УДК 004.946.5.056:378.091.212
DOI https://doi.org/10.32782/ped-uzhnu/2026-11-21

Орлов Олексій Петрович,
ORCID ID: 0000-0002-2338-118X
кандидат філологічних наук,
доцент кафедри англійської та німецької філології
Полтавський національний педагогічний університет
імені В.Г. Короленка

ЦИФРОВА ГІГІЄНА СТУДЕНТІВ ЯК ПЕДАГОГІЧНА ПРОБЛЕМА

STUDENTS' DIGITAL HYGIENE AS A PEDAGOGICAL PROBLEM

Процес диджиталізації, який розглядається у статті, є ознакою сучасного суспільства. Усі сфери суспільства охоплені цифровою трансформацією, яка вносить корективи в управління, виробництво, професійну діяльність, змінюючи цінності, комунікацію, оцінки. Цифрова трансформація освіти регламентується державними документами, аналітичними науковими дослідженнями, статистичними оцінками тих змін, які відбуваються у середній та вищій освіті. Метою статті є розгляд ризиків, пов'язаних з безпекою цифрового середовища, оскільки кібербезпека стає нагальною проблемою, зокрема для розвитку молодого покоління. До цифрових загроз належить підвищена залежність від цифрової інфраструктури, хибні посилання під час пошуку інформації в мережі, фейкові новини, перешкоди під час навчального спілкування, демотивуючий вплив на учасників навчального процесу. У статті пропонуються засоби протидії цифровим небезпекам, об'єднані поняттям цифрової гігієни – динамічної комбінації правил, знань, умінь, навичок, способів мислення та інших особистих якостей з питань інформаційно-комунікаційних та цифрових технологій, спрямованих на безпечне, раціональне та відповідальне їх використання. Модель протидії цифровим небезпекам, запропонована для студентів, охоплює етапи: обізнаність, полювання, виявлення та тренування, кожен з яких можна назвати етапом розвитку кіберстійкості. Поняття стійкості по відношенню до кібербезпеки ідентичне поняттю цифрової гігієни, але має іншу лексичну конотацію. Пропонуються деякі форми роботи з формування цифрової стійкості, зокрема створення алгоритму концентрації уваги, проведений зі студентами Полтавського педагогічного університету. Розглянуто вплив медійного простору з огляду на кіберберзагрози і кібербезпеку, оскільки саме медіа є контентом і платформою навчання студентів. Полювання та виявлення фейкової інформації, обізнаність зі шляхами пошуку інформації, критичне сприйняття контенту, вміння концентруватися на навчанні – це перспективні проблеми подальшого дослідження.

Ключові слова: диджиталізація, цифрова гігієна, цифрова стійкість, кібербезпека, кіберзагрози, фейкова інформація.

The process of digitisation discussed in this article is a hallmark of modern society. All spheres of society are affected by digital transformation, which is changing management structures, production, professional activities, values, communication and assessments. The digital transformation of education is regulated by government documents, analytical scientific research, and statistical assessments of the changes taking place in secondary and higher education. Measures to counter digital threats, united by the concept of digital hygiene, which is defined as a dynamic combination of rules, knowledge, skills, abilities, ways of thinking and other personal qualities related to information and communication technologies and digital technologies, aimed at their safe, rational and responsible use, are proposed in the article. Digital threats include increased dependence on digital infrastructure, false links when searching for information online, fake news, obstacles to educational communication, and a demotivating effect on participants in the educational process. The model for countering digital dangers proposed for students covers the following stages: awareness, hunting, detection and training, each of which can be called a stage in the development of cyber resilience. The concept of resilience in relation to cybersecurity is equivalent to digital hygiene, but has a different lexical connotation. Some forms of work on the formation of digital resilience are proposed: the creation of an algorithm for concentration of attention, conducted with students of Poltava Pedagogical University. The influence of the media space is considered in terms of cyber threats and cybersecurity, since it is the media that is the content and platform for student learning. Hunting for and identifying fake information, awareness of ways to search for information, critical perception of content, and the ability to concentrate on learning are promising topics for further research.

Key words: digitalisation, digital hygiene, digital resilience, cybersecurity, cyber threats, fake information.

Постановка проблеми. Цифрова трансформація – це масштабний та стратегічно орієнтований процес, спрямований на докорінну зміну виробничих, соціальних, ціннісних моделей, організаційної та управлінської культури. Людські активи, передовсім інтелект, стають найціннішим об'єктом інвестування, капіталом, який фінансуються все інтенсивніше як активний спосіб уникнення зростаючих глобальних ризиків.

Глобальна цифровізація визначає новий етап розвитку кібернетичних технологій, за логікою американської вченої К. Н. Хейлз [7],

обумовлений об'єднанням потужною спільною дією – інформації, керування та комунікації. Стрімкий розвиток віртуального простору та штучного розуму випереджають процес вивчення й експериментального дослідження ризиків застосування нових для людства засобів. Як образно висловився У. Фредкін, «не підпорядковані цілям сталого розвитку інформативні потоки здатні перетворити дійсність на програму, яка виконується на космічному комп'ютері» [14, с. 246]. Розуміння необхідності керування цифровано-комунікативними технологіями викликало появу низки документів, прийнятими різними країнами протягом останніх років.

Концепція цифрової трансформації, заявлена в Рекомендаціях ЮНЕСКО (2011) та Європейській Декларації (2021) орієнтована на людину, на розвиток її цифрових навичок і компетентностей та на захист її прав і принципів. Декларація охоплює різні сфери діяльності людини з дотриманням рівних прав та безпеки. Цифрове десятиліття визначається як глобальна структура, яка регламентує забезпечення цифровими засобами, опанування цифровими навичками в галузі державних послуг, бізнесі, освіті. Метою Цифрового десятиліття визначено забезпечення роботи всіх аспектів технологій та інновацій для людей упродовж десятиліття до 2030 р. Глобальні зміни вимагають застосування заходів та впровадження нових інструментів у систему освіти, оскільки традиційні методології та інструменти не забезпечують швидких рішень для потреб суспільства. Водночас людство зіткнулося з ризиками, пов'язаними з безпекою цифрового середовища, кібербезпека на державному та корпоративному рівнях активно поширюється на сферу людського фактора.

Метою статті є аналіз тенденцій переходу до комплексної цифровізації суспільства та супутніх змін в інноваційному потенціалі та освітніх потребах України, включаючи розвиток людського інтелектуального капіталу та його захист у цифровому середовищі.

Аналіз останніх досліджень і публікацій. З появою цифрових технологій соціальні інституції та галузі різного формату та напряму зазнають докорінну трансформацію комунікації, управління, навчання. Учені активно шукають оптимальних шляхів і форм роботи зі студентами, які спрямовані на захист та протидію загрозам, пов'язаних з процесами цифровізації. Просвітницька робота з володіння цифровими навичками є прерогативою освіти. Йдеться про поглиблену підготовку молодих спеціалістів до професійної діяльності в умовах цифрової трансформації. Важливість ефективного залучення інноваційних технологій у підготовку педагогічних кадрів аргументовано у програмових працях В. Бикова [1], В. Кременя [2]. Суголосною є позиція співголови Освітнього комітету Асоціації VR/AR К. Дж. Очоа, який стверджує: «освіта є рушійною силою сталості нашої економіки та функціональності людства. Освіта окремої людини – це найцінніша інвестиція країни» [11].

За останні роки значно зросла увага до процесу цифрової трансформації освіти, зокрема вищої педагогічної, оскільки від майбутніх вчителів залежить успішність цифрової реформації. І. Шопіна пропонує аналіз інформаційної безпеки у правовому аспекті, враховуючи інформаційне забезпечення діяльності; захист інформаційного ресурсу, протидію негативному інформаційному впливу [9]. О. Спірін [5] привертає увагу до потреб ефективного та безпечного розвитку інформаційно-комунікаційних технологій. Усі аспекти цифровізації розглядаються крізь призму доступності та безпеки, які є першочерговими завданнями сучасної освіти. Ряд досліджень О. Бурова, О. Бутнік-Сіверського, О. Орлюк, К. Горської [10]; Д. Елліота та Л. Квеста [13] присвячені проблемам кіберзахисту – процесу, який повинен відбуватися водночас з цифровою трансформацією. Як зазначають автори підручника «Цифрова економіка» (Т. Олешко, Н. Касьянова, С. Смерічевський), «чим "розумнішими" стають пристрої доступу, тим потенційно вище рівень вразливості власника. Поширення Інтернету речей зробить людину фактично «прозорою» для будь-яких зацікавлених осіб і структур, що, в свою чергу, породжує попит на розвиток технологій інформаційної безпеки і технологій кіберзлочинності» [6, с. 5].

Наразі на державному рівні розробляється програма кіберзахисту – цифрова гігієна, яка визначається як «динамічна комбінація правил, знань, умінь, навичок, способів мислення та інших особистих якостей з питань інформаційно-комунікаційних та цифрових технологій, спрямованих на безпечне, раціональне та відповідальне їх використання» [4]. Кабінетом Міністрів України прийнята Концепція цифрової гігієни дітей дошкільного віку (від 2 травня 2025 р. № 432-р Київ). Наступними документами очікується Концепції для інших вікових категорій.

Виклад основного матеріалу. Предметом нашого дослідження є вплив цифрового простору на людину, аналіз шляхів впровадження засобів кібербезпеки в освіті. Кібербезпека, або

«когнітивна вакцинація», за висловом О. Бурова та ін. [10], стає необхідною частиною цифрової інформації, зокрема в освіті. Студенти розглядаються як вразлива група, яка може стати головною ціллю кіберкогнітивних операцій у довгостроковій перспективі, а також як найслабша ланка системи. Кібербезпека учасників освітнього процесу має включати правовий, технічний, інформаційний, організаційний та психологічний види захисту. На думку експертів, потреба в надійних заходах кібербезпеки обумовлена підвищеною залежністю від цифрової інфраструктури; поширення кіберзлочинності, яка експлуатує страх і невизначеність користувачів. Консорціум FinTech з кібербезпеки Всесвітнього економічного форуму розробив рекомендації щодо спільного підходу до контролю кібербезпеки . Зокрема йдеться про когнітивну сферу людини, яка стала мішенню для зловмисників, а знання, спосіб мислення, критичні здібності та система життєвих цінностей молодої людини можуть бути порушені через неправильний (замінений) контент, хибні посилання під час пошуку інформації в мережі, фейкові новини, перешкоди під час навчального спілкування, демотивуючий зовнішній вплив на учасників навчального процесу тощо, оскільки «розподілене створення та зберігання інформації – це напіввідчинені двері, дистанційні учні – легка мішень, а розподілені налаштування ускладнюють виявлення порушень безпеки та контратаки» [10]. Певні ризики приховує і штучний інтелект, оскільки активно використовується для створення фейкових матеріалів, небезпечних, коли вони сприймаються як реальні.

Ще одна інноваційна технологічна тенденція в освіті пов'язана з активним впровадженням доповненої реальності (AR/VR/XR) – дієвим засобом сучасного навчання, проте небезпечним з огляду на можливість впливу на знання, спосіб мислення, критичні здібності та систему життєвих цінностей студентів.

Новітні освітні технології з можливостями включення інтерактивності, комунікабельності, творчості покращують процес навчання та викладання. Водночас нові технології породжують нові ризики. Нову ефективну стратегію в кібербезпеці пропонують Д. Елліот та Л. Квест: не лише швидкий захист, але й пошук загроз та навчання користувачів цифрової стійкості [13]. Кіберзахист, за думкою вчених, повинен бути не менш цікавим, ніж цифрові засоби навчання. Пропонується зробити одним з інноваційних понять цифрового захисту пошук загроз, або полювання.

Полювання на загрози вчені вбачають двома шляхами: виявлення загроз (реактивне, що використовується в даний час і було розроблено як у теоретичному, так і в практичному аспектах) та виявлення загроз (проактивне, що включає ретроспективне виявлення, зокрема артефактів та активності). Навчання користувачів стійкості пов'язане з усвідомленням загроз та спеціальним навчанням з кібербезпеки [13]. Загальна модель кіберзагроз у сфері освіти та підходи до їхньої протидії представлені на рис. 1.

Рис. 1. Модель навчання студентів кіберстійкості

Модель містить чотири взаємопов'язаних блоки: обізнаність, полювання, виявлення та тренування, кожен з яких можна назвати етапом розвитку цифрової стійкості. Поняття стійкості по відношенню до кібербезпеки можна урівняти з цифровою гігієною – профілактикою кіберзагроз. Окрім певної дидактичної складової цей термін – цифрова стійкість – додає процесу вироблення безумовних навичок свідоме та критичне наповнення.

Обізнаність з цифровими небезпеками обумовлена традиційними освітніми компонентами: методами навчання, освітніми програмами та навчальним контентом. Процес пізнання та комунікація передбачають усі можливості формального та інформального навчання та спілкування. Саморозвиток та критичне мислення характеризують особистісні параметри процесу пізнання та комунікації. Таким чином, процес кібербезпеки передбачає включення усіх дієвих параметрів освіти, здатних протистояти цифровим загрозам та виробити власну стійкість, починаючи до самодисципліни у користування соціальними мережами до виявлення фейкової інформації, небезпечних і вірусних каналів зв'язку.

Практичному навчанню і тренуванню навичок цифрової гігієни або стійкості можливо навчати

практично на всіх дисциплінах та позааудиторній роботі. Одним з фрагментів навчання пропонуємо аналіз книги Йоганни Гарі «Мистецтво зосереджуватися. Як у нас вкрали увагу» [3], де наводяться переконливі докази втрати студентами концентрації уваги на будь-якій тривалій розумовій діяльності. Так, авторка експериментально доводить, що студенти можуть зосереджуватися на одному завданні лише протягом 65 секунд, після чого увага розпорошується. Цей факт Й. Гарі пов'язує із впливом на когнітивні процеси людини цифрової інформації, зокрема соціальних мереж, які спеціально розроблені для того, щоб привертати нашу увагу, використовуючи функції, які реагують на наші поведінкові реакції. Психологи описали цей процес, як «періодичні підкріплення», приміром функцією «потягни для оновлення», яка утримує споживача у соціальних мережах довше, ніж заплановано. Можна помітити, що перевіряючи соціальні мережі, людина знаходиться в очікуванні чогось цікавого. Навіть якщо цього не відбувається, непередбачуваність контенту змушує повертатися для перевірки. Крім того, оскільки стрічки нескінченні, немає природної кінцевої точки прокручування контенту соціальних мереж. Такі аспекти як гейміфікація та «лайки», розроблені для того, щоб скористатися імпульсами до соціального спілкування та страхом щось втратити. Щоразу, коли перевіряються соціальні мережі, активуються тригери, відомі як гормон «гарного самопочуття», оскільки людина радіє, що на неї може чекати щось нове або цікаве. Це спонукає перевіряти та гортати сторінки знову і знову.

Поради дослідниці корисні для практичного застосування, тому дієві поради, як протистояти розкраданню розумової концентрації, формулюють студенти. Спільними зусиллями складається алгоритм самостійної регуляції щоденного використання соціальних мереж:

– поступово зменшуйте використання, встановивши таймер, щоб запобігти занадто частій перевірці телефону;

– зменшуйтеть або видаліть кількість сповіщень, які надходять безпосередньо на ваш телефон;

– спробуйте видалити всі ігри чи програми, які забирають багато вашого часу;

– зверніть увагу на кількість часу, який ви проводите за телефоном;

– обмежте кількість людей, на яких ви підписані;

– розгляньте можливість завантаження програми-блокувальника, яка обмежує доступ до соціальних мереж у певні години;

– тримайте телефон подалі від себе, коли намагаєтеся досягти чогось важливого.

Продовжуючи тему кіберстійкості в соціальних мережах, слід звернути увагу на проблеми кібербулінгу в студентських групових чатах, тролінгу, змови або шахрайства під час виконання завдань, а також домагання, публікації образливого контенту, розміщення дискримінаційних матеріалів, публікація матеріалів, що дискредитують репутацію університету або загрожують безпеці студентів чи будь-кого, пов'язаного з університетом. Порушення та обговорення цих проблем озброює знаннями та конкретними діями проти ситуацій, пов'язаних з агресивним впливом на користувачів, формує цифрову стійкість проти провокаційних дій чи висловлювань.

Існує цілий спектр можливості цифрових медіатехнологій, що дозволяє активно залучати їх до освітніх процесів. Альтернативний медіапростір може стати автономним середовищем, здатним формувати особистісне ставлення до інформації, розвивати критичне мислення та сприяти соціологізації студентської молоді. Проте треба зважати на те, що пріоритети щодо контенту та каналів розповсюдження здебільшого зосереджені навколо відеоформатів, розваг, блогерських практик різного рівня, і ця тенденція активно посилюється протягом останніх років, що дає підстави стверджувати, що роль медіа як ключового джерела полягає не лише в отриманні інформації, але й у соціальній ідентифікації. Медіа, на думку експертів, повинні повернутися до виконання соціальної функції освіти, яка є актуальнішою ніж будь-коли у світлі сучасних тенденцій, відповідальної та критичної поведінки громадян не лише як споживачів, а й як комунікаторів та продуцентів медіаповідомлень [15].

Розглядаючи медіа як контент і платформу, багато експертів називають дистанційне навчання змішаним медіа-навчанням, що дозволяє як вчителям, так і учням взаємодіяти з медійним контентом, яке не завджди є перевіреним і безпечним. Неможливо розв'язати проблему взаємодії просто надавши посилання, або придбавши програмне забезпечення та мобільний додаток. Додатки на базі штучного інтелекту, які можуть розробляти індивідуальну навчальну програму для учнів на основі їхнього рівня знань та здібностей до навчання, розвиваються повільно. Чат-боти, які займають проміжну ланку взаємодії між викладачем і студентом, можуть використовуватися як для надання зворотного зв'язку учню, так і для оцінки його валідності з високою точністю без участі вчителя. Необхідно памятати, що поширені

методи впливу, що використовуються соціальними інженерами, спрямовані на керування свідомістю об'єкта атаки та його/її емоційно-афективною сферою, а також блокування процесів раціонального та критичного мислення, маніпулювання морально-етичними установками людини.

Висновки і перспективи подальших досліджень. Цифрова трансформація освіти змінює процес навчання, управління освітніми закладами, персональні, суспільні та технологічні цінності. Глобальні зрушення ускладнюють головні принипи освіти – доступність та безпеку, оскільки навчальний процес охоплює сфери цифрових технологій і медіапростору. Цифрова гігієна (стійкість) учасників освітнього процесу повинна включати правовий, технічний, інформаційний, організаційний та психологічний види захисту, що потребує інноваційних стратегій та конкретних методик. Освітня теорія теорії та практики цифрової безпеки знаходиться на стадії формування, перспективними напрямками якої можуть стати навчальні модулі загальних і професійних дисциплін, зокрема – методик і практик для майбутніх вчителів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Биков. В. Цифровізація освіти – імператив інтеграції України у світовий інформаційний простір. *Освіта і суспільство.* 2022. № 10. С. 6. URL: https://naps.gov.ua/ua/press/about_us/2936/.

2. Вища освіта України в умовах воєнного стану та післявоєнного відновлення: виклики і відповіді: науково-аналітична доповідь / В.Г. Кремень, В.І. Луговий, П.Ю. Саух, І.І. Драч, О.М. Слюсаренко, Ю.А. Скиба, О.В. Жабенко, С.А. Калашнікова, Ж.В. Таланова, О.М. Петроє, О.Ю. Оржель, І.Ю. Регейло, М.В. Набок; за заг. ред. В.Г. Кременя. Київ: Педагогічна думка, 2023. 172 с. DOI: https://doi.org/10.37472/NAES-IHED-2023.

3. Гарі Й. Мистецтво зосереджуватися. Як у нас вкрали увагу / переклад Ю. Кузьменко. Київ : Лабораторія, 2022. 296 с.

4. Концепція цифрової гігієни дітей дошкільного віку (від 2 травня 2025 р. № 432-р Київ). URL: https://zakon.rada.gov.ua/laws/show/432-2025-%D1%80#Text.

5. Спірін О.М., Іванова С.М., Олексюк В.П., Мінтій І.С., Вакалюк Т.А., Кільченко А.В. Експеримент з розвитку компетентності з використання інформаційно-цифрових технологій для оцінювання результативності педагогічних досліджень. *Вісник післядипломної освіти. Серія «Педагогічні науки»*, 2024. № 27 (56). С. 147–170.

6. Цифрова економіка: підручник / Т.І. Олешко, Н.В. Касьянова, С.Ф. Смерічевський та ін. Київ : НАУ, 2022. 200 с.

7. Хейлз К. Н. . Як ми стали постлюдством : Віртуальні тіла в кібернетиці, літературі та інформатиці. Київ : Ніка-Центр, 2013. 426 с.

8. Шатіло О. Дефініція поняття «цифрова трансформація» у науковому дискурсі. *Сталий розвиток економіки.* 2025. № 2 (53). С. 449–454. DOI: https://doi.org/10.32782/2308-1988/2025-53-63.

9. Шопіна І. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична).* 2023. № 1. С. 27–35. DOI: https://doi.org/10.32782/2311-8040/2023-1-4.

10. Burov O., Butnik-Siverskyi O., Orliuk O., Horska K. Cybersecurity and innovative digital educational environment. *Information Technologies and Learning Tools.* 2020. vol. 80. P. 414–430. DOI: https://doi.org/10.33407/itlt.v80i6.4159.

11. Carlos J. Ochoa. Disruptive Education through Immersive Learning Technologies. VRARA Education Committee. Piacenza (Italy), 24.09.2019. URL: https://www.thevrara.com/blog2/2019/10/29/disruptiveeducation-through-immersive-learningtechnologies.

12. Duraz R., Espes D., Francq J., Vaton S. Using CVSS scores can make more informed and more adapted Intrusion Detection Systems. *Journal of Universal Computer Science*. 2024. vol. 30(9). pp. 1244–1264. DOI: https://doi.org/10.3897/jucs.131659.

13. Elliott D., Quest L. It's Time to Redefine How Data Is Governed, Controlled and Shared. Here's How. URL: https://www.brinknews.com/its-time-to-redefine-how-data-is-governedcontrolled-and-shared-heres-how/.

14. Fredkin E. Digital Mechanics : An Information Process Based on Reversible Universal Cellular Automata. *Physica D.* 1990. vol. 45 (1-3). P. 245–270.

15. Horska K., Burov O., Orliyk O. Impact of Media Technologies on Digital Educational Content in Media Sector. *Information Technologies and Learning Tools*., vol. 91 (5). P. 84–97. DOI: https://doi:10.33407/itlt.v91i5.5047.

Орлов О. П.

Дата першого надходження статті до видання: 12.12.2025
Дата прийняття статті до друку після рецензування: 09.01.2026
Дата публікації (оприлюднення) статті: 12.02.2026