

<https://doi.org/10.28925/2412-124X.2024.13.8>

УДК 378.018.43:004

**Вікторія Наумова**

<https://orcid.org/0000-0002-0114-4749>

старший викладач кафедри природничо-математичної освіти і технологій,  
Інститут післядипломної освіти,  
Київський столичний університет імені Бориса Грінченка,  
просп. Павла Тичини, 17, 02152 Київ, Україна  
[v.naumova@kubg.edu.ua](mailto:v.naumova@kubg.edu.ua)

**Оксана Бульвінська**

<https://orcid.org/0000-0002-6764-4340>

кандидат педагогічних наук, старший науковий співробітник,  
старший науковий співробітник Бібліотеки,  
Київський столичний університет імені Бориса Грінченка,  
вул. Левка Лук'яненка, 13-б, 04212 Київ, Україна  
[o.bulvinska@kubg.edu.ua](mailto:o.bulvinska@kubg.edu.ua)

**УПРАВЛІННЯ БЕЗПЕКОЮ УЧНІВ В ІНТЕРНЕТІ: ВІДКРИТІ ОСВІТНІ РЕСУРСИ НА ДОПОМОГУ ОСВІТЯНАМ**

=====

*Стаття присвячена аналізу українських і зарубіжних відкритих освітніх ресурсів, які є елементом професійного розвитку педагогів для організації роботи зі школярами щодо безпечного користування інтернетом. Підкреслено, що саме вчителі мають сформулювати в учнів навички безпечної поведінки в цифровому просторі, керування особистими даними в інтернеті, оцінки цифрового контенту, правил спілкування в соціальних мережах. Наголошено, що відкриті освітні ресурси – це навчальні, викладацькі та дослідницькі матеріали в будь-якому форматі і носії, які перебувають у суспільному надбанні і які можна вільно використовувати в освітньому процесі. До відкритих освітніх ресурсів відносимо будь-які засоби, матеріали або технології, що мають потенціал для навчання: підручники і посібники, відео- й аудіозаписи, графічні ресурси, плани уроків, тестові завдання, документи, роздатковий матеріал, програмне забезпечення тощо. Масові відкриті онлайн-курси містять нову актуальну інформацію професійного спрямування, є доступним і гнучким видом навчання та підвищення кваліфікації викладачів закладів освіти. Проаналізовані в статті українські і зарубіжні відкриті освітні ресурси щодо безпечної поведінки дітей в інтернеті систематизовано за трьома категоріями: розроблені урядовими структурами; розроблені громадськими організаціями; масові відкриті онлайн-курси. Підкреслено, що проаналізовані ресурси включають освітній, комунікаційний, інформаційний компоненти і мають беззаперечний потенціал для їх використання педагогами у навчанні дітей і батьків.*

**Ключові слова:** *безпечна поведінка в інтернеті, відкриті освітні ресурси, масові відкриті онлайн-курси, професійний розвиток педагогів, цифрове середовище.*

=====

**Вступ.** У сучасному світі інтернет став невід'ємною складовою життя суспільства. Цифрове середовище є важливим джерелом інформації під час здобуття освіти, соціалізації, саморозвитку, спілкування, побутових справ. Не секрет, що діти часто більш обізнані з цифровими технологіями, ніж дорослі, зокрема педагоги. Однак більшість учнів, незважаючи на практичні вміння користуватись інтернетом, не знають, як робити це безпечно, не розуміють загроз, які можуть їх спіткати в кіберпросторі, і не мають сформованих навичок захисту себе в цифровому просторі. Тому кібербезпека, керування персональною інформацією в інтернеті, оцінка загроз маніпуляцій у медіа, правила спілкування в соціальних мережах є важливим і обов'язковим складником підготовки дітей до існування в цифровому середовищі.

Проблема безпечної поведінки в інтернеті, подолання ризиків порушень прав дитини в цифровому середовищі, як зазначає С. Петренко (2020), є не тільки педагогічною, а й загальносуспільною, і розв'язувати її потрібно комплексно, але розпочинати формування навичок безпечної поведінки у Всесвітній мережі потрібно з молодшого шкільного віку, а можливо, навіть з дошкільного (с. 89–90).

Отже, велика роль у розв'язанні цієї проблеми відводиться педагогічним працівникам, які повинні організувати роботу з дітьми і батьками. Проте багато дорослих, які у своєму дитинстві не настільки були пов'язані з віртуальним середовищем, як сучасні діти, не мають достатньо високого рівня цифрової компетентності, не розуміють важливості інтернет-технологій у сучасному житті. Тому, як наголошують І. Цісарук зі співавторами (2023), необхідно підвищувати кваліфікацію педагогів з питань інформаційної безпеки, працювати не навздогін, а на випередження. (с. 55).

В умовах воєнного стану в Україні великого значення в професійному розвитку вчителів набуває дистанційне навчання з активним використанням відкритих освітніх ресурсів, а також масових відкритих онлайн-курсів.

**Мета статті** – охарактеризувати українські і зарубіжні відкриті освітні ресурси і масові відкриті онлайн-курси щодо безпеки в інтернеті як елементи професійного розвитку педагогів, спрямованого на те, щоб навчити вчителів працювати з дітьми і молодими людьми, а також з їхніми батьками з означеної проблеми.

#### **Результати дослідження.**

**Відкриті освітні ресурси і масові відкриті онлайн-курси.** Уперше визначення відкритих освітніх ресурсів було прийнято ЮНЕСКО на Форумі 2002 р., присвяченому впливу відкритого програмного забезпечення на вищу освіту в країнах, що розвиваються. Наразі ЮНЕСКО подає таке визначення на своєму вебсайті: відкриті освітні ресурси – це навчальні, викладацькі та дослідницькі матеріали в будь-якому форматі і носії, які перебувають у суспільному надбанні або захищені авторським правом за відкритою ліцензією, яка дозволяє безкоштовний доступ, повторне використання, повторне призначення, адаптацію та перерозподіл іншими (UNESCO, 2019).

Формати і носії відкритих освітніх ресурсів варіюються в широкому діапазоні: освітні курси, підручники і посібники, відео- й аудіозаписи, графічні ресурси, плани уроків, тестові завдання, документи, роздатковий матеріал, програмне забезпечення тощо. R. F. Filho et al. (2023) звертають увагу на наукову дискусію, що точиться навколо питання, які відкриті ресурси можна називати освітніми.

Так, E. M. Mallmann, A. Nobre (2015) підкреслюють, що однією з умов того, щоб ресурс можна було вважати освітнім, є те, що він стає структурним елементом процесу викладання-навчання. Тобто освітній ресурс – це організований, систематичний і формальний навчальний матеріал для підтримки процесу викладання та навчання (р. 624). Проте наразі переважає ширша точка зору, яка визначає освітні ресурси як будь-які

засоби, матеріали або технології, що мають потенціал для навчання і можуть бути використані з освітньою чи науковою метою.

D. Wiley, J. Hilton (2014) позначають дозволи відкритих освітніх ресурсів за допомогою 5R (англ.) (р. 134–135):

1. Зберігання (*Retain*) – право створювати, завантажувати, зберігати, володіти та контролювати копії освітнього ресурсу.
2. Повторне використання (*Reuse*) – право використовувати освітній ресурс різними способами (наприклад, на вебсайті чи в освітньому процесі, у класі).
3. Перегляд (*Revise*) – право адаптувати, коригувати, модифікувати та змінювати освітній ресурс (наприклад, перекладати іншою мовою).
4. Ремікс (*Remix*) – право поєднувати оригінальний або відредагований вміст з іншим матеріалом, щоб створити новий контент.
5. Повторне розповсюдження (*Redistribute*) – право поділитися оригінальною, переглянутою чи реміксованою копією освітнього ресурсу з іншими (наприклад, опублікувати в інтернеті чи передати іншій особі).

V. Allman et al. (2024) доповнюють характеристику відкритих освітніх ресурсів за допомогою 3R (англ.), акцентуючи увагу на вимірах інклюзивності і соціальної справедливості – *recognition* (визнання), *representation* (представництво) та *redistribution* (перерозподіл).

Відкриті освітні ресурси є зручним засобом розширення освітніх можливостей і просування рівності в освіті, вони допомагають викладачам і студентам подолати такі бар'єри, як фізична відстань, доступність та інші соціально-економічні та культурні проблеми. Завдяки безкоштовному і легкому доступу вони вважаються економічно ефективною альтернативою традиційним підручникам, особливо в країнах, що розвиваються, або для студентів із вразливих, незахищених та недостатньо представлених груп (Kuo et al., 2024). Проведені дослідження також доводять, що використання відкритих ресурсів в освіті має потенціал для підвищення академічних досягнень студентів, їх залучення і мотивації до навчання (Hosman et al., 2024; Noone et al., 2024).

Ролі відкритих освітніх ресурсів і масових відкритих онлайн-курсів у професійному розвитку вчителів природничо-математичної освіти і технологій присвячено наукову розвідку В. Наумової, О. Бульвінської (2023), в якій проаналізовано популярні українські освітні платформи, а також досвід Інституту післядипломної освіти Київського столичного університету імені Бориса Грінченка, де викладачами розроблено й впроваджено авторські навчальні курси для вчителів.

Масові відкриті онлайн-курси також є перспективним видом безперервного професійного розвитку викладачів закладів освіти, оскільки пропонують доступність, гнучкість навчання, швидке реагування на освітні потреби слухачів, зокрема нову актуальну інформацію професійного спрямування. Масові відкриті онлайн-курси дають можливість слухачеві самостійно будувати власну освітню траєкторію, економлять час і фінанси на підвищення кваліфікації (Бульвінська, Капралова, 2022).

Проаналізовані українські і зарубіжні відкриті освітні ресурси щодо безпечної поведінки дітей в інтернеті ми систематизували за трьома категоріями:

- розроблені урядовими структурами;
- розроблені громадськими організаціями;
- масові відкриті онлайн-курси.

Відзначимо, що ця систематизація досить умовна, оскільки громадські організації, які опікуються безпекою дітей у цифровому просторі, підтримуються урядовими органами; вони також можуть запропонувати онлайн-курси для освітян, батьків і школярів.

Як переконливо доводить О. Черних (2019), технології соціально-педагогічного супроводу формування безпечної поведінки учнів в інтернеті мають включати освітній, комунікаційний, інформаційний компоненти.

*Освітній компонент* надає можливість для формування базових компетентностей безпечної поведінки в інтернеті, особистісного розвитку дітей, навчання батьків і вчителів, надання допомоги для подолання проблем, що виникають під час користування інтернетом.

*Комунікаційний компонент* реалізує відкритий діалог зі школярами щодо їхнього використання інтернету, скоординовану взаємодію між батьками, вчителями, різноманітними соціальними інститутами та дітьми.

*Інформаційний компонент* передбачає надання чіткої інформації про те, які онлайн-зміст і поведінка є незаконними і завдають шкоди гідності, безпеці, приватному життю тощо, та про можливості повідомити правоохоронні органи, батьків, учителів про такі зміст і поведінку в інтернеті.

Проаналізовані нами відкриті освітні ресурси щодо безпечної поведінки дітей у цифровому середовищі відповідають усім трьом компонентам.

**Відкриті освітні ресурси, розроблені урядовими структурами.** Таким прикладом є австралійська структура «eSafety» – перша у світі спеціальна державна організація, створена в 2015 р. для забезпечення безпеки громадян в інтернеті. Сайт цієї організації містить інформацію, призначену для різної цільової аудиторії: дітей, батьків, пенсіонерів, представників корінних народів та вразливих груп населення.

Проаналізуємо контент eSafety для освітян. Він включає поради, як створити безпечніше онлайн-середовище та як запобігти кібербулінгу в школах; безкоштовні програми професійного розвитку вчителів, щоб отримати знання, навички й інструменти для гарантування безпеки своєї школи в інтернеті, а також освітні ресурси, розраховані на учнів різних класів (інформаційні бюлетені, плакати, буклети, слайди, відео, відеоігри тощо). Для вчителів початкової школи, які навчають безпеки в інтернеті та запобігання кібербулінгу, розроблені навчальні модулі, а також плани уроків з методичним рекомендаціями, як краще використати представлені ресурси в освітньому процесі.

Так, наприклад, навчальний модуль «Be Secure» містить п'ять тематичних вправ, які можна вивчати окремо або проводити цілісно. Він досліджує критичне мислення, безпеку пристроїв, захист конфіденційності, витрачання грошей в Інтернеті та отримання допомоги і підтримки.

До кінця навчання за цим модулем учні зможуть:

- визначити та встановлювати межі особистої безпеки в інтернеті;
- розвивати навички аналізувати те, з чим вони стикаються в мережі;
- розвивати навички визначення проблемних ситуацій, які можуть вплинути на безпеку в інтернеті;
- вибирати стратегії пошуку допомоги для розв'язання небезпечних ситуацій у кіберпросторі.

Навчальний пакет «Be Secure» містить анімаційне відео з теми, інтерактивну дитячу вікторину, відеогру, план уроку для вчителя, робочий аркуш учня під назвою «Мій особистий план безпеки в інтернеті», а також шаблон сертифікату, в який можна вписати прізвища і роздати учням, щоб вони додавали на нього бейджі під час проходження вікторини. План уроку також містить посилання на відповідні вебсторінки, які учні можуть переглянути в розділі «eSafety Kids» розглянутого вебсайту (Be Secure. eSafety).

Для допомоги учителям тренери-експерти eSafety проводять живі онлайн-уроки безпеки в класі. Це віртуальні вебінари, під час яких тренер розповідає за допомогою слайдів-презентацій і сприяє взаємодії учнів за допомогою модерованих чатів і опитувань.

Учні зазвичай беруть участь у таких вебінарах у шкільному класі за допомогою смарт-дошки під керівництвом свого вчителя.

В Україні навчанням дітей щодо безпечної поведінки в інтернеті опікується **Міністерство цифрової трансформації**. З 2020 р. ним запущені веб-портал і мобільний застосунок «Дія» (сервіс із надання державних послуг онлайн). Одним з найбільш інноваційних і масових проєктів на цьому порталі є Національна онлайн-платформа «Дія. Цифрова освіта». На цій платформі розміщені освітні серіали з різних питань безпечної поведінки в інтернеті для педагогів, учнів і батьків. Наразі на онлайн-платформі доступні такі освітні серіали:

- «*Основи кібергігієни*» (елементарні правила кібергігієни під час користуванні електронною поштою, соціальними мережами, мобільними гаджетами);
- «*Персональна кібергігієна*» (основні принципи інформаційної гігієни у Всесвітній мережі);
- «*Кіберняні*» (захист особистих даних в інтернеті та попередження кібератак);
- «*Безпека дітей в інтернеті для батьків*» (убезпечення дітей від шкідливого і загрозливого контенту, кібербулінгу, суїцидальних інтернет-спілок та сексуальних загроз);
- «*Про кібербулінг для підлітків*» (причини та потенційні наслідки цькування, запобігання кібербулінгу і боротьба з ним);
- «*Обережно! Кібершахраї*» (види шахрайства в інтернеті та захист від них);
- «*Персональні дані*» (керування особистою інформацією і політика конфіденційності під час використання інтернет-сервісів і сайтів).

Окрім освітніх серіалів, на онлайн-платформі «Дія. Цифрова освіта» містяться інші матеріали: *гайд «Навіщо вам кібергігієна?»* (присвячений протидії хакерству і шахраям в інтернеті), *симулятор «Персональна кібергігієна»* (для перевірки своїх знань щодо безпечної поведінки в інтернеті), *цифрограм «Кіберграм»* (тест, який перевіряє вміння захищати особисту інформацію).

*Проєкт подкастів Qwerty*, присвячений безпечній поведінці в інтернеті, розробив **Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України**. Цей проєкт названий на честь комбінації букв QWERTY, розташованих поряд на клавіатурі комп'ютера. Ця комбінація є одним із найпопулярніших паролів у світі – його використовують близько 18 мільйонів людей. У подкастах Qwerty фахівці розповідають про кібергігієну, блокчейн та хакерів, наводять кейси світових кібератак.

На сайті **Міністерства освіти і науки України** в спеціальній вкладці «*Безпека дітей в інтернеті*» розміщено важливі матеріали для батьків і педагогів. Інститут модернізації змісту освіти Міністерства освіти і науки України пропонує довідники, посібники, методичні рекомендації для вчителів, як інтегрувати питання безпеки школярів у цифровому просторі в освітні програми за допомогою інтерактивних планів уроків і робочих зошитів.

Так, посібник «*Керівництво із соціально-педагогічного супроводу формування безпечної поведінки підлітків в інтернеті*» (2018), схвалений Міністерством освіти і науки України для використання в закладах загальної середньої освіти, містить теоретичні питання безпечної поведінки в Інтернеті, опис занять та 8 тренінгових вправ з розвитку базових компетентностей безпечної поведінки підлітків в інтернеті, анкету щодо виявлення рівня безпечної поведінки підлітків в інтернеті, шаблони цифрових бейджів як мотиваторів для учнів і підтвердження розвитку вчителів, а також плани заходів для педагогів та батьків.

**Відкриті освітні ресурси, розроблені громадськими організаціями.** З 2003 р. громадська організація «**Common Sense**» (США) є провідним джерелом рекомендацій

щодо розваг і технологій у цифровому світі для сімей і шкіл. Організація висвітлює законодавство, пов'язане із цифровими технологіями, і пропонує рішення, які захищають конфіденційність споживачів, сприяють кращому зв'язку для здобувачів освіти і сімей. Фахівці Common Sense також оцінюють фільми, телевізійні шоу, подкасти, книги тощо і надають поради щодо викликів і можливостей цифрового вибору сімей.

Окрема сторінка *Common Sense Education* присвячена підтримці шкіл для розширення можливостей нового покоління цифрових громадян. Учителі можуть скористатись безкоштовною навчальною програмою із цифрового громадянства та порадами експертів. Відкриті освітні ресурси включають уроки для різних за віком учнів і темами.

Наприклад, урок для 9 класу «*Захист онлайн-репутації. Як ви можете поважати приватність інших в Інтернеті?*» містить план уроку, відео для уроку, слайди, вікторину, роздатковий матеріал, глосарій з термінами, які будуть введені на уроці, а також матеріали-поради для батьків і ресурси для залучення сім'ї (*Protecting Online Reputations. Common Sense*).

Проаналізуємо декілька українських освітніх проєктів, створених громадськими організаціями. «*Школу онлайн-безпеки дітей*» запустила громадська організація «МІНЗМІН» за сприяння Міністерства цифрової трансформації України. На сайті представлено записи і презентації онлайн-уроків, а також поради для батьків і вчителів, як забезпечити максимальну користь інтернету для дітей, які загрози чекають на дітей в онлайн-середовищі та як від них убезпечити.

МІНЗМІН також презентує перший в Україні онлайн-курс «*Цифрові права та безпека дитини*» із 7 тем, кожна з яких містить відеоурок, чек-лист (з коротким підсумком уроку, потрібними покликаннями на рекомендовану літературу, правову інформацію, відеоресурси чи кінофільми, на відеоігри з теми), тест, який допоможе перевірити засвоєння уроку.

Корисними для вчителів будуть розроблені МІНЗМІН *плани уроків про приватність в інтернеті* (для 1–4, 5–8, 9–11 класів), в які входять мета, хід уроку, словник термінів для уроку, необхідні матеріали, корисні посилання на інтернет-ресурси для проведення уроку, рекомендовані матеріали з урахуванням віку учнів.

Громадська організація «**Стоп Секстинг**» за підтримки Міністерства освіти і науки, Міністерства цифрової трансформації України та Уповноваженого Президента України з прав дитини створили навчальні матеріали для батьків і педагогів щодо упередження та протидії сексуальному насиллю в Інтернеті.

Стоп Секстинг пропонує довідкові й інформаційні матеріали, онлайн-курс, рекомендовану літературу і фільми, подкасти, онлайн-виставку для батьків. Для навчання директорів та педагогів запропонований онлайн-курс «*Безпечне онлайн-середовище у закладі освіти*» (різні курси для різних категорій освітян – директорів шкіл і вчителів).

Учителі також можуть скористатись готовими уроками щодо безпечної поведінки дітей в інтернеті. Важливо, що ці освітні ресурси систематизовані для різних категорій учнів: дошкільного віку (0–6 років), початкової школи (7–9 років), середньої школи (10–15 років), старшої школи (16–18 років), а також для дітей з особливими освітніми потребами.

Так, для учнів старшої школи Стоп Секстинг розробила такі освітні матеріали:

- Квест для 9–11 класу «Тест Білборда та кохання в інтернеті»;
- Урок для 7–11 класів «Інтимне селфі в інтернеті»;
- Урок для 7–11 класів «(Не)дитячі стосунки online»;
- Урок для 9–11 класів «(Не)безпека в час війни»;
- Урок для 9–11 класів «Онлайн-загрози в час війни: як захистити себе?»

Уроки включають посібники, плани уроків, презентації, тести, квести, додаткові роздаткові матеріали, записи вебінарів з певної теми тощо. Стоп Секстинг заохочує вчителів до проведення уроків з теми: за проведення кожного уроку передбачається сертифікат про підвищення кваліфікації.

**Масові відкриті онлайн-курси. EdX** – інтернет-платформа масових відкритих інтерактивних курсів університетського рівня, заснована Массачусетським технологічним інститутом і Гарвардським університетом у травні 2012 р., пропонує такі навчальні курси для вчителів.

Курс *«Почніть викладати комп'ютерну техніку в початкових школах: Підготовка до навчання дітей віком від 5 до 11 років»* призначений для вчителів, які тільки починають або мають невеликий досвід викладання комп'ютерної техніки для учнів початкової школи. Курс розрахований на 4 тижні, і 3-й тиждень його навчального плану присвячений безпечному, захищеному й ефективному використанню комп'ютерної техніки й інтернету. (Get Started Teaching Computing in Primary Schools: Preparing to teach 5–11 year olds. EdX).

Курс *«Навчіть підлітків обчислювати: Кібербезпека»* адресований учителям, які проводять відповідні уроки для дітей віком 14–16 років, розрахований на 3 тижні і охоплює (Teach teens computing: Cybersecurity. EdX):

- основні концепції кібербезпеки;
- різні типи кібератак: атаки соціальної інженерії, зловмисне програмне забезпечення, ін'єкції SQL, шкідливі боти та фізичні загрози для даних, пристроїв і мереж;
- інструменти для захисту даних, пристроїв і мереж: надійні паролі, біометрія, двофакторна автентифікація (2FA), антивірусне програмне забезпечення, брандмауери та CAPTCHA;
- підходи до кібербезпеки, такі, як очищення вхідних даних, добре розроблені протоколи безпеки та системи контролю доступу до даних і мережі.

Курс *«Кібербулінг»* допоможе вчителям зрозуміти, який вплив кібербулінг може мати на окремих людей і громади, а також як його розпізнати, запобігти йому чи розв'язати вже наявну проблему в таких сферах, як соціальна робота й освіта. Курс спрямований на те, щоб навчити вчителів працювати з дітьми і молодими людьми, а також з їхніми батьками для розпізнавання і готовності до втручання до того, як ситуація загостриться. Важливим кроком є також співпраця з правоохоронними органами для розроблення політики та протоколів боротьби з кібербулінгом для того, щоб жертви отримували підтримку та необхідні їм ресурси (Cyberbullying-An Overview. EdX).

Навчання за курсом «Кібербулінг» розраховано на 4 тижні. Навчальний план містить такі модулі:

- вступ до кібербулінгу;
- форми кібербулінгу;
- причини кібербулінгу;
- наслідки кібербулінгу;
- запобігання кібербулінгу та повідомлення про нього.

Слід зазначити, що проаналізовані масові відкриті онлайн-курси мають безкоштовний доступ, але платну сертифікацію, яка дає право на необмежене користування матеріалами курсу. Для тих, хто пройшов курс безкоштовно, доступ до матеріалів обмежений певним періодом.

Масові відкриті онлайн-курси на двох відомих українських освітніх платформах – **«Prometheus»** та **«EdEra»** – є повністю безкоштовними.

**Prometheus** пропонує кілька курсів із цифрової грамотності. Серед них – *«Безпека в інтернеті під час війни: практичний курс»*. Опанування його матеріалами допоможе

вчителю, батькам, учням та всім зацікавленим навчитися захищати свою особисту інформацію в цифровому середовищі й уникати онлайн-шахрайств. Мета курсу – сформулювати чи розвинути вміння критичного сприйняття інформації в інформаційному просторі, навчити безпечно й ефективно використовувати цифрові інструменти, зокрема соціальні мережі. Курс пропонує чотири модулі, а саме:

- інформаційна грамотність і безпека в інтернеті;
- комунікація та безпечна взаємодія в цифровому суспільстві;
- приватність і цифрове середовище;
- потенційні ризики та інформаційна грамотність.

Курс «*Основи інформаційної безпеки*» присвячений забезпеченню захисту гаджетів від кіберзагроз, комп'ютерних вірусів, а також захист персональної інформації у цифровому світі, зокрема власних фінансів. Курс корисний для всіх користувачів соціальних мереж, електронної пошти, покупців в онлайн-магазинах, та й усіх, хто шукає інформацію в інтернеті. Цей курс знайомить не тільки із сучасними загрозами для комп'ютерів, смартфонів, планшетів і способами захисту від шкідливого програмного забезпечення, а й з історією комп'ютерних вірусів, їх основними видами. Курс також надає інформацію про правила безпечної роботи з мобільними пристроями і захисту особистої інформації в інтернеті. Важливою частиною курсу є безпека в умовах інформаційної війни та кібервійни.

Курс «*Цифрова безпека на персональному рівні*» також призначений для широкої аудиторії. Основні теми курсу:

- цифрові загрози;
- оцінка персональних ризиків у користуванні інтернетом;
- фішинг як вид шахрайства;
- загрози використання однакових паролів на різних сайтах;
- критерії надійності паролів та генерація складних комбінацій для захисту особистої інформації;
- способи збереження паролів;
- додаткові налаштування безпеки акаунтів;
- захист гаджетів від короткочасного та тривалого фізичного доступу.

Курс «*Цифрові комунікації в глобальному просторі*» поширює знання про інформаційні технології серед початківців в інформаційному середовищі і осіб, які не мають технічних навичок. Курс дає можливість дізнатися про цифрові комунікації; веб-ресурси та їх створення; хмарні технології; основи SMM (інструментарій роботи з соціальними медіа) та цифровий етикет. До змісту курсу входить і тема захисту від кіберзагроз.

Курс «*Інформаційна безпека*» присвячений не стільки технічним засобам захисту в кіберпросторі, скільки вмінням аналізувати відомості з інтернету, викривати фейки, захищатися від неправдивої чи сумнівної інформації, уникати зловмисних маніпуляційних впливів.

Основам медіаграмотності, вмінням перевіряти інформаційні повідомлення, протистояти маніпуляціям у рекламі навчає курс «*Години медіаграмотності*» від студії онлайн-освіти «**EdEra**». Курс буде корисний для вчителів, які викладають основи медіаграмотності; його можна рекомендувати учням, батькам, освітнім управлінцям і всім, хто зацікавлений навчитися шукати інформацію, усвідомлювати її і перевіряти її правдивість.

Проаналізуємо ще декілька онлайн-курсів з медіаграмотності від EdEra. «*Very Verified: онлайн-курс з медіаграмотності*» пояснює, як орієнтуватися в інформації



довкола та як розпізнавати дезінформацію та пропаганду. Цей курс містить короткі статті, навчальні відео, інтерв'ю, інтерактивні завдання, тести та додаткові матеріали.

Платформа критичного мислення «Подумай двічі!» від EdEra теж допомагає навчитись, як не потрапити на гачок фейків і маніпуляцій в інтернеті, розвинути аналітичні уміння і отримати базові навички медіаграмотності. EdEra пропонує захопливий формат платформи – освітня онлайн-гра. Для участі в грі треба обрати персонажа серед трьох категорій – школярів, учителів або громадських організацій.

**Висновки.** Всесвітня мережа «Інтернет» стала невід'ємною складовою життя суспільства. У всьому світі спостерігається тенденція цифровізації багатьох сфер життєдіяльності людини, зокрема й освіти; інтернет несе в собі великий інформаційний та освітній потенціал. Для збереження безпеки в інтернеті діти повинні мати знання, уміння і навички, які дозволять мінімізувати негативні впливи цифрового середовища. Подолання ризиків порушень прав дитини в інтернеті покладається насамперед на батьків і педагогічних працівників. Отже, вчителі мають постійно підвищувати свою обізнаність щодо проблеми поведінки учнів у цифровому середовищі, щоб сформувати у дітей і підлітків чіткі правила і вміння користуватись інтернетом безпечно. Велику допомогу в цьому вчителям надають відкриті освітні ресурси – підручники і посібники, відео- й аудіозаписи, графічні ресурси, плани уроків, тестові завдання, документи, роздатковий матеріал, програмне забезпечення тощо, а також масові відкриті онлайн-курси як зручний та ефективний вид безперервного професійного розвитку педагогів.

Ми проаналізували українські і зарубіжні відкриті освітні ресурси щодо безпечної поведінки дітей в інтернеті і систематизували їх за трьома категоріями: розроблені урядовими структурами; розроблені громадськими організаціями; масові відкриті онлайн-курси. Проаналізовані ресурси мають беззаперечний потенціал для їх використання педагогами у навчанні дітей і батьків.

**Перспективою подальших досліджень** вважаємо розроблення практичних рекомендацій щодо ефективного використання відкритих освітніх ресурсів з безпеки дітей в інтернеті в освітньому процесі.

### Список використаної літератури

1. Бульвінська О. І., Капралова І. М. Використання масових відкритих онлайн-курсів у професійному розвитку викладачів закладів вищої освіти. *Інформаційні технології і засоби навчання*. 2022. № 2 (88). С. 273–290. DOI: <https://doi.org/10.33407/itlt.v88i2.4568>
2. Керівництво із соціально-педагогічного супроводу формування безпечної поведінки підлітків в Інтернеті. *Центр кращого інтернету*. 2018. URL: <https://betterinternetcentre.org/?p=64> (дата звернення: 1.11.2024).
3. Міністерство освіти і науки України. *Безпека дітей в інтернеті*. URL: <https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robota-ta-zakhist-prav-ditini/bezpeka-ditey-v-interneti> (дата звернення: 1.11.2024).
4. Міністерство цифрової трансформації України. *Дія. Цифрова освіта*. URL: <https://thedigital.gov.ua/projects/osvita> (дата звернення: 3.11.2024).
5. МІНЗМІН. URL: <https://minzmin.org.ua/projects/> (дата звернення: 1.11.2024).
6. Наумова В., Бульвінська О. Відкриті освітні платформи для професійного розвитку вчителів природничо-математичної освіти і технологій. *Неперервна професійна освіта: теорія і практика*. 2023. № 3 (76). С. 75–83. DOI: <https://doi.org/10.28925/1609-8595.2023.3.7>
7. Петренко С. І. Аналіз проблеми безпечної роботи учнів початкових класів у мережі інтернет. *Вісник університету імені Альфреда Нобеля. Серія «Педагогіка і психологія». Педагогічні науки*. 2020. № 1 (19). С. 85–91. DOI: <https://doi.org/10.32342/2522-4115-2020-1-19-9>
8. Стоп Секстинг. URL: <https://stop-sexting.in.ua/> (дата звернення: 3.11.2024).

9. Цісарук І., Цісарук В., Омельчук О. Інформаційна безпека учасників освітнього процесу як елемент безпечного освітнього середовища. *Науковий вісник Кременецької обласної гуманітарно-педагогічної академії ім. Тараса Шевченка. Серія: Педагогічні науки*. 2023. № 16. С. 51–57. DOI: <https://doi.org/10.32782/2410-2075-2023-16.7>
10. Черних О. О. Формування безпечної поведінки дітей в інтернеті як актуальний напрям соціально-педагогічного супроводу. *Інновації педагогічної освіти в умовах викликів сьогодення: монографія* / за наук. ред. С. Я. Харченка. Київ: Талком, 2019. С. 305–330. URL: <http://surl.li/yqdcua> (дата звернення: 1.11.2024).
11. Allman B., Kimmons R., Dickson-Deane C., Bozkurt A., Warr M., Stefaniak J., Dash M., Bondah F. E. EdTechnica: a vision of an educational publishing community of practice that is accessible, flexible, and just. *International Journal of Educational Technology in Higher Education*. 2024. № 21. Art. 37. DOI: <https://doi.org/10.1186/s41239-024-00466-1>
12. Common Sense. URL: <https://www.common sense.org/> (дата звернення: 1.11.2024).
13. EdEra. URL: <https://ed-era.com/> (дата звернення: 3.11.2024).
14. edX Online Courses. URL: <https://www.edx.org/> (дата звернення: 1.11.2024).
15. eSafety Commissioner. URL: <https://www.esafety.gov.au/> (дата звернення: 3.11.2024).
16. Filho R. C. M. F., da Silva, F.B., de Quevedo Prestes de Carvalho, C., Barros, T. M. Recommendations to Production and Sharing of Open Educational Resources with Accessibility: The ProEDU Experience. M. H. Rioux, J. Viera, A. Buettgen, E. Zubrow (Eds.). *Handbook of Disability*. Singapore: Springer, 2023. DOI: [https://doi.org/10.1007/978-981-16-1278-7\\_60-2](https://doi.org/10.1007/978-981-16-1278-7_60-2)
17. Hosman L. Nova R., Naji O. A. A. M., Alsaka L. An Overview of Arabic Language Open Educational Resources (OER) for Primary and Secondary Education and Their Use in Offline Environments. *Electronic Journal of e-Learning*. 2024. № 22 (9). DOI: <https://doi.org/10.34190/ejel.22.9.3616>
18. Kuo Y-C, Kuo Y-T, Tseng H. Exploring the Factors That Influence K-12 Teachers' Use of Open Educational Resources. *Education Sciences*. 2024. № 14 (3). Art. 276. DOI: <https://doi.org/10.3390/educsci14030276>
19. Mallmann E. M., Nobre A. Dos objetos de aprendizagem aos recursos educacionais (abertos). M. J. Gomes, A. J. Osório, & L. Valente (Eds.). *Challenges 2015: meio século de TIC na educação – Half a century of ICT in Education – Atas da IX Conferência Internacional de TIC na Educação*. Minho: Centro de Competência TIC na Educação do Instituto de Educação da Universidade do Minho, 2015. P. 622–632. URL: <https://repositorioaberto.uab.pt/handle/10400.2/6878> (дата звернення: 1.11.2024).
20. Noone J., Champieux R., Taha A., Gran-Moravec M., Hatfield L., Cronin Sh., Shoemaker Rh. Implementing open educational resources: Lessons learned. *Journal of Professional Nursing*. 2024. № 55. P. 65–69. DOI: <https://doi.org/10.1016/j.profnurs.2024.08.005>
21. Prometheus. URL: <https://prometheus.org.ua/> (дата звернення: 1.11.2024).
22. QWERTY. *Spotify*. URL: [https://podcasters.spotify.com/pod/show/qwerty05?fbclid=IwAR0t7umpfvafM61K0WZcv-AzdzPZeMsRdWoHiiT5hZjWHN6MOiRGIMKNYZ\\_8](https://podcasters.spotify.com/pod/show/qwerty05?fbclid=IwAR0t7umpfvafM61K0WZcv-AzdzPZeMsRdWoHiiT5hZjWHN6MOiRGIMKNYZ_8) (дата звернення: 1.11.2024).
23. UNESCO. Open Educational Resources. 2019. URL: <https://www.unesco.org/en/open-educational-resources> (дата звернення: 1.11.2024).
24. Wiley D., & Hilton III J. L. (2018). Defining OER-enabled pedagogy. *The International Review of Research in Open and Distributed Learning* № 19 (4). P. 133–147. DOI: <https://doi.org/10.19173/irrodl.v19i4.3601>

## References

- Bulvinska, O. I, Kapralova, I. M. (2022). Використання масових відкритих онлайн курсів у професійному розвитку викладачів закладів вищої освіти [Use of massive open online courses in the professional development of university teachers]. *Information Technologies and Learning Tools*, 2 (88), 273–290. <https://doi.org/10.33407/itlt.v88i2.4568>

- Kerivnictvo iz socialno-pedagogichnogo suprovodu formuvannya bezpechnoyi povedinki pidlitkiv v Interneti (2018). *Tsentr krashchogo internetu*. <https://betterinternetcentre.org/?p=64>
- Ministry of Education and Science of Ukraine. *Bezpeka ditei v interneti [Safety of children on the Internet]*. <https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robota-ta-zakhist-prav-ditini/bezpeka-ditey-v-interneti>
- Ministry of Digital Transformation. *Diia. Tsifrova osvita [Action. Digital education]*. <https://thedigital.gov.ua/projects/osvita>
- МИНЗМІН [MINZMIN]. <https://minzmin.org.ua/projects/>
- Naumova, V., Bulvinska, O. (2023). Vidkriti osvitni platformi dlya profesiinogo rozvitku vchiteliv prirodnicHO-matematichnoї osviti i tekhnologii [Open Educational Platforms for The Professional Development of Teachers of Science, Mathematics and Technology]. *Continuing Professional Education: Theory and Practice*, 76 (3), 75–83. <https://doi.org/10.28925/1609-8595.2023.3.7>
- Petrenko, S. I. (2020). Analiz problemi bezpechnoї roboti uchniv pochatkovikh klasiv u merezhi internet [The analysis of the problem of safe work on the internet for primary schoolchildren]. *Bulletin of Alfred Nobel University. Series: Pedagogy and Psychology*, 1 (19), 85–91. <https://doi.org/10.32342/2522-4115-2020-1-19-9>
- Tsisaruk, I., Tsisaruk, V., Omelchuk, O. (2023). Informatsiina bezpeka uchashchikiv osvitnogo protsesu yak yelement bezpechnogo osvitnogo seredovishcha [Information Security of Participants in the Educational Process as an Element of a Secure Educational Environment]. *Scientific Bulletin of Kremenets Taras Shevchenko Regional Academy of Humanities and Pedagogy. Series: Pedagogical Sciences*, 16, 51–57. <https://doi.org/10.32782/2410-2075-2023-16.7>
- Chernykh, O. O. (2019). Formuvannya bezpechnoї povedinki ditei v interneti yak aktualnii napryam sotsialno-pedagogichnogo suprovodu [Formation of children's safe behavior on the Internet as an actual direction of social and pedagogical support]. In S. Ya. Kharchenko (Ed.), *Innovatsii pedagogichnoї osviti v umovakh viklikiv sHogodennya: monografiya* (p. 305–330). Talkom. <http://surl.li/yqdcua>
- Allman, B., Kimmons, R., Dickson-Deane, C., Bozkurt, A., Warr, M., Stefaniak, J., Dash, M., Bondah, F. E. (2024). EdTechnica: a vision of an educational publishing community of practice that is accessible, flexible, and just. *International Journal of Educational Technology in Higher Education*, 21, 37. <https://doi.org/10.1186/s41239-024-00466-1>
- Common Sense*. <https://www.commonsense.org/>
- EdEra*. <https://ed-era.com/>
- edX Online Courses*. <https://www.edx.org/>
- eSafety Commissioner*. <https://www.esafety.gov.au/>
- Filho, R. C. M. F., da Silva, F.B., de Quevedo Prestes de Carvalho, C., Barros, T. M. (2023). Recommendations to Production and Sharing of Open Educational Resources with Accessibility: The ProEDU Experience. In M. H. Rioux, J. Viera, A. Buettgen, E. Zubrow (Eds.), *Handbook of Disability*. Springer. [https://doi.org/10.1007/978-981-16-1278-7\\_60-2](https://doi.org/10.1007/978-981-16-1278-7_60-2)
- Hosman, L. Nova, R., Naji, O. A. A. M., Alsaka, L. (2024). An Overview of Arabic Language Open Educational Resources (OER) for Primary and Secondary Education and Their Use in Offline Environments. *Electronic Journal of e-Learning*, 22 (9). <https://doi.org/10.34190/ejel.22.9.3616>
- Kuo, Y.-C., Kuo, Y.-T., Tseng, H. (2024). Exploring the Factors That Influence K-12 Teachers' Use of Open Educational Resources. *Education Sciences*, 14 (3), 276. <https://doi.org/10.3390/educsci14030276>
- Mallmann, E. M., & Nobre, A. (2015). Dos objetos de aprendizagem aos recursos educacionais (abertos). In M. J. Gomes, A. J. Osório, L. Valente (Eds.), *Challenges 2015: meio século de TIC na educação – Half a century of ICT in Education – Atas da IX Conferência Internacional de TIC na Educação* (pp. 622–632). Centro de Competência TIC na Educação do Instituto de Educação da Universidade do Minho. <https://repositorioaberto.uab.pt/handle/10400.2/6878>
- Noone, J., Champieux, R., Taha, A., Gran-Moravec, M., Hatfield, L., Cronin, Sh., Shoemaker, Rh. (2024). Implementing open educational resources: Lessons learned. *Journal of Professional Nursing*, 55, 65–69. <https://doi.org/10.1016/j.profnurs.2024.08.005>
- Prometheus*. <https://prometheus.org.ua/>

QWERTY.

Spotify.

<https://podcasters.spotify.com/pod/show/qwerty05?fbclid=IwAR0t7umpfvafM61K0WZcv-AzdzPZeMsRdWoHiiT5hZjWHN6MOiRGIMKNYZ8>

UNESCO (2019). *Open Educational Resources*. <https://www.unesco.org/en/open-educational-resources>

Wiley, D., & Hilton III, J. L. (2018). Defining OER-enabled pedagogy. *The International Review of Research in Open and Distributed Learning*, 19 (4), 133–147. <https://doi.org/10.19173/irrodl.v19i4.3601>

Стаття надійшла до редакції 4.11.2024

Прийнято до друку 28.11.2024

## ZARZĄDZANIE BEZPIECZEŃSTWEM UCZNIÓW W INTERNECIE: OTWARTE ZASOBY EDUKACYJNE ABY POMÓC EDUKATOROM

**Victoria Naumova**

<https://orcid.org/0000-0002-0114-4749>

Starszy wykładowca na Wydziale Edukacji Przyrodniczej I i Matematyki i Technologii,  
Instytut Kształcenia Podyplomowego,  
Kijowski Uniwersytet Metropolitalny im. Borysa Grinczenki,  
17 Pavlo Tychynyna Ave. 02152, Kijów, Ukraina, [v.naumova@kubg.edu.ua](mailto:v.naumova@kubg.edu.ua)

**Oksana Bulvinska**

<https://orcid.org/0000-0002-6764-4340>

Kandydat nauk pedagogicznych, starszy pracownik naukowy,  
Starszy pracownik naukowy w Bibliotece,  
Kijowski Uniwersytet Metropolitalny im. Borysa Grinczenki  
ul. Levka Lukyanenko 13-b, 04207, Kijów, Ukraina, [o.bulvinska@kubg.edu.ua](mailto:o.bulvinska@kubg.edu.ua)

*Artykuł poświęcony jest analizie ukraińskich i zagranicznych otwartych zasobów edukacyjnych, które wspierają rozwój zawodowy pedagogów w zakresie organizacji pracy z uczniami nad bezpiecznym korzystaniem z internetu. Podkreślono, że to właśnie nauczyciele odgrywają kluczową rolę w kształtowaniu u uczniów umiejętności bezpiecznego zachowania w przestrzeni cyfrowej, zarządzania danymi osobowymi, oceny treści cyfrowych oraz zasad komunikacji w mediach społecznościowych. Zaznaczono, że otwarte zasoby edukacyjne to materiały dydaktyczne, naukowe i badawcze w dowolnym formacie i nośniku, które znajdują się w domenie publicznej i mogą być swobodnie wykorzystywane w procesie edukacyjnym. Do otwartych zasobów edukacyjnych zalicza się podręczniki, przewodniki, nagrania wideo i audio, materiały graficzne, plany lekcji, zadania testowe, dokumenty, materiały do druku oraz oprogramowanie. Masowe otwarte kursy online (MOOC) dostarczają aktualnych informacji zawodowych i stanowią elastyczną oraz dostępną formę kształcenia i podnoszenia kwalifikacji nauczycieli. W artykule przeanalizowano ukraińskie i zagraniczne otwarte zasoby edukacyjne dotyczące bezpiecznego zachowania dzieci w internecie, klasyfikując je według trzech kategorii: Zasoby opracowane przez struktury rządowe. Zasoby stworzone przez organizacje pozarządowe. Masowe otwarte kursy online. Podkreślono, że analizowane zasoby łączą komponenty edukacyjne, komunikacyjne i informacyjne, mając ogromny potencjał do wykorzystania przez nauczycieli w pracy z dziećmi i rodzicami.*

**Słowa kluczowe:** *bezpieczne zachowanie w internecie, otwarte zasoby edukacyjne, masowe otwarte kursy online, rozwój zawodowy nauczycieli, środowisko cyfrowe.*

**MANAGING STUDENT SAFETY ON THE INTERNET:  
OPEN EDUCATIONAL RESOURCES TO HELP EDUCATORS**

**Viktoriiia Naumova**

<https://orcid.org/0000-0002-0114-4749>

Senior Lecturer of the Chair of Natural Sciences and Mathematics Education and Technologies,  
Borys Grinchenko Kyiv Metropolitan University, 17 Pavlo Tychyna Ave., 02152 Kyiv, Ukraine,  
[v.naumova@kubg.edu.ua](mailto:v.naumova@kubg.edu.ua)

**Oksana Bulvinska**

<https://orcid.org/0000-0002-6764-4340>

PhD (in Pedagogy), Senior Researcher, Senior Researcher of Library,  
Borys Grinchenko Kyiv Metropolitan University, 13-b Levko Lukianenko Str., 04207 Kyiv,  
Ukraine, [o.bulvinska@kubg.edu.ua](mailto:o.bulvinska@kubg.edu.ua)

*The article focuses on analyzing Ukrainian and international open educational resources that contribute to the professional development of educators in organizing activities for teaching students safe internet practices. It highlights the critical role of teachers in equipping students with skills for safe behavior in the digital space, managing personal data online, evaluating digital content, and adhering to communication rules on social media. The importance of open educational resources (OERs) is emphasized, defining them as educational, teaching, and research materials available in the public domain and free to use in the educational process. OERs encompass various tools, materials, or technologies with educational potential: textbooks, manuals, videos, audio recordings, graphic resources, lesson plans, test assignments, documents, handouts, software, and more. Massive Open Online Courses (MOOCs) are highlighted as a modern, accessible, and flexible means of professional development for educators, offering up-to-date professional information. The article categorizes the analyzed Ukrainian and international open educational resources for safe online behavior into three groups: those developed by government agencies, those created by non-governmental organizations, and MOOCs. It is underlined that these resources integrate educational, communication, and informational components, making them highly beneficial for educators in teaching children and parents about internet safety.*

**Keywords:** *digital environment, massive open online courses, open educational resources, professional development of educators, safe internet behavior.*