Гриценчук Олена Олександрівна,
к.п.н., старший науковий співробітник,
Інститут цифровізації освіти НАПН України, м.Київ.

БЕЗПЕКА У ІНФОРМАЦІЙНО-ЦИФРОВОМУ НАВЧАЛЬНОМУ СЕРЕДОВИЩІ: ЄВРОПЕЙСЬКИЙ ДОСВІД

Сьогодні навчання і виховання відбувається у інформаційно-цифровому навчальному середовищі, що постійно розвивається і вдосконалюється. Дані, що використовуються вчителем та учнем, зберігаються не тільки на власному комп'ютері, а все частіше розміщуються у хмарі. Учасники навчально-виховного процесу користуються хмарними сервісами, спілкуються, співпрацюють, навчаються та розвиваються засобами соціальних мереж, блогів, форумів і чатів тощо. Питання безпеки і конфіденційності в сучасному комп'ютерно орієнтованому та хмаро орієнтованому навчальному середовищі спонукає учасників освітнього процесу бути компетентними, відповідальними та свідомими користувачами.

Питання розбудови цифрового навчального середовища відображені у працях сучасних вітчизняних вчених В. Бикова, А. Гуржія, Ю. Жука, С. Іванової, І. Іванюк, В. Лапінського, А. Манако, Е. Машбиця, Н. Морзе, О. Овчарук, С. Семерікова, О. Співаковського, О. Соколюк, Н. Сороко, О. Спіріна, Ю. Триуса та ін. Серед зарубіжних дослідників. які досліджують 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 країнах Європи існує певний досвід щодо розв'язання проблеми інформаційної безпеки та конфіденційності використання цифрових технологій, що застосовуються у навчальних закладах. Найбільш гострими питаннями, що піднімаються освітянами, є: обмін персональними даними, політика щодо 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. Ньювейген, Нідерланди, у 2019 р., наголошується, що аспект інформаційної безпеки та конфіденційності – те, на чому саме має зосередитись сучасна школа [11].

Організація інформаційної безпеки та конфіденційності починається зі створення рамкових умов, тобто правил та політики закладу освіти щодо встановлення відповідальності з боку адміністрації, вчителів, учнів та всіх учасників освітнього процесу. З метою забезпечити ефективне та безпечне функціонування шкіл у інформаційно-цифровому навчальному середовищі, освітні інституції Нідерландів, країни, що є визнаним світовим лідером у галузі ІКТ (інформаційних та комунікаційних технологій), 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. Ефективне впровадження ІКТ у навчальне середовище, в якому застосовуються хмарні сервіси, цифрові ресурси і засоби, забезпечується рекомендаціями, що розроблені фахівцями у вигляді дорожньої карти (покрокового плану), спрямованої допомогти школі запровадити політику інформаційної безпеки та конфіденційності навчального закладу. 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". До розділу "Політика та відповідальність" входять такі теми, як: 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 розділку “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 містяться 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 громадська організація МІНЗМІН підготувлено переклад українською цих рекомендацій. Зміст ресурсу “7 порад для вчителів, як навчити учнів безпечної поведінки в Інтернеті” спрямований 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 в ухваленні рішень, збереження здоров’я під час роботи з цифровими пристроями, механізми захисту прав, що порушуються в інтернеті, а також способи отримати допомогу та інші [12].

Зарубіжний, зокрема, європейський досвід і практичні розробки освітньої 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 .
10. O. 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-ibp-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.

Анотація. Питання безпеки і конфіденційності в сучасному інформаційно-цифровому навчальному навчальному середовищі вимагає від учасників освітнього процесу бути компетентними, відповідальними та свідомими користувачами ІКТ. Представлено аналіз європейського та вітчизняного досвіду щодо інформаційної безпеки учасників освітнього процесу.
Ключові слова: інформаційно-цифрове навчальне середовище, інформаційна безпека, освіта, міжнародний досвід.

Abstract. The issue of security and confidentiality in the modern information and digital learning environment requires participants in the educational process to be competent, responsible and conscious users of ICT. An analysis of European and domestic experience in information security of participants in the educational process is presented.

Keywords: information and digital learning environment, information security, education, international experience.