

в (дата звернення: 24.05.2025).

4. Наказ Міністерства юстиції, МВС, Офісу Генпрокурора від 22.07.2024 № 2176/5/501/176 "Про реалізацію пілотного проєкту «Програма відновного правосуддя за участю неповнолітніх» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/z1116-24> (дата звернення: 19.05.2025).

5. General comment No. 12 (2009): The right of the child to be heard, CRC/C/GC/12 / Office of the United Nations High Commissioner for Human Rights (OHCHR). URL: <https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf> (дата звернення: 23.05.2025).

6. Recommendation CM/Rec (2018)7 of the Committee of Ministers: Guidelines to respect, protect and fulfil the rights of the child in the digital environment / Council of Europe. URL: <https://rm.coe.int/children-digital-environment-guidelines-en/16808d881a> (дата звернення: 30.05.2025).

## **ВІДПОВІДАЛЬНІСТЬ ВЧИТЕЛЯ ЗА БЕЗПЕКУ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ В ЦИФРОВУ ЕПОХУ. Кравчина О.Є.**

Інститут цифровізації освіти НАПН  
України  
ORCID ID: 0000-0002-3903-0835

Відповідальність вчителя за безпеку персональних даних дітей залишається надзвичайно важливою, особливо, з огляду на те якими темпами відбувається цифровізація освіти. Використання онлайн-платформ, освітніх додатків, хмарних сервісів та інших цифрових інструментів стало невід'ємною частиною навчального процесу, в якому учителі працюють з чутливими персональними даними учнів (такі як імена, дати народження, контакти, оцінки чи медична інформація), що збільшує ризик витоку даних. Водночас кібератаки, фішингові схеми, витоки інформації й інші загрози

активно впливають на освіту. Оскільки дані дітей є особливо вразливими й можуть стати об'єктом маніпуляцій, шахрайства або кібербулінгу, на вчителів покладається відповідальність за їхній надійний захист. Учителі мають бути прикладом у створенні безпечного цифрового простору, захищаючи інформацію про учнів та навчаючи їх основам цифрової грамотності, що допомагає дітям орієнтуватися у світі технологій і уникати шкідливих ситуацій в інтернеті. Нажаль не всі вчителі мають належний рівень знань у сфері кібербезпеки чи законодавчих вимог щодо роботи з персональними даними. Це доводить важливість інтеграції відповідних програм підвищення кваліфікації для вчителів.

У багатьох країнах законодавство регулює процедури зберігання та обробки персональних даних дітей. В Україні ухвалено кілька документів, які визначають норми захисту персональних даних у сфері освіти. У «Концепції виховання дітей та молоді в цифровому просторі» сформульовано стратегічні напрями розвитку в цифровому середовищі, одним із ключових принципів якого є забезпечення конфіденційності та безпеки [1]. Професійний стандарт «Вчитель закладу загальної середньої освіти» акцентує увагу на інформаційно-цифровій компетентності педагогів. У ньому зазначено, що викладачі мають володіти навичками захисту персональних даних учнів, використовувати безпечні інформаційні системи та дотримуватись етичних норм при роботі з конфіденційною інформацією. [2]. Освітній омбудсмен підкреслює важливість дотримання закладами освіти принципів захисту персональних даних, особливо під час використання електронних журналів, відеоконференцій та цифрових платформ. [3]. Основний нормативний акт, який регулює процеси збору, зберігання та обробки персональних даних, — це Закон України «Про захист персональних даних». У ньому уточнюється поняття персональних даних, порядок їх обробки, а також передбачені наслідки за порушення цього закону [4]. Недотримання законодавчих норм може призвести до накладення штрафів згідно зі статтею 188-39 Кодексу України про адміністративні правопорушення. [5]. Учителям необхідно

суворо дотримуватися цих правил, адже їх ігнорування загрожує не лише штрафами, а й серйозною юридичною відповідальністю.

У сучасну цифрову епоху персональні дані учнів потрапляють у зону підвищеного ризику через численні загрози, характерні для віртуального середовища. Насамперед існує ймовірність несанкціонованого доступу до інформації, що може статися внаслідок хакерських атак на освітні платформи або електронні журнали, витоку облікових даних користувачів чи використання спільних акаунтів без належних механізмів автентифікації. Іншою проблемою є неконтрольована передача або зберігання даних. Це може проявлятися через передачу персональної інформації третім сторонам без отримання згоди, а також унаслідок розміщення даних на незахищених пристроях чи в хмарних сервісах без належного рівня шифрування. Особливо небезпечним є неправильне використання зображень учнів. До таких випадків належить публікація фотографій або відео в соціальних мережах чи на сайтах навчальних закладів без належної згоди, а також поширення відеозаписів онлайн-уроків без відповідного контролю та регламентації. Додаткову загрозу становить використання ненадійного або недостатньо перевіреного програмного забезпечення. Освітні додатки без захищеної політики конфіденційності, прихований збір даних чи порушення норм GDPR або українського законодавства несуть потенційну небезпеку для приватності учнів. До цього додається людський фактор, коли помилки персоналу стають причинами витоку даних. Це може проявлятися як недбале поводження з паролями, випадкове надсилання особистої інформації стороннім особам або обговорення конфіденційної учнівської інформації у невідповідних умовах – наприклад, у відкритих публічних чи неформальних просторах. Суттєву роль у створенні загроз також відіграє відсутність чітких політик захисту даних у закладах освіти. Недостатньо сформульовані процедури обробки персональної інформації або невизначеність щодо відповідальності за їх порушення суттєво підвищують рівень уразливості. Окрему категорію загроз представляє соціальна інженерія. Фішингові атаки,

спрямовані на вчителів чи учнів для отримання доступу до конфіденційної інформації, стають ще однією поширеною небезпекою у цифровому просторі.

Обов'язки та відповідальність вчителів у сфері захисту персональних даних учнів регулюється законодавством, етичними стандартами та практичними рекомендаціями, спрямованими на збереження конфіденційності, цілісності та безпеки інформації учнів при використанні сучасних технологій. Основні напрями діяльності вчителів у цьому контексті включають такі аспекти:

1. Виконання норм законодавства. Українське законодавство, зокрема Закон України «Про захист персональних даних», встановлює чіткі вимоги щодо обробки особистої інформації. Вчителі повинні:

- збирати, обробляти, зберігати та передавати персональні дані лише за умови дотримання правових підстав, таких як письмова згода батьків або інших законних представників;
- уникати поширення даних без дозволу, за винятком випадків, що передбачені законом, наприклад, запити правоохоронних органів;
- дотримуватись норм щодо термінів зберігання та умов обробки інформації згідно із чинним законодавством.

2. Забезпечення безпеки даних. Основна роль вчителя полягає у захисті даних учнів від несанкціонованого доступу та можливого витоку особистої інформації. Тривалий захист забезпечується такими заходами, як:

- використання перевірених навчальних платформ замість особистих месенджерів або інших ненадійних каналів зв'язку;
- налаштування складних паролів, шифрування інформації та впровадження двофакторної автентифікації;
- регулярне оновлення програмного забезпечення для уникнення вразливостей системи;
- відмова від застосування сервісів із низьким рівнем захисту даних.

3. Контроль доступу до інформації. Ефективний контроль доступу допомагає зменшити ймовірність неправомірного використання даних. Вчителі повинні:

- обмежувати доступ до персональної інформації виключно уповноваженим працівникам навчального закладу;
- не передавати дані через небезпечні комунікаційні канали, як-от незашифровані електронні листи або публічні Wi-Fi мережі;
- забезпечувати фізичний захист документів та інших носіїв інформації від неправомірного доступу.

4. Розвиток культури цифрової безпеки у школярів. Одним із ключових обов'язків вчителя є формування в учнів розуміння важливості захисту власних даних. Ця робота включає:

- проведення уроків із цифрової грамотності, де роз'яснюються принципи створення надійних паролів, загроз фішингу і правила безпечного користування мережею;
- інформування про ризики публікації особистої інформації в соціальних мережах чи месенджерах;
- просвітницьку діяльність для підвищення обізнаності щодо ризиків у цифровому середовищі.

5. Дії у разі виявлення порушень безпеки даних. При підозрі або факті витоку персональної інформації вчителі повинні:

- одразу повідомити адміністрацію школи про ситуацію;
- за необхідності звернутися до відповідних органів, таких як Уповноважений з прав людини, що контролює дотримання законодавчих норм у сфері захисту персональних даних;
- сприяти розслідуванню інциденту та брати участь у заходах щодо мінімізації його наслідків.

В умовах стрімкого розвитку цифрових технологій обізнаність і дотримання стандартів захисту персональних даних є важливою частиною

професійної діяльності сучасного вчителя. Це допомагає не лише забезпечити правовий захист дітей, але й створити безпечний освітній простір для всіх. Недотримання вимог щодо обробки та зберігання цих даних може призвести до серйозних юридичних, дисциплінарних, етичних і фінансових наслідків. У сучасному академічному дискурсі відповідальність учителів трактується як комплекс обов'язків, що базуються на нормах чинного законодавства, внутрішніх регламентах освітніх закладів й етичних стандартах. Подальший аналіз розглядає ключові аспекти такої відповідальності з точки зору правового і професійного підходів.

1. Юридична відповідальність педагогів за порушення у сфері захисту персональних даних регламентується нормами законодавства України та може набувати кількох форм:

- Адміністративна відповідальність відповідно до статті 188-39 Кодексу України про адміністративні правопорушення, неналежна обробка персональних даних, зокрема їх незаконне збирання, використання чи розголошення, тягне за собою накладення штрафів. Розмір цих штрафів визначається залежно від характеру та обсягу порушення.
- Кримінальна відповідальність, оскільки умисне розголошення конфіденційної інформації, яке завдало шкоди учням або їхнім родинам, підпадає під статтю 182 Кримінального кодексу України, що передбачає покарання за порушення недоторканності приватного життя. Такі дії можуть каратися штрафами, обмеженням волі або іншими санкціями згідно із законом.
- Цивільна відповідальність, коли у випадках шкоди, спричиненої витоком персональних даних, вчитель чи освітній заклад можуть бути зобов'язані відшкодувати матеріальні або моральні збитки згідно із нормами Цивільного кодексу України. Така компенсація може включати як порушення права на конфіденційність, так і інші пов'язані втрати.

2. Дисциплінарна відповідальність, коли порушення внутрішніх правил

школи щодо роботи з персональними даними може тягнути за собою застосування дисциплінарних санкцій. Невиконання положень статуту навчального закладу або внутрішніх інструкцій може стати причиною винесення догани, тимчасового усунення від виконання обов'язків чи навіть звільнення відповідно до норм Кодексу законів про працю України. Міра дисциплінарної відповідальності залежить від важкості скоєного правопорушення, його наслідків та політики управління в межах закладу освіти.

3. Етична відповідальність вчителя має фундаментальне значення, адже захист персональних даних учнів є важливою частиною професійної етики вчителя. Одним із ключових чинників є збереження довіри учнів та їхніх батьків до педагогічного персоналу і навчального закладу загалом. Порухення конфіденційності здатне підірвати авторитет учителя та репутацію школи, а також створити несприятливу психологічну атмосферу. Моральний обов'язок вчителя передбачає дотримання принципу поваги до приватного життя учнів та їхніх сімей і відповідальне ставлення до використання довіреної їм інформації в межах освітньої діяльності.

4. Фінансові наслідки визвані необережністю дотримання норм захисту даних для самого вчителя, так і для закладу освіти. У випадку судових позовів з боку батьків або опікунів постраждалих учнів освітній заклад або його представники можуть бути зобов'язані сплатити компенсації за матеріальні чи моральні збитки.

У контексті зростаючої цифровізації освітнього процесу захист персональних даних учнів є критично важливим завданням для вчителів. Для забезпечення відповідності законодавчим вимогам, етичним стандартам і практичним потребам пропонується низка рекомендацій, спрямованих на підвищення безпеки даних та мінімізацію ризиків їх компрометації. Ці рекомендації базуються на сучасних підходах до кібербезпеки та практичного досвіду роботи з інформаційними системами в освіті. Практичні поради вчителям щодо захисту персональних даних учнів наведені на

рис.1.

| Проходження тренінгів з кібербезпеки                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Використання безпечних платформ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Мінімізація збору даних                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Співпраця з адміністрацією навчального закладу                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>● Регулярно брати участь у тренінгах і курсах із кібербезпеки, організованих сертифікованими установами чи освітніми платформами. Такі програми можуть охоплювати теми захисту даних, розпізнавання фішингових атак, безпечного використання хмарних сервісів тощо.</li> <li>● Ознайомлюватися з актуальними змінами в законодавстві, зокрема Законом України «Про захист персональних даних», через спеціалізовані семінари чи вебінари.</li> <li>● Розвивати навички роботи з інформаційними системами, які використовуються в навчальному процесі, для забезпечення їх безпечного налаштування та використання.</li> </ul> | <ul style="list-style-type: none"> <li>● Використання офіційних платформ, таких як Google Classroom, Microsoft Teams, Moodle або інших систем, що мають сертифікати безпеки та відповідають міжнародним стандартам (наприклад, GDPR для європейських аналогів).</li> <li>● Уникнення використання особистих месенджерів (наприклад, WhatsApp, Telegram) для передачі чи зберігання даних учнів, оскільки вони можуть не забезпечувати належного рівня захисту.</li> <li>● Налаштування параметрів безпеки на платформах, зокрема використання складних паролів, двофакторної автентифікації та шифрування даних.</li> </ul> | <ul style="list-style-type: none"> <li>● Збирати лише ту інформацію, яка є необхідною для виконання освітніх завдань (наприклад, ПІБ, оцінки, контактні дані батьків для комунікації).</li> <li>● Уникати накопичення надмірної інформації, яка не має прямого відношення до навчального процесу (наприклад, детальні медичні дані, якщо вони не потрібні).</li> <li>● Регулярно переглядати та видаляти застарілі дані, що більше не використовуються, відповідно до вимог законодавства щодо термінів зберігання інформації.</li> </ul> | <ul style="list-style-type: none"> <li>● Уточнювати в адміністрації наявність та зміст політики захисту персональних даних, розробленої навчальним закладом, і суворо її дотримуватися.</li> <li>● Брати участь у розробці або вдосконаленні внутрішніх регламентів, що стосуються обробки та захисту інформації.</li> <li>● Повідомляти адміністрацію про будь-які виявлені вразливості в системах або підозри на витік даних для оперативного реагування та усунення проблем.</li> </ul> |

Рис. 1. Практичні поради вчителям щодо захисту персональних даних учнів

Захист персональних даних учнів у сучасній цифровій епосі вимагає від вчителів системного підходу, що включає підвищення кваліфікації, використання безпечних технологій, зменшення обсягу збирання даних і тісну співпрацю з адміністрацією. Реалізація таких практичних рекомендацій допоможе створити безпечніше цифрове середовище, зменшити ризики порушення конфіденційності та підвищити довіру до освітньої системи. Постійне вдосконалення цифрових навичок і дотримання етичних стандартів є важливими для ефективного захисту даних у сучасних умовах.

### Список використаних джерел

1. Концепція виховання дітей та молоді в цифровому просторі.

Національна академія педагогічних наук України. 2021. 52 с. Режим доступу: <https://ipv.org.ua/wp-content/uploads/2021/08/Kontsepsiia-vykhovannia-ditey-ta-molodi-v-tsyfrovomu-prostori.pdf>

2. Професійний стандарт «Вчитель закладу загальної середньої освіти». Наказ Міністерства освіти і науки України від 29 серпня 2024 р. № 1225. м. Київ Режим доступу: <https://mon.gov.ua/npa/pro-zatverdzhennia-profesiinoho-standartu-vchytel-zakladu-zahalnoi-serednoi-osvity>

3. Права учасників освітнього процесу та дії закладу освіти. Освітній омбудсмен України. Режим доступу: <https://eo.gov.ua/>

4. Закон України «Про захист персональних даних». від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481. Режим доступу: <https://zakon.rada.gov.ua/laws/sho>.

5. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X // Відомості Верховної Ради УРСР. 1984. Додаток до № 51. Ст. 1122. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>

## **НАВЧАННЯ В ОБ'ЄКТИВІ: EDTECH ТА ТІНЬОВИЙ ПРОФАЙЛІНГ. Дубняк М.В.**

кандидат юридичних наук,  
Державна наукова установа «Інститут  
інформації, безпеки і права Національної  
академії правових наук України»  
ORCID ID: 0000-0001-7281-6568

Цифровізація освіти стрімко трансформує способи здобуття знань, водночас створюючи нові ризики для приватності та безпеки дітей. Освітні технології (EdTech) дедалі активніше інтегрують штучний інтелект, аналітику великих даних, адаптивне навчання та інші інструменти, що дозволяють здійснювати приховане збирання, обробку та використання персональних даних учнів — від академічних результатів до емоційних реакцій, стилів навчання, поведінкових патернів тощо.