УДК 005.8:004.4]:373.5

АНАЛІЗ МЕТОДІВ МОНІТОРИНГУ ПЕРСОНАЛЬНИХ ДАНИХ УЧНІВ У ПРОЄКТАХ З РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ЗАГАЛЬНООСВІТНЬОЇ ШКОЛИ

Іванов Д.А.
e-mail:dmytro.ivanov1@nure.ua
Харківський національний університет радіоелектроніки, каф. ІУС,
м. Харків, Україна

Modern information systems for comprehensive schools have become an integral part of the educational process, automating the management of student data. These systems encompass a wide range of information, from personal details and academic achievements to medical records and social activities. However, the growing volume of such data creates significant risks associated with its unintentional or malicious use. Monitoring students' personal data requires a comprehensive approach that combines technical tools, organizational mechanisms, and legal compliance. The purpose of this work is to explore modern monitoring methods, analyze their limitations, and develop an integrated solution based on artificial intelligence technologies to enhance data security in school information systems.

Сучасні інформаційні системи для загальноосвітніх шкіл стали невід'ємною частиною освітнього процесу, інтегруючи автоматизацію управління даними учнів. Вони охоплюють широкий спектр інформації: від особистих даних та академічних досягнень до медичних записів і соціальних активностей. Проте зростання обсягів таких даних створює значні ризики, пов'язані з їхнім ненавмисним або зловмисним використанням.

Моніторинг персональних даних учнів потребує комплексного підходу, який поєднує технічні інструменти, організаційні механізми та правову відповідність. Мета цієї роботи полягає у дослідженні сучасних методів моніторингу, аналізі їхніх обмежень та розробці інтегрованого рішення на базі технологій штучного інтелекту для підвищення безпеки даних у шкільних інформаційних системах.

Сучасні підходи до моніторингу персональних даних учнів базуються на трьох ключових напрямах: правовому регулюванні, технічному захисті та аналітичних інструментах. Правові механізми, такі як GDPR (GDPR - General Data Protection Regulation) або Закон України «Про захист персональних даних», вимагають від шкіл дотримуватися принципів мінімізації даних та прозорості обробки [1, 2]. Це включає проведення оцінки впливу на захист даних DPIA (DPIA – Data Protection Impact Assessment) на етапі проектування системи та розробку внутрішніх політик, що регулюють доступ до інформації. Наприклад, заборона

зберігати дані на персональних пристроях або створення комітетів з кібербезпеки для регулярного аудиту.

Аналітичні інструменти допомагають прогнозувати та мінімізувати ризики. PESTLE-аналіз оцінює вплив зовнішніх факторів на безпеку даних, тоді як FMEA (FMEA – Failure Mode and Effects Analysis) дозволяє прогнозувати наслідки збоїв у системі, таких як відмова сервера під час звітного періоду. Використання блокчейн-технологій для створення незмінних логів дій забезпечує прозорість, наприклад, фіксує, хто і коли заходив в систему.

Для подолання фрагментарності традиційних методів пропонується інтегрована модель, яка поєднує технології штучного інтелекту, машинне навчання та кібербезпеку.

Автоматизований аналіз даних за допомогою алгоритмів машинного навчання дозволяє виявляти аномалії, такі як нестандартні шаблони доступу або спроби експорту великих обсягів інформації. Наприклад, NLP-моделі можуть моніторити текстові поля для виявлення образливих коментарів. Прогнозування інцидентів на основі методу Монте-Карло дає змогу оцінити ймовірність витоку даних, враховуючи історичні атаки на освітні платформи.

Адаптивні системи безпеки інтегруються з платформами Threat Intelligence для автоматичного блокування підозрілих IP-адрес. Поведінковий аналіз (UEBA – User and Entity Behavior Analytics) допомагає виявляти дії користувачів, що відхиляються від норми, наприклад, спроби доступу до даних учня з іншого класу. Географічно розподілені сховища даних забезпечують резервне копіювання, мінімізуючи втрати під час DDoS-атак.

Взаємодія зі стейкхолдерами включає освітні ініціативи, такі як вебінари для батьків про захист даних дітей або гейміфіковані тренінги з кібербезпеки для учнів. Прозорість досягається через публікацію щорічних звітів про стан безпеки даних та впровадження чат-ботів для оперативного реагування на запити.

Проактивність є ключовою перевагою запропонованого підходу. Штучний інтелект дозволяє виявляти загрози на ранніх стадіях, наприклад, сканування вразливостей системи.

Ефективність витрат досягається за рахунок автоматизації рутинних завдань, таких як аналіз логів, що значно оптимізує ресурси IT-відділів та допомагає зосередитись на більш важливих факторах, які потребують людської уваги.

Масштабованість хмарних рішень дозволяє адаптувати систему до зростання кількості учнів або нових законодавчих вимог.

Технічна складність інтеграції штучного інтелекту з застарілими системами може вимагати значних інвестицій у модернізацію. Етичні дилеми виникають через сприйняття моніторингових інструментів як

порушення приватності, наприклад, трекінг активності учнів. Кадровий дефіцит фахівців з кібербезпеки та Data Science у сфері освіти ускладнює реалізацію складних технологій.

В умовах обмежених бюджетів та технічних можливостей українські загальноосвітні школи можуть впроваджувати низку доступних практик.

По-перше, критично важливим є навчання персоналу основам кібербезпеки: від уникання фішингових листів до правильного зберігання паролів.

По-друге, використання безкоштовних або субсидованих державою хмарних рішень (наприклад, платформи «Електронний журнал») дозволяє забезпечити базовий рівень захисту даних без необхідності вкладати кошти в дорогі технології [3].

По-третє, регулярний аудит систем за участю місцевих IT-фахівців або волонтерів допомагає виявляти вразливості на ранніх етапах.

Важливу роль відіграє співпраця з державними органами. Наприклад, ініціативи Міністерства цифрової трансформації України щодо надання школам доступних інструментів кібербезпеки або створення регіональних центрів підтримки [4]. Такі заходи дозволяють школам отримувати актуальні рекомендації та технічну допомогу без значних витрат.

Моніторинг персональних даних учнів у шкільних інформаційних системах вимагає багаторівневого підходу, що поєднує технологічні інновації, правову відповідність та культуру безпеки.

Запропонована модель на основі штучного інтелекту та машинного навчання підвищує ефективність виявлення загроз.

Для успішного впровадження необхідно розробити стандартизовані протоколи, залучити державне фінансування для навчання персоналу та активізувати комунікацію з усіма стейкхолдерами.

Список використаних джерел:

1. Закон України «Про захист персональних даних» (2023). URL: https://zakon.rada.gov.ua/ (дата звернення: 20.02.2025).

2. GDPR: Official Regulation Text (2018). URL: https://gdpr-info.eu/ (дата звернення: 20.02.2025).

3. Міністерство освіти і науки України. URL: https://mon.gov.ua/ (дата звернення: 20.02.2025).

4. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 20.02.2025).