

Інформаційні джерела:

1. Воронкова В., Нікітенко В., Метеленко Н. Еволюція концепції від смарт-освіти до смарт-економіки та смарт-бізнесу. Економіка та суспільство. 2023. № 48. <https://doi.org/10.32782/2524-0072/2023-48-17>
2. Cherep A., Voronkova V., Andriukaitiene R., Nikitenko V. The concept of creative digital technologies in the tourism business in the conditions of digitalization. Humanities Studies. 2020. Vol. 5. No. 82. P.196–209.
3. Краус К.М., Краус Н.М. Інноваційне підприємництво і цифровий бізнес: науково-економічна фіча розвитку та зміни в управлінні. Ефективна економіка. 2020. № 4. DOI: 10.32702/2307-2105-2020.4.8

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Нечитайло Ю.А., канд. техн. наук, доц.
Мироненко В.О., здоб. ВО
Державний біотехнологічний університет

Цифрова трансформація є одним із важливих актуальних процесів сучасності, що охоплює всі сфери людського життя. Цифрові технології відкривають нові можливості для розвитку економіки, освіти, медицини, культури, демократії та інших аспектів суспільства. Однак поряд із перевагами цифрова трансформація також приносить нові виклики та загрози, особливо у сфері національної безпеки. Кіберзагрози, кіберзлочинність, кібервійна, кібершпигунство, кібертероризм, кібератаки на критичну інфраструктуру, національну оборону, державне управління, виборчі системи, особисті дані громадян та інші цілі – це реальність, з якою Україна та інші країни світу зтикаються в цифрову епоху [4].

Розглянемо умови та сучасні тенденції розвитку інформаційного суспільства, а також ключові проблеми впровадження інформаційно-комунікаційних та цифрових технологій у вітчизняну освіту, які потребують вирішення, а саме формування та широке впровадження єдиного освітнього інформаційного простору України та забезпечення належного наукового супроводу цих процесів.

Розгортання та вдосконалення необхідних елементів інфраструктури регіональних інформаційно-телекомунікаційних мереж, взаємопов'язаних між собою та з глобальною мережею Інтернет, дозволяють подолати «цифрову нерівність» у різних регіонах України, зокрема в сільській місцевості; низький рівень інформаційно-комунікаційних компетентностей (ІКТ-компетентностей) та цифрової компетентності населення; використання застарілих підходів у навчанні та низьку мотивацію суб'єктів освітнього процесу щодо використання новітніх ІКТ; несформованість цілісної державної політики щодо застосування інформаційно-комунікаційних технологій в освіті, недосконалість нормативно-

правової бази, що не забезпечує побудову інформаційного суспільства і, як наслідок, стримує цифровізацію освіти в Україні.

Також маємо пріоритети, технологічні принципи побудови інформаційно-освітнього середовища, які визначають актуальні завдання розвитку комп'ютерно-орієнтованих освітніх систем, створення та використання електронних освітніх ресурсів, зокрема електронного підручника, створення середовища для неперервного розвитку цифрової компетентності суб'єктів освітнього процесу, проведення педагогічних досліджень з питань інформатизації освіти, розроблення та впровадження програми підвищення обізнаності громадян з питань інформаційної безпеки, кібербезпеки та захисту конфіденційної інформації, зокрема персональних даних, від загроз їх несанкціонованого використання [2]. У сучасному цифровому середовищі, де технологічний прогрес рухається стрімко, національна безпека стає надзвичайно вразливою перед новими загрозами та викликами.

Цифрова трансформація призводить до появи нових загроз. Однією з основних загроз є кібератаки, які можуть бути спрямовані на критичну інфраструктуру, владні системи або економічні структури. Зловмисники можуть використовувати різноманітні техніки: фішинг, атаки на інтернет-підключені пристрої, використання шкідливих програм тощо. Крім того, зростає ймовірність кібершпигунства та кібертероризму, де групи або держави можуть використовувати цифрові канали для здійснення шпигунської діяльності або для терористичних цілей.

За даними огляду найпопулярніших інцидентів безпеки за рік ресурсом IT Governance [1], який допомагає організаціям боротися із загрозою кіберзлочинності та іншими недоліками інформаційної безпеки і пропонує різноманітні ресурси, покликані зрозуміти та пом'якшити загрози, масштаби проблеми вражають. Наприклад, у грудні 2023 року кількість глобальних витоків даних і кібератак становила 2 241 916 765 порушених записів. Дослідник безпеки Джеремайя Фаулер виявив незахищену базу даних, яка розкриває понад 1,5 мільярда записів, що містять конфіденційні дані про власність мільйонів людей. Оприлюднені дані включали інформацію про власників нерухомості, адреси, дати покупки, іпотечна компанія, суму іпотечного кредиту, податкові номери, сплачені податки, особисті дані продавців, інвесторів, дані внутрішніх журналів користувачів тощо. Згідно зі звітом IBM [3] про вартість витоку даних (Cost of a Data Breach), середня вартість одного витоку для компаній у всьому світі становить 4,45 мільйони доларів. Із розвитком інструментів невпинно розвиваються й технології кіберзлочинності.

З метою протидії кіберзагрозам та забезпечення національної безпеки в умовах цифрової трансформації, сучасні методи та технології кіберзахисту відіграють вирішальну роль. Також важливим є розвиток кібербезпеки Збройних Сил України та відповідність їхніх зусиль новим формам атак та загрозам. Удосконалення кіберзахисту передбачає розробку технологій виявлення та відповіді на кібератаки в реальному часі, що вимагає постійного вдосконалення методів протидії кіберзагрозам. Попередження кіберзагроз

також включає в себе ефективну кібергігієну та навчання персоналу щодо кібербезпеки. Широкомасштабні кампанії навчань та тренінги забезпечують кінцевих користувачів та відповідальних фахівців необхідними знаннями та навичками для ефективного управління кіберзагрозами [4].

Інформаційні джерела:

1. IT Governance Blog [Електронний ресурс] // List of Data Breaches and Cyber Attacks in 2023. – 2024. – Режим доступу до ресурсу: <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>
2. Modern tasks of digital transformation of education [Електронний ресурс] // Digital Library NAES of Ukraine. – 2020. – Режим доступу до ресурсу: <https://lib.iitta.gov.ua/id/eprint/722869/>.
3. Кібербезпека в епоху цифрових технологій: думка експерта [Електронний ресурс] // Anywhere Club – Режим доступу до ресурсу: <https://aw.club/global/uk/blog/cybersecurity-in-the-digital-age>.
4. Цифрова трансформація як фактор покращення національної безпеки України [Електронний ресурс] // Центр безпекових досліджень “СЕНСС”. – 2024. – Режим доступу до ресурсу: <https://censs.org/digital-transformation-as-a-factor-in-improving-the-national-security-of-ukraine/>.

АЛГОРИТМ СИСТЕМИ АВТОМАТИЗОВАНОГО КЕРУВАННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ ВИРОБНИЦТВА МАКАРОННИХ ВИРОБІВ

**Панов А.О.
Руденко О.М.**

Державний біотехнологічний університет

Макарони – кулінарний напівфабрикат з висушеного прісного пшеничного тіста, який перед вживанням в їжу піддається варінні. Основною сировиною для виробництва макаронів є пшеничне борошно, а також питна вода. Для підвищення харчової цінності макаронів іноді використовують додаткова сировина: яйце продукти, білкові суміші та інші харчові добавки-збагачувача. Застосовується борошно з твердої і м'якою склоподібної пшениці у вигляді крупки або напівкрупки. Деякі види макаронних виробів виготовляють із хлібопекарського борошна. Додаткове сировину перетворюють в рідкі проміжні напівфабрикати [1].

Виробництво макаронних виробів включає такі основні стадії та операції:

- підготовка сировини до виробництва – зберігання, змішування, просівання і дозування борошна; приготування води і добавок-збагачувачів;
- дозування і змішування рецептурних компонентів; вакуумування крихтоподібної суміші;
- заміс і пресування тіста; формування та різання сирих тістових заготовок;
- сушка, стабілізація і охолодження тістових заготовок;