можуть аналізувати відповіді та прогрес кожного учня, щоб надавати індивідуальні завдання та матеріали, відповідні рівню їх знань;

- оцінювання та звітність, а саме, використання ШІ для автоматизації процесу оцінювання, аналізу робіт учнів та надання звітів вчителям та батькам;
- використання ігрових технологій, а саме, застосування ШІ у вигляді ігрових технологій для створення освітніх ігор, у нашому проекті – казки або коміксу, які можуть забезпечити ефективне вивчення певних концепцій, підвищуючи зацікавленість та мотивацію учнів;
- навчання на відстані та використання освітніх електронних ресурсів, а саме, застосування ШІ для створення персоналізованих онлайн-ресурсів та інтерактивних уроків, що дозволяє учням вивчати матеріал у власному темпі та у зручний час;
- підтримка вчителів, а саме, розробка інструментів ШІ полегшують вчителям адміністративні завдання, такі як складання розкладу, контроль відвідуваності та автоматизація деяких аспектів звітності, створення планів уроків, проектів та ін.;

Перспективами є створення збалансованого та ефективного плану використання ШІ у ЗЗО, сприяючи зростанню рівня освіти та підготовці учнів до вимог сучасного світу.

Список використаних джерел

Lampropoulos, Georgios. (2023). Augmented Reality and Artificial Intelligence in Education: Toward Immersive Intelligent Tutoring Systems. 10.1007/978-3-031-27166-3_8.

АНАЛІЗ КІБЕРЗЛОЧИННОСТІ ТА ЗАХОДИ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ. Сухіх А. С.

Старший науковий співробітник Інституту цифровізації освіти НАПН України, канд.пед.наук, Україна

Ключові слова: кіберзлочинність, кібербезпека, заклад загальної середньої освіти, кібератаки.

Кіберзлочинність стає дедалі серйозною проблемою як в Україні, так і в усьому світі. Зловмисники використовують все більш витончені методи для атак на

комп'ютерні системи та мережі, завдаючи шкоди як приватним особам, так і організаціям.

З початком повномасштабної агресії Росії Україна стала лідером у світі за кількістю кібератак, які спрямовані на державний та приватний сектори. Лише за 2023 року Служба безпеки України нейтралізувала майже чотири тисячі кібератак, спрямованих на пошук несанкціонованого доступу до електронного документообігу держустанов і технологічних систем інфраструктури України [1]. За результатами моніторингу подій, що відбувалися у сфері цифрових прав за період із 24 лютого по 31 серпня 2023 року кількість кібератак на державний сектор збільшилася у 15 разів за даними ГО "Платформа прав людини" (Рис. 1) [2].

	2019	2020	2021	2022	2023 (до 31 серпня 2023 року)
Кількість кібератак, здійснених на державний сектор (за інформацією Держспецзв'язку)	**16 751 440**	**8 632 641**	**2 968 801**	**241 151 834**	**180 911 186**
Кількість кібератак за результатами моніторингу, який здійснює СБУ	**1080**	**800**	**1400**	**4500**	**2500**
Кількість кібер-атак, виявлених у загальнодоступ-них джерелах	**7**	**10**	**25**	**51**	**32**

Рис. 1. Статистика кібератак на державний сектор в період із 24 лютого по 31 серпня 2023 року [2]

Зростання кількості кібератак, спрямованих на державні та приватні структури, не оминуло й освітні заклади. Існує низка причин, через які заклади загальної середньої освіти (ЗЗСО) стають мішенню для кіберхакерів:

- володіння цінними даними про учнів, викладачів та персонал, які можуть бути використані для злочинних цілей, таких як крадіжка особистих даних, шантаж або фінансові шахрайства;
- застарілі комп'ютерні системи та програмне забезпечення, які більш вразливі до кібератак;

- нестача ресурсів для вдосконалення кібербезпеки, що робить їх легкими мішенями для хакерів;

- нестача фахівців з кібербезпеки, які могли б допомогти їм оцінити ризики та вдосконалити свої системи захисту тощо.

Найпоширеніші типи атак, які можуть загрожувати ЗЗСО - це фішинг, DDoS-атаки, шпигунство, загрози на CMS та ін. В роботі [3] класифікуються за критеріями з урахуванням специфіки забезпечення кібербезпеки (Рис. 2).

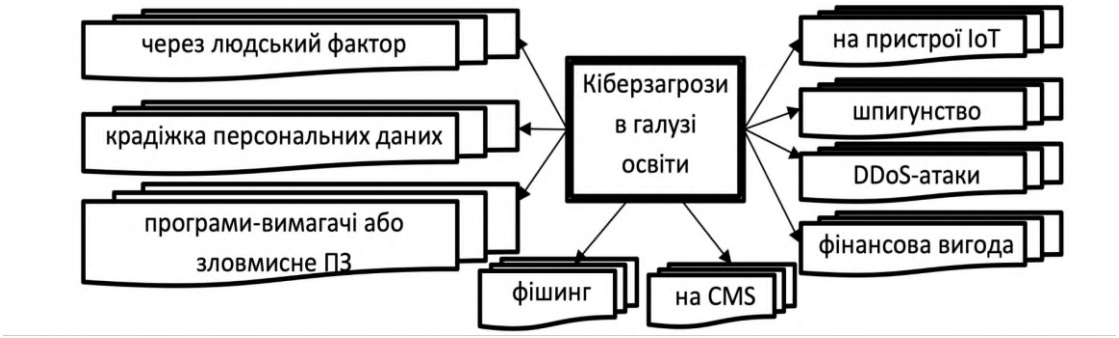

Рис. 1. Класифікація кіберзагроз в освітньому секторі [3]

Для захисту від кібератак освітнім закладам необхідно вживати комплексу заходів, що включають:

1. Підвищення обізнаності. Учні, викладачі та персонал повинні знати про кіберзагрози та розуміти, як від них захиститися. Це включає навчання основам кібербезпеки, розпізнавання підозрілих електронних листів та вебсайтів, а також використання надійних паролів.

2. Вдосконалення кібербезпеки. Освітні заклади повинні постійно оновлювати свої системи кібербезпеки, встановлювати надійні програмні та апаратні засоби захисту, використовувати антивірусне програмне забезпечення та регулярно оновлювати операційні системи та програмне забезпечення.

3. Резервне копіювання даних. Важливо регулярно створювати резервні копії всіх важливих даних, щоб у разі кібератаки їх можна було відновити. Резервні копії слід зберігати в безпечному місці, недоступному для зловмисників.

4. Співпраця з фахівцями. Освітнім закладам рекомендується співпрацювати з фахівцями з кібербезпеки, які можуть допомогти їм оцінити ризики, розробити план захисту та реагувати на кіберінциденти.

5. Вжиття заходів реагування. Має бути чіткий план дій на випадок кібератаки, який включає чітко визначені ролі та відповідальність, процедури повідомлення про інциденти та кроки з ліквідації наслідків.

Захист освітніх закладів від кібератак є спільним завданням, яке потребує постійної уваги та зусиль з боку керівництва, викладачів, персоналу та учнів. Вживаючи комплекс заходів та підвищуючи рівень обізнаності про кібербезпеку, ЗЗСО можуть значно знизити ризики стати жертвами кіберзловмисників. Важливо пам'ятати, що кіберзагрози постійно змінюються, тому ЗЗСО необхідно постійно оновлювати свої стратегії кібербезпеки та вживати заходів для захисту своїх даних та інформаційних систем.

Список використаних джерел

1. Служба безпеки України. (2023). З початку року СБУ нейтралізувала майже 4 тис. кібератак на органи влади та критичну інфраструктуру України. АрміяInform. Доступно: https://armyinform.com.ua/2022/12/26/z-pochatku-roku-sbu-nejtralizuvala-ponad-45-tys-kiberatak/
2. ППЛ (ГО «Платформа прав людини»). (2023). Війна у цифровому вимірі та права людини: Підсумковий звіт із 24 лютого 2022 року по 31 серпня 2023 року. Київ: ГО «Платформа прав людини». Доступно: https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf
3. Лук'янець, В. О., & Малюк, О. О. (2022). Кібербезпека освітніх закладів України в умовах воєнної агресії Російської Федерації. Сучасні проблеми інформатики, математики, механіки та фізики, 15(1), 171-180. Доступно: https://csecurity.kubg.edu.ua/index.php/journal/article/view/365/303

ВИКОРИСТАННЯ ЦИФРОВИХ НАРАТИВНИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ ДЛЯ РОБОТИ З ДІТЬМИ, ЯКІ ПОСТРАЖДАЛИ ВНАСЛІДОК ВІЙСЬКОВИХ ДІЙ

Тимчук Л. І.[1], Рубан Л. М.[2]

Професор кафедри соціальної реабілітації та соціальної педагогіки[1], Київський національний університет імені Тараса Шевченка; доцент кафедри іноземних мов економічного факультету[2], Київський національний університет імені Тараса Шевченка, Україна

Ключові слова: цифровий наратив, діти війни, підготовка вчителів.

Війна – складне суспільно-політичне явище, яке завдає непоправної шкоди життю і здоров’ю населенню певної країни. Найболючішим є те, що під час війни особливих страждань зазнають діти. На нашу думку, важливу місію у подоланні