У межах цього дослідження були проаналізовані важливі аспекти забезпечення інформаційної безпеки з погляду управління базами даних. На основі аналізу було визначено та обговорено чотири основні кроки забезпечення інформаційної безпеки бази даних. Загалом наведені в роботі етапи та методи забезпечення інформаційної безпеки баз даних є важливими елементами управління ризиками та збереження конфіденційної інформації. Їх впровадження може значно підвищити рівень кібербезпеки та запобігти потенційним загрозам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Smith J. The Impact of Modern Technologies on Communication Skills. *Journal of Communication Studies.* 2021. Vol. 45, № 2. P .78–92.
2. Anderson R. Et al. Insider Threats to Database Security: Case Studies and Mitigation Strategies. *Information Security Symposium.* 2023. P. 75–88.
3. Davis L. The Role of Human Error in Database Security Breaches. Security Management Magazine. 2023. Vol. 22, № 3. P. 60–73.
4. Мазур Ю. О., Зелінська О. В. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. *Прикладні аспекти сучасних міждисциплінарних досліджень:* матеріали І Всеукраїнської науково-практичної конференції (м. Вінниця, 26 листопада 2021 р.). Вінниця: ДонНУ імені Василя Стуса. 2021. С. 102–104. URL: https://jpasmd.donnu.edu.ua/issue/view/403
5. Денисюк В. В. Важливість кібербезпеки в сучасному світі. *Комп'ютерні технології обробки даних:* матеріали ІІ Всеукраїнської науково-практичної конференції (м. Вінниця, 10 грудня 2021 р.). Вінниця: ДонНУ імені Василя Стуса. URL: https://jktod.donnu.edu.ua/article/view/11614
6. Степанюк О. С., Січко Т. В. Особливості використання реляційних та нереляційних баз даних в Big Data. *Комп'ютерні технології обробки даних:* матеріали всеукр. наук.-практ. конф., м. Вінниця, 2020. С. 103–106.

УДК 004.056-028.63:37.091.2

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯЯ ЦИФРОВОЇ БЕЗПЕКИ ПІД ЧАС РЕАЛІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДАХ ОСВІТИ

О. В. Дорош, В. Ю. Василенко

Анотація. У статті досліджується питання цифрової безпеки в освітньому процесі, аналізується законодавча база та стратегічні документи, які визначають цифрову трансформацію української освіти. Акцентовано на розвитку цифрових компетентностей учасників освітнього процесу та наголошено на важливості забезпечення безпеки цифрового середовища. Були зазначені проблеми низького рівня цифрової грамотності, обмеженого доступу до комп'ютерного обладнання та інтернету, а також відсутності високоякісного цифрового освітнього контенту.

Ключові слова: цифрова безпека, цифрова грамотність, освіта, цифрові навички.

Вступ. У сучасному світі, де цифрові технології відіграють важливу роль, освіта є основою будь-якого суспільства. Освіта не тільки дає людині знання та навички, але й визначає її здатність адаптуватися до середовища, що швидко змінюється. Оскільки технології продовжують розвиватися і стають все більш взаємопов'язаними, ризик загроз для освітнього процесу є найвищим. У цьому контексті цифрова безпека стає важливою частиною освіти.

Основний розділ. Освіта – важливий аспект соціального життя, безпеки та стабільності країни, які все більше набувають числового формату. Часто інформаційний контент є засобом маніпулювання свідомістю, причиною конфліктів і негативних проявів. Питання свідомого споживання інформації, особливо в освіті, критичного аналізу та якості інформації стали стратегічними для розвитку країн на національному та міжнародному рівнях. Отже, розвиток цифрових технологій стимулює створення цифрової безпеки в закладах освіти. Сучасна освіта з березня 2020 року в основному реалізовувалась у дистанційному та/або онлайн-форматі, через це питання цифрової безпеки у вищій освіті має пріоритетне значення [1]. В умовах реформування та модернізації освітнього середовища за допомогою цифрових технологій цифрова безпека освітніх систем є основною тенденцією. Це забезпечується шляхом підвищення грамотності у використанні сучасних цифрових технологій, удосконалення правового регулювання відповідальності за порушення законодавства у сфері інформаційної безпеки молоді. Особливе значення відіграє впровадження дистанційних методів навчання на всіх рівнях освіти, активі-

зація правової освіти у сфері інформаційної безпеки у мережі Інтернет, а також вдосконалення вимог до інформаційно-освітньої роботи, яка реалізується у сфері освіти [2].

Національні та європейські документи висвітлюють питання цифровізації та цифрової безпеки у вищій освіті. 3 лютого 2021 року Міністр освіти і науки С. Шкарлет у звіті на засіданні Ради з питань освіти, науки та інновацій зазначив, що впровадження цифрової трансформації освіти і науки є пріоритетним напрямом роботи МОН (Звіт Міністерства освіти і науки України з виконання оперативного плану Міністерства освіти і науки України на 2020 рік та основні цілі на 2021 рік [3]). У багатьох нормативно-правових документах наголошується на необхідності цифровізації освіти. Зокрема, Закон України «Про освіту» визначає інформацію та комунікацію між ключовими компетентностями [4].

У проєкті Концепції Цифрової адженди України 2020 зазначено, що цифровізація має стати об'єктом національного фокусу та комплексного управління [1]. В аналізі цифрового розвитку України справедливо зауважено, що сфера «цифрових» навичок та компетенцій розвивається клаптиково, хаотично та окремо від академічної (так званої формальної) освіти. Проведення цифровізації має супроводжуватися підвищенням рівня довіри і безпеки. Інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є невід'ємними передумовами одночасного цифрового розвитку та відповідного передбачення, попередження, усунення та управління супутніми ризиками [5].

Міністерство освіти і науки України підготувало та винесло на громадське обговорення проєкт «Концепції цифрової трансформації освіти і науки до 2026 року», який візуалізує комплексне системне стратегічне бачення цифрової трансформації в цих сферах та відповідає засадам реалізації органами виконавчої влади принципів державної політики цифрового розвитку, постанові Кабінету Міністрів України від 30 січня 2019 року. Цією постановою затверджено реалізацію засад національної політики цифрового розвитку органом виконавчої влади [6]. Про необхідність розвитку «електронного навчання і формування цифрової компетентності учасників освітнього процесу» йдеться у наказі МОН України «Про затвердження Положення про Національну освітню електронну платформу» (Наказ Міністерства освіти і науки України № 523 від 22.05.2018) [1].

Сучасні освітні та наукові системи мають пройти фундаментальну цифрову трансформацію та адаптуватися до глобальних тенденцій цифрового розвитку, щоб кожен міг успішно реалізувати свій потенціал. Сьогодні все більше професій вимагають набуття цифрових компетенцій високого рівня та володіння новітніми технологіями. Проєкт Концепції спрямований на подолання низки проблем, зокрема:

- низький рівень цифрових компетентностей учасників освітнього процесу;
- застарілий зміст освіти з навчальних предметів інформаційної галузі;
- недостатня кількість комп'ютерного обладнання та відсутність широкосмугового доступу до інтернету в закладах та установах системи освіти і науки;
- відсутність якісного цифрового освітнього контенту для здобуття освіти;
- відсутність актуальної, достовірної інформації про здобувачів освіти, педагогічних та науково-педагогічних працівників, а також науковців для прийняття управлінських рішень та моніторингу ефективності політик;
- забюрократизованість процесів внутрішнього документообігу закладів та установ освіти і науки;
- незручність отримання послуг та сервісів у системі освіти, недоступність наукових ресурсів та інфраструктур тощо [6].

Цифрова безпека базується на цифровій компетентності. Цифрова компетентність є однією з 8 ключових компетенцій, визначених ЄС для повноцінного життя та діяльності. У 2021 році Міністерство цифрової трансформації України розробило Рамку цифрових компетенцій громадян України (Description of the Digital Competencies Framework for Citizens of Ukraine, 2021). Наразі ця Рамка містить 4 виміри, 6 сфер, 30 компетентностей та 6 рівнів володіння цифровими

компетентностями. Безпека у цифровому середовищі є однією з шести сфер компетентностей, визначених у першому Вимірі. До цієї сфери віднесено такі компетентності:

- захист пристроїв: безпечне підключення до інтернету вимагає здатності захищати пристрої та цифровий вміст, розуміння ризиків і загроз у цифровому середовищі; розуміння заходів безпеки та захисту, беручи до уваги питання надійності та конфіденційності;
- захист персональних даних і безпека в інтернеті передбачає дотримання правил: конфіденційності в цифровому просторі; розуміння того, як ідентифікаційна інформація використовується та поширюється, зберігаючи здатність захистити себе та інших від небезпеки.

Як використовуються ваші особисті дані:

- захист особистих даних споживача від шахрайства та зловживань вимагає знання найважливіших правових положень щодо захисту споживачів в інтернеті;
- уміння ідентифікувати підозрілі інтернет-магазини та порівнювати ціни; вживати заходів для захисту прав споживачів;
- захист здоров'я та благополуччя передбачає здатність уникати ризиків і загроз фізичному та психічному здоров'ю під час використання цифрових технологій; здатність захистити себе та інших від можливих небезпек у цифровому середовищі (наприклад, кіберзалякування, фішинг); про цифрові технології знання для забезпечення соціального добробуту та соціальної інтеграції;
- охорона навколишнього середовища передбачає визнання впливу цифрових технологій та їх використання на навколишнє середовище;
- враховуючи масштаби та рівень проблеми, потрібно звернути особливу увагу на формування медіакомпетентності, критичного мислення, цифрової обізнаності та доброчесності в процесі здобуття вищої освіти [1].

Цифровізація освітнього процесу в Україні принесла численні переваги, але також створила нові ризики та загрози цифровій безпеці. Використання цифрових технологій в освіті зробило навчальні заклади вразливими до кібератак, витоків даних та інших загроз цифровій безпеці. Ці ризики можуть поставити під загрозу конфіденційність, цілісність і доступність освітніх даних, піддаючи здобувачів, викладачів і персонал різним ризикам і загрозам. Тому важливо визначити потенційні загрози та вжити необхідних заходів для забезпечення цифрової безпеки освітнього процесу.

Висновки. Підсумовуючи, можна зазначити, що важко переоцінити важливість цифрової безпеки в освітньому процесі в Україні. Оскільки технології все частіше використовуються в освіті, існує багато загроз для цифрової безпеки, які необхідно вирішити. Проте було вжито заходів для забезпечення цифрової безпеки в освітньому процесі, включно зі впровадженням політики кібербезпеки та навчання викладачів і здобувачів безпечним цифровим практикам.

Переваг забезпечення цифрової безпеки в освіті багато, зокрема захист конфіденційної інформації та сприяння безпечному і надійному навчальному середовищу. Загалом важливо, щоб цифрова безпека залишалася головним пріоритетом освітнього процесу в Україні. Важливо впроваджувати політику кібербезпеки, яка захищає конфіденційну інформацію та забезпечує безпечне й захищене середовище навчання.

Abstract. The article examines the issue of digital security in the educational process and analyzes the legislative framework and strategic documents that determine the digital transformation of Ukrainian education. Attention is focused on the development of digital competences of participants in the educational process and the importance of ensuring the security of the digital environment is emphasized. New challenges were noted, such as low levels of digital literacy, limited access to computer equipment and the Internet, and a lack of high-quality digital educational content.

Keywords: digital security, digital literacy, education, digital skills.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Прокоф'єва М. О., Султанова Л. Ю. Аналіз досліджень з цифрової безпеки в галузі вищої освіти. *Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій*: матеріали ІІ Всеукр. наук.-практ. конф., м. Глухів, 01 квітня 2022 року Глухів, 2022. С. 260–262.

2. Близнюк М. Цифрова безпека освітнього процесу: Європейський поступок Естонії та перспективи України. *Наукові записки*. URL: https://lib.lntu.edu.ua/sites/default/files/2023 (дата звернення: 09.10.2023).

3. Звіт Міністерства освіти і науки України з виконання оперативного плану Міністерства освіти і науки України на 2020 рік та основні цілі на 2021 рік. URL: https://mon.gov.ua/storage/app/media/rizne/2021/03.02.2021/ZVIT%20MINISTERSTVA%20OSVITY%20I%20NAUKY%20UKRAYINY%20Z%20VYKONANNYA%20OPERATYVNOHO%20PLANU.pdf (дата звернення: 09.10.2023).
4. Про освіту: Закон України від 05.09.2017 р. № 2145-VIII. Дата оновлення: 02.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2145-19 (дата звернення: 10.10.2023).
5. Ляхоцька Л. Л., Ляхоцький В. П. Цифрова освіта і наука – запорука національної безпеки України. Національна безпека України у викликах новітньої історії: кол. монографія. Київ: ДП «Експрес-об'ява», 2019. С. 277–289.
6. Концепція цифрової трансформації освіти і науки. URL: https://mon.gov.ua/ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorennya (дата звернення: 10.10.2023).

УДК 004.415.3

ПРОЄКТУВАННЯ ЗАСТОСУНКУ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ТА КОНТРОЛЮ ОСОБИСТИХ ФІНАНСІВ

А. О. Ємельянова, О. В. Зелінська

Анотація. У дослідженні подана інформація про процес проектування вебзастосунку інтелектуального аналізу і контролю власних фінансів. Описуються механізми збору і аналізу даних, зазначаються необхідні обчислення для здійснення аналітики грошових операцій. Наводиться опис основних технологій реалізації, а саме мови програмування JavaScript та її інтерфейсної бібліотеки React.js, їх тенденції розвитку, переваги та особливості використання. Результати проведених досліджень є основою і відіграють важливу роль у подальшій розробці вебзастосунку – програмній реалізації.

Ключові слова: вебзастосунок, електронний контроль фінансів, інтелектуальний аналіз даних, JavaScript, React.js.

Гроші відіграють мало не першочергову роль у житті людини, тому відстежування власних фінансів є надзвичайно важливим і актуальним питанням у сучасному світі. Знання того, скільки грошей має людина, які витрати вона повинна зробити та скільки грошей очікувати, допомагає планувати своє життя та забезпечувати фінансову стабільність. Відсутність контролю над особистими фінансами може призвести до низки проблем, як-от накопичення боргів, витрат, що перебільшують дохід, неспроможність забезпечити себе необхідними товарами та послугами, нестабільність фінансів тощо.

Додаток для контролю за фінансами може допомогти зрозуміти, куди йдуть гроші, де можна зекономити та як краще розпланувати свій бюджет. Вебзастосунок для контролю за особистими фінансами повинен надавати користувачу зручні інструменти для відстеження своїх доходів та витрат, аналізу своєї фінансової ситуації та планування витрат на майбутнє.

Метою статті є проєктування застосунку, який має полегшити ведення та контроль особистих фінансів із елементами інтелектуального аналізу даних на основі мови програмування JavaScript та її популярної і широко використовуваної інтерфейсної бібліотеки React.js.

Механізм аналізу даних включає кілька кроків і методів, які допомагають отримати інсайти з великого обсягу даних. Загальний опис механізму даних зображений на рис. 1.

Рис. 1. Механізм аналізу даних

Розглянемо більш детально кожен крок процесу аналізу даних [1–3].