

Малицька І.Д.

Інститут цифровізації освіти НАПН України,

irina_malitskaya@ukr.net

ORCID ID 0000-0003-1598-0120

ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ШКОЛЯРІВ У ВЕЛИКІЙ БРИТАНІЇ

У сучасному цифровому світі одним із ключових елементів забезпечення прав людини стає питання захисту персональних даних. Дані дітей, які є вразливою категорією населення, потребують особливої уваги. У Великій Британії шкільна система зобов'язана дотримуватися суворих норм щодо збору, зберігання та обробки персональної інформації учнів.

Захист даних дітей у школах регулюється низкою законодавчих актів, серед яких головну роль відіграють UK GDPR, який базується на основних положеннях Загального регламенту захисту даних (GDPR - *General Data Protection Regulation*), прийнятим Європейським Союзом [1]. Документ містить принципи обробки персональних даних, які застосовуються у всіх сферах, включно з освітою за принципами: законності, справедливості і прозорості; обмеженню обробки та зберігання даних, їх мінімізації та точності, цілісності і кофіденційності, а також підзвітності [2].

Крім цього у 2018 році був прийнятий *Закон про захист даних*, в якому уточнюються положення UK GDPR і конкретизуються правила щодо обробки даних дітей. У ньому передбачено, що обробка персональних даних дітей до 13 років може бути надана тільки батьками або опікунами. Також зазначено, що освітні установи зобов'язані призначати відповідальних осіб, які відповідають за захист даних [3].

Для забезпечення безпеки даних, що зберігаються, у школах Великої Британії використовується спеціалізоване програмне забезпечення – системи управління інформацією (MIS – *Management Information System*), як-от: Arbor, Bromcom, RM Integris. Такі системи зберігають інформацію про учнів: ім'я та прізвище, дата

народження, адреса, інформація про навчальні досягнення, особливі потреби. Програмне забезпечення має вбудовані функції безпеки: шифрування, контроль доступу, історію змін [4], [5].

Особлива увага приділяється кібербезпеці, запобіганню витокам даних школи. З цією метою впроваджується: антивірусне програмне забезпечення (Sophos, ESET); міжмережеві екрани (фаєрволи); системи виявлення вторгнень (IDS); резервне копіювання даних. Такі заходи допомагають захистити інформацію від хакерських атак, які останнім часом стають все частішими – зокрема, в 2024 році понад 300 шкіл у Британії зазнали кіберзлому [6].

Крім цього проводиться постійний моніторинг активності учнів, їх цифрової поведінки. Для виявлення потенційно небезпечних запитів, фільтрації вебконтенту та захисту від шкідливих програм використовується програмне забезпечення таке як: Smoothwall Monitor [7], Impero [8], Securus [9]. NetSupport DNA [10]. Системи дозволяють школам блокувати доступ до небезпечних сайтів і виявляти підозрілу активність у мережі, наприклад, спроби несанкціонованого доступу до даних учнів.

Школи у Великій Британії зобов'язані мати чіткі політики щодо захисту даних, які оприлюднюються на їхніх вебсайтах. Політики освітньої установи включають процедури збору, зберігання та використання даних, а також механізми реагування на порушення безпеки. Управління інформаційного комісара (Information Commissioner's Office, ICO) є головним регулятором, який стежить за отриманням всіх норм [11].

Згідно з законом, кожна школа повинна мати посадову особу з питань захисту даних (DPO Data Protection Officer), яка контролює дотримання політик, проводить перевірки, взаємодіє з батьками та державними органами. Виконання таких обов'язків може виконувати як працівник, призначений адміністрацією школи, так і зовнішній консультант [12].

Регулярна підготовка вчителів та адміністрації учбового закладу з цифрової безпеки є обов'язковою вимогою та контролюється місцевими освітніми органами. Для запобігання випадковому витоку даних шкільний персонал проходить навчання

з кібергігієни, тренінги з основ GDPR, інструктажі з обробки конфіденційної інформації.

Захист персональних даних дітей у британських школах – це комплексне завдання, яке охоплює юридичні, технічні та організаційні аспекти. Законодавство Великої Британії забезпечує високий рівень контролю за обробкою інформації, а школи впроваджують сучасні інструменти для збереження конфіденційності учнів. Водночас з розвитком цифрових технологій зростають і загрози, тож система захисту даних потребує постійного вдосконалення. Важливим є не лише дотримання нормативів, але й створення культури поваги до приватності учнів.

Список використаних джерел

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
2. UK General Data Protection Regulation (UK GDPR). 2016. URL: <https://www.legislation.gov.uk/eur/2016/679/contents>
3. Data Protection Act 2018. UK Public General Acts. 2018. URL: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
4. Arbor Education – MIS for schools and MATs. URL: <https://arbor-education.com>
5. Bromcom. URL: <https://bromcom.com/>
6. 330 UK schools hacked – pupil data sold on dark web. The Sun. 2024. URL: <https://www.thesun.co.uk/news/27831561/pupil-images-sold-paedos-school-data-hack/>
7. Smoothwall Monitor. URL: <https://smoothwall.com/solutions/monitor>
8. Impero. URL: <https://www.imperosoftware.com/>
9. Securus. URL: <https://www.securus-software.com/>
10. NetSupport DNA. URL: <https://www.netsupportdna.com/>
11. Data protection in schools / GOV.UK. 2023. URL: <https://www.gov.uk/guidance/data-protection-in-schools>.

12.Data protection policies and procedures. GOV.UK. 2023. URL:
<https://www.gov.uk/guidance/data-protection-in-schools/data-protection-policies-and-procedures>