УДК 378.091-043.86:004.05 **DOI 10.58407/visnik.263911**

Лілік Ольга

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

Бивалькевич Леонід

https://orcid.org/0000-0002-5500-416X
ResearcherID 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

РОЗВИТОК КУЛЬТУРИ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ФОРМУВАННЯ ІНФОРМАЦІЙНО-ЦИФРОВОЇ ГРАМОТНОСТІ В ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Мета статті – *схарактеризувати особливості розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності в здобувачів вищої освіти.*

Методологія. *У процесі визначення особливостей розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності в здобувачів вищої освіти було застосовано такі методи наукового дослідження: аналіз робочих програм з освітніх компонентів, пов'язаних із кібербезпекою і цифровими технологіями, з огляду на їхнє змістове наповнення й вимоги до рівня навчальних досягнень студентів; аналіз наукової літератури з проблеми дослідження, що дав змогу сформулювати теоретичні засади дослідження; метод спостереження за освітнім процесом у закладах вищої освіти, на основі чого було визначено суперечності в розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності здобувачів вищої освіти; систематизації й узагальнення для формулювання висновків.*

Дослідження передбачало врахування окремих положень кількох методологічних підходів, а саме: компетентнісного (врахування зафіксованих у відповідних освітньо-професійних програмах загальних і фахових компетентностей, програмних результатів навчання); аксіологічного (формування в здобувачів вищої освіти уявлення про нетикет як особливу форму етикету, а також цілеспрямований вплив на ціннісно-світоглядну сферу студентів); діяльнісного (залучення здобувачів вищої освіти до виконання завдань, спрямованих на формування інформаційно-цифрової компетентності); особистісно орієнтованого (врахування особистісних рис та індивідуального досвіду здобувачів вищої освіти у процесі формулювання навчальних завдань).

Наукова новизна. *У статті досліджено особливості розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності в здобувачів вищої освіти.*

Висновки. *Обґрунтовано, що культура кібербезпеки – це сукупність знань, переконань, навичок та моделей поведінки, спрямованих на захист інформації та протидію кіберзагрозам у цифровому просторі. Констатовано, що в межах освітнього процесу в закладах вищої освіти культуру кібербезпеки доцільно розвивати в контексті формування інформаційно-цифрової грамотності здобувачів. З'ясовано, що одним зі шляхів розвитку культури кібербезпеки вважаємо розроблення й упровадження в освітній процес освітньої компоненти «Основи кібербезпеки», яка сприятиме формуванню в студентів системи необхідних знань, а також дієвих практичних навичок щодо безпечного користування інформаційною сферою, що в сукупності сприятиме підвищенню рівня цифрової грамотності й обізнаності в системі кібербезпеки. Доведено, що ефективному опануванню цієї навчальної дисципліни сприятиме впровадження до її змісту онлайнових курсів на платформі Cisco Networking Academy, а також застосування сучасних педагогічних технологій, як-от: технологія проєктів, технологія case-study, технологія перевернутого навчання.*

Ключові слова*: культура кібербезпеки, інформаційно-цифрова грамотність, здобувачі вищої освіти, цифрові технології, заклад вищої освіти, освітня компонента.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Як свідчать психологічні й педагогічні дослідження, тотальна інформатизація й комп'ютеризація, життя у віртуальному просторі впливають на розвиток нового покоління й специфіку сприйняття ним навчальної інформації, а в перспективі – і на формування компетентностей, необхідних для ефективної професійної діяльності й життєдіяльності в соціумі загалом.

Варто також наголосити, що процеси диджиталізації призвели і до появи низки загроз, як-от: маніпулятивні впливи, дезінформація, втрата особистих даних тощо. Це актуалізує необхідність цілеспрямованої підготовки молодого покоління до протидії усім викликам, що постають в умовах інформатизованого середовища, а водночас до активного використання його переваг у навчальній діяльності й повсякденному житті, а також до застосування новітніх досягнень техніки у своїй навчальній і подальшій професійній діяльності. У цьому контексті на особливу увагу заслуговує інформаційно-цифрова компетентність як одна з десяти ключових компетентностей Нової української школи, що не лише дає можливість особистості бути сучасною, а й безпосередньо сприяє формуванню основ культури кібербезпеки для безпечного й повноцінного функціювання людини у віртуальному середовищі [2]. Саме розвиток культури кібербезпеки в контексті формування в здобувачів освіти інформаційно-цифрової компетентності і має стати пріоритетним завданням закладів загальної середньої (особливо в старшій профільній школі) й вищої освіти на сучасному етапі.

Аналіз останніх публікацій, у яких започатковане розв'язання проблеми. Різноманітні аспекти формування інформаційно-цифрової компетентності в здобувачів середньої і вищої освіти були розкриті в наукових публікаціях Ю. Запорожцевої, Н. Куриленко, І. Сліпухіної, С. Мєняйлова, В. Бикова, О. Спіріна, О. Пінчук, С. Литвинової, О. Бурова, С. Семерікова. До проблеми формування цифрової та інформаційної грамотності ми також зверталися в попередніх публікаціях [6; 7; 8] зокрема і в контексті формування базових компетентностей із кібербезпеки [2].

У контексті формування культури кібербезпеки варто звернути увагу на наукові праці В. Ду (Wenliang «Kevin» Du), присвячені стратегіям підготовки студентів до професійної діяльності в галузі кібербезпеки, а також формуванню їхніх компетентностей у сфері цифрових технологій і кібербезпеки [12]. Окрім того, важливим є положення наукових публікацій М. Таддео (Mariarosaria Taddeo), спрямовані на аналіз етичних, соціальних та політичних аспектів кібербезпеки, зокрема принципів усвідомленого й відповідального використання цифрових технологій [14], а також ідеї А. Сасс (Angela Sasse) щодо поведінкових аспектів безпеки, зокрема особливостей людських реакцій на загрози у віртуальному просторі [13].

З-поміж українських науковців у контексті проблеми формування культури кібербезпеки в здобувачів освіти варто згадати про Є. Гайович та С. Тополянського, які досліджували ризики для цифрової інфраструктури закладів вищої освіти, персональних даних здобувачів і викладачів, а також для функціювання освітніх платформ [4]. У наукових працях В. Коваленко та Т. Осипчук досліджено цифрову компетентність учителів у контексті кібербезпеки, зокрема визначено рівні цифрових компетентностей, описано проблеми готовності викладачів до викладання основ кібербезпеки, обґрунтовано потребу в постійному професійному розвитку учителів і викладачів у сфері кібербезпеки [5]. В. Биков, О. Буров, Н. Дементієвська довели, що кібербезпека відображає не лише технічні аспекти функціювання особистості у віртуальному просторі, а й правові, організаційні та психологічні [3].

Актуальність досліджуваної проблеми детермінована ще і суперечностями, що виникають у процесі реалізації освітньо-професійних програм підготовки майбутніх фахівців різних спеціальностей у закладах вищої освіти й перешкоджають формуванню інформаційно-цифрової компетентності й культури кібербезпеки: зміст навчальних дисциплін, спрямованих на 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 технологій захисту; кадрова проблема, що полягає у відсутності висококваліфікованих викладачів-практиків, які активно працюють у сфері кібербезпеки; недостатня кількість практико орієнтованих занять у межах зазначених навчальних дисциплін.

Відповідно, постає необхідність розроблення стратегії для подолання зазначених суперечностей задля ефективного розвитку в здобувачів вищої освіти культури кібербезпеки в контексті формування в них інформаційно-цифрової грамотності.

Мета статті – схарактеризувати особливості розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності в здобувачів вищої освіти.

Висвітлення процедури теоретико-методологічного та/або експериментального дослідження із зазначенням методів дослідження. У процесі визначення особливостей розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності в здобувачів вищої освіти було застосовано такі методи наукового дослідження: аналіз робочих програм і силабусів з освітніх компонентів, пов'язаних із кібербезпекою і цифровими технологіями з огляду на їхнє змістове наповнення й вимоги до рівня навчальних досягнень студентів; аналіз наукової літератури з проблеми дослідження, що дав змогу сформулювати теоретичні засади дослідження; метод спостереження за освітнім процесом у закладах вищої освіти, на основі чого було визначено суперечності в розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності здобувачів вищої освіти; систематизації й узагальнення для формулювання висновків.

Дослідження передбачало актуалізацію окремих положень кількох методологічних підходів, а саме: компетентнісного (врахування зафіксованих у відповідних освітньо-професійних програмах загальних і фахових компетентностей, програмних результатів навчання, що відображають рівень сформованості інформаційно-цифрової компетентності); аксіологічного (формування в здобувачів вищої освіти уявлення про нетикет, а також цілеспрямований вплив на ціннісно-світоглядну сферу студентів); діяльнісного (залучення здобувачів вищої освіти до виконання завдань, спрямованих на формування інформаційно-цифрової компетентності); особистісно орієнтованого (врахування особистісних рис та індивідуального досвіду здобувачів вищої освіти у процесі формулювання навчальних завдань).

Виклад основного матеріалу дослідження. В умовах стрімких соціокультурних трансформацій кіберзахист із суто технічного процесу перетворюється на повсякденну практику кожного користувача чи організації, а відтак є підстави говорити про культуру кібербезпеки, яку розглядають здебільшого як сукупність знань, переконань, навичок та моделей поведінки, спрямованих на захист інформації та протидію кіберзагрозам у цифровому просторі [14].

Дослідники зазначають [12; 13; 14], що до основних складників кіберкультури належать кібергігієна (базові щоденні звички (використання складних унікальних паролів, увімкнена двофакторна автентифікація, регулярне оновлення програмного забезпечення), обізнаність щодо потенційних загроз (усвідомлення того, як діють фішинг, соціальна інженерія, шкідливі програми та маніпуляційні техніки), безпечне поводження з даними (усвідомлений підхід до зберігання, передавання та знищення конфіденційної інформації, як особистої, так і робочої), відповідальний цифровий слід (обізнаність щодо наслідків публікації особистих даних у соціальних мережах та відкритих джерелах).

Відповідно, на думку науковців [3; 4; 5; 12; 13; 14], є такі основні шляхи розвитку культури кібербезпеки:

– формальне, неформальне й інформальне навчання, зокрема опанування нормативних і вибіркових освітніх компонентів, проходження спеціальних тренінгів та курсів на цифрових освітніх платформах;

– упровадження певних правил під час користування засобами передавання інформації в громадських установах і в корпоративній політиці, що призводить до формування певних звичок безпечного функціювання у мережі Інтенет (наприклад, «правило чистого робочого столу»);

– державні ініціативи, спрямовані на впровадження обов'язкових стандартів кібергігієни для державних органів та навчальних закладів.

Для реалізації зазначених шляхів, а відтак і для ефективного розвитку в здобувачів вищої освіти культури кібербезпеки в контексті формування в них інформаційно-цифрової компетентності було розроблено й упроваджено в освітній процес із підготовки майбутніх фахівців за освітньо-професійною програмою Професійна освіта (Цифрові технології) освітню компоненту «Основи кібербезпеки» [1], метою викладання якої було формування у студентів системного розуміння фундаментальних принципів захисту інформації, сучасних кіберзагроз, методів та засобів забезпечення безпеки інформаційних систем, мереж і даних [1]. На нашу думку, актуальність і практична значущість цієї освітньої компоненти зумовлені зростанням рівня кіберзагроз і стрімким розвитком технологій кібератак, економічним розвитком і переходом до цифрових моделей захисту національної безпеки України, увідповідненням міжнародним стандартам захисту інформації.

Аналіз робочих програм і силабусів із цієї освітньої компоненти дав підстави для висновку, що на сьогодні недостатньо розробленими залишаються теоретичні засади викладання цієї навчальної дисципліни й формулювання методичних рекомендацій щодо пошуку оптимальних форм, методів і засобів навчання.

Вибір методичного інструментарію для опанування навчальної дисципліни «Основи кібербезпеки» передусім зумовлюється вимогами до рівня освітніх досягнень здобувачів вищої освіти, які передусім 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» зафіксовано, що здобувачі вищої освіти мають опанувати чотири змістові модулі: «Вступ до кібербезпеки», «Безпека каналів передачі та інфраструктури. Захист операційних систем і кінцевих точок», «Принципи та інструменти кібербезпеки», «Управління доступом, брандмауери, хмарна безпека» [1]. У навчальному плані на опанування цієї навчальної дисципліни передбачено лекційні (24 години) і практичні (24 години) заняття, а також самостійна робота студентів (72 години).

Якість засвоєних знань безпосередньо залежить від методичного інструментарію, який застосовує викладач. У попередній публікації ми вже акцентували на необхідності інтеграції до змісту

цієї освітньої компоненти глобальних навчальних ресурсів [7], зокрема матеріалів і сервісів міжнародної освітньої цифрової платформи Cisco Networking Academy [8]. Зокрема на базі зазначеної освітньої платформи є можливість пройти курси з Introduction to Cybersecurity (вступ до кібербезпеки) [10] та Cybersecurity Essentials (основи кібербезпеки) [11], які відповідають сучасним світовим стандартам у галузі кібербезпеки, передбачають 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. До переваг цієї платформи варто віднести гнучкість, мобільність і відновлюваність курсу (студент сам вирішує, коли краще проходити курс, а результати виконання зберігаються й можуть бути використані для моніторингу освітньої діяльності здобувачів).

У контексті формальної освіти, на нашу думку, ефективним буде звернення викладача освітньої компоненти «Основи кібербезпеки» до сучасних педагогічних технологій. У попередніх публікаціях нами було визначено, що використання педагогічних технологій в освітньому процесі закладів вищої освіти має низку переваг, зокрема: сприяє трансформації теоретичних положень у систему методичних рекомендацій і вказівок; створює передумови для аналізу й систематизації практичного досвіду і особливостей його використання в нових умовах; зумовлює необхідність розроблення відповідного змістового наповнення навчальної дисципліни, оптимальних методів контролю для досягнення мети; створює умови для економії часу й сил викладача, звільняє час для індивідуального й особистісного розвитку студентів; дає змогу продукувати гнучку структуру освітнього процесу, що вирізняється здатністю до корекції завдяки постійному зворотному зв'язку під час поетапного відтворення педагогічної технології [8].

З-поміж педагогічних технологій, які матимуть особливе значення для розвитку культури кібербезпеки в контексті формування інформаційно-цифрової грамотності здобувачів вищої освіти, на нашу думку, особливу ефективність матимуть такі: технологія проєктів (має безпосередній зв'язок із практикою, стимулює розвиток самостійності, відповідальності за роботу і результат, сприяє реалізації принципів індивідуалізації й диференціації навчання, а також студентоцентризу), технологія case-study (забезпечує реалізацію проблемно-ситуаційного навчання або здійснення якісного студентського наукового дослідження, передбачає детальний розгляд реальної чи змодельованої ситуації), технологія перевернеого навчання (дає змогу зосередитися на виконанні практичних завдань і розгляді конкретних ситуацій за умови самостійного попереднього опрацювання здобувачами теоретичного матеріалу з певної теми).

Висновки і перспективи подальших досліджень. Отже, культура кібербезпеки – це сукупність знань, переконань, навичок та моделей поведінки, спрямованих на захист інформації та протидію кіберзагрозам у цифровому просторі. У межах освітнього процесу в закладах вищої освіти культуру кібербезпеки доцільно розвивати в контексті формування інформаційно-цифрової грамотності здобувачів. Одним зі шляхів розвитку культури кібербезпеки вважаємо розроблення й упровадження в освітній процес освітньої компоненти «Основи кібербезпеки», яка сприятиме формуванню в студентів системи необхідних знань, а також дієвих практичних навичок щодо безпечного користування інформаційною сферою, що в сукупності сприятиме підвищенню рівня цифрової грамотності й обізнаності в системі кібербезпеки. Ефективному опануванню цієї навчальної дисципліни сприятиме впровадження до її змісту онлайнових курсів на платформі Cisco Networking Academy, а також застосування сучасних педагогічних технологій, як-от технологія проєктів, технологія case-study, технологія перевернеого навчання.

Перспективи подальших досліджень пов'язані з упровадженням освітньої компоненти «Основи кібербезпеки» до циклу загальної підготовки інших освітньо-професійних програм (наприклад, Середня освіта (Трудове навчання та технології), Професійна освіта (Транспорт), Професійна освіта (Аграрне виробництво, переробка сільськогосподарської продукції та харчові технології)), а також обгрунтування ефективного методичного інструментарію для розвитку культури кібербезпеки в контексті формуванні інформаційно-цифрової компетентності здобувачів вищої освіти.

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. Бивалькевич Л., Лілік О., Носовець Н. Формування базових компетентностей із кібербезпеки в здобувачів вищої освіти: організаційні й методичні аспекти. *Вісник Національного університету «Чернігівський колегіум» імені Т.Г. Шевченка.* 2025. Вип. 35 (191). С. 116-122.
   Byvalkevych, L.M., Lilik, O.O., Nosovets N.M. (2025). Formuvannia bazovykh kompetentnostei iz kiberbezpeky v zdobuvachiv vyshchoi osvity: orhanizatsiini y metodychni aspekty [Formation of basic cybersecurity competencies in higher education students: organizational and methodological aspects]. *Visnyk Natsionalnoho universytetu «Chernihivskyi kolehium» imeni T.H. Shevchenka – Bulletin of the T.H. Shevchenko National University «Chernihiv Colehium»,* 35 (191), 116-122. [in Ukrainian].

3. 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].

4. 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. 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].

5. 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].

6. 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].

7. 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].

8. Лілік О., Носовець Н., Бивалькевич Л. Технологічний концепт розвитку професійної компетентності майбутніх учителів. *Вісник Національного університету «Чернігівський колегіум» імені Т.Г. Шевченка*. 2023. Вип. 24 (180). С. 176-182.
Lilik, O.O., Nosovets, N.M., Byvalkevych, L.M. (2023). Tekhnolohichnyi kontsept rozvytku profesiinoi kompetentnosti maibutnikh uchyteliv [Technological concept of developing professional competence of future teachers]. *Visnyk Natsionalnoho universytetu «Chernihivskyi kolehium» imeni T.H. Shevchenka – Bulletin of the T.H. Shevchenko National University «Chernihiv Colehium»*. 24 (180), 176-182. [in Ukrainian].

9. 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].

10. 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].

11. 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].

12. Du W. Situation aware security system and method for mobile devices. URL: https://patentimages.storage.googleapis.com/08/43/ef/4a963d7fd74c11/US20120 309354A1.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].

13. 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].

14. 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].

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

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

DEVELOPMENT OF CYBERSECURITY CULTURE IN THE CONTEXT OF FORMING INFORMATION AND DIGITAL LITERACY IN HIGHER EDUCATION STUDENTS

The purpose of the article *is to characterize the features of the development of cybersecurity culture in the context of the formation of information and digital literacy in higher education students.*

Methodology*. In the process of determining the features of the development of cybersecurity culture in the context of the formation of information and digital literacy in higher education students, the following scientific research methods were applied: analysis of work programs on educational components related to cybersecurity and digital technologies, taking into account their content and requirements for the level of students' academic achievements; analysis of scientific literature on the research problem, which made it possible to formulate the theoretical foundations of the study; a method of observing the educational process in higher education institutions, on the basis of which contradictions in the development of a cybersecurity culture in the context of the formation of information and digital literacy of higher education students were identified; systematization and generalization for the formulation of conclusions.*

The study involved taking into account individual provisions of several methodological approaches, namely: competency-based (taking into account general and professional competencies, program learning outcomes recorded in the relevant educational and professional programs); axiological (forming higher education students of the idea of netiquette as a special form of etiquette, as well as targeted influence on the value and worldview sphere of students); activity-based (involving higher education students in performing tasks aimed at the formation of information and digital competence); personally oriented (taking into account personal traits and individual experience of higher education students in the process of formulating educational tasks).

The scientific novelty. *The authors of this article examine the features of the development of cybersecurity culture in the context of the formation of information and digital literacy in higher education students.*

Conclusions*. It is substantiated that cybersecurity culture is a set of knowledge, beliefs, skills and behavioral models aimed at protecting information and countering cyber threats in the digital space. It is stated that within the educational process in higher education institutions, cybersecurity culture should be developed in the context of the formation of information and digital literacy of students. It is found that one of the ways to develop cybersecurity culture is to develop and implement the educational component «Fundamentals of Cybersecurity» in the educational process, which will contribute to the formation of a system of necessary knowledge in students, as well as effective practical skills for the safe use of the information sphere, which in turn will contribute to increasing the level of digital literacy and awareness in the cybersecurity system. It has been proven 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, as well as the use of modern pedagogical technologies, such as project technology, case-study technology, and flipped learning technology.*

Key words: *cybersecurity culture, information and digital literacy, higher education students, digital technologies, higher education institution, educational component.*

Стаття надійшла до редакції: 01.04.2026

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