

Безпека персональних даних¹

Безпека персональних даних

[Що таке персональні дані та які дані зберігаються на освітніх платформах](#)

[Загальні поради щодо безпеки при навчанні онлайн](#)

[Підготовка пристроїв, мереж та інструментів](#)

[Збереження конфіденційності під час реєстрації/входу на навчальні платформи](#)

[Параметри безпеки для відеоконференцій](#)

Що таке персональні дані та які дані зберігаються на освітніх платформах

Оскільки при змішаному навчанні частина освітнього процесу відбувається онлайн, а його учасники використовують різні цифрові платформи та застосунки, безпека персональних даних стає важливим аспектом організації освітнього процесу закладу освіти.

В Україні захист даних регулюється [Законом України «Про захист персональних даних»](#), що був прийнятий у 2010 році та набув чинності у 2011 році. Цей закон запровадив норми, покликані захищати конфіденційні дані та приватну інформацію громадян під час їх обробки та зберігання у різноманітних базах даних.

Відповідно до закону персональні дані – це відомості чи сукупність відомостей про фізичну особу, яку ідентифіковано або може бути ідентифіковано. Інформація, що ідентифікує особу, – це будь-яка інформація про фізичну особу, якою володіє установа, включаючи (1) будь-яку інформацію, яку можуть використати для ідентифікації або відстеження особистості людини. Наприклад, це можуть бути ім'я, номери соціального страхування, дата і місце народження, дівоче прізвище матері або біометричні записи; а також (2) будь-яка інша інформація, що пов'язана з фізичною особою (скажімо, медична, освітня, фінансова та робоча інформація).

Дані, зібрані освітніми онлайн-платформами, складаються здебільшого з персональних даних, отриманих від здобувачів освіти, їхніх батьків/опікунів та викладачів. Обробку персональних даних із електронних баз освітнього закладу здійснюють на підставі надання закладу освіти письмових згод педагогів, здобувачів освіти та/або їхніх батьків на таку обробку. Ці дані зберігають у закладі освіти як власника персональних даних.

Це такі категорії даних:

а) персональні дані здобувача освіти: інформація, що стосується конкретного здобувача освіти, включаючи особисту інформацію (прізвище, ім'я, по батькові, дата народження тощо), контактну інформацію (група, номер телефону, електронна пошта й домашня адреса), інформацію про навчання (успішність, результати тестів, файли, інформація про доступ до платформи).

¹ Уривок з посібника “Методологія змішаного навчання для закладів професійної (професійно-технічної) освіти” (2021).

б) персональні дані батьків/опікунів: інформація, що стосується батьків/опікунів здобувачів освіти, включаючи персональну інформацію, інформацію про здобувачів освіти, інформацію про доступ до платформи.

в) персональні дані викладачів: інформація, що стосується викладачів, включаючи їх персональну інформацію, контактну інформацію (посада, група(и), номер телефону, електронна пошта та домашня адреса), викладацьку інформацію (курси, освітні програми), а також інформацію про доступ до платформи.

Загальні поради щодо безпеки при навчанні онлайн

Під час запровадження онлайн-компонента до освітнього процесу важливо розуміти, що учасники взаємодіятимуть у різних середовищах з різними «правилами гри» та етикетом. Не всі правила етикету та безпеки, які діють у реальному світі, спрацьовують у світі віртуальному. Проте варто виробити спільні правила нетикету (або мережевого етикету^[1]) для роботи на навчальній платформі закладу: як комунікувати, що розміщувати і та інше. Важливо, щоб ці правила всі знали, розуміли їх і мали до них доступ.

Для всіх учасників освітнього процесу необхідно провести додаткове навчання про безпеку онлайн та захист персональних даних. Важливо також встановлювати різний рівень доступу: що можуть переглядати та робити на платформі всі користувачі, тільки педагоги, тільки адміністратори, всі здобувачі освіти та/чи окремі здобувачі освіти (наприклад, доступ до власних робіт, персональна інформація, інформація про академічні досягнення). Якщо ви працюєте в Google Classroom чи Moodle, всі ці налаштування доступу можливі.

Окремо необхідно провести навчання для тих, хто має адміністративний доступ до навчальної платформи. Їх варто поінформувати про те, що становить загрозу безпеці, а також заохотити їх встановити програмне забезпечення для захисту персональних даних, яке буде спрацьовувати та вживати коригувальних заходів, якщо комп'ютер буде зламано.

Варто зважати також і на доступ до платформи. Важливо, щоби тільки авторизовані користувачі могли зайти на платформу, вводячи додатковий пароль. Необхідною є аутентифікація даних здобувачів освіти, що обмежить спроби входу в систему сторонніх осіб. Щоб забезпечити доступ до навчального середовища реальним здобувачам освіти (тобто справжніми людям, а не інтернет-ботам), необхідно засвідчити особу здобувача освіти. Для цього пропонуємо використовувати Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart – Повністю автоматизований публічний тест Тюрінга для розрізнення комп'ютерів і людей), це один із різновидів заходів безпеки, відомий як аутентифікація «виклик-відповідь».

Код перевірки захищає від спаму й крадіжки паролів. Для перевірки необхідно пройти тест, який підтверджує, що дії виконує людина, а не комп'ютерна програма, яка намагається отримати доступ до захищеного паролем акаунту. Під час перевірки користувач бачить на екрані два елементи: текстове поле та випадкову послідовність викривлених букв і/або цифр. Щоб пройти перевірку, потрібно ввести в поле зображені символи.

Обов'язково використовуйте програму Captcha, яку легко інтегрувати в навчальне середовище. Captcha можна інтегрувати в процес реєстрації. Також можна встановити обмеження, скільки разів хтось може спробувати увійти. Це допоможе стримати сторонніх осіб, оскільки у них менше шансів підібрати правильний пароль випадково.

Важливим аспектом безпеки під час змішаного навчання є запобігання незаконному використанню змісту. Для цього можливо змінювати формати або спосіб подання матеріалу. Наприклад, підвантажуйте документи у форматі PDF – їх складніше змінювати. Також не забувайте про дотримання авторського права та академічну доброчесність – не лише здобувачів освіти, але й педагогічного колективу, коли йдеться про наповнення обраної платформи вмістом.

Захищаючи персональні дані в онлайн-навчанні, важливо враховувати ще кілька аспектів: підготовку пристроїв, мереж та інструментів онлайн-навчання, збереження конфіденційності під час реєстрації/входу на навчальні платформи^[2].

Підготовка пристроїв, мереж та інструментів

Перш ніж навчатись в онлайн-середовищі, варто налаштувати пристрої, мережі, інструменти та ознайомитися з політикою конфіденційності, адже все це є основними аспектами захисту персональних даних.

Для захисту персональних даних насамперед потрібно налаштувати та захистити цифрові пристрої. Сюди входять:

- **Налаштування пристрою:**

- використання ліцензійного програмного забезпечення;
- регулярне оновлення програмного забезпечення;
- встановлення антивірусної програми та firewall (міжмережевий екран, фаєрвол);
- встановлення паролю на вхід (для цього слід використовувати складний унікальний пароль, який містить великі літери, маленькі літери, спеціальні символи, а його розмір складає не менше 14 символів. Унікальність передбачає, що кожен обліковий запис повинен мати власний пароль);
- налаштування «блокування пристрою» на період, коли за ним ніхто не працює. Для Windows – це блокування клавішами Win+L, в Mac-комп'ютерах блокування кришки переводить пристрій в режим сну та запитує пароль під час наступного входу;
- видалення історії з браузера та кешу. Коли ви працюєте в інтернеті, то сторінки, на які ви заходите, відправляють на ваш комп'ютер невеликі файли та індексують усі ваші дії. Щоб інформація, яку шукали користувачі, залишалась анонімною, слід видаляти такі тимчасові файли, наприклад, за допомогою програми CCleaner;
- створення резервних копій важливих файлів. Це можна робити у хмарних сховищах (наприклад, Google Диск, Dropbox, Microsoft OneDrive).

- **Керування підключенням до мережі**

Безпека мережі не дозволяє неавторизованим користувачам та хакерам отримати доступ до мережі Wi-Fi та пристроїв, які її використовують. Важливо підключитися і користуватися інтернетом безпечно, а для цього варто використовувати щонайменше закриту мережу із встановленим паролем для входу.

- **Вибір та встановлення навчальних інструментів:**

- завантаження додатків та програм тільки з офіційних сайтів і власних магазинів програм операційних систем, таких як Microsoft Store, Apple App Store, Google Play Store тощо;
- перевірка адреси вебсайту: вебсайти без шифрування SSL^[3]/TLS або без необхідних сертифікатів не можуть гарантувати захист персональних даних. У більшості випадків, якщо адреса сайту починається з http://, треба бути обачними із розміщенням персональних даних. Натомість, якщо адреса сайту починається з https://, це означає, що сайт має сертифікати безпеки, тому розміщення персональних даних на ньому вважається захищеним.

- **Перегляд політики конфіденційності**

Закони, що стосуються захисту персональних даних, обробки інформації та конфіденційності, вимагають від провайдерів надавати клієнтам інформацію про політику конфіденційності. Зазвичай у ній детально викладають важливу інформацію про дані, включаючи те, яку інформацію збирає платформа/додаток, як компанія її використовує, з ким ділиться та як захищає. Цією інформацією мають володіти викладачі, адміністрація та здобувачі освіти.

Де можна знайти цю інформацію на різних платформах:

- Zoom: <https://zoom.us/ru-ru/privacy-and-security.html>
- Google: <https://policies.google.com/privacy?hl=uk>
- Microsoft: <https://privacy.microsoft.com/uk-ua>
- Moodle: <https://moodle.org/admin/tool/policy/view.php?policyid=1>
- Viber: <https://www.viber.com/ru/terms/viber-privacy-policy/>
- Edmodo: <https://go.edmodo.com/privacy-policy>

Збереження конфіденційності під час реєстрації/входу на навчальні платформи

Під час входу на будь-які навчальні платформи першим і найважливішим кроком є реєстрація на платформі. Користувачі часто ігнорують важливість цього кроку: не зберігають та забувають ім'я користувача/пароль, передають пароль іншим, що призводить до витоку інформації, втрати пароля та інше. Як можна цьому зарадити?

- Захист та обережне ставлення до паролів: використовуйте надійний пароль для створення облікового запису; нікому не передавайте свій пароль; не пишіть паролі входу до облікового запису у нотатках і не залишайте у відкритому доступі.

- Використання менеджера паролів: створення для кожного облікового запису унікальних паролів провокує труднощі з їхнього збереження. Для полегшення цього завдання можна використовувати менеджери паролів. Наприклад, у користувачів Mac OS є вбудований менеджер Keychain, який автоматично зберігає паролі. LastPass – це онлайн-менеджер паролів для тих облікових записів, які створюють онлайн. KeePass – це офлайн-менеджер, де можна самостійно гарантувати безпеку паролів.
- Ігнорування невідомих повідомлень та посилань. Не натискайте на посилання чи вкладення в невідомих повідомленнях. Завжди краще вводити URL-адресу безпосередньо в браузер, щоб уникнути ризику потрапити на фішинговий сайт.
- Використовуйте двофакторну аутентифікацію. Все частіше провайдери допомагають захистити ваш обліковий запис, вимагаючи введення одноразового коду, а також звичайного пароля.
- Перевіряйте облікові записи щодо будь-якої підозрілої діяльності та негайно звертайтеся до провайдерів, якщо побачите щось невідповідне.

Параметри безпеки для відеоконференцій

Оскільки сьогодні в Україні частка синхронного онлайн-навчання досить значна, а відеоконференції використовують багато викладачів, окремо розповімо, що варто зробити, аби взаємодія викладача і здобувача освіти була максимально ефективною. З цим допоможе:

- попередня реєстрація для учасників. Ця функція фіксує адресу електронної пошти всіх користувачів, що перебувають в аудиторії, і може допомогти з оцінюванням присутніх користувачів;
- використання ідентифікатора конференції та пароля для входу у конференцію. Створіть пароль і відправте його здобувачам освіти, щоб у віртуальну аудиторію входили лише ті, кому це потрібно;
- відключення входу раніше за організатора: здобувачі освіти не зможуть зайти у конференцію, якщо туди ще не зайшов організатор;
- вимкнення відео та звуку у здобувачів освіти. Це дозволить заблокувати неналежну поведінку під час заняття або зміст, що відволікає;
- видалення учасника або переведення його в режим очікування (в Zoom): якщо небажаний користувач все-таки зміг увійти у віртуальну аудиторію, ви можете легко видалити його в меню «Учасники» або відправити в залу очікування;
- блокування чату: викладачі можуть обмежувати роботу чату в аудиторії, щоб здобувачі освіти не могли відправляти один одному приватні повідомлення. Ми рекомендуємо керувати доступом до чату за допомогою елементів управління на панелі інструментів в конференції (а не відключати його

повністю), щоб здобувачі освіти могли взаємодіяти з викладачем за такої необхідності;

- налаштування демонстрації екрану: щоб запобігти демонстрації випадкового змісту, у налаштуваннях можна обмежити, хто може демонструвати екран: «тільки організатор», «організатор та учасники».

І ще один важливий момент: не викладайте та не розповсюджуйте відео з відеоконференції у відкритому доступі без попередньої згоди на те усіх учасників і учасниць занять (наприклад, Zoom дозволяє збирати таку згоду чи незгоду через спеціальну форму перед початком зустрічі). Якщо хтось категорично не погоджується на відеофіксацію дуже важливого для вас заняття, можна спробувати домовитися про компромісне рішення – незгодні вимикають камеру на час запису.

[1] Інші поширені назви для нетикету: мережевий нетикет, Інтернет-етикет, тобто, правила поведінки та спілкування у мережі Інтернет.

[2] Personal Data and Privacy Protection in Online Learning. Guidance for Teachers, Students and Parents. June 2020. Version 1.0. Smart Learning Institute of Beijing Normal University (SLIBNU), 2020 in partnership with UNESCO IITE and UNESCO INRULED

[3] SSL-сертифікат – це цифровий підпис, який дозволяє забезпечити безпечне зашифроване з'єднання між вебсервером (сайтом) і вебклієнтом (браузером) за допомогою протоколу HTTPS.