УДК 378.091-043.86:004.05 DOI 10.58407/visnik.253417

Бивалькевич Леонід

https://orcid.org/0000-0002-5500-416X
Researcher ID AAO-3658-2020
Scopus-Author ID 60001243200

Кандидат педагогічних наук,
доцент кафедри лісового господарства та агротехнологій,
Національний університет «Чернігівський колегіум» імені Т.Г. Шевченка
(Чернігів, Україна) E-mail: manofmystery@ukr.net

Лілік Ольга

https://orcid.org/0000-0002-5187-1944
Researcher ID GQB-0015-2022

Доктор педагогічних наук, професор,
професор кафедри української мови,
літератури та журналістики,
Національний університет «Чернігівський колегіум» імені Т.Г. Шевченка
(Чернігів, Україна) E-mail: lilik8383@ukr.net

Носовець Наталія

https://orcid.org/0000-0003-1536-4870

Кандидат педагогічних наук, професор,
професор кафедри педагогіки, психології і методики технологічної освіти,
Національний університет «Чернігівський колегіум» імені Т. Г. Шевченка
(Чернігів, Україна) E-mail: ppmtpn@gmail.com

ФОРМУВАННЯ БАЗОВИХ КОМПЕТЕНТНОСТЕЙ ІЗ КІБЕРБЕЗПЕКИ В ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ: ОРГАНІЗАЦІЙНІ Й МЕТОДИЧНІ АСПЕКТИ

Мета статті *– обґрунтувати організаційні й методичні аспекти формування базових компетентностей із кібербезпеки в здобувачів вищої освіти.*

Методологія*. У процесі дослідження організаційних і методичних аспектів формування базових компетентностей із кібербезпеки в здобувачів вищої освіти застосовано такі методи: аналіз робочих програм з освітніх компонентів, пов'язаних із кібербезпекою й цифровими технологіями; аналіз наукової літератури з проблеми дослідження; спостереження за освітнім процесом у закладах вищої освіти; систематизації й узагальнення для формулювання висновків.*

Дослідження здійснене на основі застосування положень кількох методологічних підходів, зокрема: компетентнісного, оскільки формування базових компетентностей із кібербезпеки варто здійснювати з огляду на зафіксовані у відповідних освітньо-професійних програмах загальні й фахові компетентності; аксіологічного, адже функціювання особистості в інтернет-мережі вимагає дотримання нею певного етикету; діяльнісного, що передбачає активне залучення здобувачів вищої освіти до виконання завдань, пов'язаних із кібербезпекою; особистісно орієнтованого, що полягає у врахуванні індивідуального досвіду здобувачів вищої освіти, а також їхніх інтересів і вподобань.

Наукова новизна *полягає в тому, що вперше було обґрунтовано особливості інтеграції до змісту освітньої компоненти «Основи кібербезпеки» онлайнових курсів, розміщених на платформі Cisco Networking Academy*

Висновки*. На підставі врахування швидкого розвитку кіберзагроз, пов'язаних із викраденням персональних даних та іншої надзвичайно важливої інформації, обґрунтовано доцільність формування в студентів базових компетентностей із кібербезпеки. Доведено важливість опанування здобувачами вищої освіти навчальної дисципліни «Основи кібербезпеки», яка дає студентам фундаментальні знання про те, як не стати жертвою кіберзлочину, забезпечити елементарний захист персональної інформації, здобути дієві*

практичні навички безпечного користування інформаційною сферою, а також сприятиме формуванню цифрової грамотності й обізнаності в системі кібербезпеки. Відповідно, освітня компонента «Основи кібербезпеки» є фундаментом для подальшого професійного зростання в ІТ галузі та кібербезпеки. Обґрунтовано, що ефективному опануванню цієї навчальної дисципліни сприятиме впровадження до її змісту онлайнових курсів на платформі Cisco Networking Academy.

***Ключові слова**: основи кібербезпеки, кібербезпека, цифрова освітня платформа, здобувачі вищої освіти, цифрові технології, інформаційні технології в галузі, заклад вищої освіти.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Стрімкий розвиток цифровізації, сучасних інформаційних технологій і систем, призвів до виникнення нових кіберзагроз у всіх соціальних сферах, появи все складніших і масштабніших кіберінцидентів, які призводять до серйозних збитків і втрати важливої інформації. На основі аналізу сучасного стану кібербезпеки виявлено, що рівень кібератак зростає щорічно на 15–20%, водночас вони стають ще складнішими для виявлення і протидії. Відповідно, суспільство потребує підготовки конкурентоспроможних спеціалістів із цифрових технологій і кібербезпеки, які зможуть застосувати набуті знання і практичні навички, а також нові інструменти в інформаційному просторі. З цього приводу Є. Гайович і С. Тополянський зауважують, що ключовими факторами успішного забезпечення кібербезпеки є рівень підготовки учасників освітнього процесу, їхня відповідальність і професійні навички [3].

Особливо загрозлива ситуація склалася в Україні, яка тривалий час перебуває в умовах кібервійни та є на сьогодні найбільш інформаційно атакованою країною світу. На сучасному етапі в нашій країні популярними стають DDoS-атаки на державні установи, приватні компанії, підприємства критичної інфраструктури, фішинг, атаки програм-вимагачів. Відповідно, в умовах кіберконфліктів і гібридних атак на інформаційну сферу питання кібербезпеки набуло державного рівня. Саме така ситуація вимагає збільшення кваліфікованих фахівців у сфері кібербезпеки та цифрових технологій на усіх рівнях. Відтак важливою складовою сучасної професійної підготовки в закладах вищої освіти стає формування в студентів базових компетентностей із кібербезпеки, розвиток технічних навичок і формування відповідальної цифрової поведінки, уміння забезпечувати власну інформаційну безпеку, оцінювати ризики й ухвалювати зважені рішення. Водночас аналіз наукових публікацій і досвід професійної діяльності дали змогу визначити певні суперечності, пов'язані з інформаційною безпекою, що виникають у процесі реалізації освітньо-професійних програм підготовки відповідних фахівців у закладах вищої освіти: зміст навчальних дисциплін, що передбачають опанування комп'ютерних технологій та формування інформаційної грамотності здобувачів, не відповідає сучасним вимогам; недостатність матеріального та програмного забезпечення в закладах вищої освіти для моделювання кібератак і розроблення захисту; брак кваліфікованих викладачів-практиків, які активно працюють у сфері кібербезпеки; недостатня кількість практико орієнтованих занять.

Це й зумовлює необхідність розроблення й упровадження в освітній процес із підготовки майбутніх фахівців за освітньо-професійною програмою Професійна освіта (Цифрові технології) навчальної дисципліни «Основи кібербезпеки», «Інформаційні технології в галузі» [1], актуальність якої детермінована такими ключовими факторами: зростанням кіберзагроз і стрімким розвитком технологій кібератак, економічним розвитком і переходом до цифрових моделей захисту національної безпеки України, увідповідненням міжнародним стандартам захисту інформації. При цьому постає необхідність розроблення теоретичних засад викладання цієї навчальної дисципліни й формулювання методичних рекомендацій щодо пошуку оптимальних форм, методів і засобів навчання.

Аналіз останніх публікацій, у яких започатковане розв'язання проблеми. Питання кібербезпеки загалом та особливості упровадження елементів інформаційної безпеки в освітньому процесі закладів вищої освіти досліджувало чимало українських і зарубіжних науковців. У цьому контексті варто згадати В. Ду (Wenliang «Kevin» Du), який розробив стратегії підготовки студентів до професійної діяльності в галузі кібербезпеки, опублікував низку праць із формування навчальних програм та розвитку студентських компетентностей у сфері цифрових технологій і кібербезпеки [9]; М. Таддео (Mariarosaria Taddeo), яка займається етичними, соціальними та політичними аспектами кібербезпеки, зокрема принципами відповідального використання цифрових технологій [11]; А. Сасс (Angela Sasse), яка зосереджена на поведінкових аспектах безпеки, зокрема вивчає, як люди реагують на загрози, як вони сприймають політику безпеки та як треба вивчати ці положення в межах відповідних навчальних дисциплін [10]. Окрім того, варто згадати про наукові пошуки дослідницьких груп з адаптивного навчання (Я Викопал, П. Седа (Jan Vykopal, Pavel Seda) та інші [13]), які працюють над розробленням адаптивних середовищ для тренування кібербезпеки, ставлять за мету підлаштовування складності завдань під рівень навчальних досягнень студента; Д. Гуйтема, А. Вонг (Dylan Huitema та Albert Wong) досліджують особливості інтеграції ігрофікації у навчальні програми, доводять, що це допомагає підвищити активність студентів [12].

Варто згадати також і про напрацювання українських науковців, які займаються питаннями кібербезпеки в освіті: Є. Гайович та С. Тополянський, які обґрунтовують, що сучасні заклади вищої освіти піддаються реальним кіберзагрозам, а це створює ризики для цифрової інфраструктури університетів,

персональних даних студентів і викладачів, а також для функціювання освітніх платформ [3]; В. Коваленко та Т. Осипчук досліджують цифрову компетентність учителів у контексті кібербезпеки в закладах загальної середньої освіти, зокрема вони визначили рівні цифрових компетентностей учителів, описали проблеми готовності викладачів до викладання кібербезпеки, обґрунтували потребу в постійному професійному розвитку учителів у сфері кібербезпеки [4]; В. Биков, О. Буров, Н. Дементієвська, які проаналізували кібербезпеку інформаційного та освітнього середовища як частину педагогічного простору, обґрунтували, що кібербезпека відображає не лише технічні аспекти, а й правові, організаційні та психологічні [2]. Варто також зауважити, що до питань цифрової та інформаційної грамотності ми також зверталися в попередніх публікаціях [5; 6] у контексті дотичних тем, проте досліджувану проблему на сьогодні не можна вважати розв'язаною, вона потребує ґрунтовного, системного й науково обґрунтованого підходу.

Мета статті – обґрунтувати організаційні й методичні аспекти формування базових компетентностей із кібербезпеки в здобувачів вищої освіти.

Висвітлення процедури теоретико-методологічного та/або експериментального дослідження із зазначенням методів дослідження. У процесі дослідження організаційних і методичних аспектів формування базових компетентностей із кібербезпеки в здобувачів вищої освіти застосовано такі методи: аналіз робочих програм з освітніх компонентів, пов'язаних із кібербезпекою і цифровими технологіями для характеристики їхнього змістового наповнення й вимог до рівня навчальних досягнень студентів; аналіз наукової літератури з проблеми дослідження, що дало змогу окреслити теоретичні аспекти порушеного питання; метод спостереження за освітнім процесом у закладах вищої освіти, який дав змогу визначити проблеми, пов'язані з кібербезпекою й цифровими технологіями, що потребують нагального розв'язання; систематизації й узагальнення для формулювання висновків.

Дослідження здійснене на основі застосування положень кількох методологічних підходів, зокрема: компетентнісного, оскільки формування базових компетентностей із кібербезпеки варто здійснювати з огляду на зафіксовані у відповідних освітньо-професіних програмах загальні й фахові компетентності; аксіологічного, адже функціювання особистості в інтернет-мережі вимагає дотримання нею певного етикету, а також певного рівня сформованості морально-етичних норм; діяльнісного, що передбачав активне залучення здобувачів вищої освіти до виконання завдань, пов'язаних із кібербезпекою; особистісно орієнтованого, що полягає у врахуванні індивідуального досвіду здобувачів вищої освіти, а також їхніх інтересів і вподобань.

Виклад основного матеріалу дослідження. Відповідно до навчального плану, освітня компонента «Основи кібербезпеки» є складовою нормативної підготовки за освітньо-професійною програмою першого (бакалаврського) рівня вищої освіти «Професійна освіта (Цифрові технології)», також частково деякі теми з кібербезпеки розглядаються при вивченні дисципліни «Інформаційні технології в галузі» (комп'ютерні інтернет мережі, налаштування та кібербезпека). Водночас наголосимо на доцільності упровадження цієї освітньої компоненти до циклу загальної підготовки інших освітньо-професійних програм (наприклад, Середня освіта (Технології), Професійна освіта (Транспорт), Професійна освіта (Аграрне виробництво, переробка сільськогосподарської продукції та харчові технології)), оскільки вона має соціальну значущість і вирізняється особливою актуальністю.

Навчальна дисципліна «Основи кібербезпеки» спрямована на формування у студентів системного розуміння фундаментальних принципів захисту інформації, сучасних кіберзагроз, методів та засобів забезпечення безпеки інформаційних систем, мереж і даних [1]. Предметом її вивчення є основні поняття, моделі та принципи кібербезпеки, види, методи й механізми забезпечення інформаційної безпеки в комп'ютерних системах і мережах; технології Cisco для забезпечення безпеки мереж; сучасні кіберзагрози, способи їх виявлення та протидії ним; основи організаційного та технічного забезпечення безпеки; правила безпечного користування інформаційно-комунікаційними технологіями; фундаментальні принципи захисту мереж, систем та даних; роль людини в цих процесах; соціальна інженерія та фактори ризику; методи оцінювання ризиків та управління інцидентами; компоненти, архітектура та функції систем кіберзахисту [1].

Відповідно, у результаті вивчення навчальної дисципліни «Основи кібербезпеки» студенти мають знати: основні поняття, принципи та моделі кібербезпеки; типи кіберзагроз, атак, шкідливого програмного забезпечення та методи їхньої ідентифікації; особливості роботи мережевих протоколів та їхньої уразливості; архітектуру безпечної мережі; принципи роботи систем моніторингу безпеки; основи криптографії (шифрування, хеш-функції); моделі доступу та механізми автентифікації; процеси реагування на інциденти; структуру та роботу засобів Cisco для кіберзахисту. При цьому вони мають уміти аналізувати кіберзагрози та оцінювати ризики в інформаційних системах; конфігурувати мережеві технології безпеки у Cisco Packet Tracer; виявляти та класифікувати ознаки фішингу та соціальної інженерії; аналізувати журнали подій, мережевий трафік; розробляти заходи кібергігієни та рекомендації для користувачів; формувати звіти щодо кіберінцидентів та проводити базове розслідування; налаштовувати базові засоби захисту каналів зв'язку [1].

У робочій програмі з освітньої компоненти «Основи кібербезпеки» передбачено опанування чотирьох змістових моделів: «Вступ до кібербезпеки», «Безпека каналів передачі та інфраструктури. Захист операційних систем і кінцевих точок», «Принципи та інструменти кібербезпеки», «Управління доступом, брандмауери, хмарна безпека» [1]. Водночас досвід викладання цієї навчальної дисципліни дає

підстави для висновку, що, окрім лекційних (24 години) і практичних (24 години) занять, які передбачені навчальним планом, важливо правильно організувати самостійну роботу студентів (72 години).

Відповідно, для розв'язання проблем і суперечностей, що виникли у межах професійної підготовки в закладах вищої освіти, необхідна інтеграція та впровадження глобальних навчальних ресурсів, які системно розвиваються і оновлюються. Як було вже констатовано в попередній публікації [6], використання цифрових освітніх платформ сприятиме суттєвому розширенню доступу до якісної освіти та навчання протягом усього життя, а також забезпеченню комплексної й повноцінної участі окремих університетів у світовій системі вищої освіти. Власне, особливості опанування дистанційних освітніх курсів на деяких платформах (MIT Open Course Ware, EdX, Coursera, EdEra і Prometeus) були схарактеризовані в згаданій статті [6]. Доцільно, на нашу думку, зосередитися на тих ресурсах, які будуть ефективними саме в контексті освітньої компоненти «Основи кібербезпеки».

Одним із найактуальніших способів підготовки, на нашу думку, є міжнародна освітня цифрова платформа Cisco Networking Academy [7], яка дає змогу оволодіти професією за допомогою провідної системи курсів, що містять актуальну інформацію, яка відповідає світовому стандарту у сфері захисту кіберзахисту, містить теоретичний, практичний і лабораторний матеріал у форматі віртуальної лабораторії Cisco Packet Tracer, яка пропонує всі відомі інструменти налагодження і захисту мереж і систем, відтворює реальну імітацію роботи сучасної комп'ютерної техніки.

На базі освітньої платформи Cisco Networking Academy є можливість пройти курси з Introduction to Cybersecurity (вступ до кібербезпеки) [8] та Cybersecurity Essentials (основи кібербезпеки) [9], які відповідають сучасним світовим стандартам у галузі кібербезпеки, пропонують застосування симуляцій комп'ютерного обладнання та мережевих систем та інтерактивні вправи, навчальні відео та презентації за кожною темою матеріалу, а після успішного проходження курсу здобувач може отримати професійний сертифікат.

Зауважимо, що опанування навчальної дисципліни «Основи кібербезпеки» на базі платформи Cisco Networking Academy [7] має низку переваг, зокрема: практичні й семінарські роботи на платформі курсу Cybersecurity Essentials [9] максимально наближені до реальних умов завдяки віртуальній симуляції обладнання і програмного забезпечення; опанування цього курсу не потребує використання потужних комп'ютерних ресурсів, може реалізовуватись у комп'ютерних класах університету або через дистанційне використання платформи зі стаціонарного персонального комп'ютера або ноутбука. Як засвідчує досвід, проходження курсу сприяє формуванню технічних навичок, розвиває критичне мислення студента і впливає на розвиток цифрової грамотності та безпечної поведінки користувача. Позитивне підкріплення досягається шляхом отримання міжнародного сертифікату Cisco. До переваг цієї платформи варто віднести гнучкість, мобільність і відновлюваність курсу (студент сам вирішує, коли краще проходити курс, а результати виконання зберігаються й піддаються аналізу).

При цьому викладач освітньої компоненти «Основи кібербезпеки» має пам'ятати, що інтеграція модулів курсу Cisco Cybersecurity Essentials до відповідних тем цієї навчальної дисципліни потребує певної адаптації, зокрема контексті використання середовища програми Packet Tracer для виконання практичних-семінарських робіт; використання контролю за пройденим матеріалом на платформі; розроблення навчальної програми відповідно до стандартів; перенесення виконаної роботи студентом на платформу Moodle.

Висновки і перспективи подальших досліджень. Отже, на підставі врахування швидкого розвитку кіберзагроз, викрадення персональних даних та іншої надзвичайно важливої інформації, обґрунтовано доцільність формування в студентів базових компетентностей із кібербезпеки. Обґрунтовано важливість опанування здобувачами вищої освіти навчальної дисципліни «Основи кібербезпеки», яка дає студентам фундаментальні знання про те, як не стати жертвою кіберзлочину, забезпечити елементарний захист персональної інформації, здобути дієві практичні навички безпечного користування інформаційною сферою, а також сприятиме формуванню цифрової грамотності й обізнаності в системі кібербезпеки. Відповідно, освітня компонента «Основи кібербезпеки» є фундаментом для подальшого професійного зростання в ІТ галузі та кібербезпеки. Обґрунтовано, що ефективному опануванню цієї навчальної дисципліни сприятиме впровадження до її змісту онлайнових курсів на платформі Cisco Networking Academy.

Перспективи подальших досліджень убачаємо в апробації інших онлайнових ресурсів зі сфери кібербезпеки, а також у відборі методів, прийомів і засобів, які сприятимуть підвищенню компетентностей здобувачів у галузі інформаційної безпеки.

References

1. Бивалькевич Л. М. Основи кібербезпеки: робоча програма. Чернігів: НУЧК, 2025. 12 с.
   Byvalkevych, L. M. (2025). Osnovy kiberbezpeky: robocha prohrama [Fundamentals of Cybersecurity: Work Program]. Chernihiv: NUChK. [in Ukrainian].
2. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*. 2019. Том 70. № 2. С. 313–331.
   Bykov, V., Burov, Yu, Dementievska, N. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cyber Security in a Digital Learning Environment]. *Informatsiini tekhnolohii i zasoby navchannia – Information Technologies and Learning Tools,* 70, 2, 313–331. [in Ukrainian].

3. Гайович Є., Тополянський С. Кібербезпека в системі сучасної вищої освіти: реалії та перспективи подальшого розвитку. *Науковий вісник Ужгородського університету. Серія: Педагогіка. Соціальна робота*. 2025. № 1(56). С. 45–50. URL : https://doi.org/10.24144/2524-0609.2025.56.45-50.
Haiovych, Ye., Topolianskyi, S. (2025). Kiberbezpeka v systemi suchasnoi vyshchoi osvity: realii ta perspektyvy podalshoho rozvytku [Cybersecurity in the system of modern higher education: realities and prospects for further development]. *Naukovyi visnyk Uzhhorodskoho universytetu. Seriia: Pedahohika. Sotsialna robota – Scientific Bulletin of Uzhhorod University. Series: Pedagogy. Social Work*, (1(56), 45–50. [in Ukrainian].

4. Коваленко В., Осипчук Т. Проблема розвитку цифрової компетентності з кібербезпеки вчителів ЗЗСО. *Фізико-математична освіта.* 2024. Том 39. № 2. С. 35–42.
Kovalenko, V., Osypchuk, T. (2024). Problema rozvytku tsyfrovoi kompetentnosti z kiberbezpeky vchyteliv ZZSO [The problem of developing digital competence in cybersecurity of teachers of secondary schools]. *Fizyko-matematychna osvita – Physical and mathematical education*, 39, 2, 35–42. [in Ukrainian].

5. Лілік О., Бивалькевич Л. Формування цифрової грамотності майбутніх учителів в умовах дистанційного навчання. *Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка.* 2021. № 14-15 (170-171). С. 21–26.
Lilik, O., Byvalkevych, L. (2021). Formuvannia tsyfrovoi hramotnosti maibutnikh uchyteliv v umovakh dystantsiinoho navchannia [Formation of digital literacy of future teachers in conditions of distance learning]. *Visnyk Natsionalnoho universytetu «Chernihivskyi kolehium» imeni T.H. Shevchenka – Bulletin of the T.H. Shevchenko National University «Chernihiv Colehium»*, 14-15 (170-171), 21-26. [in Ukrainian].

6. Лілік О. О., Бивалькевич Л. М. Використання цифрових освітніх платформ у професійній підготовці майбутніх учителів. *Вісник Національного університету «Чернігівський колегіум» імені Т.Г. Шевченка. 2025*. Вип. 33 (189). С. 121–126.
Lilik, O. O., Byvalkevych, L. M. (2025). Vykorystannia tsyfrovykh osvitnikh platform u profesiinii pidhotovtsi maibutnikh uchyteliv [Use of digital educational platforms in the professional training of future teachers]. *Visnyk Natsionalnoho universytetu «Chernihivskyi kolehium» imeni T.H. Shevchenka – Bulletin of the T.H. Shevchenko National University «Chernihiv Colehium»*, 33 (189), 121–126. [in Ukrainian].

7. Cisco Networking Academy. Cisco Systems, Inc., 2025. URL: https://www.netacad.com.
Cisco Networking Academy (2025). Cisco Systems, Inc. Retrived from: https://www.netacad.com. [in English].

8. Cisco Networking Academy. Introduction to Cybersecurity: online course. Cisco, 2025. URL: https://surli.cc/mdmrlv.
Cisco Networking Academy. Introduction to Cybersecurity: online course. Cisco (2025). Retrived from: https://surli.cc/mdmrlv. [in English].

9. Cisco Networking Academy. Cybersecurity Essentials: online course. Cisco, 2025. URL: https://surl.li/bggihf.
Cisco Networking Academy. Cybersecurity Essentials: online course. Cisco (2025). Retrived from: https://surl.li/bggihf. [in English].

10. Du W. Situation aware security system and method for mobile devices. URL: https://patentimages.storage.googleapis.com/08/43/ef/4a963d7fd74c11/US20120309354A1.pdf.
Du, W. (2012). Situation aware security system and method for mobile devices. Retrived from: https:// patentimages.storage.googleapis.com/08/43/ef/4a96 3d7fd74c11/US20120309354A1.pdf. [in English].

11. Sasse A. How to t (r) ap users' mental models. Human Factors in Information Technology. North-Holland, 1991. P. 59–79.
Sasse, A. (1991). How to t (r) ap users' mental models. Human Factors in Information Technology. North-Holland, 59–79. [in English].

12. Taddeo M. Defining trust and e-trust: from old theories to new problems. International journal of technology and human interaction (IJTHI). 2009. Vol.5. Is. 2. P. 23-35.
Taddeo, M. (2009). Defining trust and e-trust: from old theories to new problems. International journal of technology and human interaction (IJTHI), 5, 2, 23-35. [in English].

13. Huitema D., Wong A. Case study in gamification for cybersecurity education. URL: https://arxiv.org/abs/2502.06706.
Huitema, D., & Wong, A. (2025). Case study in gamification for cybersecurity education. Retrived from: https://arxiv.org/abs/2502.06706. [in English].

14. Vykopal J., Seda P., et al. Smart adaptive learning environments for cybersecurity skills. URL: https://arxiv.org/abs/2307.05281.
Vykopal, J., Seda, P., et al. (2023). Smart adaptive learning environments for cybersecurity skills. Retrived from: https://arxiv.org/abs/2307.05281. [in English].

Byvalkevych Leonid

https://orcid.org/0000-0002-5500-416X
Researcher ID AAO-3658-2020
Scopus-Author ID 60001243200

PhD in Pedagogical Science,
Associate Professor, Associate Professor Department
of Forestry and Agricultural Technologies,
T. H. Shevchenko National University «Chernihiv Colehium»
(Chernihiv, Ukraine) E-mail: manofmystery@ukr.net

Lilik Olha

https://orcid.org/0000-0002-5187-1944
ResearcherID GQB-0015-2022

Doctor of Pedagogical Sciences,
Professor, Professor of the Department
of Ukrainian Language, Literature and Journalism,
T.H. Shevchenko National University «Chernihiv Colehium»
(Chernihiv, Ukraine) E-mail: lilik8383@ukr.net

Nosovets Nataliia

https://orcid.org/ 0000-0003-1536-4870

PhD in Pedagogical Sciences, Professor,
Professor of the Department of Pedagogy, Psychology and
Methodology of Technological Education,
T. H. Shevchenko National University «Chernihiv Colehium»
(Chernihiv, Ukraine) E-mail: ppmtpn@gmail.com

FORMATION OF BASIC COMPETENCES IN CYBERSECURITY IN HIGHER EDUCATION STUDENTS: ORGANIZATIONAL AND METHODOLOGICAL ASPECTS

The purpose of the article is to substantiate the organizational and methodological aspects of the formation of basic cybersecurity competencies in higher education students.

***Methodology**. In the process of studying the organizational and methodological aspects of the formation of basic cybersecurity competencies in higher education students, the following methods were used: analysis of work programs on educational components related to cybersecurity and digital technologies; analysis of scientific literature on the research problem; method of observing the educational process in higher education institutions; systematization and generalization for formulating conclusions. The study was carried out on the basis of the application of the provisions of several methodological approaches, in particular: competency-based, since the formation of basic cybersecurity competencies should be carried out taking into account the general and professional competencies recorded in the relevant educational and professional programs; axiological, since the functioning of an individual in the Internet network requires compliance with certain etiquette; activity-based, which involved the active involvement of higher education students in performing tasks related to cybersecurity; personality-oriented, which involved taking into account the individual experience of higher education students, as well as their interests and preferences.*

*The **scientific novelty** lies in the fact that for the first time the features of integration into the content of the educational component «Fundamentals of Cybersecurity» of online courses posted on the Cisco Networking Academy platform were substantiated.*

***Conclusions**. Taking into account the rapid development of cyber threats, theft of personal data and other extremely important information, the feasibility of forming basic cybersecurity competencies in students is substantiated. The importance of higher education students mastering the academic discipline «Fundamentals of Cybersecurity» is substantiated, which provides students with fundamental knowledge about how not to become a victim of cybercrime, ensure basic protection of personal information, acquire effective practical skills for safe use of the information sphere, and also contribute to the formation of digital literacy and awareness in the cybersecurity system. Accordingly, the educational component «Fundamentals of Cybersecurity» is the foundation for further professional growth in the IT industry and cybersecurity. It is substantiated that the effective mastery of this academic discipline will be facilitated by the introduction of online courses on the Cisco Networking Academy platform into its content.*

***Key words:** cybersecurity, digital educational platform, higher education students, digital technologies, higher education institution.*

Стаття надійшла до редакції 20.12.2025 р.

*Рецензент: доктор педагогічних наук, професор **Світлана Грищенко***