

## ДО ПРОБЛЕМИ БЕЗПЕЧНОГО ІНФОРМАЦІЙНО-ЦИФРОВОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА: ДОСВІД НІДЕРЛАНДІВ

Сучасний навчально-виховний процес відбувається у інформаційно-цифровому навчальному середовищі, що постійно розвивається і вдосконалюється. Учасники навчально-виховного процесу працюють на сучасних обчислювальних пристроях, користуються мережею інтернет, хмарними сервісами, спілкуються, співпрацюють, навчаються та розвиваються, застосовуючи соціальні мережі, блоги, форуми і чати тощо. Питання безпеки і конфіденційності спонукає учнів та вчителів бути компетентними, відповідальними та свідомими користувачами інформаційно-комунікаційних технологій (ІКТ) в процесі навчання і виховання.

Проблемам розбудови цифрового навчального середовища присвячені роботи вітчизняних вчених В. Бикова, А. Гуржія, Ю. Жука, С. Іванової, І. Іванюк, В. Лапінського, С. Литвинової, А. Манако, Е. Машбиця, Н. Морзе, О. Овчарук, О. Пінчук, С. Семерікова, О. Співаковського, О. Соколюк, Н. Сороко, О. Спіріна, Ю. Триуса та ін. Серед зарубіжних дослідників, які вивчають дану проблему слід назвати Дж. ван Браака, Дж.Тоундера, Дж. Вогта, П. Фіссера [1-10]. Автори зосереджують увагу на теоретичних та практичних аспектах розвитку цифрового середовища, зокрема, питаннях безпеки.

У розвинених європейських країнах існує суттєвий досвід розв'язання проблеми інформаційної безпеки та конфіденційності застосування ІКТ у навчально-виховному процесі. Найбільш актуальними є такі питання, як: обмін персональними даними, надійність паролів, кодекс поведінки для безпечного використання цифрових ресурсів та персональних даних, угоди про соціальні медіа, тощо. У звіті Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, що пройшов у м. Ньюейген, Нідерланди, у 2019 р., наголошується, що аспект інформаційної безпеки та конфіденційності – те, на чому саме має зосередитись сучасна школа [11].

Основою інформаційної безпеки та конфіденційності є рамкові документи, тобто правила та політика навчального закладу відносно встановлення порядку застосування ІКТ та відповідальності з боку адміністрації, вчителів, учнів та всіх учасників освітнього процесу щодо їх використання. Освітні інституції Нідерландів, країни, що є визнаним світовим лідером у галузі ІКТ, фонд Kennisnet (<https://www.kennisnet.nl>) у співпраці з Громадською Радою в галузі середньої освіти (<https://www.vo-raad.nl/>), Громадською Радою в галузі початкової освіти (<https://www.poraad.nl/>) та Громадською Радою з питань охорони здоров'я у 2019 р. запропонували оновлений підхід до формування і впровадження політики інформаційної безпеки та конфіденційності. З метою реалізації кроків освітньої політики у галузі інформаційної безпеки було створено наповнений інструментарієм національний веб-портал з інформаційної безпеки для шкіл та забезпечено умови комфортного переходу на нього з існуючих шкільних сайтів. Для підтримки ефективного впровадження ІКТ у навчальне середовище, в якому застосовуються хмарні сервіси, цифрові ресурси і засоби, створено рекомендації, що розроблені фахівцями у вигляді дорожньої карти (покрокового плану), спрямованої допомогти школі впровадити політику інформаційної безпеки та конфіденційності навчального закладу в життя. Дорожня карта складається із п'яти розділів: “Політика та відповідальність”, “Визначення обмежень та ризиків”, “Прозорий обмін персональними даними”, “Обробка та зберігання персональних даних”

та “Оцінювання”. Основними темами розділу “Політика та відповідальність” є: політика інформаційної безпеки, конфіденційність, ролі та обов’язки. Кодекс поведінки щодо безпечного використання ресурсів та персональних даних ІКТ, політика щодо паролів та процедура повідомлення про інциденти з порушення безпеки – аспекти, на яких зосереджується увага розділу “Визначення обмежень та ризиків”. Питання конфіденційності за замовчуванням та конфіденційності процесу розробки, угоди про соціальні медіа, обмін персональними даними та ін. розкриваються у розділі “Прозорий обмін персональними даними”. Угоди про обробку та зберігання даних, правила та юридичне підґрунтя містяться у розділі “Обробка та зберігання персональних даних”. Інструкції щодо процесів підзвітності та інформування висвітлені у розділі “Оцінювання”. До інструментарію, що забезпечує політику інформаційної безпеки та конфіденційності, також належить укладений глосарій, що визначає основні терміни та поняття, серед яких: анонімізація, псевдонімізація, аутентифікація, матриця авторизації, хмара, мінімізація даних, шифрування, хакерство, аналіз ризиків, конфіденційність, конфіденційність за замовчуванням, шифрування та ін.

Міжнародний союз зв’язку (МСЗ), опікуючись питаннями цифрової безпеки молоді, розробив рекомендації, зокрема, для освітян, щодо захисту дітей у цифровому середовищі. Нещодавно в Україні за ініціативи Міністерства цифрової трансформації та підтримки МСЗ фахівцями громадської організації МІНЗМІН підготовлено переклад українською цих рекомендацій. Зміст ресурсу “7 порад для вчителів, як навчити учнів безпечної поведінки в Інтернеті” зосереджений на висвітленні двох основних аспектів, а саме: цифрового середовища навчального закладу та поведінки у такому середовищі. Ознайомитись з ресурсом можна за посиланням на сайті <https://nus.org.ua>.

Міністерство науки і освіти України у 2021 р. розробило рекомендації щодо безпеки дітей у цифровому просторі для освітян. Пропедевтична робота має бути зосереджена на таких напрямках, як: права людини у цифровому середовищі, електронна участь у процесі ухваленні рішень, збереження здоров’я під час роботи з цифровими пристроями, механізми захисту прав, що порушуються в інтернеті, а також способи отримати допомогу та багато інших [12].

Зарубіжний досвід, зокрема, досвід Нідерландів і практичні розробки освітньої міжнародної спільноти, можуть стати у нагоді вітчизняним фахівцям для подальшого розвитку освітньої політики у напрямку цифрової безпеки, створенню рамкових орієнтирів для розбудови ефективного та безпечного інформаційно-цифрового навчального середовища.

#### **Список використаних джерел:**

1. В.Ю. Биков, та В.Г. Кремень, “Категорії простір і середовище: особливості модельного подання та освітнього застосування”, Теорія і практика управління соціальними системами: філософія, психологія, педагогіка, соціологія, No2, с. 3-16, 2003.
2. В.Ю. Биков, та ін. Теоретико-методологічні засади інформатизації освіти та практична реалізація інформаційно-комунікаційних технологій в освітній сфері України, Монографія, Компринт, м. Київ, Україна, 2019.
3. В.Ю. Биков, та ін. Формування інформаційно-освітнього середовища навчання старшокласників на основі технологій електронних соціальних мереж, Монографія, Педагогічна думка, м. Київ, Україна, 2018.
4. Ю.О. Жук, “Особистісний простір учня в комп’ютерно-орієнтованому навчальному середовищі”, Інформаційні технології і засоби навчання, т. 29, No3, 2012. [Електронний ресурс]. Доступно: <http://journal.iitta.gov.ua/index.php/itlt/article/view/693/508>.
5. А.М. Гуржій, В.В. Лапінський, та Л.А. Карташова, Електронні освітні ресурси як суспільне явище, “Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми”, No 44, с. 14-22, 2016.

6. Н.В. Морзе, та С.М. Співак, “Формування сучасного хмаро орієнтованого персоналізованого освітнього середовища враховуючи ікт-компетентність учасників навчального процесу “, Відкрите освітнє е-середовище сучасного університету, No3, с.274-282, 2017. doi: 10.28925/2414-0325.
7. О.В. Овчарук та ін., Розвиток інформаційно-комунікаційної компетентності вчителів в умовах хмаро орієнтованого навчального середовища: методичний посібник. Київ, Україна: Літера ЛТД, 2019.
8. А.В. Яцишин, та ін., Цифрова трансформація відкритих освітніх середовищ. Монографія. Київ, Україна: ФОП О.В. Ямчинський, 2019.
9. P. Fisser, J. Voogt, J. Tondeur, and J. van Braak, “TPACK: kennis en vaardigheden voor ICTintegratie”, Weten Wat Werkt en Waarom”, Kennisnet. Zoetermeer, vol. 2, no. 2, pp. 22-29, juni 2013. [Електронний ресурс]. Доступно: [https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/4w/4w\\_magazine\\_2013-2.pdf](https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/4w/4w_magazine_2013-2.pdf) .
10. О. Ovcharuk, I. Ivaniuk, N. Soroko, O. Gritsenchuk, and O. Kravchyna , “The use of digital learning tools in the teachers' professional activities to ensure sustainable development and democratization of education in European countries”, in E3S Web of Conferences, 166 (10019), 2020. [Електронний ресурс].
11. Звіт Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, Нідерланди, 2019. [Електронний ресурс]: <https://www.kennisnet.nl/artikel/verslag-landelijk-congres-ibr-in-het-onderwijs-2019/>. Дата звернення: Лист.11,2019.
12. Рекомендації для проведення закладами освіти додаткових профілактичних заходів серед дітей та інформування батьків щодо компетентностей безпечної поведінки у цифровому середовищі. Додаток до листа МОН України від 10.03.2021 р. №1/9-128.