Розділ IV. Кіберзахист у цифровому освітньому середовищі: зовнішні та внутрішні ризики

Буров О.Ю., Литвинова С.Г., Пінчук О.П.

Як зазначено в матеріалах Всесвітнього економічного форуму в Давосі (2024), «Оскільки технологічні зміни прискорюються, існує нагальна потреба в підтримці систем освіти в управлінні новими можливостями та ризиками. Якщо ними правильно керувати, технології, зокрема штучний інтелект (ШІ), пропонують унікальну можливість допомогти освітнім системам увімкнути освіту 4.0 – підхід до викладання та навчання, який зосереджується на наданні учням здібностей, навичок, ставлень і цінностей, які відповідають майбутньому. Розроблена глобальною коаліцією освітніх експертів, практиків, політиків і бізнес-лідерів, Освіта 4.0 служить комплексною структурою, яка окреслює ключові перетворення, необхідні в початковій і середній освіті для сприяння кращим освітнім результатам» [1, с. 3]. Водночас, це супроводжується небажанням як системи освіти, так і держави в цілому захищати суб'єктів від інформаційних, психологічних та когнітивних інтервенцій, які можуть вплинути на становлення особистості за таких обставин як на змістовному, так і на особистісному рівнях, не зважаючи на те, що «у 2023 році світ зіткнувся з поляризованим геополітичним порядком, численними збройними конфліктами, скептицизмом і запалом щодо наслідків майбутніх технологій і глобальною економічною невизначеністю. У цьому складному ландшафті економіка кібербезпеки зростала в геометричній прогресії швидше, ніж глобальна економіка в цілому, і випереджала зростання в технологічному секторі» [2, с.4]. Нові виклики часу та нові напрями розвитку суспільства – Суспільство 4.0, Освіта 4.0, проникнення новітніх технологій у всі сфери життя, «гібридна» війна – вимагають розуміння ключових проблем, викликів та питань, пов'язаних з безпеки освітнього процесу в цифровому навчальному

середовищі (ЦНС), зокрема безпеки всіх безпосередніх учасників, організаторів освіти, держави, а також безпеки цифрового освітнього контенту [3], розширення когнітивної війни, основною метою якої є зміна та спотворення когнітивної моделі життя, особливо молоді [4]. Відповідно, існує нагальна потреба захистити когнітивну, ідеологічну, інтелектуальну та розвивальну діяльність освіти та людського капіталу, оскільки людина все ще залишається найслабшою ланкою в Системі [5].

Беручи до уваги ще і досвід пандемії, з'являються нові проблеми, викликані життям і діяльністю, з боку безпеки, пов'язаних з цим факторами та способами їх уникнення, а також нові інструменти та механізми. Таким чином, потребує вирішення проблема розвитку та впровадження інформаційно-комунікаційних технологій (ІКТ) в освіту [6]. Однак слід мати на увазі, що нові інформаційні технології призводять до фундаментальних і глобальних процесів, які трансформують суспільний розвиток. Проте, окрім позитивного впливу, який вони мають, нові фактори та умови, природно, породжують серйозні проблеми, загрози та ризики [7]. Як зазначається ще раніше в матеріалах Всесвітнього економічного форуму в Давосі (2020 рр.) та Організації Об'єднаних Націй [8], проблема кібербезпеки (КБ), яка торкається практично всіх сфер життя і діяльності людини, є особливо гострою через багато причин, але насамперед у контексті повної інформатизації освіти [9]. Це означає, що людина стає найважливішою одиницею життєво важливої інфраструктури держави, але доцільно розглядати питання не кібербезпеки (Системи), а кіберзахисту (людини як елемента Системи).

*Мета дослідження: р*озробити концепцію та методику системи кібербезпеки учасників освітнього процесу в цифровому навчальному середовищі (інтеграція людського та кіберфізичного системного підходу).

Розглядаючи навчання як вид діяльності в інтеграції людина-система [10], сучасного учня можна розглядати як оператора-дослідника, який діє в цифровому навчальному середовищі. Успішне навчання передбачає взаємну адаптацію між людиною як учасником освітнього процесу (УОП) та

інструментами діяльності з використанням індивідуальних когнітивних здібностей у мережах, у тому числі соціальних [11] та в мінливому цифровому середовищі загалом [12]. З іншого боку, можливе використання методів і прийомів ергономіки для оцінки безпеки учня в навчальному процесі [13]. Питання кібербезпеки стали наріжним каменем після того, як комп'ютерні технології перестали бути прерогативою великих наукових центрів. Поява та поширення локальних і глобальних мереж змінило сприйняття та розуміння кібербезпеки, відповідних тенденцій, проблем і викликів, оскільки виникли нові риси навчального середовища.

Мережі як активні агенти освітнього процесу. З часом цифрові мережі стають центром нашого життя, а соціальні мережі перетворюються на нове соціальне середовище. Ці мережі мають не тільки позитивний вплив, але й становлять реальну загрозу освіті та безпеці держави. Компоненти мережі у спрощеному вигляді можна представити у вигляді вузла, інтерфейсу, з'єднання та мережі [3]. Вузли — це «агенти» мережі: *люди* (творці ресурсу та його контенту, адміністратори ресурсу, звичайні чи випадкові користувачі), *техніка* (термінальні станції, комп'ютери, гаджети тощо) та *інформаційні засоби* (бази даних, бази знань, системи керування тощо). Залежно від своєї сутності, агенти мають власний інтерфейс і канали зв'язку для взаємодії з іншими агентами, які можуть стати мішенню для кібератаки. Мережа набуває ознак самостійного фактору, що впливає на її властивості, функціонування та користувачів, а також систему в цілому. ЦНС — це тріадний кіберпростір: (1) *інформація* в її цифровому представленні: статична (файли, записані на носії) та динамічна (пакети, потоки, команди тощо); (2) *технічна інфраструктура* (ІКТ, програмне забезпечення, бази даних тощо); (3) *інформаційна взаємодія* між суб'єктами («агентами») через передану інформацію (1) та обробку (2).

Загрози учасникам освітнього процесу, породжені кіберпростором. З огляду на те, що сучасні студенти народилися в епоху цифрових технологій, можна стверджувати, що кіберпростір є і залишатиметься надзвичайно важливою частиною поля битви ідеології та цивілізації. Спектр загроз з боку

відкритого кіберпростору постійно розширюється. Якщо десять років тому загрози для школярів можна було звести до відносно невеликої кількості груп (вірусні атаки, кіберзлочинність, небезпека інтернет-серфінгу) [14], то сьогодні різноманітність небезпек і загроз значно зросла і продовжує зростати, що впливає на всі можливі дії людини в Інтернеті [15]. На часі експерти виділяють такі 7 аспектів культури кібербезпеки (КБ), що потребують урахування під час проєктування та використання ІКТ (Рис.1):

Ставлення до КБ – почуття та переконання співробітників щодо безпеки, протоколи та питання. *Поведінка* – дії та діяльність людини, яка мають прямий або опосередкований вплив на безпеку організації/закладу. *Пізнання* – розуміння, знання та обізнаність щодо питань безпеки та діяльності. *Спілкування* – якість каналів зв'язку для обговорення тем, пов'язаних із безпекою, сприяння почуттю причетності та надавати підтримку з питань безпеки та звітування про інциденти. *Відповідність* – знання письмової політики безпеки та те, наскільки працівники її дотримуються. *Норми* – знання та дотримання неписаних правил поведінки в організації. *Відповідальність* – як працівники сприймають свою роль як критичний фактор у підтримці або загрозі безпеці організації.

Рис. 1. Аспекти культури безпеки.

Культура безпеки розуміється різною мірою в її галузях та різних країнах Європи. Як концепція, вона все частіше приймається та часто обговорюється серед фахівців із безпеки, особливо в секторах із традиційно високим рівнем цифровізації, таких як фінанси, банківська справа та IT. В інших галузях культура безпеки часто розглядається пізніше в циклі зрілості кібербезпеки — планується звернути увагу лише після початкового етапу усвідомлення безпеки. Однак в освіті когнітивні здібності та особливості УОП майже не обговорювалися, оскільки більшість досліджень, як правило, зосереджені на організаційних питаннях кібербезпеки. У той же час виявлено, що найбільшу загрозу для студентів становлять приховані активні загрози, які з позиції ергономіки можна оцінити як ієрархічний набір показників: інтегрований (комплексний); три групи індикаторів – рівень небезпеки, викликаної вірусними атаками, кіберзлочинністю та інтернет-серфінгом; набір окремих індикаторів, що містять набір певних загроз [3].

Сфери кібербезпеки. Освіта не визнається критичною сферою. Проте сучасні студенти можуть працювати в подібних сферах у найкоротші терміни переважно завдяки впровадженню нових освітніх технологій [16] загалом, у тому числі розподілених [17] та адаптивних [18], а також доповненого та віртуального середовища [19]. Тому вони потребують захисту та відповідного навчання. Крім того, недостатньо розкритим питанням у цій сфері є процедури визначення спільних можливих цільових груп кібербезпеки (наприклад, учні/студенти, вчителі, діти/молодь, менеджери освіти, загальне населення країни). Залежно від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати на п’ять груп: правові, технічні, інформаційні, організаційні та психологічні [3]. Моделювання впливу кіберзагроз може бути ефективним, якщо забезпечує об’єктивне вимірювання реакції індивідів на цей вплив, тобто психофізіологічну реакцію. Ми почали це дослідження з метою моделювання впливу різноманітних факторів (інформаційних, соціальних,

психологічних, когнітивних тощо) на людину з оцінкою її стану до та після їх дії. Кінцевою практичною метою дослідження є розробка методології оцінки факторів впливу та ризикометрії з урахуванням індивідуальних та групових особливостей потенційних об'єктів насильницької дії.

Результати та обговорення

Положення цього дослідження ґрунтуються на результатах участі одного з авторів у Експертній групі НАТО HFM-259 «Human Systems Integration Approach to Cyber Security» [20], попередніх експериментальних дослідженнях, спрямованих на аналіз когнітивної роботи людини в цифровому просторі під час впливу внутрішніх і зовнішніх факторів, у тому числі різних видів навантаження [21]. Ці результати повністю відповідають сучасним тенденціям кібербезпеки, викликаним пандемією. Результати показали стрімке зростання поширення зловмисного програмного забезпечення, програм-вимагачів, що супроводжується появою програм-вимагачів як послуги, полювання на загрози як відповідь на активізацію зловмисної активності в мережах, виявлення мережі та реагування. Було доведено, що зловмисники постійно вдосконалюють свої здібності щодо обману людей, що є найбільшою загрозою для у 2024 році та викликає нові тенденції в цій проблемі. За даними Forbes, у 2024 р. очікується, що вартість кіберзлочинів досягне $10.5 трл., а головними трендами вивчення у цій сфері є такі [22]:

- Критика навичок кібербезпеки.
- Генеративний ШІ, що використовується з обох сторін битви навколо КБ.
- Фішингові атаки нового рівня.
- Кібербезпека в залі засідань.
- Кібератаки IoT.
- Кіберстійкість – за межами кібербезпеки.
- Нульова довіра.
- Кібервійна та фінансовані державою кібератаки.

- Навички програмного забезпечення стають усе більш важливими для фахівців з кібербезпеки.
- Регламент кібербезпеки.

До цього можна ще додати:

o Злам акаунтів користувачів соціальних мереж із наступним використанням персональних і банківських даних.

o Загрози з Dark Web.

o Зловмисне програмне забезпечення як послуга та наймані хакери: використання служб і хакерів у зловмисних цілях.

В освіті фокус має бути зміщений з персональних даних на стан УОП та його/її здатність протистояти атаці (у т.ч. відновлюватися після неї), тобто мають бути розроблені не тільки і не стільки засоби кібербезпеки (в традиційному розумінні), скільки засоби кібер-захисту УОП (КЗ). Відповідні навички повинні включати знання кібербезпеки, навчання та кібер-гігієну. Перевірка результатів базується на:

- використанні метрик для вимірювання успіху програм навчання та визначення ймовірного успіху;
- показниках, які включають як короткострокові, так і довгострокові цілі, оскільки вони допомагають виміряти, як рівень безпеки учасників покращується з часом.

Поряд з оцінкою суб'єктивної реакції особи, що зазнала кібер-впливу, дослідження оцінює її психологічні та фізіологічні зміни, у тому числі викликані прихованою дією на свідомість. Для досягнення поставленої мети планується вивчити пул добровольців та зміни їх електрокардіограми та електроенцефалограми внаслідок симуляції впливу як традиційних гаджетів (звичайних пристроїв для входу в кіберпростір), так і окремих пристроїв доповненої/віртуальної реальності. Експериментальні дослідження передбачають як онлайн, так і домашні спостереження за допомогою записів електрофізіологічних параметрів, а також окулярів і планшетів віртуальної

реальності. Проект вимагає залучення експертів у різних галузях, які мають великий досвід у проведенні експериментальних досліджень з використанням мережевих технологій, аналізі даних, а також розробці нових науково-методичних інструментів.

Нам вдалося досягти наступного. По-перше, ми розробили прототип (програмне забезпечення для онлайн-тестування) системи кібербезпеки УОП у ЦНС. По-друге, ми переглянули методи оцінки впливу кібернебезпек на УОП та їх показники ризику на основі показників психологічних і фізіологічних змін, спричинених кібер-небезпеками. Потім ми розробили рекомендації щодо кібербезпеки УОП з урахуванням людського чинника в ЦНС та індивідуальних/групових особливостей психологічної/психофізіологічної реакції старшокласників на вплив кібер-небезпеки. Нарешті, особливий інтерес становлять наші пропозиції щодо структури та обсягу навчальних матеріалів, спрямованих на формування загальної культури кібербезпеки в ЦНС як складової системи кібербезпеки УОП.

Наше дослідження має низку ефективних і цінних застосувань в освітньому середовищі (Рис.2).

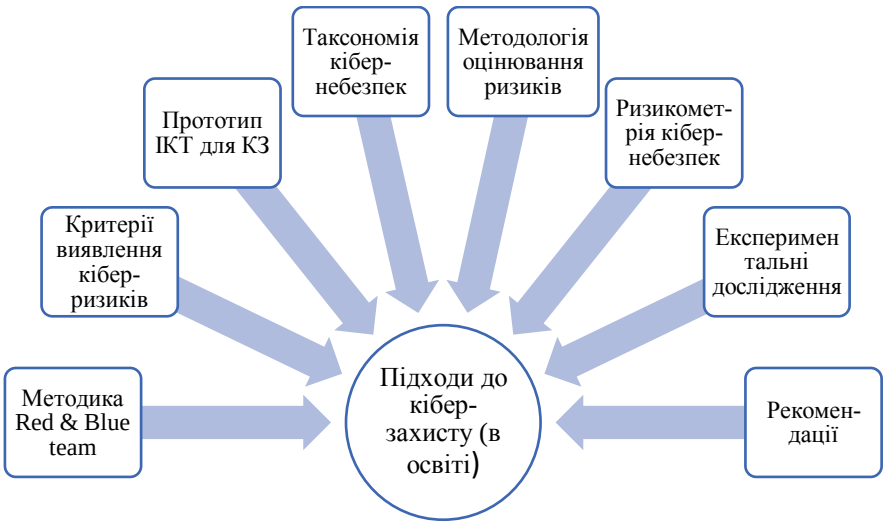

Рис.2 Шляхи кібер-захисту в освіті

Наведена на Рис.2 модель є розвитком ідей та моделі, опублікованих у [23]. Це дослідження є першим кроком до покращення нашого розуміння кіберзахисту в ЦНС.

Ми плануємо продовжити наші дослідження:

- Забезпечити методичну підтримку для врахування та пом'якшення впливу небезпечних факторів на УОП у цифровому навчальному середовищі.
- Розробити рекомендації щодо кібер-захисту для УОП у цифровому навчальному середовищі з урахуванням факторів, пов'язаних з людиною.
- Дослідити психолінгвістичні аспекти гуманітарної складової кібер-захисту [24].

Список використаних джерел

1. Shaping the Future of Learning: The Role of AI in Education 4.0, April 2024. *World Economic Forum*. 2024. URL: https://www.weforum.org/publications/shaping-the-future-of-learning-the-role-of-ai-in-education-4-0/.
2. Jurgens J., Dal Cin P. Global Cybersecurity Outlook 2024, January 2024. *World Economic Forum*. 2024. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.
3. Bykov V. Y., Burov O. Y., Dementievska N. P. Cybersecurity in digital educational environment. *Inf. Technol. Learn. Tools*. 2019. 70(2). P.313-331.
4. Pocheptsov G. The War in Cognitive Space. 2017 URL: https://nesterdennez.blogspot.com/2017/08/global-permanent-war_39.html.
5. Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? / Z. Yan et al. *Computers in Human Behavior*. 2018. Vol. 84. P. 375-382.
6. Li C., Lalani F. The COVID-19 pandemic has changed education forever. This is how. 2020. URL: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/.
7. Schools of the Future: Defining New Models of Education for the Fourth Industrial Revolution. *World Economic Forum*. 2020. URL: http://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf.
8. Pipikaite A., Davis N. Why cybersecurity matters more than ever during the coronavirus pandemic. *World Economic Forum*. 2020. URL: https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity .
9. Guterres António. The future of education is here. Launch of the policy brief: education during COVID-19 and beyond. *United Nations*. August 04, 2020. URL: https://www.un.org/en/coronavirus/future-education-here.

10. Pinchuk O., Burov O., Lytvynova S. Learning as a Systemic Activity. *Advances in Human Factors in Training, Education, and Learning Sciences. AHFE 2019. Advances in Intelligent Systems and Computing* / Karwowski W., Ahram T., Nazir S. (eds). Springer: Cham. 2019. Vol 963. P. 335-342. DOI : https://doi.org/10.1007/978-3-030-20135-7_33.
11. Lytvynova S., Burov O. Methods, Forms and Safety of Learning in Corporate Social Networks. *ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*: Proceedings of the 13th Int. Conf. on ICT in Education, Research and Industrial Applications. (Kyiv, Ukraine, 2017, May 15-18). 406—413. URL: http://ceur-ws.org/Vol-1844/10000406.pdf.
12. Digital transformation of learning environment: aspect of cognitive activity of students. *Proceedings of the 6th Workshop on Cloud Technologies in Education (CTE 2018)* / Pinchuk O.P. et al. (Kryvyi Rih, Ukraine, December 21, 2018). CEUR Workshop Proceedings, # 2433, 90-101.
13. Advances in Human Factors in Cybersecurity. *Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity* / Ahram T., Karwowski W. (eds.). July 24-28, 2019, Washington D.C., USA.
14. Bandara I., Ioras F., Maher K. Cyber Security Concerns in E-Learning Education. *Proceedings of ICERI2014 Conference, IATED*. 2014, 0728-0734.
15. KnowBe4 Security Culture Regional Guide 2024. *KnowBe4*. URL: https://www.knowbe4.com/hubfs/2024-Security-Culture-Report-Research_EN-US.pdf?hsCtaTracking=7beca419-e8e2-4ff2-bb53-ba5e45019345%7C4a8c297a-e4c2-4d65-b8eb-62e976423eb7.
16. Greenberg A. Emerging Threats: Cybersecurity Forecast 2025. *Threat Intelligence*. November 2024. URL: https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025.
17. Ergonomics of cyberspace. Mathematical modeling to create groups of operators for error-free and timely implementation of functions in a distributed control system / Lavrov E. et al. *CEUR Workshop Proceedings*. 2020. V. 2740. P. 380-385.
18. AL: An Adaptive Learning Support System for Argumentation Skills. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu HI USA: ACM* / Wambsganss Thiemo et al. 2021. P. 1–14. DOI:10.1145/3313831.3376732. ISBN 978-1-4503-6708-0. S2CID 218482749.
19. Application of augmented reality technologies for preparation of specialists of new technological era. *Application of augmented reality technologies for preparation of specialists of new technological era, Augmented Reality in Education: Proceedings of the 2nd International Workshop (AREdu 2019)*, Kryvyi Rih, Ukraine, March 22 / Iatsyshyn A. V. et al. 2020. P. 181-200. URL: http://ceur-ws.org/Vol-2547/paper14.pdf.
20. Human Systems Integration Approach to Cyber Security. STO-TR-HFM-259. STO/NATO 2020. June 2020. 112 pp.
21. Burov O., Tsarik O. Educational workload and its psychophysiological impact on student organism. *Work*. 2012. V. 41, Supplement 1. P. 896-899.

22. Marr B. The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now. *Forbes*. 2024. URL: https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/.
23. Cyber Safety in the Digital Educational Environment: External and Internal Risks. Advances in Intelligent Systems and Computing / Burov O. et al. / D. Russo et al. (Eds.): IHSI 2021, AISC 1322. 2021. P. 364–370. DOI: https://doi.org/10.1007/978-3-030-68017-6_54.
24. Krylova-Grek Yu., Burov O. A content analysis software system for efficient monitoring and detection of hate speech in online media. *CTE 2023*: *11th Workshop on Cloud Technologies in Education, December 22, 2023, Kryvyi Rih, Ukraine*. CEUR-WS.org. Vol-3679. Paper.06.pdf.