DOI 10.18372/2786-5487.1.18755
УДК 37.09

Радомський Ігор Петрович
кандидат педагогічних наук, доцент,
Інститут педагогічної освіти і освіти дорослих
імені Івана Зязюна НАПН України,
м. Київ, Україна
radomski@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У ЗМІШАНОМУ НАВЧАННІ В УМОВАХ ВІЙНИ

Анотація. *Створення безпечного освітнього середовища, формування інформаційно-цифрової компетентності учасників освітнього процесу, збереження їх персональних даних, дотримання правил захищеного користування інтернет-ресурсами є важливими показниками якості освіти. Виділено інформацію, якою оперують заклади освіти в Україні та яка потребує захисту, групи об'єктів, на які може здійснюватися навмисний або ненавмисний вплив. Окреслено шляхи, а також перелік різноманітних інструментів та заходів, використання яких сприятиме забезпеченню інформаційної безпеки здобувачів освіти у цифровому освітньому просторі закладів освіти.*

Ключові слова: *інформаційна безпека, змішане навчання, цифровий освітній простір закладу освіти.*

Annotation. *Creating a safe educational environment, developing the information and digital competence of participants in the educational process, preserving their personal data, and complying with the rules for the secure use of Internet resources are important indicators of the quality of education. The author identifies the information operated by educational institutions in Ukraine that needs to be protected and the groups of objects that may be subject to intentional or*

unintentional influence. The author outlines the ways and a list of various tools and measures that will help ensure the information security of students in the digital educational space of educational institutions.

Key words: *information security, blended learning, digital educational space of an educational institution.*

Постановка проблеми, її актуальність. Пандемія COVID-19 а потім безпрецедентний напад росії на Україну 24 лютого 2022 року спричинили кардинальні зміни в освітній сфері держави, перевівши навчання у змішаний та он-лайн формат.

Зрозуміло, що прискорене переміщення навчання в Інтернет не супроводжувалося належною підтримкою [1].

Це, в свою чергу, порушило питання конфіденційності інформації учасників освітнього процесу та проблем інформаційної безпеки в освітньому онлайн-середовищі. Активне використання Інтернету у змішаному навчанні породжує питання інформаційної безпеки.

Отже, зростає і ступінь зацікавленості у підвищенні рівня безпеки та конфіденційності усіх учасників освітнього процесу через загрози, які виникають повсякчас, а саме: дезінформація, маніпуляція, фейкові новини, вірусні атаки, шахрайство, пропаганда терористичної та екстремістської діяльності тощо.

З початком війни Україна стала ціллю чисельних кібератак, які охопили як державні установи, організації, так і звичайних громадян. Наразі створення безпечного освітнього середовища, збереження персональних даних учасників освітнього процесу, формування інформаційно-цифрової компетентності, дотримання правил захищеного користування інтернет-ресурсами в кіберпросторі є важливими показниками якості освіти [2, с. 22].

Для забезпечення функціонування освітніх закладів та нормальної життєдіяльності усіх учасників освітнього процесу система інформаційної безпеки повинна мінімізувати ризики пошкодження баз даних, викрадення

масивів конфіденційних відомостей, а також гарантувати неможливість проникнення в навчальні приміщення пропаганди, яка негативно впливає на свідомість учасників освітнього процесу [3, с. 390 - 391].

Аналіз останніх досліджень і публікацій. Проблематику інформаційної безпеки активно досліджують українські та закордонні науковці: І. Арістова, А. Гальчинський, П. Друкер, Я. Жаліло, О. Зощенко, М. Роуз, Е. Тофлер, Ф. Фукуяма та інші. Так, проблематику розробки стратегії інформаційної безпеки у закладах освіти України досліджують О. Чубукова та І. Пономаренко [3]. Дослідники А. Резгі та А. Маркс розглянули основні фактори формування інформаційної безпеки, дослідили головні напрямки інформаційної обізнаності та цифрової компетентності [4]. А. Шарма розглянув ключові аспекти забезпечення кібербезпеки сучасних закладів освіти [5]. Незважаючи на проведені наукові розвідки залишається актуальною потреба подальших досліджень шляхів забезпечення інформаційної безпеки учасників освітнього процесу в цифровому освітньому просторі закладів освіти.

Мета статті. Враховуючи що проблематика інформаційної безпеки учасників освітнього процесу у цифровому освітньому просторі є досить складною та вимагає комплексного підходу до її розв’язання, мета нашого дослідження полягає у визначенні основних проблем заначеного напрямку та шляхів забезпечення інформаційної безпеки учасників освітнього процесу в цифровому освітньому просторі закладу освіти.

Виклад основного матеріалу. Науковці зазначають, що інформаційна безпека закладу освіти представляє собою складну систему, яка передбачає захист наявного в організації інформаційного простору та унеможливлює пошкодження або викрадення персональних даних усіх учасників освітнього процесу, а також інформації, що дозволяє установі функціонувати та має грошову, освітню, інтелектуальну цінність тощо. Забезпечення ефективного функціонування системи безпеки передбачає витрати певних грошових ресурсів у рамках розробленої стратегії захисту даних. При розробці стратегії доцільно врахувати фактори зовнішнього та внутрішнього середовища,

оскільки досягнення оптимального результату можливе лише за умови знаходження рівноваги між наявними можливостями та бажаними результатами [3, с. 391]. Таким чином, забезпечення інформаційної безпеки пов’язане з роботою всіх структурних підрозділів закладу освіти.

Серед *інформації, якою оперують заклади освіти в Україні та яка потребує захисту* можна виокремити*:*

- Персональні дані учасників освітнього процесу. В Україні 1 червня 2010 року було прийнято Закон України «Про захист персональних даних» [6], що передбачає комплекс заходів захисту приватної інформації та встановлює відповідальність за її неправомірне розповсюдження.

- Інформація, що забезпечує освітній процес в закладі освіти (інформаційні бази бібліотеки, бази різноманітних даних, освітні програми тощо). Захист зазначеної інформації спрямований на недопущення її часткового або повного пошкодження, що може порушити стабільне функціонування закладу освіти. Інформація, що забезпечує освітній процес може містити елементи інтелектуальної власності. Обмеження доступу до фінансової інформації здійснюється з метою недопущення махінацій.

- Наукові напрацювання з ознаками інтелектуальної власності та захищені законодавством. Отримані в процесі наукових досліджень результати, а також згенеровані в процесі дані, потребують захисту як продукти інтелектуальної власності. Особливу увагу потрібно приділяти обмеженню доступу до інформації, що генерується на етапі апробації та не отримала вигляд комплексного наукового продукту, який опублікований або запатентований відповідними науковцями [7].

Виділяються групи об'єктів, на які може здійснюватися навмисний або ненавмисний вплив в закладі освіти:

- комп'ютерна техніка та інші апаратні засоби, які можуть бути пошкоджені в результаті механічної дії, інтеграції шкідливого програмного забезпечення тощо;

- спеціалізоване програмне забезпечення, яке використовується для функціонування закладу освіти або безпосередньо застосовується в освітньому процесі та може повністю або частково втрати функціональність внаслідок хакерських атак, активації вірусів або інших шкідливих дій;

- інформація закладів освіти, яка зберігається на різних носіях та використовується для забезпечення функціонування зазначених установ;

- здобувачі освіти, які відносяться до групи ризику внаслідок їх вразливості до негативного інформаційного впливу, що може завдати шкоди їм безпосередньо або призвести до агресивної поведінки по відношенню до оточуючих або закладу освіти [8];

- персонал закладу освіти, який під впливом зовнішніх факторів або за власними мотивами може негативно вплинути на інформаційну безпеку закладу освіти, частково або повністю знищивши інформацію, використавши її в особистих інтересах або передавши дані третім особам.

До проблем інформаційної безпеки можна віднести такі фактори як:

- використання застарілих і свідомо небезпечних платформ; встановлення піратського програмного забезпечення;

- низька кваліфікація обслуговуючого персоналу (або взагалі відсутність фахівця з підтримки інформаційних систем);

- відсутність практики регулярного контролю безпеки.

Як зазначає освітній омбудсмен України [9], в Україні поки що відсутня чітко визначена нормативна база, яка б регулювала безпеку роботи учасників освітнього процесу в Інтернеті під час змішаного та дистанційного навчання, у тому числі, – безпеку роботи з персональними даними. Але ніщо не заважає використовувати на практиці ті норми законодавства, які ми вже маємо. У листі МОН № 1/9-609 від 02.11.2020 року «Щодо організації дистанційного навчання» наголошується, що всі учасники освітнього процесу мають дотримуватися вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі, а основним законом із питання захисту персональних даних в Україні є Закон України «Про захист

персональних даних» [6], і саме його потрібно брати за основу для роботи з персональними даними та їхнього захисту.

Сучасні технології кібербезпеки освітнього процесу передбачають забезпечення захисту на 5-ти рівнях, як-от: нормативно-правовий; морально-етичний; адміністративно-організаційний; фізичний і технічний [3, с. 393 - 394].

Нормативно-правовий. Комплексна організація протидії незаконним заволодінням даними або їх знищенням базується на чинній нормативно-правовій базі України [6; 10].

Морально-етичний. Однією з ключових функцій освітньої системи є формування в здобувачів освіти системи моральних цінностей, які є позитивними орієнтирами у суспільстві. Формування у здобувачів освіти системи цінностей зменшує ймовірність скоєння правопорушень даною категорією населення, в тому числі на території закладів освіти [11].

Адміністративно-організаційний. Передбачає розробку внутрішніх інструкцій, які регламентують особливості використання комп'ютерного обладнання, специфіку роботи з інформацією та її носіями. Крім того, необхідно сформувати правила доступу здобувачів освіти до мережі Інтернет в комп'ютерних класах, порядок блокування небезпечного для даної категорії населення контенту, заборона на користування власними носіями інформації.

Фізичний. У межах даного напряму передбачається формування пропускної системи згідно з рівнем доступу до приміщень, в яких розміщуються носії інформації закладу освіти. В приміщення допускаються лише авторизовані користувачі, а використання ними інформації здійснюється суворо в межах їх прав доступу до даних.

Встановлені паролі повинні регулярно змінюватись з метою мінімізації ризиків заволодіння інформацією третіми особами або її знищення. До заходів фізичного захисту може бути віднесено обов'язкове копіювання важливої інформації на диски комп'ютерів, які не мають доступу до мережі Інтернет [12].

Технічний. Для забезпечення якісного захисту інформації в закладах освіти необхідно використовувати спеціалізоване програмне забезпечення, яке дає

можливість виявляти потенційні загрози та реалізовувати заходи боротьби з ними. В умовах недостатнього рівня фінансування заходів, які орієнтовані на забезпечення інформаційної безпеки освітніх закладів, більшість установ використовує лише антивіруси та безкоштовні програмні продукти у сфері боротьби з незаконним порушенням інформаційних систем. Передбачається встановлення фільтрів, які обмежують доступ здобувачів освіти до певних ресурсів в мережі Інтернет. Потрібно встановити контроль за доступом учасників освітнього процесу до електронної пошти. Також необхідно запровадити заборону на копіювання певних видів інформації з комп'ютерів освітнього закладу.

Цікавими є наукові доробки О. Нич та О. Соя в яких дослідники виокремили функціональну модель процесу забезпечення інформаційної безпеки учнів у цифровому освітньому просторі закладів загальної середньої освіти. Зазначена модель може бути адаптована і для використання у закладі вищої освіти. Вона включає наступні етапи:

1. Аналіз потенційних загроз та ризиків у цифровому освітньому просторі – проводиться оцінка потенційних загроз та ризиків, що можуть виникнути у цифровому освітньому просторі, таких як віруси, шкідливі програми, хакерські атаки, крадіжка даних тощо.

2. Розробка стратегії забезпечення інформаційної безпеки – визначаються основні напрямки заходів забезпечення інформаційної безпеки, такі як встановлення антивірусного програмного забезпечення, захист мережевого трафіку, шифрування даних тощо.

3. Впровадження заходів забезпечення інформаційної безпеки – здійснюється впровадження заходів забезпечення інформаційної безпеки, які були розроблені на попередньому етапі.

4. Моніторинг та аналіз ефективності заходів забезпечення інформаційної безпеки – відбувається моніторинг та аналіз ефективності заходів забезпечення інформаційної безпеки, щоб виявити можливі проблеми та недолік та вжити необхідні заходи для їх усунення.

5. Навчання учнів про безпеку в цифровому просторі – організовуються освітні заходи для учнів про безпеку в цифровому просторі, які містять роз'яснення основних правил безпеки, використання безпечних паролів, захист від шкідливих програм тощо.

6. Обмін досвідом та знаннями між різними освітніми установами – здійснюється налагодження комунікації між освітніми установами з метою визначення та апробації якнайкращих практик та підходів до забезпечення інформаційної безпеки учасників освітнього процесу [13, с. 110].

Ці поетапні заходи дозволяють забезпечити надійний захист здобувачів освіти від можливих мережевих загроз та ризиків; підсилити безпеку їхніх особистих даних та інформації, що зберігається на комп'ютерах та мобільних пристроях; сприяють підвищенню рівня їхньої культури безпечної поведінки у цифровому освітньому просторі.

Інформаційну безпеку учасників освітнього процесу допоможе також забезпечити використання різноманітних інструментів та заходів, зокрема:

- захист мережі та комп'ютерів від зловмисних програм та вірусів;
- захист особистих даних учнів та їхньої інформації від несанкціонованого доступу;
- використання безпечних паролів та авторизація доступу до ресурсів;
- навчання здобувачів освіти з питань безпеки в Інтернеті та цифровому просторі;
- контроль за використанням учнями комп'ютерів та мобільних пристроїв;
- створення політики безпеки та її виконання;
- розробка плану дій у разі кібератаки або порушення безпеки даних;
- постійне оновлення програмного та апаратного забезпечення;
- використання захисту від DDoS-атак та інших шкідливих дій;
- проведення аудиту безпеки та виявлення потенційних загроз [13, с. 110].

Висновки. Отже, у сучасному світі цифрові технології пронизують усі сфери життя, не є винятком і освітній простір. Це створює нові можливості для

організації змішаного та дистанційного навчання, але також приносить загрози їхній інформаційній безпеці.

Тому проблематика інформаційної безпеки учасників освітнього процесу у цифровому освітньому просторі є досить складною та вимагає комплексного підходу до її розв'язання. Подальші дослідження цього напрямку дозволять оперативно визначати проблеми та шляхи їх вирішення, удосконалювати рекомендації щодо забезпечення інформаційної безпеки учасників освітнього процесу в цифровому освітньому просторі закладу освіти при запровадженні змішаного навчання.

Матеріали підготовлено у межах виконання проєкту (2022.01/0098) «Максимізація ефективності ресурсів змішаного навчання в закладі вищої педагогічної освіти у воєнний час і повоєнного відновлення України» за грантової підтримки Національного фонду досліджень України.

Список використаних джерел

1. Walsh, L. L., Arango-Caro, S., Wester, E. R., & Callis-Duehl, K. (2021). Training faculty as an institutional response to COVID-19 emergency remote teaching supported by data. *CBE–Life Sciences Education*, *20* (3), ar. 34. URL: https://doi.org/10.1187/cbe.20-12-0277 (дата звернення: 29.02.2024).

2. Черних О. Кібербезпека учасників освітнього процесу в умовах воєнного стану. *Інформаційний, науково-методичний журнал «Освіта Сумщини».* 2023. № 1 (57). С. 22-24.

3. Чубукова О. Ю. Інформаційна безпека у навчальних закладах України. *Вісник Київського національного університету технологій та дизайну. Серія Економічні науки. Спецвипуск : Ефективність організаційно-економічного механізму інноваційного розвитку вищої освіти України*: матеріали VIII Міжнародної науково-практичної конференції, 5 жовтня 2018 р., м. Київ. С. 388-395. URL: https://er.knutd.edu.ua/handle/123456789/10312 (дата звернення: 29.02.2024).

4. Rezgui Y., Marks A. Information security awareness in higher education: An exploratory study. *Computers & Security*. 2008. Vol. 27, no. 7-8. P. 241–253. URL: https://doi.org/10.1016/j.cose.2008.07.008 (дата звернення: 29.02.2024).

5. Sharma A. Review on Major Cyber security Issues in Educational Sector. *International Journal of Computer Sciences and Engineering*. 2021. Vol. 9, № 12. P. 26–29. URL: https://doi.org/10.26438/ijcse/v9i12.2629 (дата звернення: 29.02.2024).

6. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI (з останніми змінами, внесеними згідно із Законом № 3585-IX від 22.02.2024). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 29.02.2024).

7. Top Cyber security Threats Active in the Education Sector Today – and Why You Should Care. URL: https://www.csoonline.com/article/3250862/security/top-cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html (дата звернення: 29.02.2024).

8. Ślusarczyk B. Sustainable Development Policies of the European Union as Expressions of Socio-Economic Security / B. Ślusarczyk, A. Wolak-Tuzimek. *Bezpecnostne Forum 2014 Security Forum, Zbornik Vedeckych Prac*. – Wydawnictwo Belianum, Banska Bystrica, 2014. S. 344–350.

9. Як захистити персональні дані під час дистанційного навчання: поради для педагогів, батьків та учнів. URL: https://eo.gov.ua/yak-zakhystyty-personalni-dani-pid-chas-dystantsiynoho-navchannia-porady-dlia-pedahohiv-batkiv-ta-uchniv/2021/01/20/ (дата звернення: 29.02.2024).

10. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII (з останніми змінами, внесеними згідно із Законом № 3549-IX від 16.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 29.02.2024).

11. How to help young learners stay safe on the internet. URL: https://www.britishcouncil.org/voices-magazine/how-help-young-learners-stay-safe-internet (дата звернення: 29.02.2024).

12. Data Copy Protection. URL: https://www.truscont.com/solutions/data-protection (дата звернення: 29.02.2024).

13. Нич О. В. Соя О.М. Дослідження проблеми інформаційної безпеки учнів у цифровому освітньому просторі закладу загальної середньої освіти. *Теорія і практика використання інформаційних технологій в умовах цифрової трансформації освіти: матеріали Всеукраїнської науково-практичної конференції, 29 червня 2023 року*. – Київ : Вид-во УДУ імені Михайла Драгоманова, 2023. С. 109-112.