завдання, розроблені на платформі LearningApps. Вони забезпечують можливість швидкого зворотного зв'язку та дозволяють учнівству самостійно оцінювати рівень засвоєння навчального матеріалу.

Таким чином, цифрові інструменти в підручнику виконують різні функції: пояснювальну, тренувальну та контролюючу. Їх поєднання створює цілісне освітнє середовище, яке сприяє формуванню ключових компетентностей здобувачів освіти.

Апробація розроблених цифрових компонентів показала, що їх використання підвищує зацікавленість учнівства у вивченні хімії, сприяє кращому розумінню навчального матеріалу та розвитку пізнавальної активності.

Інтеграція цифрових технологій у структуру підручника з хімії є ефективним засобом модернізації навчального процесу в умовах Нової української школи. Використання доповненої реальності, інтерактивних вправ на платформі Wordwall та завдань для самоконтролю на платформі LearningApps дозволяє створити цілісну систему цифрової підтримки навчання.

Застосування таких технологій сприяє підвищенню мотивації учнівства, покращенню розуміння навчального матеріалу та розвитку ключових компетентностей. Перспективи подальших досліджень пов'язані з розширенням функціональних можливостей цифрових компонентів підручника та їх адаптацією до різних рівнів освіти.

Список використаних джерел

1. Державний стандарт базової середньої освіти, затверджений постановою КМУ від 30 вересня 2020 р. №898. URL: https://zakon.rada.gov.ua/laws/show/898-2020-%D0%BF#Text.

2. Мідак Л.Я. Хімія: підручник для 8 класу закладів загальної середньої освіти/ Л.Я. Мідак, О.В. Кузишин, Ю.Д. Пахомов, Х.В. Буждиган. Тернопіль: Астон, 2025. 272 с.

3. Wang L.-H. et al. Effects of digital game-based STEM education on students' learning achievement: a meta-analysis // International Journal of STEM Education. 2022. V.9, N 26. DOI: https://doi.org/10.1186/s40594-022-00344-0.

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УЧНІВ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Мінський Владислав Олександрович
здобувач першого рівня вищої освіти спеціальності Середня освіта (Інформатика)
Тернопільський національний педагогічний університет імені Володимира Гнатюка
minskyj_vo@fizmat.tnpu.edu.ua
Карабін Оксана Йосифівна
кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання
Тернопільський національний педагогічний університет імені Володимира Гнатюка
karabin@tnpu.edu.ua

У сучасному світі цифрові технології стали невід'ємною частиною освітнього процесу та життя здобувачів освіти, які є активними учасниками цифрового середовища, що відкриває широкі можливості для навчання, саморозвитку та комунікації, але водночас створює низку потенційних ризиків. Зокрема, інтенсивне використання інтернету, соціальних мереж та онлайн-

платформ для навчання створює чимало ризиків для інформаційної безпеки. Найбільш вразливими до таких загроз стають здобувачі, оскільки вони часто не володіють кібербезпекою та не дотримуються безпечної цифрової поведінки, що означає, що вони не тільки вразливі до різних загроз, але й можуть самі спричиняти або ставати загрозами. Зазначимо, що актуальність дослідження підтверджується зростанням кількості кіберзлочинів, а також поширенням дезінформації та її психологічним впливом на молодь.

Нині в умовах війни, у якій перебуває Україна, загрози інформаційній безпеці учнів набувають не лише індивідуального, а й національного виміру, бо інформаційне середовище набуває ознак гібридного протистояння, де інформація виступає інструментом впливу, маніпуляції та дестабілізації. Здобувачі освіти, як активні користувачі цифрових платформ, стають однією з цільових аудиторій інформаційно-психологічних операцій. Недостатній рівень цифрової грамотності може призвести не лише до особистих втрат, але й до потенційної шкоди інформаційній безпеці держави. Наприклад, сьогодні у соціальних мережах і месенджерах активно поширюються фейкові новини про перебіг бойових дій, маніпулятивні відео та фото, спрямовані на виклик страху чи паніки. Такий контент провокує тривожність і дезорієнтацію. Здобувачі можуть ставати об’єктами вербування через соціальні мережі, заохочуватися до поширення ворожого матеріалу, маніпулятивних онлайн-ігор або «челенджів», що передбачає поширення завдань із фотографування об’єктів інфраструктури або пересування техніки під виглядом «квестів». Під час війни активізується і кіберзлочинність. Поширеними є кібербулінг, фішинг та онлайн-шахрайство. Шахраї активніше використовують для маніпуляцій фейкові збори «на ЗСУ», підроблені благодійні фонди, повідомлення про «допомогу» або «виплати». Користувачі мереж можуть отримувати повідомлення про «грошову допомогу для постраждалих» із проханням ввести дані картки. Відтак вони часто необережно публікують особисту інформацію в соціальних мережах: фото, місце проживання, номер телефону, заклад освіти. Відкрита інформація створює ризики крадіжки особистих даних, використання її у злочинних цілях, цифрового стеження.

Часте встановлення невідомих застосунків або перехід за підозрілими покликанням в інтернеті здобувачами освіти може призвести до зараження пристрою вірусами чи шпигунськими застосунками. Наслідком цього може стати втрата даних, доступ сторонніх осіб до акаунтів, порушення роботи ґаджетів. А надмірне перебування здобувачів освіти в цифровому середовищі може призводити до зниження академічної успішності, порушення сну, соціальної ізоляції, формування залежної поведінки. Така ситуація актуалізує необхідність системної роботи з здобувачами освіти через проведення тренінгів, роз’яснення ризиків та дотримання правил цифрової гігієни, через використання складних паролів, двофакторної аутентифікації, обмеження доступу до особистих даних, а також формування відповідальної онлайн-поведінки, культури відповідального споживання і поширення інформації серед учнівської молоді.

Отже, проблема інформаційної безпеки здобувачів освіти у цифровому середовищі є важливою в сучасних умовах, вона активно обговорюється в царині педагогіки, психології та комунікації. Значна увага приділяється питанням медіаграмотності як ключової передумови безпечної поведінки в цифровому

середовищі. Зокрема, О. Волошенюк та В. Іванов підкреслюють, що розвиток критичного мислення та навичок аналізу медіаконтенту є основою формування інформаційної стійкості особистості. Дослідники наголошують, що медіаосвіта має інтегруватися в освітній процес як наскрізна компетентність [1]. Формуванню навичок безпечної онлайн-поведінки, відповідального створення та поширення контенту сприяє інтеграція медіаосвіти в освітній процес, зокрема на уроках інформатики, які є вагомим інструментом впровадження медіаосвіти. Дослідники Г. Зима, О. Федоренко, А. Фесенко, у статті «Розвиток медіаграмотності учнів під час вивчення інформатики» пропонують використовувати різні практичні завдання, що сприяють комплексному розвитку навичок здобувачів для їхньої адаптації в сучасному інформаційному середовищі. Науковці розглядають медіаграмотність як базову компетентність, що дозволяє учням протистояти фейкам, маніпуляціям і шкідливому контенту [4].

Що стосується кібербулінгу як специфічної форми цифрового насильства, то він трактується як соціально-психологічне явище, що трансформує процес соціалізації. Через особисті образливі коментарі та повідомлення, поширення чуток або компрометуючих матеріалів, створення фейкових акаунтів він має довготривалі негативні наслідки для психічного здоров’я дітей. Результати кібербулінгу включають емоційний стрес, зниження самооцінки, тривожність та соціальну ізоляцію. Про що наголошує Л. Найдьонова у своєму науковому дослідженні [2]. Дослідниця І. Пилипишина вважає кібербулінг формою електронного насильства. Зауважимо, що кібербулінг став серйозною загрозою у віртуальному просторі. Утім, кібербулінг є динамічним явищем, адже з кожним роком стає більш небезпечним, а кількість осіб, які постраждали від нього, збільшується. Кібербулінг порушує не лише емоційне та соціальне благополуччя, але й безпеку, яка є одним з основних прав людини [3, с. 141]. Відтак науковці наголошують на необхідності формування кібергігієни як складової інформаційної культури користувача. Особлива увага приділяється необхідності впровадження концепції кібергігієни, яка розглядається як інструмент для формування індивідуальної стійкості громадян, зокрема учнів, до загроз в інформаційному просторі. Кібергігієна передбачає створення умов для захисту користувачів від деструктивного впливу через систематизацію знань, навичок і поведінкових практик у цифровому середовищі.

Обумовимо, що інформаційна безпека здобувачів освіти у цифровому середовищі виступає незмінно важливим елементом освітньої діяльності, адже з кожним днем використання цифрових технологій стає все поширенішим. Основними загрозами, які можуть виникати в цьому контексті, є різноманітні прояви кібершахрайства, такі як кібербулінг, спроби отримати доступ до конфіденційних даних через фішинг, витік особистої інформації, вплив шкідливого програмного забезпечення чи масове розповсюдження дезінформації. Зазначені фактори здатні створити значний тиск як на емоційний і психологічний стан здобувачів освіти, так і на їхній загальний рівень безпеки в цифровому просторі.

Для ефективної протидії зазначеним загрозам необхідно застосовувати комплексний підхід, що охоплює три рівні заходів: освітні, технічні та соціальні. Освітній компонент передбачає цілеспрямоване формування у здобувачів

цифрової грамотності, включно з навичками безпечного користування інтернетом та критичного мислення щодо отримання та оцінки інформації. Технічні заходи включають впровадження сучасних засобів захисту віртуального середовища та регулярне оновлення програмного забезпечення з метою мінімізації можливих ризиків. Соціальний аспект акцентує увагу на важливості виховання відповідального ставлення до власного інформаційного контенту, пропагування етичності у взаємодії в мережі та створення підтримуючого середовища між однолітками.

Таким чином, найбільш ефективні стратегії захисту здобувачів освіти від цифрових загроз ґрунтуються на формуванні критичної свідомості та розумінні відповідального ставлення до інформації і технологій щодо безпеки в інформаційному просторі. Значну роль у цьому процесі відводиться вчителеві як посереднику між здобувачами освіти і цифровим середовищем, який має формувати навички критичного мислення та безпечної поведінки.

Список використаних джерел

1. Іванов В. Ф., Волошенюк О. В. Медіаосвіта та медіаграмотність : підручник / за наук. ред. В. В. Різуна. Київ : Центр вільної преси, 2012. 352 с.

2. Найдьонова Л. А. Кібербулінг у підлітковому рейтингу інтернет-небезпек. *Психологічні науки: проблеми і здобутки*, 2018. Вип. 1. С. 141–159.

3. Пилипишина І. І. Протидія кібербулінгу як забезпечення права дитини на безпеку. *Науковий вісник Ужгородського національного університету. Серія : Право*, 2024. Т. 1, № 83. С. 141–150.

4. Федоренко О., Фесенко А., Зима Г. Розвиток медіаграмотності учнів під час вивчення інформатики. *Збірник наукових праць фізико-математичного факультету ДДПУ*, 2024. № 14. С. 66–74.

ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ПЕДАГОГІВ

Міщук Антон Юрійович
здобувач третього рівня вищої освіти спеціальності Математика
Волинський національний університет імені Лесі Українки
anton.mi.ju@gmail.com

Сучасна освіта функціонує в умовах тотальної цифровізації та постійного обміну інформацією. Це вимагає від майбутніх педагогів не лише глибоких знань із предметів, а й здатності ефективно працювати з інформаційними потоками, критично оцінювати медіаконтент та навчати цих навичок своїх здобувачів освіти. Актуальність розвитку медіаграмотності зростає через значне поширення маніпуляцій та дезінформації. Тому цілеспрямоване навчання студентів педагогічних коледжів критичному сприйняттю медіа стає обов’язковим елементом їхньої професійної підготовки.

Проблема медіаграмотності перебуває в центрі уваги як вітчизняних (Т. Бешок, В. Биков, Г. Васянович, Д. Вербівський, О. Волошенюк, О. Жмурко, С. Литвинова, В. Підгурська, Т. Цегельник ін.) так і зарубіжних дослідників (Д. Бакінгем, Р. Хоббс, Г. Дженкінс, Н. Карр, Д. Келлнер, Дж. Шейр, В. Поттер та