ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

Професійна освіта

УДК 378.091:005.336.2:004.056

DOI https://doi.org/10.5281/zenodo.18492575

Сутність і структура управлінської компетентності майбутніх фахівців з кібербезпеки

Гузар Богдан Ярославович

аспірант кафедри сфери обслуговування, технологій та охорони праці, Тернопільський національний педагогічний університет імені Володимира Гнатюка, Україна, місто Тернопіль, вулиця М. Кривоноса, 2

https://orcid.org/0009-0004-1123-9364

Прийнято: 15.01.2026 | Опубліковано: 30.01.2026

Анотація: *У статті здійснено комплексний теоретичний аналіз сутності та структури управлінської компетентності майбутніх фахівців з кібербезпеки в контексті сучасних викликів цифрового суспільства, глобалізації інформаційного простору та зростання рівня кіберзагроз. Обґрунтовано, що ефективна професійна діяльність фахівців з кібербезпеки передбачає не лише наявність спеціальних технічних знань і навичок, а й сформовану здатність до управління процесами, ресурсами, персоналом та ризиками у сфері інформаційної безпеки. Доведено, що управлінська компетентність є важливою складовою професійної компетентності майбутніх фахівців з кібербезпеки та виступає інтегративною характеристикою їх готовності до виконання управлінських функцій у професійній діяльності. Уточнено зміст поняття «управлінська компетентність майбутніх фахівців з кібербезпеки», яку визначено як здатність особистості ефективно здійснювати управлінську діяльність у сфері кібербезпеки на основі системи професійних знань, управлінських умінь, практичного досвіду, ціннісних орієнтацій,*

відповідальності та здатності до самоаналізу й саморозвитку. На основі узагальнення наукових підходів вітчизняних і зарубіжних дослідників виокремлено структурні компоненти управлінської компетентності, зокрема мотиваційно-ціннісний, когнітивний, операційно-діяльнісний, комунікативний та рефлексивно-оцінний, розкрито їх зміст та взаємозв'язок.

Ключові слова: *управлінська компетентність, професійна підготовка, майбутні фахівці з кібербезпеки, структура компетентності, вища освіта.*

The Essence and Structure of Managerial Competence of Future Cybersecurity Specialists

Huzar Bohdan

Postgraduate student at the Department of Service, Technology, and Occupational Safety, Volodymyr Hnatiuk Ternopil National Pedagogical University, Ukraine, Ternopil, 2 M. Kryvonosa Street

Abstract: *The article provides a comprehensive theoretical analysis of the essence and structure of managerial competence of future cybersecurity specialists in the context of contemporary challenges of the digital society, globalization of the information space, and the growing level of cyber threats. It is substantiated that effective professional activity of cybersecurity specialists requires not only the availability of specialized technical knowledge and skills, but also a well-developed ability to manage processes, resources, personnel, and risks in the field of information security. It is proved that managerial competence is an essential component of the professional competence of future cybersecurity specialists and serves as an integrative characteristic of their readiness to perform managerial functions in professional activity. The content of the concept of "managerial competence of future cybersecurity specialists" is clarified and defined as an individual's ability to effectively carry out managerial activities in the field of cybersecurity based on a system of professional knowledge, managerial skills, practical experience, value*

orientations, responsibility, and the capacity for self-analysis and self-development. Based on the generalization of scientific approaches of domestic and foreign researchers, the structural components of managerial competence are identified, namely motivational-value, cognitive, operational-activity, communicative, and reflexive-evaluative, and their content and interrelations are revealed.

Keywords: *managerial competence, professional training, future cybersecurity specialists, competence structure, higher education.*

Постановка проблеми. Стрімкий розвиток цифрових технологій, глобалізація інформаційного простору та зростання кількості й складності кіберзагроз зумовлюють підвищені вимоги до професійної підготовки фахівців з кібербезпеки. Сучасні умови професійної діяльності вимагають від таких фахівців не лише ґрунтовних технічних знань і практичних умінь у сфері захисту інформаційних ресурсів, а й здатності ефективно виконувати управлінські функції, зокрема планувати та координувати діяльність у сфері кіберзахисту, приймати обґрунтовані управлінські рішення в умовах невизначеності, управляти ризиками, персоналом і ресурсами, а також організовувати командну взаємодію під час реагування на кіберінциденти [18, 20, 22].

Разом із тим, аналіз освітньої практики та наукових досліджень свідчить про наявність суперечності між зростаючими вимогами ринку праці до рівня управлінської підготовленості фахівців з кібербезпеки та недостатньою теоретичною розробленістю сутності й структури їх управлінської компетентності в системі професійної освіти. У більшості освітніх програм акцент зроблено головно на формуванні технічних компетентностей, тоді як управлінський складник часто має фрагментарний або другорядний характер. Це ускладнює підготовку майбутніх фахівців до виконання управлінських функцій у професійній діяльності та знижує ефективність їхньої роботи в умовах сучасних кіберзагроз.

Відтак, актуалізується потреба в ґрунтовному теоретичному осмисленні поняття управлінської компетентності майбутніх фахівців з кібербезпеки,

визначенні її структури та змісту, а також обґрунтуванні її місця в системі професійної підготовки у закладах вищої освіти. Розв'язання зазначеної проблеми сприятиме вдосконаленню освітніх програм і підвищенню якості підготовки майбутніх фахівців з кібербезпеки відповідно до сучасних потреб суспільства та вимог професійної діяльності.

Аналіз останніх досліджень і публікацій. У сучасних наукових дослідженнях управлінська компетентність розглядається як важливий чинник професійної діяльності фахівців у технологічно складних і динамічних галузях. Вітчизняні науковці Н. М. Бібік [2], Л. М. Карамушка [9] та ін. аналізують управлінську компетентність у межах компетентнісного та діяльнісного підходів, наголошуючи на її інтегративному характері та зв'язку з результативністю професійної діяльності.

У зарубіжних дослідженнях управлінська компетентність трактується як сукупність особистісних характеристик і професійних умінь, що забезпечують ефективне управління в умовах складних організаційних контекстів та високого рівня невизначеності. Зокрема у працях H. Mintzberg [21] значна увага приділяється здатності управлінця інтегрувати різнорідну інформацію та ухвалювати рішення в умовах часових обмежень і ризиків.

У контексті цифрової трансформації професійної діяльності у працях E. Ilieva, D. Ivanova [19] управлінська компетентність розглядається як поєднання технологічних знань із лідерськими, комунікативними та управлінськими навичками, необхідними для ефективної діяльності в цифровому середовищі.

Водночас дослідження у сфері кібербезпеки переважно зосереджені на формуванні технічних та інформаційно-аналітичних компетентностей. Так, О. К. Юдін і О. В. Матвійчук-Юдіна [16] розглядають професійну підготовку фахівців з кібербезпеки крізь призму відповідності міжнародним стандартам, підкреслюючи необхідність системного підходу до формування їхніх професійних компетентностей.

У сучасних дослідженнях підкреслюється, що формування цифрово-компетентного менеджера включає не лише традиційні технічні знання, а й управлінські та лідерські навички [19, 22].

Хоча прямих досліджень щодо управлінської компетентності у кібербезпеці в Україні небагато, суміжні праці з компетентностей в інших сферах показують тенденцію до інтеграції управлінського компонента. Зокрема, С. С. Кудінов [10] розглядає формування компетентностей у кібербезпеці крізь призму протидії загрозам кібертероризму. Також варто враховувати дослідження фахівців у галузі кібербезпеки В. В. Горлинського і Б. В. Горлинського [5], яке підкреслює перспективи побудови системи відповідних компетентностей для майбутніх фахівців.

У контексті дослідження управлінської компетентності майбутніх фахівців з кібербезпеки Гузар Б. [6] зосереджує увагу на теоретико-методичних засадах її формування в процесі професійної підготовки. У роботі ґрунтовно обґрунтовано доцільність застосування тренінгових технологій як ефективного педагогічного інструментарію розвитку управлінських умінь, навичок прийняття рішень і командної взаємодії у сфері кіберзахисту. Особливий акцент зроблено на структурних компонентах управлінської компетентності та механізмах їх цілеспрямованого й системного формування.

Аналіз сучасних безпекових викликів у площині державного управління здійснює Гончарук Ю. [4], розглядаючи функціонування публічного управління в системі національної кібербезпеки в умовах гібридної війни. У дослідженні висвітлено складні управлінські виклики, пов’язані з координацією суб’єктів кібербезпеки, ухваленням рішень за умов високої невизначеності та зростання загроз. Сформульовані висновки поглиблюють розуміння управлінського контексту професійної діяльності фахівців з кібербезпеки.

Проблематика модернізації професійної підготовки у сфері кібербезпеки представлена у працях Різака В. та ін. [14], де увагу зосереджено на впровадженні інноваційних підходів у підготовку магістрів. Дослідниками обґрунтовано значення інтеграції сучасних освітніх технологій і

міждисциплінарних підходів у процес формування професійних компетентностей. Окреслені підходи опосередковано підкреслюють важливість розвитку управлінських умінь як складової професійної готовності майбутніх фахівців з кібербезпеки.

Системний аналіз чинників формування компетентностей у галузі кібербезпеки здійснюють Горлинський В. та ін. [5], розглядаючи підготовку фахівців як багатовимірний процес. У дослідженні визначено структуру професійних компетентностей та аргументовано роль організаційних і управлінських чинників у професійній підготовці. Отримані результати формують теоретичне підґрунтя для включення управлінської компетентності до цілісної системи підготовки майбутніх фахівців з кібербезпеки.

У межах аналізу цифровізації освітнього процесу Арсенович Л. [17] приділяє увагу інструментарію підвищення рівня цифрової компетентності фахівців із кібербезпеки. Дослідження акцентує на використанні сучасних цифрових засобів і методів навчання, що забезпечують готовність до діяльності в складному та динамічному цифровому середовищі. Отримані висновки мають важливе значення для формування управлінської компетентності, зокрема в аспектах прийняття рішень і управління процесами цифрової трансформації.

Питання прикладної спрямованості базової підготовки фахівців з кібербезпеки висвітлюють Рутаньова Н. та ін. [23], зосереджуючись на ролі математичних дисциплін у професійному становленні. Автори обґрунтовують необхідність орієнтації математичної підготовки на практичні завдання кіберзахисту та розвиток аналітичного мислення. Запропоновані підходи сприяють формуванню когнітивного компонента управлінської компетентності майбутніх фахівців з кібербезпеки.

Практикоорієнтований підхід до формування компетентностей майбутніх фахівців з кібербезпеки представлено у дослідженні Кальченка В. та ін. [8], присвяченому ініціативі «студентські кібербригади». У роботі наголошено на розвитку командної взаємодії, відповідальності та практичних умінь реагування

на кіберінциденти. Такий формат підготовки сприяє формуванню управлінських і комунікативних складових професійної компетентності.

Організаційні аспекти професійної підготовки в кризових умовах аналізує Арсенович Л. [1], розглядаючи функціонування освітньої системи у сфері кібербезпеки в умовах особливого періоду. У дослідженні висвітлено управлінські рішення, спрямовані на адаптацію освітнього процесу до підвищених безпекових викликів. Зроблені висновки підкреслюють роль управлінської компетентності у забезпеченні стійкості професійної освіти.

Проблематику розвитку лідерського потенціалу в умовах цифровізації освіти розкривають Харківська А. та ін. [15], аналізуючи процес професійної підготовки здобувачів вищої освіти. Автори визначають педагогічні умови формування лідерських і комунікативних умінь, необхідних для ефективної взаємодії в освітньому та професійному середовищі. Отримані результати є релевантними для обґрунтування мотиваційно-ціннісного та комунікативного компонентів управлінської компетентності майбутніх фахівців з кібербезпеки.

Узагальнюючи підходи до професійної підготовки в ІТ-галузі, Галицький О. та ін. [3] аналізують особливості формування професійної компетентності фахівців комп’ютерних наук. У роботі розкрито структуру професійної компетентності та взаємозв’язок її складових у процесі фахової підготовки. Представлені результати створюють теоретичне підґрунтя для інтеграції управлінської компетентності в систему підготовки майбутніх фахівців з кібербезпеки як суміжної галузі.

Виділення невирішених раніше частин загальної проблеми. Аналіз сучасних наукових досліджень і публікацій свідчить про зростаючий інтерес вчених до проблеми формування професійної компетентності фахівців з кібербезпеки, зокрема в аспекті розвитку їх технічних, інформаційно-аналітичних та комунікативних умінь. Водночас більшість наукових праць зосереджена переважно на технологічних аспектах підготовки майбутніх фахівців з кібербезпеки або на загальних питаннях професійної компетентності

[5, 16], тоді як управлінський компонент залишається недостатньо систематизованим і концептуально опрацьованим [11, 12].

Незважаючи на наявність окремих досліджень, присвячених управлінським, лідерським та організаційним навичкам фахівців технічних спеціальностей, у науковій літературі відсутнє єдине трактування поняття «управлінська компетентність майбутніх фахівців з кібербезпеки», а також чітке визначення її структури з урахуванням специфіки професійної діяльності у сфері кіберзахисту. Недостатньо дослідженими залишаються питання взаємозв'язку управлінської компетентності з професійними кібербезпековими компетентностями, а також механізми їх інтеграції в процесі фахової підготовки у закладах вищої освіти.

Формулювання цілей статті (постановка завдання). Метою статті є теоретичне обґрунтування сутності управлінської компетентності майбутніх фахівців з кібербезпеки та визначення її структури в контексті сучасних вимог до професійної підготовки у закладах вищої освіти. Для досягнення поставленої мети у статті передбачено розв'язання таких завдань:

1. Проаналізувати наукові підходи вітчизняних і зарубіжних дослідників до трактування поняття управлінської компетентності.

2. Уточнити зміст поняття «управлінська компетентність майбутніх фахівців з кібербезпеки» з урахуванням специфіки їх професійної діяльності.

3. Визначити та охарактеризувати структурні компоненти управлінської компетентності майбутніх фахівців з кібербезпеки.

4. З'ясувати місце управлінської компетентності в системі професійної компетентності фахівців з кібербезпеки.

5. Обґрунтувати доцільність інтеграції управлінської підготовки в процес професійної освіти майбутніх фахівців з кібербезпеки.

Висвітлення основного матеріалу дослідження. У сучасній науковій літературі поняття управлінської компетентності розглядається в межах різних наукових підходів, що зумовлює багатоваріантність його трактувань та відсутність єдиного універсального визначення. Загалом управлінську

компетентність інтерпретують як інтегративне утворення, що поєднує професійні знання, управлінські вміння, особистісні якості, ціннісні орієнтації та досвід управлінської діяльності [2, 9, 12].

У працях вітчизняних дослідників управлінська компетентність переважно розглядається з позицій компетентнісного та діяльнісного підходів. Так, низка науковців визначає управлінську компетентність як здатність особистості ефективно здійснювати управлінську діяльність на основі засвоєних знань, сформованих умінь і навичок, а також готовності до прийняття відповідальних рішень у професійних ситуаціях. Зокрема Бібік Н.М. наголошує, що «компетентність виявляється не лише в обсязі засвоєних знань, а передусім у здатності діяти ефективно в умовах невизначеності» [2, с.8]. У межах цього підходу акцент робиться на практичній спрямованості управлінської компетентності, її зв'язку з реальними умовами професійної діяльності та результативністю управлінських рішень. Дослідники також підкреслюють важливість ціннісно-мотиваційного компонента, що забезпечує усвідомлене та відповідальне виконання управлінських функцій.

Водночас у вітчизняній педагогічній науці управлінська компетентність часто розглядається як складова професійної компетентності фахівця, що формується в процесі цілеспрямованої професійної підготовки у закладах вищої освіти. У цьому контексті особлива увага приділяється структурі управлінської компетентності, яка зазвичай включає когнітивний, операційно-діяльнісний, мотиваційний, комунікативний і рефлексивний компоненти.

У сучасній педагогічній науці управлінська компетентність розглядається як інтегративне професійно-особистісне утворення, що поєднує управлінські знання, уміння, ціннісні орієнтації та готовність до відповідальної діяльності в реальних професійних умовах. Такий підхід акцентує, що управлінська компетентність не зводиться до формального володіння знаннями, а виявляється у здатності особистості ефективно діяти в професійній діяльності.

У межах компетентнісного підходу управлінська компетентність трактується як здатність особистості застосовувати знання й уміння в умовах

професійної невизначеності та відповідальності, що є особливо актуальним для сфери кібербезпеки [2].

Зарубіжні дослідники розглядають управлінську компетентність як багатовимірну характеристику, що забезпечує ефективність управління в умовах організаційної складності, динамічних змін і високого рівня ризику. У цьому контексті управлінська діяльність пов'язується з необхідністю прийняття рішень в умовах невизначеності та обмеженого часу і трактується переважно в руслі системного, особистісно орієнтованого та лідерського підходів [21, 22]. У міжнародних дослідженнях управлінська компетентність визначається як сукупність компетенцій, що забезпечують ефективне керівництво організаціями та командами в умовах динамічних змін, невизначеності та високого рівня ризиків. Особливий акцент робиться на розвитку лідерських якостей, стратегічного мислення, здатності до комунікації, управління змінами та міждисциплінарної взаємодії.

У зарубіжній науковій літературі поширеним є підхід, відповідно до якого управлінська компетентність розглядається як поєднання hard skills (професійні та аналітичні знання) і soft skills (комунікативні, емоційні, соціальні та лідерські здібності). Такий підхід підкреслює необхідність балансу між технічною обізнаністю та здатністю ефективно працювати з людьми, що є особливо актуальним для управлінської діяльності у високотехнологічних сферах, зокрема кібербезпеці. Дослідники управління підкреслюють, що управлінська діяльність у сучасних організаціях здійснюється в умовах невизначеності та часових обмежень і потребує від керівника здатності інтегрувати різнорідну інформацію під час ухвалення рішень [21].

Таким чином, аналіз наукових підходів вітчизняних і зарубіжних дослідників свідчить, що управлінська компетентність розглядається як складне багатовимірне утворення, яке поєднує знання, уміння, особистісні якості та ціннісні орієнтації й забезпечує готовність фахівця до ефективної управлінської діяльності. Водночас специфіка трактування цього поняття залежить від

 ISSN: 2786-9458

наукової школи, галузі дослідження та професійного контексту, що зумовлює необхідність його уточнення для майбутніх фахівців з кібербезпеки.

Управлінська компетентність майбутніх фахівців з кібербезпеки має специфічний зміст, зумовлений особливостями їх професійної діяльності, яка здійснюється в умовах високого рівня невизначеності, динамічності кіберзагроз, обмеженого часу на прийняття рішень та підвищеної відповідальності за захист інформаційних ресурсів. На відміну від управлінської компетентності фахівців інших галузей, управлінська компетентність у сфері кібербезпеки поєднує управлінські функції з глибоким розумінням технічних, організаційних і правових аспектів інформаційної безпеки [16, 20].

У контексті даного дослідження управлінську компетентність майбутніх фахівців з кібербезпеки доцільно розглядати як інтегративну професійно-особистісну характеристику, що відображає їх здатність ефективно планувати, організовувати, координувати та контролювати діяльність у сфері кіберзахисту, приймати обґрунтовані управлінські рішення під час попередження, виявлення та реагування на кіберінциденти, а також забезпечувати взаємодію між учасниками процесів інформаційної безпеки.

Зміст управлінської компетентності майбутніх фахівців з кібербезпеки охоплює не лише систему управлінських знань і вмінь, а й здатність до стратегічного та критичного мислення, управління ризиками, командної роботи, комунікації з технічними й нетехнічними стейкхолдерами, дотримання етичних норм і правових вимог у сфері кібербезпеки. Важливою складовою є також готовність до постійного професійного саморозвитку, що зумовлено швидкими темпами розвитку інформаційних технологій і трансформацією кіберзагроз.

З огляду на це, уточнене поняття управлінської компетентності майбутніх фахівців з кібербезпеки відображає її міждисциплінарний характер та спрямованість на забезпечення ефективного управління процесами кібербезпеки в умовах сучасного цифрового середовища, що дозволяє розглядати її як необхідну складову професійної підготовки у закладах вищої освіти.

Враховуючи наукові підходи до структури управлінської компетентності та специфіки професійної діяльності у сфері кібербезпеки, управлінську компетентність майбутніх фахівців з кібербезпеки доцільно розглядати як багатокомпонентне утворення, що забезпечує готовність до ефективного виконання управлінських функцій у процесі професійної діяльності. Аналіз наукових підходів до структури управлінської компетентності свідчить про її багатокомпонентний характер. У працях вітчизняних дослідників управлінська компетентність розглядається як система взаємопов'язаних компонентів, що забезпечують цілісність управлінської діяльності. Зокрема, Л. М. Карамушка виокремлює мотиваційний, когнітивний, операційно-діяльнісний, комунікативний і рефлексивний компоненти управлінської компетентності [9].

Мотиваційно-ціннісний компонент відображає систему професійних мотивів, ціннісних орієнтацій і ставлень майбутніх фахівців до управлінської діяльності у сфері кібербезпеки. Він передбачає усвідомлення значущості управлінських рішень для забезпечення інформаційної безпеки, відповідальне ставлення до професійних обов'язків, готовність діяти в умовах ризику та дотримання етичних і правових норм.

Когнітивний компонент охоплює сукупність управлінських, фахових і міждисциплінарних знань, необхідних для здійснення управлінської діяльності у сфері кібербезпеки. До його змісту належать знання з теорії управління, ризик-менеджменту, стратегічного планування, інформаційної та кібербезпеки, а також нормативно-правового регулювання у сфері захисту інформації.

Операційно-діяльнісний компонент характеризує сформованість практичних управлінських умінь і навичок, зокрема здатність планувати й організовувати діяльність у сфері кіберзахисту, координувати роботу команди, приймати управлінські рішення в умовах невизначеності, управляти кіберінцидентами та оцінювати ризики. Цей компонент забезпечує реалізацію управлінських функцій у практичній професійній діяльності.

Комунікативний компонент відображає здатність майбутніх фахівців з кібербезпеки до ефективної професійної взаємодії з різними суб'єктами

кіберпростору, зокрема членами команди, керівництвом, замовниками та іншими зацікавленими сторонами. Він включає навички ділового спілкування, ведення переговорів, аргументації управлінських рішень і роботи в міждисциплінарних командах.

Рефлексивно-оцінний компонент передбачає здатність до самоаналізу, самоконтролю та оцінювання результатів власної управлінської діяльності, а також готовність до професійного самовдосконалення. Він забезпечує усвідомлення сильних і слабких сторін управлінських рішень, корекцію професійної поведінки та адаптацію до змін у сфері кібербезпеки.

Таким чином, визначені структурні компоненти управлінської компетентності майбутніх фахівців з кібербезпеки перебувають у тісному взаємозв'язку та в сукупності забезпечують їх готовність до ефективної управлінської діяльності в умовах сучасного цифрового середовища.

Професійна компетентність фахівців з кібербезпеки є складним інтегративним утворенням, що охоплює сукупність знань, умінь, навичок, ціннісних орієнтацій і особистісних якостей, необхідних для ефективного виконання професійних завдань у сфері захисту інформації та кіберпростору [7, 11, 12]. У структурі професійної компетентності майбутніх фахівців з кібербезпеки традиційно виокремлюють технічну, інформаційно-аналітичну, правову, комунікативну та етичну складові. Водночас сучасні умови професійної діяльності зумовлюють необхідність включення до цієї системи управлінської компетентності як її невід'ємного компонента.

Управлінська компетентність у системі професійної компетентності фахівців з кібербезпеки виконує інтегрувальну та координувальну функції, забезпечуючи узгодженість і цілеспрямованість реалізації інших професійних компетентностей. Саме управлінська компетентність дозволяє фахівцеві не лише застосовувати технічні знання на практиці, а й ефективно організовувати процеси кіберзахисту, координувати діяльність учасників, розподіляти ресурси та приймати відповідальні рішення в умовах підвищеного ризику та часових обмежень. Дослідник С. С. Кудінов у своїх дослідженнях наголошує, що

формування компетентностей фахівців у сфері кібербезпеки повинно враховувати управлінські аспекти протидії кіберзагрозам, зокрема в умовах кризових ситуацій та кібертероризму [10].

На відміну від суто технічних компетентностей, управлінська компетентність має надпрофесійний (метакомпетентнісний) характер, оскільки забезпечує реалізацію управлінських функцій незалежно від конкретних технологічних засобів чи інструментів кібербезпеки. Вона інтегрує результати опанування фахових знань, комунікативних умінь і правових норм, сприяючи формуванню цілісної готовності майбутніх фахівців до виконання професійних ролей, пов'язаних із плануванням, організацією, контролем і удосконаленням діяльності у сфері кібербезпеки.

У цьому контексті акцентуємо, що професійна компетентність фахівця формується як цілісна система, в якій управлінські та комунікативні компетентності виконують координуючу й інтегративну функції щодо фахових знань [11].

Таким чином, управлінська компетентність посідає ключове місце в системі професійної компетентності фахівців з кібербезпеки, виступаючи умовою ефективної реалізації інших компетентностей і забезпечуючи перехід від виконавського рівня професійної діяльності до рівня управління процесами та командами. Її цілеспрямоване формування в процесі професійної підготовки у закладах вищої освіти є необхідною передумовою підготовки конкурентоспроможних фахівців з кібербезпеки, здатних діяти в складних і динамічних умовах сучасного цифрового середовища.

Сучасні умови розвитку цифрового суспільства та зростання кількості й складності кіберзагроз зумовлюють потребу в підготовці фахівців з кібербезпеки, здатних не лише виконувати технічні завдання, а й ефективно управляти процесами забезпечення інформаційної безпеки. Дослідники Юдін О. К., Матвійчук-Юдіна О. В. наголошують, що «професійна підготовка фахівців з кібербезпеки має забезпечувати не лише технічну готовність, а й здатність до організації та управління процесами захисту інформації» [16, с.52].

Відтак, професійна діяльність у сфері кібербезпеки все частіше пов'язана з організацією командної роботи, управлінням ресурсами, прийняттям стратегічних і тактичних рішень, координацією дій під час реагування на кіберінциденти та взаємодією з різними стейкхолдерами. У зв'язку з цим інтеграція управлінської підготовки в процес професійної освіти майбутніх фахівців з кібербезпеки є об'єктивно необхідною.

Доцільність такої інтеграції зумовлена, по-перше, потребами ринку праці, який висуває вимоги до фахівців з кібербезпеки як до потенційних керівників підрозділів, проєктів або команд кіберзахисту. По-друге, управлінська підготовка сприяє формуванню в майбутніх фахівців здатності до системного та стратегічного мислення, управління ризиками, прогнозування наслідків управлінських рішень і адаптації до змін у кіберпросторі. По-третє, інтеграція управлінських знань і вмінь із фаховими дисциплінами дозволяє подолати фрагментарність професійної підготовки та забезпечити цілісність формування професійної компетентності.

Крім того, управлінська підготовка в процесі професійної освіти майбутніх фахівців з кібербезпеки створює передумови для розвитку їхніх комунікативних, лідерських і рефлексивних умінь, що є необхідними для ефективної взаємодії в міждисциплінарних командах і прийняття відповідальних рішень у кризових ситуаціях. Інтеграція управлінського компоненту може здійснюватися через міждисциплінарні навчальні курси, проєктну та ситуаційну діяльність, моделювання управлінських рішень у сфері кібербезпеки, що підвищує практичну спрямованість професійної підготовки.

У своєму дослідженні Л. М. Карамушка зазначає, що «у структурі управлінської компетентності доцільно виокремлювати мотиваційно-ціннісний, когнітивний, операційно-діяльнісний, комунікативний і рефлексивний компоненти, що забезпечують цілісність управлінської діяльності» [9].

Отже, інтеграція управлінської підготовки в процес професійної освіти майбутніх фахівців з кібербезпеки є доцільною та необхідною умовою формування їхньої управлінської компетентності, підвищення якості

 ISSN: 2786-9458

професійної підготовки та забезпечення готовності до ефективної діяльності в умовах сучасних викликів кіберпростору [13, 22, 24].

Висновки.#У результаті проведеного теоретичного аналізу встановлено, що в умовах цифрової трансформації суспільства та зростання рівня кіберзагроз управлінська компетентність набуває особливої значущості в системі професійної підготовки майбутніх фахівців з кібербезпеки. Доведено, що ефективна професійна діяльність у сфері кібербезпеки потребує не лише сформованих технічних знань і вмінь, а й здатності до управління процесами, ресурсами, персоналом і ризиками в умовах невизначеності та підвищеної відповідальності.

Уточнено зміст поняття «управлінська компетентність майбутніх фахівців з кібербезпеки», яке визначено як інтегративну професійно-особистісну характеристику, що відображає готовність і здатність майбутніх фахівців ефективно здійснювати управлінську діяльність у сфері кіберзахисту на основі системи управлінських і фахових знань, практичних умінь, ціннісних орієнтацій, відповідальності та здатності до самоаналізу й професійного саморозвитку.

Визначено та охарактеризовано структурні компоненти управлінської компетентності майбутніх фахівців з кібербезпеки, зокрема мотиваційно-ціннісний, когнітивний, операційно-діяльнісний, комунікативний та рефлексивно-оцінний, які перебувають у тісному взаємозв’язку та забезпечують цілісність цього феномену. З’ясовано, що управлінська компетентність посідає ключове місце в системі професійної компетентності фахівців з кібербезпеки, виконуючи інтегрувальну та координувальну функції щодо реалізації інших професійних компетентностей.

Обґрунтовано доцільність інтеграції управлінської підготовки в процес професійної освіти майбутніх фахівців з кібербезпеки як необхідної умови підвищення якості їх професійної підготовки та забезпечення готовності до виконання управлінських функцій у професійній діяльності [6, 10, 12]. Перспективи подальших досліджень вбачаються у визначенні педагогічних умов, розробленні методик і засобів формування управлінської компетентності

майбутніх фахівців з кібербезпеки, а також у створенні інструментарію оцінювання рівня її сформованості.

Список використаних джерел

1. Арсенович Л. А. Стан організації професійної підготовки фахівців із кібербезпеки в умовах особливого періоду. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 4. С. 18–26. URL: https://scholar.archive.org/work/ndy3g3i22bgldltpvvbnrooveu/access/wayback/https://chasopys-ppp.dp.ua/index.php/chasopys/article/download/255/223

2. Бібік Н. М. Компетентнісний підхід: рефлексивний аналіз. *Освіта України*. 2004. № 47. С. 6–9.

3. Галицький О. В., Микитенко П. В. Особливості формування професійної компетентності фахівців комп'ютерних наук. *Педагогічна Академія: наукові записки*. 2025. № 14. URL: https://pedagogical-academy.com/index.php/journal/article/download/607/494

4. Гончарук Ю. Публічне управління в системі національної кібербезпеки: виклики гібридної війни та напрями адаптації. *Forestry Education and Science: Current Challenges and Development Prospects*. 2025. С. 28–32. URL: https://conf.nltu.edu.ua/index.php/nltu150/article/download/395/275

5. Горлинський В. В., Горлинський Б. В. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки. *Інформаційна безпека*. 2020. № 2. С. 45–52.

6. Гузар Б. Теоретико-методичні засади формування управлінської компетентності майбутніх фахівців з кібербезпеки з використанням тренінгових технологій. *Педагогічна Академія: наукові записки*. 2025. № 25. URL: https://pedagogical-academy.com/index.php/journal/article/download/1559/1418

7. Зязюн І. А. Філософія педагогічної дії. Київ : НПУ імені М. П. Драгоманова, 2008. 608 с.

8. Кальченко В., Любчак В., Ободяк В., Пугач І. Формування компетентностей майбутніх фахівців кібербезпеки завдяки ініціативі

«студентські кібербригади». *Кібербезпека: освіта, наука, техніка*. 2025. № 3(31). С. 188–197. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/1006/853

9. Карамушка Л. М. Психологія управління. Київ : Либідь, 2012. 384 с.

10. Кудінов С. С. Формування компетентностей фахівців національної системи кібербезпеки в умовах сучасних загроз. *Наукові записки*. 2021. Вип. 30. С. 98–105.

11. Овчарук О. В. Професійні та управлінські компетентності фахівців у цифровому суспільстві. *Педагогічні науки*. 2021. № 78. С. 34–41.

12. Пометун О. І. Компетентнісна модель підготовки фахівців у вищій освіті: сучасні виклики. *Український педагогічний журнал*. 2022. № 4. С. 5–14.

13. Пуховська Л. П. Трансформація професійної підготовки фахівців в умовах цифровізації освіти. *Професійна освіта: методологія, теорія та технології*. 2022. № 15. С. 12–20.

14. Різак В., Опачко М., Дешко Н. Інноваційний підхід у фаховій підготовці магістрів з кібербезпеки. *Фізико-математична освіта*. 2023. Т. 38, № 4. С. 62–67. URL: https://fmo-journal.org/index.php/fmo/article/download/276/184

15. Харківська А., Прокопенко А., Отрошко Т. Формування лідерської компетентності здобувачів вищої освіти у процесі професійної підготовки в умовах цифровізації та змішаного навчання. *Освіта. Інноватика. Практика*. 2025. Т. 13, № 6. С. 116–120. URL: https://www.oip-journal.org/index.php/oip/article/download/636/455

16. Юдін О. К., Матвійчук-Юдіна О. В. Concept of forming professional competencies of specialists in information technologies and cyber security. *Information Technology and Security*. 2018. Vol. 6, No. 2. P. 49–55.

17. Arsenovych L. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Кібербезпека: освіта, наука, техніка*. 2022. № 3(15). С. 93–109. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/338/281

18. European Union Agency for Cybersecurity (ENISA). Cybersecurity Skills Development in the EU. Luxembourg, 2023.

19. Ilieva E., Ivanova D. Technological knowledge, soft skills and management & leadership skills: three pillars for the digitally competent manager. *Economic Alternatives*. 2021. No. 1. P. 30–38.

20. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022.

21. Mintzberg H. Managing. San Francisco : Berrett-Koehler Publishers, 2009. 320 p.

22. OECD. Education in the Digital Age: Developing Skills for Cybersecurity. Paris : OECD Publishing, 2023.

23. Rotanova N., Shabelnyk T., Krivenko S., Lazarevska Y. Проблема підготовки фахівців з кібербезпеки: прикладна спрямованість математичних дисциплін. *Кібербезпека: освіта, наука, техніка*. 2021. № 1(13). С. 123–132. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/285/247

24. UNESCO. Digital Skills and Competence Development in Higher Education. Paris, 2024.

 ISSN: 2786-9458