СЕКЦІЯ: ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ

USE OF AI TOOLS FOR AUTOMATED RECOGNITION OF CYBERBULLYING AND TOXIC CONTENT IN STUDENT GROUPS

Sushko Volodymyr
applicant for the first level of higher education in the specialty of Secondary Education (Informatics)
Ternopil Volodymyr Hnatiuk National Pedagogical University
volodyasushko1999@gmail.com
Skaskiv Hanna
assistant of the Department of Informatics and Methods of its Teaching
Ternopil Volodymyr Hnatiuk National Pedagogical University
skaskivg@tnpu.edu.ua

By 2026, the digitalization of the educational environment has reached a stage where most communication among students occurs in messengers and closed social groups. As noted in previous studies, the Internet has become not only a source of information but also a primary means of socialization, which carries risks of cyber offenses [1]. The most acute problem remains cyberbullying – systemic harassment that often remains unnoticed by educators under remote learning conditions.

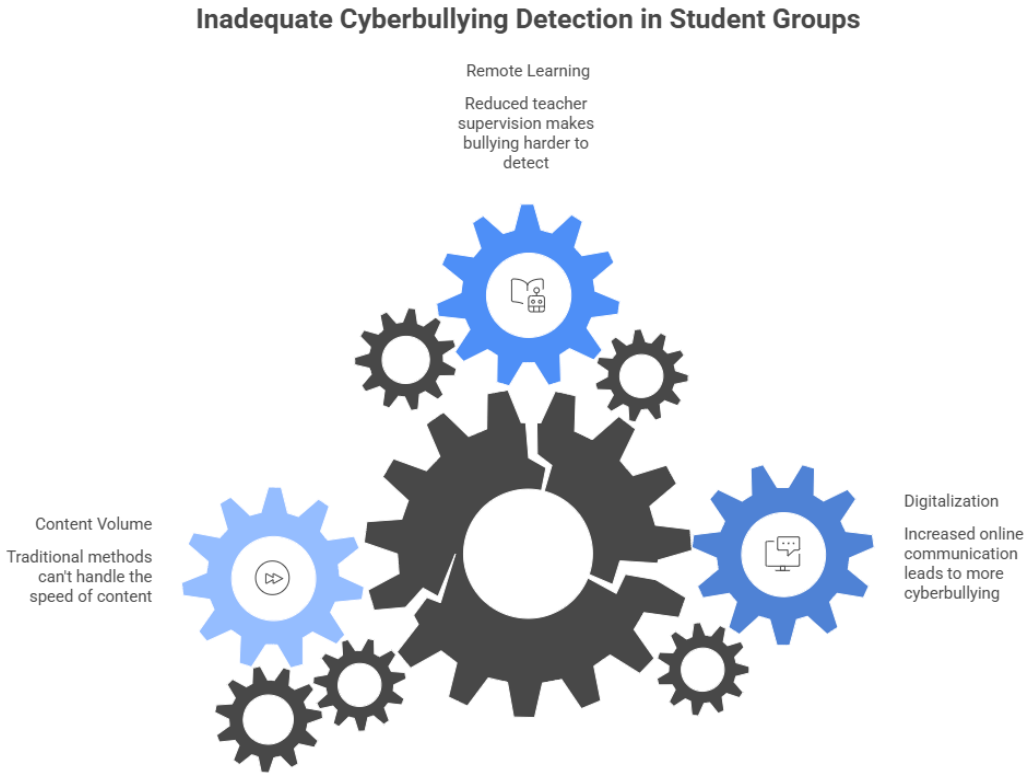

Fig. 1. Cyberbullying Detection in Student Grops

The importance of this topic arises from the fact that traditional supervisory methods in education – such as teacher moderation of online discussions – are no longer sufficient to manage the sheer speed and volume of digital content. Artificial Intelligence (AI) enables a shift from reactive conflict resolution to proactive prevention, which is essential for maintaining a safe learning environment (fig. 1).

The concept of *cyberproductivity in education* is actively explored by leading scholars within the conference organizing committee. For instance, Hanna Skrypka [3] emphasizes cyber literacy and the detection of harmful content. Oleksii Smirnov [4] focuses on technical measures for safeguarding information systems and software.

Meanwhile, others [2] examine legal frameworks and the protection of children's rights in the digital sphere. Despite this strong theoretical foundation, practical implementation of automated AI monitoring systems in general secondary education institutions (GSEI) remains insufficiently studied.

A critical challenge lies in balancing child safety with respect for privacy – lkoften referred to as "digital shadows." Moreover, further research is needed on adapting Natural Language Processing (NLP) algorithms to youth-specific slang and on detecting toxic «memes,» which frequently serve as subtle instruments of bullying (fig. 2).

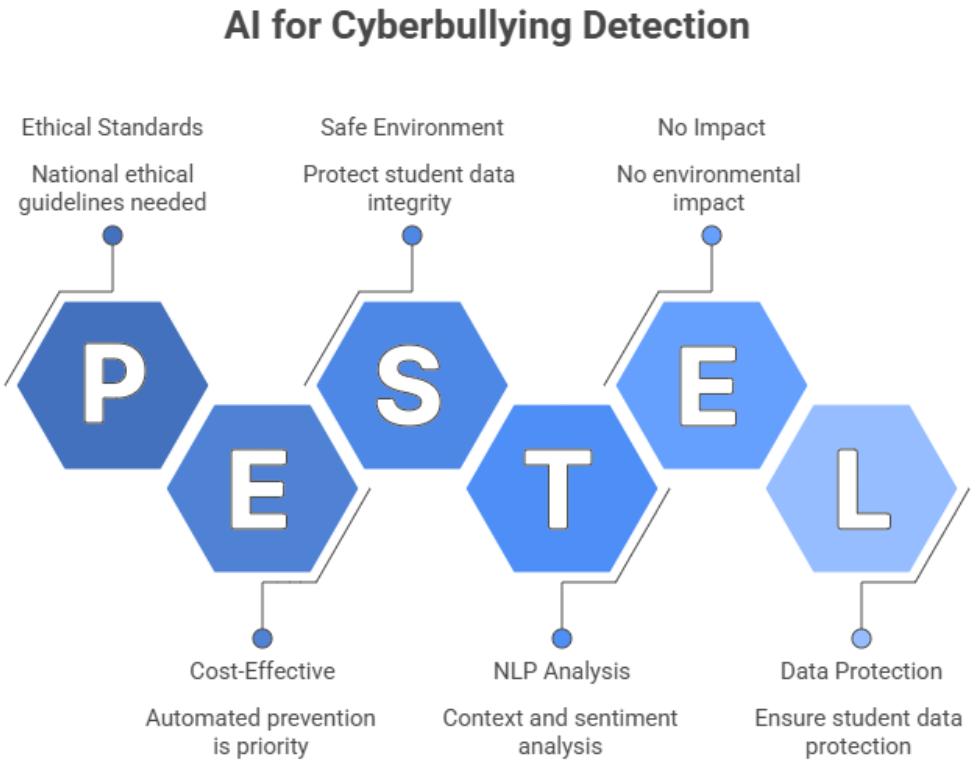

Fig. 2. Automated Protection System

A comprehensive technological review identifies several critical building blocks for effective AI-driven monitoring in student groups:

*Contextual Language Processing (NLP)***.** Beyond simple profanity filters, advanced NLP modules can interpret subtle forms of harmful communication such as sarcasm, passive aggression, or veiled intimidation by analyzing sequences of messages rather than isolated words.

Emotional Climate Assessment. Sentiment analysis tools track the overall tone of group interactions. A sudden drop in positivity or an increase in hostility may signal the onset of conflict or the marginalization of a particular student.

Discreet Alert Mechanisms. Instead of direct intervention, automated systems generate anonymous reports for school psychologists or administrators once toxicity reaches a critical threshold, ensuring timely but non-intrusive support.

Adaptive Learning to Youth Slang. AI modules must continuously update their linguistic models to recognize evolving slang, abbreviations, and coded expressions used by students, which often conceal harmful intent.

Detection of Visual and Meme-Based Toxicity. Since bullying frequently spreads through images and memes, integrated recognition systems can flag harmful visual content alongside textual analysis, broadening the scope of protection.

Data Security and Privacy Safeguards. To maintain trust, these systems must incorporate strong encryption and privacy protocols, ensuring that monitoring does not compromise students' rights or expose sensitive information.

Integrating these tools into platforms such as Moodle or Google Classroom ensures both the protection of student data and the integrity of educational content. AI-driven recognition of cyberbullying is not merely a technical enhancement but a vital element of holistic security strategies. Automation enables early threat detection, reducing psychological harm among students.

References

1. On the Basic Principles of Ensuring the Cybersecurity of Ukraine: Law of Ukraine of Oct 5, 2017, No. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed: 03.04.2026).

2. Child Safety in the Digital Space: MES recommendations for pedagogical workers and parents. URL: https://mon.gov.ua/news/bezpeka-ditey-u-tsifrovomu-prostori-mon-nadae-rekomendatsii-dlya-pedagogichnikh-pratsivnikiv-ta-batkiv (accessed: 06.04.2026).

3. Skrypka H. V. Recognition of fakes in social networks as a component of cyber literacy of a modern teacher. *Child Safety on the Internet: Prevention, Education, Interaction*: collection of materials of the IV All-Ukrainian scientific-practical conf. (Kropyvnytskyi, Feb 10, 2025). Kropyvnytskyi: "V. Sukhomlynskyi KOIPPO", 2025. P. 45–48 (in Ukrainian). URL: https://koippo.kr.ua/arhiv/zvit_kz_koippo_2022.pdf.

4. Smirnov O., Smirnova T., Konoplitska-Slobodeniuk O., Buravchenko K., Kravchuk O., Kozirova N. & Smirnov S. Research of Technologies for Ensuring Cybersecurity of IAAS, PAAS and SAAS Cloud Services. Electronic Professional Scientific Edition: Cybersecurity: Education, Science, Technique. 4(24), 2024. pp. 6–27. URL: https://doi.org/10.28925/2663-4023.2024.24 (accessed: 05.04.2026 in Ukrainian).

ІНТЕГРАЦІЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЮ ДІЯЛЬНІСТЬ ДЛЯ ПІДВИЩЕННЯ ЇЇ ЕФЕКТИВНОСТІ

Гавришків Надія Григорівна
спеціаліст вищої категорії, викладач циклової комісії інформатики та комп'ютерних дисциплін
Галицький фаховий коледж імені В'ячеслава Чорновола
n.gavrychkiv@gmail.com
Слєпцова Ольга Ярославівна
спеціаліст вищої категорії, викладач циклової комісії інформатики та комп'ютерних дисциплін
Галицький фаховий коледж імені В'ячеслава Чорновола
olgasleptcova30@gmail.com

Сьогодні освіта опинилася в точці, де ігнорування алгоритмів штучного інтелекту стає неможливим, а їх сліпе копіювання – ризикованим. Сучасний розвиток освіти відбувається в умовах стрімкої цифровізації, що зумовлює активне впровадження інструментів штучного інтелекту в освітній процес. Зміни, спричинені цифровими трансформаціями, впливають і на роль викладача, який поступово переходить від позиції основного джерела знань до організатора та координатора навчальної діяльності [3]. Водночас використання інструментів штучного інтелекту відкриває перспективи для індивідуалізації навчання, підвищення його ефективності та оптимізації професійної діяльності викладача. Разом із тим виникає необхідність забезпечення балансу між застосуванням