

УДК 004.056-028.63:378]:005.336.4(1-87)

*Дорош О. В., здобувач вищої освіти,  
Василенко В. Ю., канд. наук з соц. ком.,  
старший викладач кафедри інформаційних технологій,  
Донецький національний університет імені Василя Стуса*

## **ЦИФРОВА БЕЗПЕКА В ОСВІТІ: ДОСВІД ЗАРУБІЖНИХ КРАЇН**

Ключові слова: цифрова безпека, цифрова компетентність, освіта, цифрові технології.

**Вступ.** Цифрова безпека в освіті є критичною проблемою, яка останніми роками привертає все більше уваги. Зі швидким розвитком технологій освітні заклади все більше покладаються на цифрові платформи для надання своїх послуг, що робить їх більш уразливими до цифрових загроз, як-от кібератаки та витоки даних. Отже, цифрова безпека в освітній діяльності стала ключовим питанням, яке привернуло багато уваги останніми роками. Поточний стан цифрової безпеки в освіті в усьому світі дуже відрізняється. Сучасний етап розвитку людської цивілізації визначається як перехід до суспільства знань і характеризується якісно новими вимогами до розвитку освіти.

**Актуальність.** Цифрова компетентність стала важливою частиною основних стратегічних рекомендацій і стандартів у розвинутих країнах в усьому світі та предметом занепокоєння в освітній політиці багатьох країн. У той час, як деякі країни запровадили потужні заходи цифрової безпеки, інші все ще намагаються подолати виклики цифрових загроз. Ці загрози цифровій безпеці мають значні наслідки впливу на освіту, життя людей і безпеку країни.

Розвиток цифрових технологій стимулює створення цифрової безпеки в галузі вищої освіти. Оскільки сучасна освіта поступово переходить у дистанційний та/або online-формат, то питання цифрової безпеки в галузі вищої освіти має пріоритетне місце [1].

Сьогодні США є провідною країною в цифровізації індустрії освіти та використанні цифрових технологій для трансформації навчання, встановлюючи план майбутнього для інших країн. Як і США, ЄС постійно сприяє розвитку високоєфективної європейської екосистеми цифрової освіти, спрямованої на покращення цифрових можливостей і навичок громадян. Були створені загальний регламент ЄС із захисту даних (GDPR) і Закон США про захист конфіденційності дітей в інтернеті (COPPA) для регулювання використання технологій в освіті. Ці правила вимагають від навчальних закладів отримання згоди батьків перед збором особистої інформації дітей віком до 13 років і вжиття відповідних заходів безпеки для захисту цієї інформації [3].

Щоб подолати виклики та ризики, пов'язані з цифровою безпекою в освіті, Швеція запустила програми медіаграмотності для різних цільових груп, зокрема учнів та вчителів. Ці програми включають у себе інтерактивні тренінги, семінари спрямовані на підвищення обізнаності про цифрові загрози та відповідальне використання інформації в онлайн-середовищі.

Система освіти Сінгапуру запровадила кілька успішних стратегій цифрової безпеки для захисту даних учнів і запобігання кібератакам. Вони включають: впровадження національної структури кібербезпеки в усіх школах, проведення регулярних тренінгів з кібербезпеки для персоналу й використання багатофакторної автентифікації та шифрування для захисту даних і запобігання несанкціонованому доступу. Запровадивши ці заходи, Сінгапур зміг підтримувати високий рівень безпеки та захистити конфіденційну інформацію своїх громадян.

Цифрова трансформація вищої освіти в Угорщині наголошує на актуальності проблеми формування цифрової компетентності в угорських вищих навчальних закладах. Оскільки технічний прогрес розвивається швидкими темпами, а цифровізація вже проникла в усі сфери життя, зокрема в систему освіти, цифрова компетентність зумовлює неминучість трансформації процесу навчання в навчальних закладах з урахуванням реалій інформаційного суспільства [5]. Тому необхідно використовувати електронні технології, пропонувані економіками ЄС.

Досвід Естонії показує, що важливо інтегрувати цифрові технології в освітній процес, але одночасно надавати належну увагу заходам забезпечення цифрової безпеки, щоб забезпечити надійність та конфіденційність освітньої інформації. Естонія першою реалізувала концепцію електронної держави, яка не лише позитивно впливає на економіку країни, а й дає змогу створити мережеву структуру суспільства (рис. 1) [4].



Рисунок 1 – Найпопулярніші категорії державних електронних послуг на прикладі Естонії та України [4]

Онлайн-система естонської шкільної освіти існує за тими ж ключовими принципами, що й електронна держава. Держава гарантує приватність даних

учнів і студентів, дозволяючи доступ до інформації лише самим особам, їх батькам та вчителям. Ця інформація надійно захищена, і доступ до неї можливий лише за допомогою цифрової ідентифікації [4].

Незважаючи на те, що багато країн досягли прогресу у впровадженні заходів цифрової безпеки в освіті, проблеми та успіхи залишаються. До поширених проблем належать: недостатня обізнаність і підготовка вчителів і студентів, недостатнє фінансування заходів цифрової безпеки, труднощі з дотриманням технологій, що швидко розвиваються. Україна обрала шлях євроінтеграції, який зосереджений на стратегіях розвитку держав-членів ЄС в інформаційній сфері. Потрібно працювати в цьому напрямі, вивчаючи досвід різних країн для прискорення власних перетворень. Метою модернізації української вищої освіти є створення такої моделі навчального процесу, яка б оптимально поєднувала кращі вітчизняні та зарубіжні традиції. Поєднання гуманістичних традицій української та зарубіжної педагогіки досвіду формування особистості, здатної до активних і самостійних дій, допоможе створити модель динамічної, плинної та конкурентоспроможної освітньої системи.

Цифрова трансформація характеризується поєднанням передового європейського та українського досвіду й технологій, поширенням інноваційних креативних технологій та нових процесів, а також створення інтелектуальних продуктів і послуг. Тому необхідно використовувати електронні технології, пропоновані економіками ЄС [2].

### **Висновки**

Безпека цифрової освіти має вирішальне значення для всіх країн. Кожна країна розробляє власні підходи та стратегії, які базуються на її індивідуальних особливостях і вимогах. Однак головною метою є забезпечення безпечного та захищеного простору для навчання та розвитку. Через стрімкий розвиток цифрових технологій важливо постійно оновлювати підходи до цифрової безпеки, щоб усунути нові небезпеки та зберегти безпеку освіти. Важливо, щоб країни продовжували обмінюватися досвідом і покращувати заходи цифрової безпеки для забезпечення безпеки цифрових освітніх просторів.

### **Список використаних джерел**

1. Султанова Л., Прокоф'єва М. Цифрова безпека в галузі вищої освіти. *Освіта дорослих: теорія, досвід, перспективи*. 2022. № 21(1). С. 106–117.
2. Андрюкайтене Р. Цифрова трансформація електронної освіти в країнах європейського союзу. *Розвиток сучасної науки та освіти: реалії, проблеми якості*. 2021. № 10(87). С. 88–91.
3. Шпарик О. Цифрова трансформація середньої освіти: спільні стратегічні вектори США та країн ЄС. *Український педагогічний журнал*. 2022. № 3. С. 33–43.
4. Близнюк М. М., Дебре О. С. Цифрова безпека освітнього процесу: європейський поступ Естонії та перспективи України. *Наукові записки Бердянського державного педагогічного університету*. 2022. № 1. С. 65–77.
5. Осадча К. П., Букша М. В. Особливості цифрової трансформації вищої освіти Німеччини. *Digital transformation and technologies for sustainable development all branches of modern education, science and practice*. 2023. Part 3. P. 70–74.