**Гриценчук Олена Олександрівна**,
науковий співробітник,
Інститут інформаційних технологій і засобів навчання НАПН України (м.Київ).
ORCID:
ORCID ID: 0000-0003-3173-7649
helenakyiv2017@ukr.net

# ДО ПРОБЛЕМИ ГРОМАДЯНСЬКОЇ КОМПЕТЕНТНОСТІ ВЧИТЕЛЯ ТА БЕЗПЕКИ У ІНФОРМАЦІЙНО-ОСВІТНЬОМУ СЕРЕДОВИЩІ: ДОСВІД НІДЕРЛАНДІВ

Основними пріоритетами освіти і виховання громадянина у сучасному суспільстві, які визнані більшістю європейських країн та Україною, є цінності, проголошені Радою Європи, а саме: верховенство права, демократія та права людини. Освітні процеси сьогодні відбуваються у інформаційному цифровому світі й вимагають від педагогів компетентностей як у галузі громадянської освіти, так і у використанні ІКТ. Громадянська компетентність учасників навчально-виховного процесу, і вчителів зокрема, безпосередньо пов'язана з відповідальним ставленням до інформації та володінням ІКТ, повагою до приватного життя, толерантністю та етичною поведінкою у цифровому світі та ін., що дає можливість забезпечити політику конфіденційності та безпеки у інформаційно-освітньому середовищі.[1], [2].

У розвинених країнах Європи, зокрема Нідерландах, існує певний досвід щодо розв'язання проблеми інформаційної безпеки та конфіденційності використання цифрових технологій, що застосовуються у школі. Найбільш гострі питання, що піднімаються голландськими освітянами, з якими стикається школа, такі: обмін персональними даними, політика щодо паролів, кодекс поведінки для безпечного використання цифрових ресурсів та персональних даних, угоди про соціальні медіа, тощо. У звіті Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, що пройшов у м. Ньювейген, Нідерланди, у 2019 р., наголошується, що аспект інформаційної безпеки та конфіденційності – те, на чому саме має зосередитись сучасна школа [3].

Організація інформаційної безпеки та конфіденційності починається зі створення рамкових умов, тобто правил та політики закладу щодо встановлення відповідальності з боку адміністрації, вчителів та учнів. З метою забезпечити ефективне та безпечне функціонування шкіл у інформаційно-освітньому середовищі, голландський фонд Kennisnet (https://www.kennisnet.nl) у 2019 р. запропонував оновлений підхід до формування і впровадження політики інформаційної безпеки та конфіденційності, розроблений завдяки плідній співпраці фонду з Громадською Радою в галузі середньої освіти (https://www.vo-raad.nl/), Громадською Радою в галузі початкової освіти (https://www.poraad.nl/) та Громадською Радою з питань охорони здоров'я. Для реалізації оновленого підходу також створено наповнений інструментарієм єдиний веб-портал з інформаційної безпеки для шкіл та забезпечено умови комфортного переходу на нього з попередніх шкільних сайтів. Ефективне впровадження ІКТ у навчальне середовище, в якому застосовуються хмарні сервіси, цифрові ресурси і засоби, забезпечується рекомендаціями, що розроблені фахівцями у вигляді дорожньої карти (покрокового плану), які можуть допомогти школі запровадити політику інформаційної безпеки та конфіденційності навчального закладу. Дорожня карта складається із п'яти розділів, що називаються: *політика та відповідальність, визначення обмежень та ризиків, прозорий обмін персональними даними, обробка та зберігання персональних даних та оцінка*. Розділ І. Політика та відповідальність складається з таких тем: політика інформаційної безпеки та конфіденційність та ролі та обов'язки. Кодекс поведінки щодо безпечного використання ресурсів та персональних даних ІКТ, політика щодо паролів та процедура поівідомлення про інциденти з порушення безпеки – аспекти розділу ІІ. Визначення обмежень та ризиків. Питання конфіденційносі за замовчуванням та конфіденційності процесу розробки, угоди про соціальні медіа, обмін

персональними даними та ін. розкриваються у розділі III Прозорий обмін персональними даними. Угоди про обробку та зберігання даних, правила та юридичне підґрунтя містяться у Розділ IV. Обробка та зберігання персональних даних. Інструкції щодо процесів підзвітності та інформування містяться у розділі V. Оцінка. До інструментарію, що забезпечує політику інформаційної безпеки та конфіденційності, також належить укладений глосарій, що визначає основні терміни та поняття, серед яких: анонімізація, псевдонімізація, аутентифікація, матриця авторизації, хмара, мінімізація даних, шифрування, хакер, аналіз ризиків, конфіденційність, конфіденційність за замовчуванням, шифрування та ін.

Сучасний навчально-виховний процес відбувається у інформаційно-освітньому середовищі, яке постійно розвивається і змінюється. Сьогодні це комп'ютерно орієнтоване та хмаро орієнтоване навчальне середовище, що ставить питання безпеки і конфіденційності на новий щабель, спонукає учасників освітнього процесу бути компетентними, відповідальними та свідомими користувачами та мати громадянську позицію. Дані, які використовуються вчителем або учнем, зберігаються не тільки на власному комп'ютері, а все частіше розміщуються у хмарі, учасники навчально-виховного процесу користуються хмарними сервісами, спілкуються, співпрацюють, навчаються й розвиваються засобами соціальних мереж, блогів, форумів і чатів тощо. Тому зарубіжний досвід і практичні розробки Нідерландів, зокрема, можуть стати у нагоді вітчизняним фахівцям. Перспективами для подальших пошуків можуть бути практичні розробки уроків з безпеки та конфіденційності, що є невід'ємною складовою громадянської освіти.

**Список використаних джерел:**


1. UNESCO ICT Competency Framework for Teachers. Paris, UNESCO, 2011. [Електронний ресурс]: http://unesdoc.unesco.org/images/0021/002134/213475e.pdf. Дата звернення: Лист.11,2019.
2. European Framework for the Digital Competence of Educators: DigCompEdu. 2017. [Електронний ресурс]. Режим доступу: https://www.ec.europa.eu/jrc/en/digcompedu.pdf. Лист.11,2019.
3. Звіт Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, Нідерланди, 2019. [Електронний ресурс]: https://www.kennisnet.nl/artikel/verslag-landelijk-congres-ibp-in-het-onderwijs-2019/. Дата звернення: Лист.11,2019.