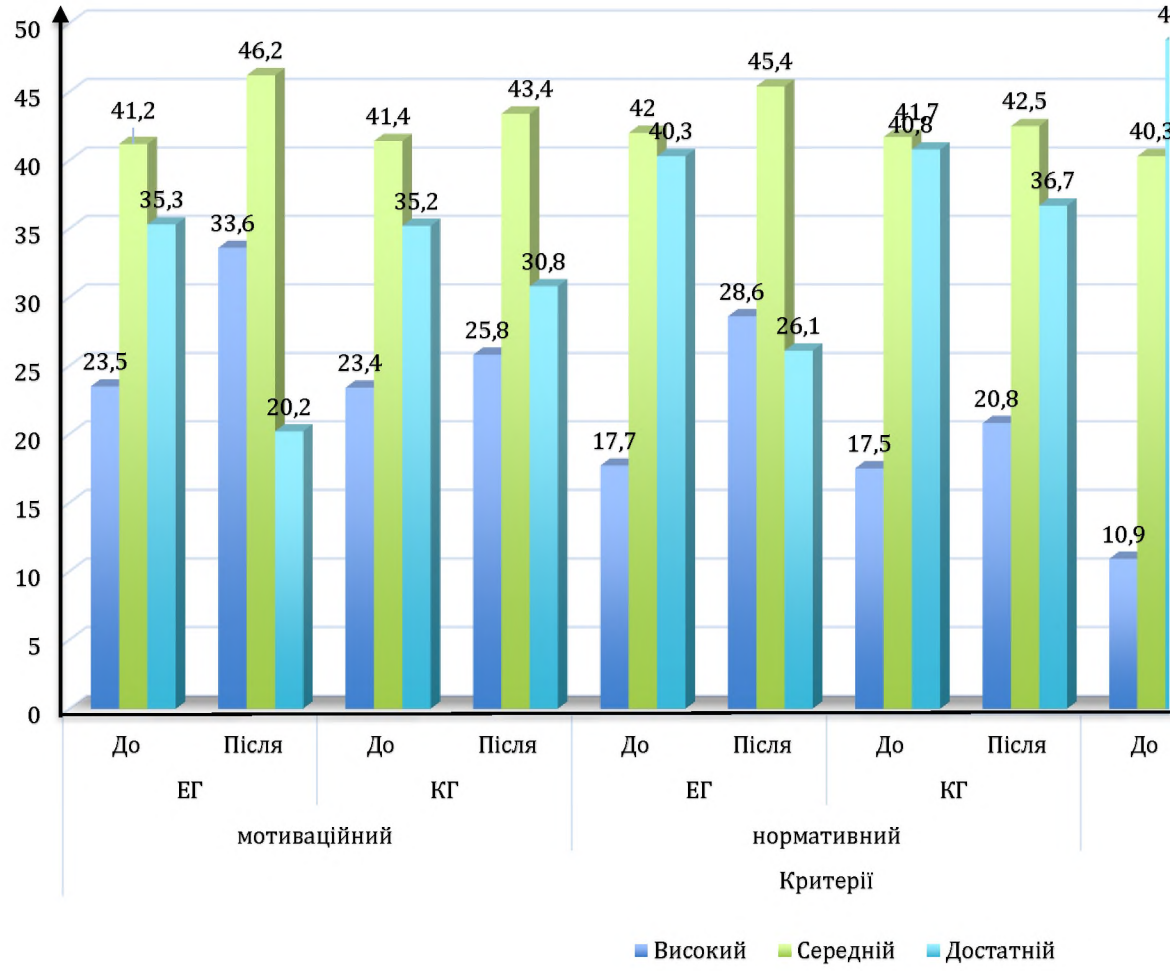

Рис. 3.3 Порівняльний аналіз рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у ЕГ та КГ до (констатувальний етап) і після (формувальний етап) педагогічного експерименту, у %

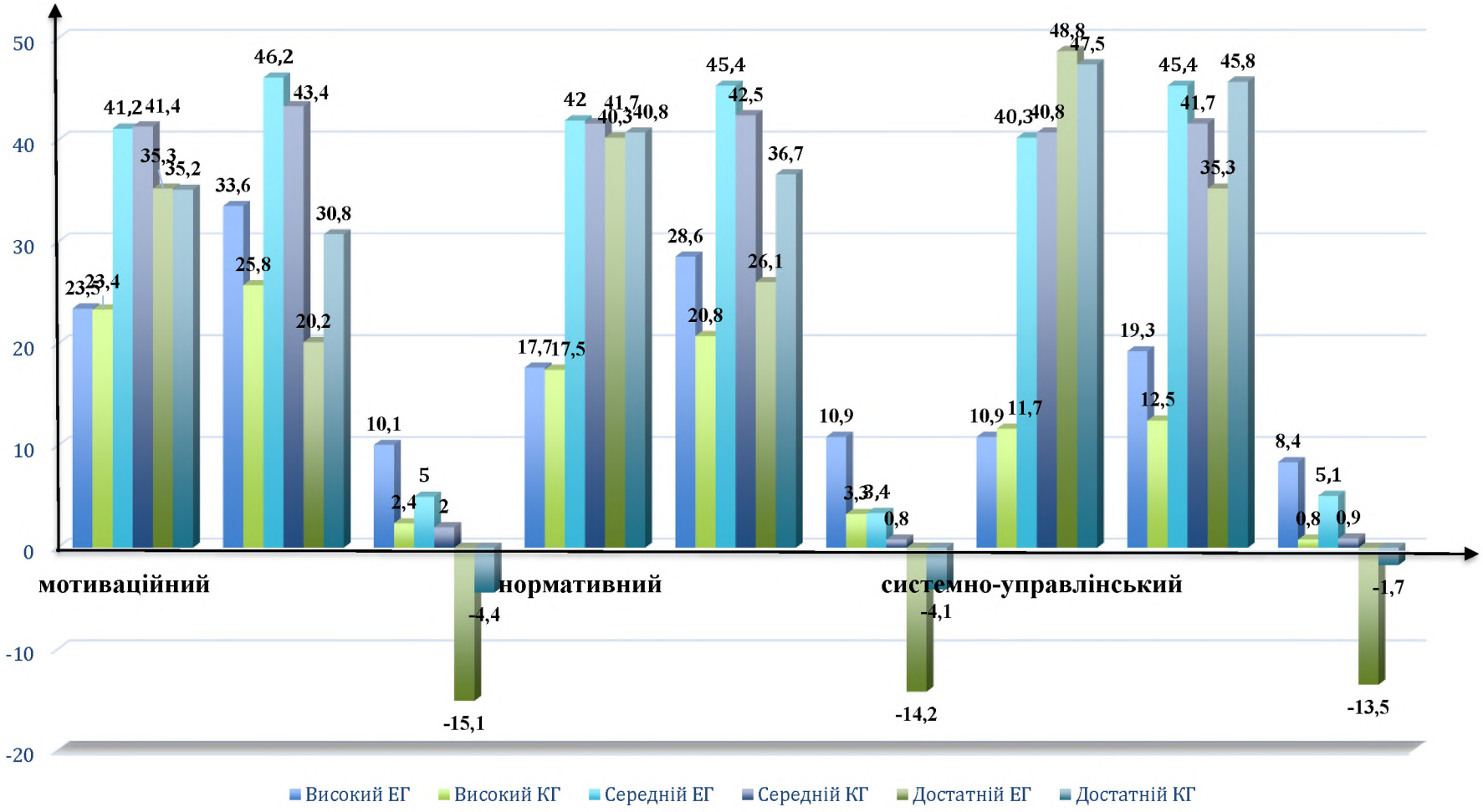

Рис. 3.4 Зведені показники рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у ЕГ та КГ до (констатувальий етап) і після (формувальний етап) педагогічного експерименту, у %

Експертне оцінювання ефективності моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здійснено експертами за параметральною метрикою встановлення рівнів її сформованості за розробленим інтегрованим питальником оцінювання якостей, здібностей, здатностей, готовності, компетенцій та компетентності/відповідальності.

Згідно теорії ймовірності експериментально підтверджено ефективність розробленої та обгрунтованої моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Задля якісного аналізу розробленої моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій здійснено експертну оцінку на основі анкетування (табл. 3.7).

Таблиця 3.7

Якісні критерії ефективності організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій

Показник ефективності	Значення показника	Оцінка ефективності
P_i	$0,8 \leq P_i \leq 0,99$	Висока
	$0,6 \leq P_i \leq 0,79$	Середня
	$0,4 \leq P_i \leq 0,59$	Достатня

Висновки до третього розділу

Встановлено у ході експериментальної перевірки ефективності впровадження моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій та її верифікації у педагогічних умовах (формування сприятливого середовища плекання інформаційної культури; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу та мережева інформаційна безпека системи) під час

організації педагогічного експерименту (у етапах –камеральний, мотиваційний, констатувальний, формувального та праксеологічний) обгрунтовані результати релевантності сформованості формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій.

Мотиваційний етап педагогічного дослідження організовано з метою встановлення позитивної мотивації майбутніх фахівців до реалізації інформаційної безпеки в межах експериментального майданчика (Український державний університет імені Михайла Драгоманова, Бердянський державний педагогічний університет та Харківський національний автомобільно-дорожній університет, що провадять професійну підготовку здобувачів вищої освіти галузі знань А Освіта, спеціальності А15 Професійна освіта за спеціалізаціями – Цифрові технології; Електроніка, метрологія і радіотелекомунікації освітнього ступеня «Бакалавр»).

На констатувальному етапі дослідження здійснено діагностику зрізу залишкових знань у здобувачів освіти ЕГ і КГ за розробленою авторською аенкетою і встановлено аліквотні результати етапу.

На формувальному етапі педагогічного експерименту показники рівнів сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій встановлено (у %) у ЕГ та КГ відповідно за розробленим критеріальним апаратом її діагностики на рівнях– достатньому (відповідно 20,2 і 30,8% за мотиваційним критерієм, 26,1 і 36,7% – за нормативним, 35,3 і 45,8% – за системно-управлінським); середньому (46,2 і 43,4% за мотиваційним критерієм, 45,4 і 42,5% – за нормативним, 45,4 і 41,7% – за системно-управлінським) та високому (25,6 і 36,8% за мотиваційним критерієм, 19,8 і 30,5% – за нормативним, 10,5 і 30% – за системно-управлінським).

Експертизу оцінювання реалізовано за 100-бальною шкалою і представлено у звіті загального експертного заключення експертів-практиків, педгогів та стейкходлжерів галузі електроніки, метрології та

раіотелекомунікацій. Встановлено ефективністі моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у сукупності 85 балів.

Список використаної літератури до третього розділу

1. Пошук і обробка інформації професійного спрямування: навчальний посібник/авторський колектив: Титова Н.М., Рідей Н.М., Настрадін В.П., Присяжнюк М.М. Київ: Видавництво Ліра-К, 2024. 170с.

2. Інформаційна безпека та кібербезпека держави: навчальний посібник/Н.М.Титова, Н.М.Рідей, В.П.настрадін, М.М.Присяжнюк, С.М. Мамченко, С.В.Артюх, Р.О.Яворська/за загальною ред. М.М. Присяжнюка. Київ: Видавництво Ліра-К, 2024, 224 с.

3. Ridei N., Tytova N., Kanova L., Slonovska O., Panchenko L. Educational policy of life quality of social and cultural forms of the educational organization throughout life. *Amazonia Investiga*. 2022. Т.11. №56. pp.73-81.

ВИСНОВКИ

1. Здійснено аксіологічний та порівняльний аналіз тезаурусу, стану і перспектив педагогічної проблеми досліджень у академічних надбаннях.

Сформульовано з уточненням предметно-об'єктного поля та цільового призначення досягнення мети – визначення тлумачення «професійна підготовка майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій»:

– система набуття (оновлення), зміни та розвитку професійної компетентності з реалізації інформаційної безпеки – «Контрольні цілі для інформаційних та суміжних технологій» (з англ. – Control Objectives for Information and Related Technology), бібліотека інфраструктури інформаційних технологій (з англ. – Information Technology Infrastructure Library), спільний бренд Міжнародної Організації зі Стандартизації (з англ. –International Organization for Standardization, ISO) та Міжнародної Електротехнічної Комісії (з англ. – International Electrotechnical Commission, IEC) у галузі знань А Освіта зі спеціальності А15 «Професійна освіта» за спеціалізаціями «цифрові технології» та «Електроніка, метрологія та радіотелекомунікації» у ЗВО, що забезпечує майбутнім фахівцям ефективність професійної та соціальної зайнятості у відповідності до соціального замовлення та семантики професійних середовищ і середовища життя у контексті стратегії національної безпеки, в тому числі інформаційної та кібербезпеки (технічного, інженерного, криптографічного, організаційного захисту систем);

– з огляду об'єктного поля педагогічної проблеми дослідження *процес* професійної підготовки – здобуття освітньої кваліфікації «Бакалавр з професійної освіти» для уможливлення працевлаштування згідно переліку професій (ДК 2010 з доповненнями) та переліку посад (3340 педагог професійного навчання, 3340 майстер виробничого навчання; 3114 технічні фахівці в галузі електроніки та телекомунікацій: технік обчислювального (інформаційно-обчислювального) центру; технік із конфігурованої

комп'ютерної системи; 3121 фахівець з інформаційних технологій; 3439 інші технічні фахівці в галузі управління: фахівець із організації інформаційної безпеки) та відповідно визначених за Стандартом вищої освіти України першого (бакалаврського) рівня, галузь знань 01 – «Освіта / Педагогіка» зі спеціальність 015 «Професійна освіта (за спеціалізаціями)» (затверджено наказом Міністерства освіти і науки України від 21.11.2019 р. № 1460) закладів освіти (профільної середньої, професійної (професійно-технічної), позашкільної, фахової передвищої), підприємств/установ/організацій галузі освіти, науки й інноватики та сфери за видами економічної діяльності; за видами (технічно-урбаністичної, фізико-хімічної, організаційно-управлінської, правничої, соціально-психологічної) безпеки у захисті від ризиків і небезпек, базуючись на конфіденційності, цілісній єдності, транспарентності інформаційних даних (з англ. – CIA Traid), передбачення, запобігання та усунення засобами управління доступом, кодифікації моніторингу при реалізації політики інформаційної безпеки та рівнях захисту інформаційних даних (систем управління інформаційною безпекою (з англ. – Information security management system, ISMS), комплексних систем захисту інформації; архітектури ієрархії уповноважених інформаційних установ і задіяних зі провадження інформаційної діяльності та систем менеджменту інформаційної безпеки;

– з огляду предметного поля дослідження – *сучасна модель організації формування професійної компетентності* до реалізації інформаційної безпеки майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у забезпеченні середовищ безпеки – інформаційного простору України; української громадянської ідентичності, інформаційного суспільства полікультурного діалогу; правового захисту соціальних гарантій доступу користувачів до інформації за цільовим призначенням, медіакультури та забезпечення медіаграмотності різночинних категорій соціальних груп (в тому числі здобувачів освіти та професійно зайнятих фахівців галузі А Освіта та галузей за видами економічної діяльності); інформаційної реінтеграції

громадян України (вимушено переміщених і тих, хто проживає на тимчасово окупованих територіях); систем/мереж/процесів стратегічних інформаційно-комунікаційних технологій, соціокультурних комунікацій; кіберпростору; управління якістю життя.

Визначено з уточненням у контексті педагогічної проблеми як об'єкту дослідження – «*процес професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій*»:

- *структурно-логічний, функціональний, організаційний алгоритм* забезпечення освітнього процесу зі здобуття/надання системних наукових знань, набуття та розвитку практичних навичок і умінь забезпечення інформаційної безпеки шляхом оволодіння майбутніми фахівцями професією за спеціальністю, що забезпечується через формальне навчання в ЗВО у співпраці зі стейкхолдерами та громадськістю, завершується присвоєнням визначеної кваліфікації згідно освітнього ступеня опанованого циклу підготовки;

- *мета процесу професійної підготовки* – забезпечення відповідності професійної компетентності регламентам якості й безпеки, адаптації та становлення згідно вимог кон'юнктури ринку праці та майбутній професійний розвиток фахівців з пролонгацією зайнятості впродовж життя;

- *послідовність трансформації станів/комплекс алгоритмізованої* навчально-науково-пізнавальної, науково-дослідної, науково-технічної, консультативно-дорадчої, інформаційно-аналітичної, методичної, експертно-аналітичної, організаційно-управлінської та адміністративної видів діяльності учасників освітнього процесу, спрямованих на досягнення цільової мети дослідження (розробка, теоретичне обґрунтування та експериментальна перевірка моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій), мети навчання (забезпечення релевантності навчальних досягнень здобувачів освіти), освітньої мети стратегії

політики інформаційної безпеки (забезпечення та нарощення спроможності професійного кадрового потенціалу фахівців з професійною компетентністю до реалізації інформаційної безпеки сфери електроніки, метрології та радіотелекомунікацій за семантикою середовищ професійної зайнятості);

- *складна система організації* – дослідження обраної педагогічної проблеми (стан і перспективи розробленості; тезаурус; нормативно-правове та технічне регулювання; методичного органайзеру й інформаційно-технологічної підтримки дослідження та впровадження розробленої моделі й методики організації процесу професійної підготовки майбутніх фахівців; педагогічний експеримент встановлення ефективності однойменних моделі та методики на базі розробленого критеріального апарату формування зведень дослідження); організації навчання – упорядкування та справочинства суб'єкт-суб'єктної взаємодії усіх учасників освітнього процесу та зацікавлених сторін у змішаному, дистанційному, мобільному та традиційному форматі для забезпечення (науково-, навчально-методичної, інформаційно-технологічної, критеріальної метрики оцінювання й коригування якості навчальних результатів (досягнень у рівнях сформованості професійної компетентності майбутніх фахівців у циклах (загальної та професійної) теоретичної та практичної (індивідуальної та групової) підготовки) освітнього ступеня «Бакалавр» за визначеною освітньою кваліфікації «Бакалавр з професійної освіти»;

- *комплекс професіоналізації* у етапах профорієнтації, набуття професійної компетентності, адаптації у професійному середовищі у практичній підготовці; професійному становленні та розвитку;

- *архітектура та функції процесу навчання* – сприймання-мотивації, осмислення-пізнання, закріпленні-повторення, інтеграції-узагальнення, систематизації-набуття системи наукових знань, практичного втілення навичок, умінь, компетенцій у синтезі професійної компетентності зі спроможністю і соціальною відповідальністю; функціональністю організаційно-правової, організаційно-управлінської, аналітично-прогностичної функцій процесу

професійної підготовки кадрів сфери електроніка, метрологія та радіотелекомунікації.

2. Проваджено контент-, формально-логічний та компаративний аналізи міжнародного та національного нормативно-правового забезпечення особливостей професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки для сфери електроніки, метрології та радіотелекомунікацій за функціональним призначенням.

Встановлено, що нормативно-правові акти зачасту не встигають за темпами інформаційно-технологічного розвитку, що призводить до виникнення невідповідностей регулювання новітніх інформаційних загроз. Освітні стандарти потребують суттєвого перегляду у частині інтеграції міждисциплінарних освітніх компонентів та посилення практичної складової у виробничих/інституційних умовах партнерства з працедавцями, зокрема шляхом впровадження симуляційних методик і методів, проблемних лабораторій, полігонів, кейс-стаді та активного інтенсивного формування й розвитку «м'яких навичок». Дефіцит необхідних ресурсів та відсутність міжнародної інтеграції у сфері стандартизації та сертифікації, також є критичними чинниками, що здійснюють загрози конкурентоспроможності українських фахівців на світовому ринку праці.

3.Розроблено та обґрунтувано проєктування моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації для організації професійної підготовки майбутніх фахівців спеціальності А5 Професійна освіта (спеціалізацій – Цифрові технології та Електроніка, метрологія та радіотелекомунікації) з освітньою кваліфікацією – бакалавр професійної освіти у підсистемах: цільовій, змістовій, методично-організаційній, процесній та результативній. У цільовій підсистемі моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації визначено мету інформаційної безпеки (посилення

спроможностей зі організації інформаційної безпеки держави, інформаційних середовищ зайнятості, сервісу інформаційних ресурсів, інструментів з підтримки стратегій соціальної і інформаційної політики для стабілізації, захисту й оборони державної суверенності, територіальної консолідації цілісності України, демократичної культури, гарантій соціального і правового захисту кожного громадянина) та мету організації прцесу (формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для забезпечення сфери електроніки, метрології та радіотелекомунікацій). Враховано цільові соціальні потреби у реалізації стратегії інформаційної політики, безпеки і забезпеченні належного рівня інформаційної культури в Україні та соціальне замовлення на реалізацію освітньої політики якості й безпеки, зокрема соціальної безпеки коекурентоспроможними педагогічними кадрами з професійною компетентністю до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомункацій. Здійснено добір підходів і принципів до інформаційної безпеки, підходів і принципів соціальної політики та методологічних підходів і принципів наукового пізнання, організації та управління професійною підготовкою для впровадження моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації як абрису системи і процесу професійної підготовки майбутніх фахівців зі забезпечення набуття професійної компетентності до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій у стратегічному баченні триадної єдності КОДу, де К – культура, О – освіта, Д – держава при реалізації та нарощенні культур-потенціалу інформаційної безпеки майбутнього кадрового забезпечення спеціалізацій – електроніки, метрології та радіотелекомунікацій та цифрових технологій.

У синергетичній єдності підсистем моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації – методично-

організаційній, змістовій та процесній – реалізовано як у етапах процесів дослідження (камерального, мотиваційного, констатувального, формувального та праксеологічного), так і професійної підготовки (профорієнтаційного, навчально-пізнавального – загального, професійно-орієнтованого, спеціального, технологічного, релевантного) розроблено та упроваджено – КВАРТЕТ освітніх модулів (соціальна та інформаційна політика, метрологія (стандартизація, випробування і вимірювання), інформаційний менеджмент та інформаційна безпека та технології) з виокремленими освітніми компонентами.

Розроблено та сформовано методичний органайзер комплексу методів (організації, дослідження, навчання, безпеки), форм (організації, системи/процесу), засобів/інструментів технічного регулювання (міжнародних інституцій, Закони України, міжнародних державних засобів технічного регулювання організації професійної підготовки та інформаційної безпеки), інформаційно-технологічного забезпечення та моделі/підходів організації управління і інформаційною безпекою у сферах освіти, науки й інноватики та галузі електроніки, метрології та радіотелекомунікацій.

Виокремлено та обґрунтовано педагогічні умови реалізації професійної підготовки майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій, а саме – формування сприятливого середовища плекання інформаційної культури; укомплектування інструментарію інформаційно-технологічного забезпечення/сервісу та забезпечення мережевої інформаційної безпеки системи/процесу (формування професійної компететності до реалізації інформаційної безпеки у майбутніх фахівців для забезпечення галузі електроніки, метрології та радіотелекомунікацій).

Результативну підсистему моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікації представлено у розробленому критеріальному апараті діагностики рівнів (достатній, середній і високий) сформованості професійної компетентності до реалізації інформаційної безпеки

у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій за критеріями (мотиваційний, нормативний та системно-управлінський).

4. Експериментально перевірено ефективність моделі організації формування професійної компетентності майбутніх фахівців до реалізації інформаційної безпеки у сфері електроніки, метрології та радіотелекомунікацій у виокремлених педагогічних умовах на основі розробленого критеріального апарату оцінювання рівня сформованості (професійної компететності).

Встановлено, що позитивну динаміку рівнів сформованості сформованості професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій на рівнях за критеріями у %: мотиваційним – високий рівень у ЕГ (+10,1) та КГ (+2,4); середній у ЕГ (+5,0) та КГ (+2,0); нормативним – високий рівень у ЕГ (+10,9) та КГ (+3,3); середній у ЕГ (+3,4) та КГ (+0,8); системно-управлінським – високий рівень у ЕГ (+8,4) та КГ (+0,8) та середній у ЕГ (+5,1) та КГ (+0,9) за рахунок

Бальне оцінювання реалізовано за 100-бальною шкалою і представлено у звіті загального експертного заключення експертів-практиків, педгогів та стейкходлжерів галузі електроніки, метрології та раіотелекомунікацій. Встановлено ефективністі моделі організації формування професійної компетентності до реалізації інформаційної безпеки у майбутніх фахівців для сфери електроніки, метрології та радіотелекомунікацій у сукупності 85 балів.

ДОДАТКИ

Додаток А

Характеристика методів організації

Методи організації	**Особливості базису**	**Характер впливу**
Адміністративні	Влада та дисципліна	Прямий, обов'язковий
Економічні	Грошовий інтерес	Непрямий, через вигоду
Соціально-психологічні	Емоції та потреби	Непрямий, через переконання
Правові	Закон та норми	Обов'язковий, захисний

Додаток Б

Характеристика методів формування безпеки підготовки

Методи безпеки	**Роль у навчанні**	**Ключові навички та уміння здобувачів освіти**
Організаційні	Створення правил гри	Написання регламентів та аудит
Антивірусні	Захист робочих місць	Аналіз шкідливого програмного забезпечення (з англ. – Malware Analysis)
DPL	Захист конфіденційності	Налаштування лінгвістичного аналізу
SIEM	Управління інцидентами	Кореляція подій та активного пошуку кіберзагроз (з англ. – Threat Hunting)

Додаток В

Розподіл функціоналу майбутніх фахівців згідно матриці «Виконавець, відповідальний, експерт, інформований» (RACI)

R (з англ. – Responsible) – безпосередній виконавець

A (з англ. – Accountable) – відповідальний за організацію управління та за результативність процесу (одна особа)

C (з англ. – Consulted) –консультант-експерт.

I (з англ. – Informed) – проінформовані особи щодо результатів або фактів завершення процесів.

Таким чином метрологія забезпечується формування професійних компетентностей майбутніх фахівців, а метрологія забезпечує достовірність, інформаційна безпека гарантує кіберзахист, а інформаційний менеджмент відповідає за якість результатів системної організації процесів.

Визначено ключові показники ефективності мультидисциплінарного фахівця, що поєднує інформаційну безпеку, метрологію та телекомунікації Для

оцінювання роботи майбутнього фахівця в цій тріаді використовують показники, що виходять за межі суто технічної справності, охоплюючи безпеку життєдіяльності та стійкість критичних процесів:

1. Показники метрологічної та інформаційної надійності. Коефіцієнт достовірності даних (з англ. – Data Integrity Rate) є часткою вимірювальних операцій, що успішно пройшли автоматизовану верифікацію цілісності. Цей показник демонструє здатність системи виявляти спроби викривлення чи підміни даних зловмисниками. Час детектування аномалій (з англ. – Mean Time to Detected, далі – MTTD) це середній час виявлення несанкціонованого втручання в процес електронних засобів вимірювальної техніки або радіоканалів. Відсоток вчасно повірених засобів інформаційної безпеки вказує на своєчасність калібрування приладів, що безпосередньо впливають на безпеку (наприклад, детектори витоку газу чи вимірювачі ЕМВ).

2. Показники безпеки життєдіяльності та охорони праці. Коефіцієнт електромагнітної сумісності (з англ. – EMC Index): статистика випадків, коли випромінювання телекомунікаційних засобів створювало перешкоди для функціонування медичного устаткування або життєво важливих систем автоматики. Ступінь нормативної захищеності робочих місць: відсоток інженерно-технічних локацій, які успішно пройшли сертифікацію на відповідність стандартам Держпраці та МОЗ за критеріями випромінювання та електротехнічної безпеки. Показник нульового травматизму (з англ. – Zero Harm Rate): повна відсутність інцидентів або ушкоджень здоров'я, що могли бути спричинені програмними помилками в інформаційних каналах керування або некоректною роботою автоматизованих систем захисту.

3. Критерії ефективності інформаційного менеджменту. Гарантований рівень доступності (з англ. – Service Level Agreement, SLA): тривалість безвідмовної роботи мереж екстреного оповіщення та каналів спеціального зв'язку (цільовий показник зазвичай 99.9%). Швидкість відновлення (з англ. – Recovery Time Objective, RTO) це інтервал часу, протягом якого необхідно повністю відновити цілісність метрологічних баз даних або працездатність

вузлів зв’язку після успішної кібератаки чи технічного збою. Індекс захищеності активів: відсоткове співвідношення всіх облікованих та взятих під захист пристроїв (датчиків, сервірів, терміналів) до їх фактичної загальної кількості в інфраструктурі підприємства згідно з ISO/IEC 27001.

Таблиця В

Приклад звітності фахівця

Показник	**Цільове значення**	**Факт**
Цілісність метрологічних даних	100%	99.8%
Час реакції на збій зв’язку	< 5 хв	3 хв
Перевищення норм ЕМВ на робочих місцях	0	0

Додаток Г

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті в наукових фахових виданнях України

1. **Магілевський В.В.** Формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних. *Педагогічна Академія: наукові записки*. 2025. №14. URL: https://pedagogical-academy.com/index.php/journal/article/view/572

2. **Магілевський В.В.** Підготовка майбутніх фахівців до інтеграції сучасних методів захисту даних у сфері електроніки та метрології. *Інноваційна педагогіка*. 2025. №82, Том 2.С. 99-107.

3. **Магілевський В.В.** Використання сучасних стандартів інформаційної безпеки у професійній підготовці фахівців радіотелекомунікацій. *Інноваційна педагогіка*. 2025. №83, Том 2. С. 111-117

4. **Магілевський В.В.**, Рідей Н.М. (2025) Оцінка ефективності освітніх програм для підготовки фахівців до інформаційної безпеки у сфері радіотелекомунікації. *Наукові інновації та передові технології*, 2025. Випуск №9(49). С. 1927-1945.

Статті у зарубіжних наукових періодичних виданнях

5. **Mahilevskyi V.** Content analysis of technical regulation means for training future specialists to implement information security in the field of electronics, metrology, and radiotelecommunications. *Paradigm of knowledge*. 2025. Vol 5, № 69. URL: https://naukajournal.org/index.php/Paradigm/issue/view/276.

Наукові праці, які засвідчують апробацію матеріалів дисертації

6. **Магілевський В.В.** Цифрові інструменти педагогічного супроводу майбутніх фахівців радіотелекомунікацій у сфері інформаційної безпеки. *Збірник матеріаів VIII Міжнародної науково-практичної конференції «Сучасні світові тенденції розвитку науки та інформаційних технологій»*, 29–30 травня 2025 р. м. Одеса. С. 8-14.

7. **Магілевський В.В.** Педагогічні умови формування готовності майбутніх фахівців до забезпечення інформаційної безпеки у сфері телекомунікацій. *Збірник матеріалів XVI Міжнародної науково-практичної конференції «Актуальні проблеми сучасної науки та освіти»,* 7-8 листопада 2025 року, Львів. С. 66-69.

Додаток Д

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

№ п/п	Назва конференції, конгресу, симпозіуму, семінару	Місце та дата проведення	Форма участі
1.	III Міжнародна науково-практична конференція «Проблеми та інновації професійної і технологічної освіти: реалії, досвід, перспективи»	Чернігів, 2024	заочна
2.	VIII Міжнародна науково-практична конференція «Сучасні світові тенденції розвитку науки та інформаційних технологій»	Одеса, 2025	тези
3.	XVI Міжнародна науково-практична конференція «Актуальні проблеми сучасної науки та освіти»	Львів, 2025	тези
4.	Міжнародна науково-практична конференція «Наука в добу глобальних трансформацій: інтеграція знань, інновацій та суспільного розвитку»	Київ, 2025	заочна
5.	VIII Міжнародна науково-методична конференція «Передові технології реалізації освітніх ініціатив»	Переяслав, 2025	заочна