

пов'язаного з некоректним втручанням дорослого у внутрішній світ дитини.

Отож, особистісно орієнтований підхід до виховання передбачає забезпечення учням права на свободу вибору власної ціннісної позиції, створення умов для реального здійснення цього вибору за наявності внутрішньої готовності дитини до подолання дисгармонії у власному досвіді, поведінці, спілкуванні та діяльності. Такий підхід формує основу для розвитку самостійної, духовно багатой та соціально відповідальної особистості.

ЛІТЕРАТУРА

1. Бех І.Д. Особистісно зорієнтоване виховання : наук.-метод. посібник / М-во освіти України, Ін-т змісту і методів навчання. Київ, 1998. 204 с.

2. Бех І.Д. Особистісно-орієнтована модель виховання як науковий конструктор. URL: http://library.udpu.org.ua/library_files/psuh_pedagog_probl_silsk_shkolu/3/vupysk_21.pdf

Олексій МІНАШКІН
(Львів)

ЦИФРОВА БЕЗПЕКА В УМОВАХ ЗАКЛАДУ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ: РЕАЛІЇ ТА ВИКЛИКИ

Використання цифрових технологій у закладах загальної середньої освіти (ЗЗСО) стало звичною складовою освітнього процесу. Онлайн-ресурси, цифрові платформи та засоби комунікації активно використовуються у навчальній діяльності учнів. Разом із розширенням можливостей цифрового середовища актуалізуються і питання безпеки. Йдеться не лише про технічний захист інформації, але й про ситуації, що виникають у процесі взаємодії учнів із цифровим контентом та іншими користувачами. У багатьох випадках такі ризики не завжди усвідомлюються або недооцінюються.

У сучасних наукових підходах цифрова безпека розглядається як складова ширшого явища, пов'язаного з формуванням цифрових компетентностей особистості [1; 2]. Це передбачає не тільки

володіння цифровими інструментами, але й здатність безпечно та відповідально використовувати їх у навчальній діяльності.

Особливої уваги потребує освітнє середовище закладу загальної середньої освіти, де відбувається формування базових моделей поведінки учнів. У цьому контексті важливо не лише інформувати про можливі загрози, але й створювати умови для усвідомленого застосування знань у практичних ситуаціях.

Отже, проблема цифрової безпеки в школі набуває комплексного характеру і потребує розгляду з урахуванням реальних умов освітнього процесу, що дає змогу визначити основні виклики та окреслити напрями їх подолання.

Цифрове середовище дедалі більше впливає на організацію освітнього процесу в ЗЗСО. Це стосується не лише використання окремих інструментів, але й зміни способів взаємодії учнів з інформацією та між собою [3]. У таких умовах питання безпечної роботи з цифровими ресурсами поступово виходить за межі технічного супроводу і пов'язується із повсякденною освітньою практикою.

У дослідженнях, присвячених цифровим компетентностям, питання безпеки постають як одна з умов ефективної роботи з цифровими ресурсами. У європейських підходах акцентується не лише на технічному володінні інструментами, але й на здатності використовувати їх у спосіб, що не створює ризиків для користувача та інших учасників взаємодії [1; 2]. У такому контексті цифрова безпека – це не окремий напрям, а складова повсякденної діяльності в цифровому середовищі. Водночас особливості шкільної практики показують, що використання цифрових технологій не завжди супроводжується належною увагою до питань безпеки. В освітньому процесі акцентовано переважно на виконанні завдань із застосуванням цифрових інструментів, тоді як умови їхнього безпечного використання залишаються другорядними. У результаті учні знайомі з окремими правилами, проте не мають достатнього досвіду їх застосування в реальних ситуаціях.

У роботах, що досліджують поведінку дітей у цифровому середовищі, підкреслюється, що учні не завжди розпізнають небезпечні ситуації або надають їм належного значення [4]. У багатьох випадках рішення ухвалюються ситуативно, без урахування можливих наслідків, що впливає на рівень безпечності їхньої діяльності в мережі. У зв'язку з цим доцільно розглядати

цифрову безпеку у взаємозв'язку з інформаційною культурою особистості. У педагогічних дослідженнях вона описується через особливості роботи з інформацією, ставлення до неї та характер дій у відповідних ситуаціях [5]. Такий підхід дає можливість ширше інтерпретувати цифрову безпеку, пов'язуючи її не лише з дотриманням правил, але й із формуванням відповідальної поведінки в процесі взаємодії з цифровим середовищем.

Організація освітнього процесу дає змогу виокремити чинники, що впливають на рівень цифрової безпеки. Насамперед йдеться про те, як учні оцінюють можливі ризики під час роботи з цифровими ресурсами. У багатьох випадках взаємодія з цифровим середовищем сприймається як звична частина повсякденної діяльності, що знижує уважність до потенційно небезпечних ситуацій.

Іншою важливою особливістю є розрив між знаннями і реальною поведінкою. Учні можуть знати основні правила безпеки, однак не завжди застосовують їх на практиці. Це проявляється, зокрема, у недотриманні правил конфіденційності, використанні ненадійних ресурсів або необережному поширенні персональних даних [4]. Така ситуація свідчить про те, що проблема цифрової безпеки має не лише когнітивний, але й поведінковий характер.

Значно впливає на рівень цифрової безпеки також освітнє середовище. Якщо питання безпеки не є складовою навчальної діяльності і не підкріплюється практичними завданнями, учні не формують відповідних навичок. У цьому випадку знання залишаються переважно теоретичними і не переходять у стійкі моделі поведінки.

Важливу роль у цьому процесі відіграє педагог. У сучасних підходах передбачається, що він має не лише використовувати цифрові технології, але й гарантувати безпечні умови їх застосування [2]. Проте на практиці рівень готовності педагогів до розв'язання цих завдань може відрізнятися, що також впливає на загальний стан цифрової безпеки в закладі освіти.

З урахуванням зазначених особливостей підвищення рівня цифрової безпеки потребує комплексного підходу. Йдеться про поєднання теоретичної підготовки з практичним досвідом, створення умов для аналізу реальних ситуацій та формування відповідального ставлення до цифрової діяльності. Такий підхід сприяє не лише засвоєнню правил, але й виробленню моделей поведінки, які застосовуються у повсякденній практиці.

Узагальнюючи викладене, можна зазначити, що цифрова безпека в умовах закладу загальної середньої освіти визначається особливостями організації освітнього процесу та характером взаємодії учнів із цифровим середовищем. Її рівень залежить не лише від обсягу засвоєної інформації, але й від здатності застосовувати її в конкретних ситуаціях, що виникають у повсякденній навчальній діяльності.

Цифрова безпека в умовах закладу загальної середньої освіти формується під впливом сукупності чинників, з-поміж яких важливу роль відіграють особливості освітнього середовища, рівень підготовки педагогів та характер взаємодії учнів із цифровими ресурсами. Вона не обмежується технічними аспектами і пов'язана з реальними практиками використання цифрових технологій в освітньому процесі.

В умовах сучасної школи забезпечення цифрової безпеки має нерівномірний характер. Активне використання цифрових інструментів не завжди супроводжується належною увагою до питань безпечної взаємодії з ними. Це проявляється у недостатньому рівні усвідомлення ризиків, а також у відмінностях між засвоєними знаннями та їх практичним застосуванням у конкретних ситуаціях. Труднощі гарантування безпечної поведінки пов'язані не лише з рівнем обізнаності учнів, але й із відсутністю сформованого досвіду дій у ризикованих ситуаціях. У багатьох випадках цифрове середовище сприймається як звичне і відносно безпечне, що знижує критичність у прийнятті рішень і впливає на характер поведінки.

Підвищення рівня цифрової безпеки потребує зміщення акцентів в освітньому процесі. Йдеться про посилення ролі практичних форм роботи, використання ситуаційних завдань, а також формування відповідального ставлення до цифрової діяльності як складової повсякденної поведінки учнів.

Отже, гарантування цифрової безпеки в ЗЗСО треба розглядати як складний педагогічний процес, що поєднує зміст навчання, організацію освітнього середовища та формування відповідних моделей поведінки в цифровому просторі.

ЛІТЕРАТУРА

1. Vuorikari R., Punie Y., Carretero Gomez S., Van den Brande G. DigComp 2.0: The Digital Competence Framework for Citizens. Luxembourg : Publications Office of the European Union, 2016. 48 p.

2. Redecker C. European Framework for the Digital Competence of Educators (DigCompEdu). Luxembourg : Publications Office of the European Union, 2017. 95 p.

3. European Commission. Digital Education Action Plan 2021–2027: Resetting education and training for the digital age. Brussels : European Union, 2021. 24 p.

4. Livingstone S., Stoilova M., Nandagiri R. Children's data and privacy online: growing up in a digital age. *Journal of Children and Media*. 2021. Vol. 15, No. 2. pp. 212–229.

5. Трифаніна Л. Інформаційна культура підлітків у сучасному освітньому середовищі: монографія. Київ, 2019. 210 с.

Тетяна НАДІМ'ЯНОВА,
Роман БЕЙЗИК
(Дрогобич)

ОПТИМІЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ, УСКЛАДНЕНОГО ВІЙНОЮ В УКРАЇНІ

Проблема оптимізації системи сучасної української освіти в умовах глобальних змін, що охопили усі сфери нашого буття, не випадкова. Україна переживає важкі часи, пов'язані з війною, яка триває п'ятий рік. Це не може не відобразитись на життєдіяльності дітей, їхньому навчанні, вихованні, яке проходить у непростих умовах. Та незважаючи на це, реформа Нової української школи триває. Так, з 1 вересня 2027 р. планується перехід на 12-річну систему навчання; посилюється увага до підвищення якості середньої освіти; відбувається реформа створення академічних ліцеїв, де учні зможуть обирати профіль навчання; на державному рівні продовжується створення безпечових умов – будівництво або ремонт укриттів закладів освіти тощо.

На кінець 2025 р. в Україні були повністю зруйновані 423 заклади загальної середньої освіти, 7 мільйонів дітей – це діти війни. Саме для них мають бути створені якнайкращі умови не просто виживання, а виховання і навчання.

Тому оптимізація системи освіти, яка розрахована на особистість нової епохи, є необхідною і важливою умовою у розв'язанні складних та гострих завдань, що стоять сьогодні перед