Інженерно-технічні заходи цивільного захисту (цивільної оборони) та містобудування: посібник. К.: КІМ, 2007, 2008. 636 с., 152 с.

5. Безпека під час навчання рекомендації щодо організації укриття. URL: https://mon.gov.ua/ua/news/bezpeka-pid-chas-navchannya-rekomendaciyi-shodo-organizaciyi-ukrittya (дата публікування: 28.07.2022).

6. Особливості організації 2022/23 навчального року. URL:https://mon.gov.ua/ua/news/osoblivosti-organizaciyi-202223-navchalnogo-roku (дата публікування: 06.07.2022).

7. Щодо здійснення заходів захисту вихованців під час освітнього процесу в умовах воєнного стану та надзвичайних ситуацій. URL: https://uied.org.ua/wpcontent/uploads/2022/04/shhodo_zdijsnennya_zahodiv_zahystu_vyhovancziv_pid_chas_osvitnogo_proczesu_v_umovah_voyennogo_stanu_ta_nadzvychajnyh_sytuacziyah.pdf (дата публікування: квітень 2022).

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В РЕАЛІЯХ ПОЧАТКОВОЇ ШКОЛИ: ОСНОВНІ ВИКЛИКИ ТА РІШЕННЯ

Ліненко Н. І.

Ліцей № 6 "Лідер" Полтавської міської ради

Анотація. *Стаття присвячена аналізу викликів, які виникають в контексті забезпечення кібербезпеки в початковій школі. Розглядаються основні аспекти, пов'язані з кібербезпекою в освітньому середовищі для дітей, батьків та вчителів. Стаття висвітлює важливість розуміння кіберзагроз та вміння дітей використовувати цифрові технології безпечно. Розглядаються ключові виклики, такі як нестача належної технічної інфраструктури, недостатня підготовка вчителів до роботи з кібербезпекою, відповідальність батьків у контролі та навчанні дітей, а також відповідальне використання технологій в освітньому процесі. Описано можливі рішення для забезпечення кібербезпеки в початковій школі, такі як розвиток цифрової грамотності*

серед учнів, навчання вчителів кібербезпеці, співпраця між школою, батьками та відповідними організаціями, а також впровадження заходів захисту персональних даних та відповідального використання технологій в освітньому процесі.

Ключові слова: *кібербезпека, початкова школа, діти, батьки, вчителі, технічна інфраструктура, освітній процес, цифрова грамотність, безпекова поведінка в мережі, захист персональних даних, кіберзагрози, співпраця, відповідальне використання технологій, родинне та шкільне середовище.*

З ростом використання комп'ютерів, планшетів, смартфонів та доступу до Інтернету в початкових школах, діти стають більш вразливими перед можливими кіберзагрозами. Оскільки діти у цьому віці можуть бути вразливі до різних кіберзагроз, вони можуть бути більш схильні до впливу шкідливих контенту, кіберзнущань, онлайн-шахрайства та інших загроз. Поряд з тим, ризик витоку особистої інформації, неправильного використання соціальних мереж та інших цифрових інструментів також може бути високим серед дітей початкової школи. Батьки, вчителі та адміністрація школи мають бути свідомими про ці ризики та вживати заходів для забезпечення кібербезпеки дітей в цьому віковому діапазоні.

За даними Кіберполіції України, кількість випадків кібербулінгу, кібершантажу, розповсюдження дитячої порнографії та інших кіберзлочинів, пов'язаних з дітьми, постійно зростає. Згідно з дослідженням компанії McAfee "Діти та електронні пристрої: 2021", лише 27% батьків свідомо навчають своїх дітей про кібербезпеку, тоді як 43% дітей віком від 8 до 12 років вважають, що мають достатні знання щодо кібербезпеки, хоча це не завжди відповідає дійсності. За даними Pew Research Center, більше 80% дітей в США віком 6-12 років мають власний смартфон або планшет, але менше 50% батьків встановлюють обмеження на використання цих пристроїв та контролюють вміст, до якого діти мають доступ. Діти початкового шкільного віку можуть бути вразливі до ризиків, пов'язаних з використанням соціальних мереж,

онлайн-комунікації та небезьпекової поведінки. За даними досліджень, більше 60% дітей віком від 8 до 12 років мають акаунти в соціальних мережах, і вони можуть бути вразливі до кібербулінгу, неприпустимого контенту та незнайомців, з якими вони взаємодіють онлайн.

Використання технологій у навчальному процесі, включаючи дистанційну освіту, зокрема через пандемію COVID-19 та воєнний стан в країні, питання кібербезпеки стає ще більш актуальним. Забезпечення безпечного користування технологіями та Інтернетом має бути важливою частиною педагогічної роботи в початкових школах.

Заходи щодо кібербезпеки в початковій школі можуть допомогти навчити дітей правилам безпечного користування Інтернетом, захищати свою особисту інформацію, розпізнавати небезпечний контент, відповідно взаємодіяти в цифровому середовищі та реагувати на кіберзагрози.

Одним з важливих аспектів забезпечення кібербезпеки в початковій школі є освіта дітей, батьків та педагогів щодо кібербезпеки. Діти мають бути ознайомлені з основними правилами безпечного користування Інтернетом, включаючи використання сильних паролів, не розголошення особистої інформації, обережне завантаження файлів та відкриття посилань, розпізнавання шкідливого контенту та повідомлень, а також процедури повідомлення про кіберзагрози.

Важливо проводити навчання дітей про основні правила кібербезпеки, такі як ніколи не розголошувати свої особисті дані в Інтернеті, не розміщувати приватні фотографії чи відео відкрито, не відкривати незнайомі посилання та не спілкуватися з незнайомими особами онлайн без дозволу батьків чи вчителів. Забезпечення використання фільтрів контенту на комп'ютерах і відеоіграх в школі, щоб запобігти доступу до непридатного контенту, такого як насильство, наркотики або порнографія. Вчити дітей використовувати сильні паролі та не ділитися ними з іншими особами, крім батьків або вчителів. Також варто регулярно міняти паролі на облікових записах, щоб уникнути несанкціонованого доступу. Важливо переконатися, що використовувані

додатки та програми відповідають віковим можливостям дітей і мають безпечні налаштування приватності. Вчити дітей завжди запитувати дозвіл вчителя або батьків перед встановленням нових додатків або програм на пристрої. Бути пильними до можливних кіберзагроз, таких як віруси, шкідливі програми, фішингові атаки тощо. Пояснити дітям, що вони не повинні відкривати незнайомі файли, посилання чи відповідати на підозрілі електронні повідомлення або листи. Наголошувати, що можна використовувати лише довірені та безпечні веб-ресурси, такі як освітні сайти, пошукові системи, електронні бібліотеки та інші джерела з перевіреною інформацією. Також повинні бути обережні при використанні соціальних мереж, форумів або чат-кімнат, де можуть з'явитися неприпустимі вміст або небажані контакти.

Важливо співпрацювати з батьками та вчителями для забезпечення кібербезпеки в початковій школі. Залучення батьків до навчання дітей правилам кібербезпеки вдома, співпраця з вчителями для проведення навчальних заходів та організації безпечного інтернет-середовища в школі можуть допомогти забезпечити кібербезпеку дітей. Батьки та вчителі мають бути освіченими щодо ризиків, які виникають при використанні Інтернету дітьми, і вміти надавати підтримку та нагадувати правила кібербезпеки. За даними досліджень, менше 30% батьків регулярно обговорюють з дітьми правила безпеки в Інтернеті та використання цифрових технологій. Вчителі можуть включати в педагогічну практику уроки з кібербезпеки, розповідати про реальні приклади кіберзагроз, проводити тренінги та семінари для батьків та учнів. Важливо встановити обмеження на час, витрачений дітьми на використання електронних пристроїв, таких як комп'ютери, планшети або смартфони. Забезпечення регулярних перерв від екрану, зміна активностей та включення режиму безпечного перегляду можуть бути корисними відповідними заходами.

Забезпечення кібербезпеки в початковій школі є важливим аспектом виховання дітей в цифровому світі. Це може включати проведення регулярних навчальних заходів, тренінгів та семінарів для дітей, батьків та вчителів з

питань кібербезпеки. Діти повинні навчатися визнавати потенційні загрози в Інтернеті та розуміти, як поводитися в безпечний спосіб.

Поруч з цим, важливо також встановлювати технічні заходи безпеки, такі як антивірусне програмне забезпечення, брандмауери, фільтри веб-контенту та інші засоби захисту на комп'ютерах шкільної мережі та інших електронних пристроях, що використовуються в навчальному процесі.

Ефективне забезпечення кібербезпеки в початковій школі вимагає комплексного підходу, включаючи навчання дітей правилам кібербезпеки, використання технічних засобів захисту, співпрацю з батьками та вчителями, а також постійний моніторинг та оновлення заходів безпеки з метою забезпечення безпечного користування Інтернетом та іншими електронними ресурсами.

Список використаних джерел

1. Cox Communications. (2019). National Survey Finds Cyberbullying and Screen Time Among Top Concerns for Parents in America. Retrieved from https://www.cox.com/aboutus/newsroom/national-survey-finds-cyberbullying-and-screen-time-among-top-concerns-for-parents-in-america.html

2. Education Week. (2021). Cybersecurity in K-12 Schools: Urgent Needs and Key Challenges. Retrieved from https://www.edweek.org/technology/cybersecurity-in-k-12-schools-urgent-needs-and-key-challenges/2021/04

3. Коваленко О. В. Теоретичні засади проектування системи забезпечення кібербезпеки України. *Derzhavne upravlinnya udoskonalennya ta rozvytok*. 2022. № 10. URL: https://doi.org/10.32702/2307-2156.2022.10.12 (дата звернення: 12.04.2023).

4. Бабич Є. Ю. Забезпечення кібербезпеки в Україні : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/5102 (дата звернення: 12.04.2023).

5. International Society for Technology in Education (ISTE). (2017). ISTE Standards for Students. Retrieved from https://www.iste.org/standards/for-students

6. National Cybersecurity Alliance. (2020). Stay Safe Online. Retrieved from https://staysafeonline.org/

ЦИФРОВІЗАЦІЯ ЯК ЕЛЕМЕНТ ОХОРОНИ КУЛЬТУРНИХ ОБ'ЄКТІВ В УМОВАХ ВІЙНИ

Лук'яненко О. В.

Полтавський національний педагогічний університет ім. В. Г. Короленка

Анотація: *у статті розкривається питання збереження пам'яток культури та мистецтва в Україні в період російсько-української війни. Визначаються вихідні позиції та стандартні механізми реагування на випадок загрози об'єктам культури у ході воєнних дій та подається огляд мотивів та можливості цифровізації пам'яток.*

Ключові слова: *цифровізація, об'єкти культури, музеї, доповнена реальність, російсько-українська війна.*

Відкрита агресія російської федерації проти України 24 лютого 2022 року стала новим етапом боротьби за національну минувшину, осібне місце в якій відіграють пам'ятки культури та мистецтва. Їхня безпека, як і безпека громадян, стала частиною щоденної роботи спеціалістів різних установ та організацій – від музейних працівників, на яких покладена безпосередня відповідальність за їхнє збереження, до працівників МНС та Національної поліції, котрі стали причетними до порятунку об'єктів культури з-під завалів та з вогню у розтрощених росією українських містах та селах. Їх можна характеризувати як борців за порятунок національної пам'яті від культурного геноциду – цілеспрямованих атак загарбника, поєднаних з практикою заборони, вилучення та знищення української літератури, викрадення культурних цінностей та архівних документів, і русифікації окупованих територій.