ФОРМУВАННЯ ЦИФРОВОЇ СТІЙКОСТІ УЧНІВ – АКТУАЛЬНЕ ЗАВДАННЯ СУЧАСНОЇ УКРАЇНСЬКОЇ ШКОЛИ

Пінчук О.П.
к. пед. н., с. н. с., заступниця директора з науково-експериментальної роботи
ORCID: https://orcid.org/0000-0002-2770-0838, pinchuk@iitlt.gov.ua
Інститут цифровізації освіти НАПН України
Буров О.Ю.
д. т. н., с.д.
провідний науковий співробітник відділу цифрової трансформації НАПН України
ORCID: https://orcid.org/0000-0003-0733-1120, burov.alexander@gmail.com
Інститут цифровізації освіти НАПН України

Неконтрольований доступ до Інтернету, активна включеність до соціальних медіа, використання смартфонів з одного боку надає підліткам можливості використовувати потужне інформаційне поле з колосальною кількістю відомостей, даних і зв'язків між ними, а з іншого – наражає їх на потенційні загрози: кіберзалякування та порушення конфіденційності, зокрема. Навчитися орієнтуватися в цифровому світі, адаптуватися та протистояти викликам – актуальне завдання загальної середньої освіти.

У світовій освітній практиці концептуалізовано поняття цифрової стійкості (digital resilience). Стійкість, на думку Angela Y. Lee та Jeffrey T. Hancock [1] може служити цінною теоретичною основою для спрямування зусиль на допомогу дітям отримати переваги від сучасних цифрових технологій і, водночас, бути захищеними від їх потенційної шкоди. У психології розвитку [2] стійкість відноситься до здатності людей успішно адаптуватися до викликів, що загрожують їхньому функціонуванню або здоровому розвитку. У [3] автори концептуалізують стійкість як те, що люди «виживають краще, ніж очікувалося, зважаючи на труднощі». Різноманітність індивідуальних особистісних характеристик, контекстуальних факторів і факторів навколишнього середовища можуть впливати на те, як люди сприймають і реагують на стресори [4]. Оскільки діти починають використовувати технології в ранньому віці, один із способів захистити їх від несприятливих наслідків – це підвищити їхні цифрові навички та грамотність у безпечному навчальному середовищі, щоб підготувати їх до вирішення ризикованих ситуацій в Інтернеті, перш ніж вони з ними зіткнуться. Так чи інакше, але всі визначення цифрових навичок (digital skills) та цифрових компетентностей (цифрові компетентності (digital competences) стосуються здатності людей прагматично та інтуїтивно реагувати на виклики та можливості цифрових технологій.

Зміни у сфері освіти в Україні, як у всьому світі були суттєвими, носили характер трансформаційних. Проте, протягом 2022-2023 рр. економічні, соціальні та культурні проблеми пандемії доповнилися проблемами війни, що консолідувала навколо України багато країн і народів. За даними ООН, більше 8 млн українців залишили батьківщину внаслідок початку інтервенції росії у 2022 р., з них 4.8 млн отримали тимчасовий захист у країнах Європи [5]. За тими ж даними, серед отримувачів тимчасового захисту приблизно 33% складають діти, тобто більше 1.5 млн. Як наслідок, ці факти вплинули на світову спільноту та створили глобальні виклики: 1) залучення сотень тисяч школярів різного віку до існуючих і стабільних шкільних систем приймаючих країн; 2) актуальна необхідність інтеграції та гармонізації здібностей цих молодих людей і вчителів із суспільством приймаючої країни; 3) необхідний час адаптації та когнітивні розриви через порушення соціального, когнітивного та освітнього розвитку українських школярів у нових умовах. Головною складністю є ймовірність втрати ними мотивації до навчання та цінностей, професійних орієнтирів.

Глобальні завдання та можливі рішення щодо освіти української молоді потребують урахування декількох нових факторів:

1. Система освіти українських здобувачів знань *de facto* перетворилася на три паралельні системи: українську, іноземну (вимагає інтеграції українських переміщених школярів та вчителів із системою приймаючої країни) та змішану (учні навчаються дистанційно в Україні та водночас у школах приймаючої країни).

2. Нове завдання для країн ЄС, які приймають українських школярів та вчителів, підтримати новоприбулих, а не залишити обдарованих та мотивованих дітей поза суспільством, адаптувати їх до нового ринку робочої сили.

3. «Розмивання» кордонів між освітніми системами різних країн через взаємовплив освітньо-пізнавальних систем (зокрема України) та країн Заходу.

4. У забезпеченні якісної освіти дітей України в умовах війни зростаючого значення набули культурний інтелект (внаслідок виникнення змішаного культурно-етнічного соціального середовища), використання цифрових технологій (навчання в змішаному та дистанційному форматі), інформаційно-психологічна безпека кібер-простору (кібер-безпека та кібер-захист).

У [6] розглянуто проблеми кібербезпеки (cyber security, CyS) учасників освітнього процесу, акцентується увага на тому, що ці проблеми не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають включати такі види захисту: правові, технічні, інформаційні, організаційні та психологічні. Серед психологічних засобів забезпечення кібербезпеки пропонується виокремити когнітивні, оскільки населення в цілому та особливо діти і молодь все частіше стають об'єктами кібер-атак, насамперед, їх когнітивна сфера, стаючи найбільш уразливою (слабкою) ланкою мережі. У людино-центричних мережах, що становлять постійно зростаючу частку серед загальних мереж, сама мережа набуває нових властивостей, діючи як самостійний складник (на додаток до таких факторів як вузол мережі, інтерфейс і зв'язки між вузлами). Загрози учасникам навчально-виховного процесу з боку кіберпростору доцільно розглядати як пасивні та активні, розробляючи адекватні засоби захисту та життєстійкості системи “суб’єкт освітнього процесу - засоби навчання – навчальне середовище”. Найбільш значущими серед кібер-загроз для учасників навчально-виховного процесу відзначаються методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки. Як складником підготовки учасників навчально-виховного процесу з питань кібербезпеки пропонується використовувати “кібер-вакцинацію”, тобто формування усвідомленого чуттєвого досвіду перебування під дією кібер-загрози та протидії їй як систему тренувальних заходів, які включають, крім традиційних методів, тренувальні “кібер-атаки”, а також формування знань і умінь стійкості (відновлення) по відношенню до кібер-загроз. Пропонується подальші дослідження проблеми зосередити на детальному розробленні видів загроз учасникам освітнього процесу, а також методам протидії. Особливе місце має зайняти проблематика стійкості до кібер-небезпек, яка може використовувати досвід підготовки операторів емерджентних галузей, у тому числі діагностування поточного стану людини та необхідне коригування з метою оптимізації її діяльності.

У широкому розумінні можливими цілями впливу кібербезпеки (окрім об’єктів критичної інфраструктури) можуть бути: бази даних, персональні дані, зокрема фінансові, засоби масової інформації, соціальні мережі, освіта та професійна підготовка, підручники, історіографічні видання. Організаційні засоби вирішення питань CyS пропонується розглядати як: інформування, навчання суб’єктів освітнього процесу основам культури кібербезпеки, створення спеціальних засобів CyS, розповсюдження засобів CyS, контроль використання, контроль контуру та поверхні кіберзахисту.

Кілька областей найбільш критичних і невідкладних потреб та прогалин знань, що розглядаються в програмах кібер-досліджень країн НАТО та інших країн, можна визначити як такі: психосоціальні, культурні, концептуальні та організаційні аспекти кібербезпеки. Слід

виділити такий аспект як тренування стійкості користувачів до дії кібер-загроз, тобто навчання “кібер-виживанню”.

Хоча технологічні рішення розробляються у відповідь на кібер-атаки, зростає поінформованість про те, що роль людської діяльності та прийняття рішень в галузі CyS має вирішальне значення для підвищення ефективності відповідей на виникаючі загрози. Особливо це важливо з точки зору майбутньої робочої сили, оскільки молодь є особливо чутливою до зовнішнього впливу і є найбільш активною частиною «мережевого населення».

У такому контексті набули підвищеної важливості дві нові тенденції в останні роки: кібер-ризики, пов’язані з широким *використанням хмарних технологій* (cloud security, ClS) в освіті, та стрімке *впровадження штучного інтелекту* (AI) в різні сфери життєдіяльності людини, у тому числі, в освітню діяльність. З огляду на проблеми сьогоднішні та найближчого часу, світові експерти дають такі рекомендації щодо майбутнього кібербезпеки.

Основи ClS: (1) Знайте своє середовище. (2) Зосередьтеся на запобіганні та безпечному дизайні. (3) Розширюйте можливості своїх розробників. (4) Узгодження та автоматизація з політикою як кодом [7]. (5) Вимірюйте те, що має значення.

Загрози безпеці, що створюються за допомогою AI: (1) Широкомасштабний, масовий, дуже переконливий фішинг (AI створює реалістичні та персоналізовані фішингові повідомлення, які важко відрізнити від справжнього спілкування; AI автоматизує створення об'єктів, завдяки чому зловмисникам швидше та простіше створювати переконливі повідомлення; генерація природної мови - AI створює текст, схожий на створений людиною, завдяки чому фішингові електронні листи виглядають справжніми). (2) Дипфейки – зображення, голос і відео. Діпфейки – це синтетичні засоби масової інформації, в яких людину на наявному зображенні чи відео замінюють на чужу подобу (способи: зміна обличчя, клонування голосу, маніпуляція з відео).

У процесі цифрової трансформації суспільства, а також кібер-війни як складника воєнних дій росії проти України перед педагогічною та психологічною науками постають нові проблеми, нові виклики, що потребують оперативного дослідження та створення на цій основі методологічних і методичних розробок.

Список літератури:

1. Angela Y. Lee, & Jeffrey T. Hancock. (2023). Developing digital resilience: An educational intervention improves elementary students’ response to digital challenges. Computers and Education Open, 5, 100144. https://doi.org/10.1016/j.caeo.2023.100144.

2. Masten, A., & Barnes, A. (2018). Resilience in Children: Developmental Perspectives. Children, 5(7), 98. https://doi.org/10.3390/children5070098

3. Allison S. Troy, Emily C. Willroth, Amanda J. Shallcross, Nicole R. Giuliani, James J. Gross, & Iris B. Mauss. Psychological Resilience: An Affect-Regulation Framework. (2023). Annual Review of Psychology, 74:1, 547-576. https://doi.org/10.1146/annurev-psych-020122-041854

4. Twenge, J. M., Martin, G. N., & Campbell, W. K. (2018). Decreases in psychological well-being among American adolescents after 2012 and links to screen time during the rise of smartphone technology. Emotion, 18(6), 765–780. https://doi.org/10.1037/emo0000403

5. Botelho V., & Hägele H. Integrating Ukrainian refugees into the euro area labour market. European Central Bank. The ECB Blog. 1 March 2023. https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog.230301~3bb24371c8.en.html

6. Биков В. Ю., Буров О. Ю., & Дементієвська Н.П. (2019). Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, 70(2), 313–331. https://doi.org/10.33407/itlt.v70i2.2876

7. The Five Fundamentals of Cloud Security White Paper. https://go.snyk.io/five-fundamentals-of-cloud-security.html.

8. Буров, О.Ю., Гриб'юк, О.О., Іванова, С.М., Пінчук, О.П., Соколюк, О.М., & Сухіх, А.С. (2023). Інформаційно-аналітичні матеріали до Спільного засідання Національної

академії педагогічних наук України й Комітету педагогічних наук Польської академії наук «Діти війни: як допомогти і убезпечити», (23 червня 2023 р.). https://lib.iitta.gov.ua/id/eprint/736189.