https://doi: 10.26565/2074-8167-2025-57-11
УДК 378:004.94

Олександр Сергійович Пасічник
кандидат педагогічних наук, доцент, доцент кафедри іноземних мов[1]
bez-nicka@ukr.net, https://orcid.org/0000-0002-0665-2099

Олена Олексіївна Пасічник
кандидат педагогічних наук, доцент, доцент кафедри іноземних мов[1]
bez-nicka@ukr.net, https://orcid.org/0000-0003-0792-2406

[1]*Хмельницький національний університет*
вул. Інститутська, 11, м. Хмельницький, Україна, 29016

ФОРМУВАННЯ ЦИФРОВОЇ ГРАМОТНОСТІ У СТУДЕНТІВ ІТ-СПЕЦІАЛЬНОСТЕЙ ПІД ЧАС ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ ПРОФЕСІЙНОГО СПРЯМУВАННЯ

У статті обґрунтовано актуальність питання формування цифрової грамотності (digital literacy) у студентів ІТ-спеціальностей у контексті сучасних вимог. На основі аналізу наукових праць визначено поняття цифрової грамотності як інтегральної здатності усвідомлено, критично й безпечно застосовувати цифрові технології для пошуку інформації, взаємодії, створення контенту та розв'язання професійних завдань.

Запропоновано практичні завдання, адаптовані для занять з англійської мови в групах ІТ-спеціальностей, спрямованих на поєднання мовної підготовки з розвитком технічних умінь. До них належать: аналіз відкритих джерел (OSINT), оцінювання кібергігієни, ідентифікація фішингових повідомлень, виявлення упереджень у наборах даних, критичний перегляд коду з акцентом на типові вразливості, аналіз ліцензій та безпеки програмних бібліотек, а також робота з умовами договорів користувача. Пропоновані завдання передбачають використання автентичних матеріалів, формування критичного мислення та розвиток англомовної технічної термінології.

Практична спрямованість завдань полягає у відтворенні реальних ситуацій, в яких студенти опиняються під час навчання та майбутньої професійної діяльності: оцінювання ризиків, робота з даними, розуміння політик безпеки, комунікація технічною англійською мовою. Отриманий досвід сприяє підвищенню цифрової грамотності, зміцненню навичок кібербезпеки й формуванню відповідального цифрового громадянства.

Ключові слова: *ІТ-спеціальності; професійна іншомовна підготовка; цифрова грамотність; зміст навчання.*

Як цитувати: Пасічник О. О., Пасічник О. С. Формування цифрової грамотності у студентів ІТ-спеціальностей під час вивчення іноземної мови професійного спрямування. *Наукові записки кафедри педагогіки.* 2025. № 57. С. 134–143. https://doi: 10.26565/2074-8167-2025-57-11

In cites: Pasichnyk, O., Pasichnyk, O. (2025). Shaping Digital Literacy of IT-Students in the Process of Foreign Language Acquisition for Professional Purpose. *Scientific notes of the pedagogical department,* 57. 134–143 https://doi: 10.26565/2074-8167-2025-57-11. [In Ukrainian].

Постановка проблеми. Поряд із *компетентностями*, *перевернутим класом (flipped classroom)* та *змішаним навчанням (blended learning)*, термін *цифрова грамотність* (*digital literacy*), а також його синоніми (*digital competences, digital skills*) є одним із нових понять, що доповнило постійно зростаючий перелік освітніх термінів в останні десятиліття.

Становлення терміна «*digital literacy*» пов'язано зі стрімким розвитком інформаційних технологій та змінами підходів до того, як люди сприймають та генерують нову інформацію. Його появі передували поняття, які стосувалися навичок роботи з комп'ютером чи медіатекстами. Зокрема, акцентувалося на комп'ютерній грамотності (*computer literacy*), що передбачало вміння користуватися комп'ютером, та медіаграмотності (*media literacy*) – здатності критично оцінювати медіаповідомлення. Поняття медіаграмотності постало в середині XX ст., як відповідь на пропаганду, рекламу, та потребу в критичному мисленні, щоб протистояти їм. Появу нового терміна «*digital literacy*» пов'язують з P. Gilster, який звертав увагу на здатність розуміти й використовувати інформацію в різних форматах із різних джерел, коли вона здобувається за допомогою комп'ютерів [9]. Термін швидко набув популярності, хоча у перші роки свого існування акцентувалося здебільшого на технічних навичках (як працювати з комп'ютером та здобувати інформацію). Однак, із розширенням можливостей інтернету, соціальних медіа і цифрових технологій зміст поняття розширився та передбачав такі складні концепти, як розуміння *контексту, культури, етики цифрового використання* [1], а також суспільні й освітні виміри, зокрема стосовно того, як цифрова грамотність стає необхідною в цифровому суспільстві. Поряд з іншими спеціальностями фахівці IT-сфери потребують формування навичок цифрової грамотності, оскільки їхня діяльність пов'язана з постійною взаємодією з цифровими системами, значними обсягами інформації та прийняттям критично важливих рішень. Цифрова грамотність для них не лише загальна компетентність, а фундамент, покликаний гарантувати якість, безпеку і розвиток технічних продуктів.

Аналіз останніх досліджень і публікацій. Як було визначено наприкінці 1990-х років, *цифрова грамотність* передбачає *здатність розуміти та використовувати інформацію в різних форматах і з широкого спектра джерел*, коли її здобувають за допомогою комп'ютера, і, зокрема, через інтернет [9, с. 6]. Це визначення можна вважати своєрідною «відправною точкою» для досліджень означеного питання, оскільки з часом цифрові тексти та практики стали набагато складнішими. Поширення мобільних медіа, а згодом і штучного інтелекту, забезпечило появу абсолютно різних моделей взаємодії людей з інформаційними джерелами. Кожна технологічна інновація створює все нові й нові контексти, які по-різному впливають на те, як осмислюється поняття *цифрової грамотності*. У 2001 р. D. Bawden проаналізував наявні концепції цифрової грамотності [11]. Його пошуки зорієнтовано на встановлення подібностей та точок перетину з іншими сферами грамотності, як-от *інформаційна грамотність* та *комп'ютерна грамотність*. D. Bawden стверджує, що *цифрова грамотність* не передбачає лише набір функціональних умінь і компетенцій, наголошуючи на важливості контексту, зокрема соціокультурного, в процесі смислотворення в інформаційних науках.

Дослідники D. O'Brien і C. Scharber розглядають цифрову та традиційну грамотність як різні точки одного континууму. Не протиставляючи традиційну друковану та цифрову грамотність, вони стверджують, що освіта має «переплітати нові цифрові грамотності зі старими або вже усталеними формами грамотності» [17, с. 67]. Окрім того, науковці наголошують, що цифрову грамотність варто розглядати як таку, що еволюціонує, оскільки цифрові практики «формують і водночас формуються молоддю – як у школі, так і поза нею» [17, с. 66].

Дослідниця I. Sander вважає звуженим розуміння цифрової грамотності як набору технічних навичок і пропонує концепт *critical big data literacy***,** що передбачає не лише вміння працювати з даними, а й усвідомлювати, критично аналізувати та діяти щодо систем великої кількості даних (*big data*) і їхніх соціотехнічних наслідків. Науковиця поєднує підходи з критичних дата-досліджень, медіаграмотності й громадянської освіти та досліджує, як онлайн-інструменти (тренажери, візуалізації, гайди) можуть сприяти такій грамотності [22].

Досліджуючи питання цифрової грамотності, було виявлено, що поряд із науковцями самі заклади освіти дедалі частіше визначають цифрову грамотність як необхідну складову сучасної освіти. Для прикладу, University of York у Великій Британії має відповідні рекомендації – «*Supporting students' digital literacies: a Practical Guide*» [28]. Наявність таких рекомендацій не є одиничним випадком. Більш

того, дедалі частіше поняття цифрової грамотності фігурує під час конструювання змісту навчальних програм (*curriculum design*), а окремі дослідники закликають інтегрувати *цифрові компетентності* в усі дисципліни, а не лише у спеціальні курси [15]; особливо загострилася увага на такому вимірі цифровізації під час COVID-19. Окремі університети створюють власні рамки (*frameworks*) для цифрових компетенцій студентів, які окреслюють, які саме компетентності має бути сформовано, та акцентується на тому, що університетське середовище має підтримувати набуття цифрових навичок, які допомагають жити, вчитися і працювати в цифровому світі [12]. Оскільки це поняття розглядають не лише в теоретичному, а й у практичному вимірі, освітнє середовище має досягти єдності щодо його трактування – від цього залежатимуть шляхи реалізації технології та змістове наповнення. Практика засвідчує складність у формулюванні остаточного визначення інноваційних термінів, і цифрова грамотність не є винятком. Характерною особливістю цього поняття є те, що багато закладів освіти пропонують власне трактування. Зокрема, в оглядовій статті G. Walton [29] зібрав приклади того, як різні університети трактують цифрову грамотності. Наведемо декілька з них:

… здатність знаходити, оцінювати, використовувати, поширювати та створювати контент, використовуючи інформаційні технології та Інтернет (Cornell University, 2015).

… здатність використовувати цифрові технології, засоби комунікації або мережі для пошуку, оцінювання, використання та створення інформації. Це також уміння розуміти й використовувати інформацію в різних форматах із широкого спектра джерел, коли вона подається за допомогою комп'ютерів, а також здатність людини ефективно виконувати завдання в цифровому середовищі (University of Illinois, 2014).

… упевнене та критичне використання інформаційних і цифрових технологій для розвитку в академічній, особистій і професійній сферах (Leeds Metropolitan University, 2011).

… поряд із умінням знаходити та використовувати цифрова грамотність охоплює комунікацію, співпрацю й командну роботу, соціальну обізнаність у цифровому середовищі, розуміння електронної безпеки та створення нової інформації. Цифрова грамотність ґрунтується на критичному мисленні та оцінюванні інформації (Open University, 2012).

Один з університетів перетворює власне визначення цифрової грамотності на конкретне зобов'язання перед студентами:

Студенти розвиватимуть свої медіаграмотності, зокрема навички комунікації за допомогою цифрових систем, що відповідають їхнім спеціальностям. Ми сприятимемо розвитку здатності студентів орієнтуватися в складному інформаційному просторі, ставити під сумнів достовірність і надійність нефільтрованої інформації, взаємодіяти з науковими публікаціями та брати більшу відповідальність за власне навчання (University of South Australia, 2015).

Попри зазначені відмінності, можемо констатувати тенденцію до уніфікації поняття *цифрової грамотності* з метою зробити його більш вимірюваним і таким, що піддається порівнянню в дедалі глобалізованішому освітньому середовищі. У цьому контексті варто зазначити, що міжнародна видавнича й оцінювальна компанія *Pearson Education* запровадила сертифікацію з питань цифрової грамотності, щоб сприяти ефективному використанню технологій (*IC3 Digital Literacy Certification* через платформу *Certiport*). Окрім того, *UNESCO* розробляла рамку для вимірювання цифрової грамотності, яка визначає систему навичок (які охоплюють технічні та професійні аспекти) [25]. Рамки та визначення, запропоновані такими міжнародними організаціями, зорієнтовані на стандартизацію поняття *цифрової грамотності* в «інструментальному» сенсі, акцентуючи увагу на навичках, орієнтованих на професійну діяльність.

У контексті нашого дослідження варто зазначити, що деякі науковці розвинули означену проблему та вивчення питання кореляції між *цифровою грамотністю* і *вміннями програмувати* [9]. Хоча вміння програмувати – це насамперед *computational thinking* та *syntax-specific skills*, а цифрова грамотність охоплює ширший спектр питань (інформаційну, медійну, комунікаційну, безпекову грамотність, етичні аспекти), дослідники виявили, що цифрова грамотність є тією фундаментальною навичкою, сформованість якої позитивно впливає на віру особи в здатність писати код прямо та опосередковано підвищує самоефективність у сфері обчислювального мислення (*computational thinking self-efficacy*). Попри те, що це дослідження стосувалося учнів закладів загальної середньої освіти, а не сформованих фахівців чи студентів, вважаємо його ілюстративним та таким, що стверджує значущість підвищення цифрової грамотності (не лише «вміння користуватися гаджетом», а й навички

інформаційного опрацювання, безпеки, вирішення проблем) як корисного фундаменту для відчуття учнями здатності у програмуванні та споріднених сферах діяльності.

Вважаємо значущими не лише наявні теоретичні розробки щодо визначення змістового поняття цифрової грамотності, а й практичні напрацювання у цій галузі. Активне розроблення цих питань розпочалося на початку 2000-х років. Одну з найбільш ранніх праць, що пов'язує теоретичну модель із прикладними завданнями, підготував Y. Eshet-Alkalai. Дослідник запропонував концептуальну модель цифрової грамотності (*photo-visual, reproduction, branching, information, socio-emotional literacies*) [5]. У 2012 році він оновив модель, додавши шостий компонент – грамотність реального часу (*real-time thinking literacy*), пов'язану з умінням швидко обробляти великі потоки інформації в реальному часі (стрічку новин, чати тощо) [7]. А в подальших емпіричних дослідженнях використовував *практичні завдання* (наприклад: планування подорожі в невідому країну, робота з гіпертекстом тощо) для тестування кожного типу грамотності. Так само D. Belshaw сформулював «*essential elements of digital literacies*», надав практичні приклади та вправи, спрямовані на розвиток когнітивних, комунікативних та інших компонентів цифрової грамотності [3]. W. Ng запропонував модель, яка інтегрує технічну, когнітивну та соціально-емоційну складові цифрової грамотності. Цю класифікацію використовують для проєктування навчальних завдань (щоб охопити всі три складові) [16]. Рекомендації *DigCompEdu* (для викладачів) від 2017 р. містять чітко визначені компетенції та приклади навчальних завдань, які можна адаптувати для формування та оцінювання цифрових компетенцій студентів [20]. Цю рамку широко використовують під час розроблення курсів і завдань у Європі.

Дослідники T.Giese, M. Wende, S. Bulut, R.Anderl описують власний досвід інтеграції концепції цифрової грамотності у навчальну програму бакалаврату для інженерних спеціальностей [7]. Метою було озброїти студентів не лише теоретичними знаннями про дані, а й практичними навичками їхньої роботи: збирання, обробки, аналізу та інтерпретації даних у контексті інженерної освіти. Науковці вчергове обґрунтували, що цифрова грамотність – це не лише «комп'ютерні навички», а *інтегрована компетентність*, критично важлива для сучасних інженерів. А тому обстоювали, що в умовах швидкого зростання обсягів даних і потреби приймати обґрунтовані рішення на їх основі, такі навички стають ключовими. Їхній підхід може бути використано як модель для інших інженерних факультетів або дисциплін, пов'язаних із важливою роботою з даними.

Мета дослідження **–** проаналізувати основні виміри цифрової грамотності для фахівців ІТ-сфери, екстраполювати їх на процес іншомовної підготовки, розробити завдання для формування навичок цифрової грамотності ІТ-фахівців.

Виклад матеріалу дослідження і основні результати. ІТ-фахівці не лише користуються комп'ютером – вони постійно перебувають у центрі інформаційного поля як його творці, модератори, аналітики та захисники. Взаємодія зі значними обсягами інформації, її аналітика, перетворення, оцінювання достовірності, захист і етичне використання потребують від ІТ-фахівця особливого рівня сформованості цифрової грамотності. Як уже зазначалося, цифрові компетентності охоплюють не лише технічні уміння і навички, а й здатність критично оцінювати інформацію, розуміти її походження, упередженість і можливі маніпуляції [25].

Аналіз наукової літератури [5; 18; 20; 26] та досвід роботи зі студентами дає змогу розглядати цифрову грамотність фахівця ІТ за такими складниками:

- *інформаційна грамотність* **–** здатність шукати, відбирати, оцінювати та критично інтерпретувати інформацію з цифрових джерел (пошук можливих технічних рішень і документації для наявних проблем; оцінювання достовірності джерел; аналіз точності та актуальності інформації тощо);
- *цифрова комунікація та взаємодія* – вміння ефективно і безпечно взаємодіяти онлайн (дотримання правил онлайн-етикету; управління цифровою ідентичністю, спільна робота з цифровими документами та проєктами);
- *створення цифрового контенту* – здатність створювати, модифікувати, поєднувати та ліцензувати цифрові матеріали;
- *цифрова безпека* (*cyber hygiene*) – вміння ідентифікувати загрози та захищати дані, пристрої й облікові записи (приватність і контроль цифрового сліду; розпізнавання фішингу та соціальної інженерії; безпечна робота з даними, мережами та сервісами тощо);
- *розв'язання технічних проблем і цифрова автономність* – уміння ефективно працювати з цифровими інструментами й вирішувати технічні завдання (робота з новими технологіями, інтерфейсами, мо-

вами програмування; здатність самостійно шукати рішення і навчатися; діагностика технічних помилок; встановлення та налаштування програм; базове адміністрування систем);
– *робота з даними* (data literacy) – здатність працювати з цифровими даними та розуміти їхню якість (збір, очищення та інтерпретація даних; базова статистика; розуміння упередженості в даних (bias));
– *цифрова креативність та інновації* – здатність використовувати цифрові технології для створення нових рішень (застосування ШІ-інструментів для оптимізації власної роботи; здатність обирати технологію для вирішення конкретної задачі);
– *критичне мислення та етичне використання технологій* – уміння аналізувати вплив технологій на суспільство, розпізнавати дезінформацію та упередження (*bias*) в ШІ-алгоритмах, дотримуватися етичних норм (авторські права, стійкість, інклюзивність тощо) та приймати відповідальні рішення в цифровому середовищі.

Особливої актуальності цифрова грамотність набуває в умовах, коли більшість контенту та активності в інтернеті (пости, коментарі, лайки, меми, відео в *YouTube* та треди на форумах) генерується не живими людьми, а ботами, алгоритмами та штучним інтелектом, а справжні користувачі становлять лише незначну меншість. Це так звана теорія «мертвого інтернету», коли значна частина активності штучна і продовжує зростати. Однак таку ситуацію вже вважають не теорією, а задокументованою реальністю, яку визнають дослідники [19].

Аналіз фахових публікацій з теми дослідження [4; 13; 14] дає змогу стверджувати, що нездатність орієнтуватися в новій інформаційній сфері та невідповідність підготовки фахівця критеріям цифрової грамотності може спричинити таке:
– поширення вразливостей, зважаючи на довіру до застарілих, фейкових джерел коду чи бібліотек; це може потенційно призвести до компрометації систем та витоку даних;
– можливість стати жертвою фішингових тактик та соціальної інженерії (йдеться, зокрема, і про маніпулятивні атаки на основі психологічного тиску);
– посилення ризиків внутрішніх загроз та несанкціонованого доступу, з огляду на нехтування принципами *zero trust* та безпекою власних і корпоративних даних;
– створення упереджених алгоритмів, зважаючи на некритичне використання даних з відтворенням упереджень, закладених у різних ШІ моделях;
– слабку організацію даних, хаотичну комунікацію, ігнорування стандартів ведення документації;
– порушення етичних та правових норм під час роботи з даними користувачів (ігнорування принципів конфіденційності тощо);
– перевантаження інформацією (*data overload*) та неефективне використання цифрових інструментів, що знижує продуктивність та призводить до помилкових рішень у проєктах;
– надмірну залежність від зовнішньої ІТ-підтримки, з огляду на брак навичок самостійного вирішення проблем, що спричиняє затримки в розробленні та підвищені витрати.

З метою формування вмінь і навичок цифрової грамотності доцільно інтегрувати відповідні завдання в зміст навчальних дисциплін, зокрема предмет «Іноземна мова для професійних цілей». Мета завдань полягає у формуванні навичок критичного мислення на основі здобутих знань та досвіду, вміння здійснювати технічний пошук, читати документацію, надавати оцінку рівню безпеки та ліцензування, а також формування вмінь і навичок академічного письма іноземною мовою.

Пропонуємо декілька завдань (англійською мовою), які ми апробували в процесі іншомовної підготовки (також супроводжуються відповідними посиланнями, які стали основою розроблених завдань):

Завдання «OSINT on Yourself» (OSINT про себе) [23; 24]

In 40 minutes, collect as much publicly available information about yourself as possible using only open sources (search engines, social media, public registries, cached data, people search tools). Then:

1. Classify findings into:
   – identifiers (emails, usernames)
   – digital traces
   – behavioural patterns
   – leaked credentials
2. Prepare a privacy hygiene plan: what should be deleted/changed/restricted.

Завдання «Library Anatomy» (Анатомія бібліотеки) [30**]**

Choose any library/package (e.g.: npm, PyPI, Crates.io). Analyse the following:

1. Find:
   – date of the latest commit;
   – the number of contributors (include link to the contributors' page).
2. Check for known vulnerabilities (use: GitHub Security Advisories, NVD, osv.dev).
   – Assess the licence (permissive or restrictive?)
   – is it compatible with commercial use / your project?
3. Identify risks (e.g., abandoned project, single-maintainer problem).
4. Write a 300–350 word technical report summarising whether the library can be safely used.

Завдання «Phishing or Not?» (Фішинг чи ні?)

You are given 10 authentic email screenshots (GitHub, AWS, npm, banks, delivery services etc.). For each message:

1. Decide whether it is phishing or legitimate.
2. Highlight at least three indicators (e.g., domain mismatch, header anomalies, suspicious CTA (Call to Action), linguistic red flags).
3. Provide a short justification in English (2-3 sentences per item).

Завдання «Bias Hunting» (Виявлення упереджень) [27]

Choose an open dataset (e.g., CelebA, Adult Income, COMPAS, IMDB Reviews). Identify and document at least three types of bias (i.e. sampling bias, label bias, measurement/feature bias, representation bias, historical bias)/

For each bias:

4. Provide a 2–3 sentence explanation (EN).
5. Suggest one mitigation strategy (e.g., re-sampling, re-weighting, data augmentation, relabeling).

Завдання «Critical Code Review» (Критичний код-рев'ю)

Work in pairs. Analyse the provided code fragment which contains intentional security flaws, such as:

- hard-coded secrets
- outdated or vulnerable dependencies
- SQL injection
- unsafe file handling
- missing input validation

Your task is to:

1. Identify the issues;
2. Classify them (type, severity);
3. Propose safe alternatives, explaining them in English.

Завдання «Terms of Service Forensics» (Аналіз умов договору користувача) [11]

Students analyze Terms of Service of any popular service (e.g.: Discord, GitHub, Figma). They have to identify clauses that affect:

- your data rights;
- IP ownership;
- content moderation;
- liability limitations.

Write a 150-word reflection if the service is safe for personal or professional use.

Запропоновані завдання спрямовано на формування у студентів елементів цифрової грамотності, які безпосередньо інтегрують мовні вміння з реальними цифровими практиками (OSINT-аналізом, кібергігієною, критичним розбором програмного коду, виявленням упереджень у даних, оцінюванням вразливостей у бібліотеках тощо). Вони допомагають студентам не лише розвивати англомовну компетентність, а й оволодівати базовими інструментами інформаційної безпеки, цифрової етики та технічного мислення. Водночас інтеграція таких завдань до процесу іншомовної підготовки вимагає від викладача іноземної мови певного рівня технічної компетентності, причому йдеться не про глибоку спеціалізацію, а про базову обізнаність у напрямах кібербезпеки, аналізу даних, основ програмування та роботи з відкритими джерелами. Тому доцільним є міжкафедральне співробітництво: зокрема, консультації з викладачами профільних ІТ-дисциплін, спільне розроблення методичних матеріалів або запрошення експертів для коротких майстер-класів.

Окремо маємо зазначити, що наведені завдання ще не інтегровано до навчальної програми як обов'язковий компонент курсу. Натомість йдеться про етап успішної апробації в умовах аудиторного навчання. Практика засвідчує, що студенти демонструють високий рівень мотивації, їх залученість значно підвищується, оскільки завдання мають чітку практичну спрямованість і сприяють розвитку критичного мислення. Отримані результати апробації дають змогу розглядати ці вправи як перспективний елемент оновленого курсу англійської мови для ІТ-спеціальностей.

Висновки та перспективи подальших досліджень. Проведене дослідження дає підстави стверджувати, що цифрова грамотність посідає чільне місце в професійній діяльності сучасного ІТ-фахівця та визначає його ефективність на індивідуальному та командному рівні. У статті було визначено сутність цифрової грамотності як комплексу умінь і навичок, що охоплюють критичну оцінку інформації, роботу з цифровими інструментами, безпечну поведінку в онлайн-середовищі, здатність до вирішення технічних проблем і адаптацію до нових технологічних рішень.

Узагальнення досліджуваних взаємозв'язків засвідчує, що цифрова грамотність не є ізольованою компетентністю. Вона тісно корелює з іншими видами професійної діяльності, зокрема програмуванням, аналізом даних, кібербезпекою, інформаційним пошуком, командною взаємодією та управлінням цифровими продуктами. Що вищим є рівень цифрової грамотності, то краще ІТ-фахівець орієнтується у складних технічних екосистемах, прогнозує ризики та ухвалює обґрунтовані рішення.

Запропоновані завдання дають змогу створювати передумови для розвитку цифрової грамотності на основі практичних сценаріїв, максимально наближених до реальних умов професійної діяльності. Аналіз бібліотек, виявлення фішингових листів, пошук упередженості у відкритих наборах даних, робота з OSINT тощо забезпечують не лише формування технічних навичок, а й розвиток критичного мислення, уважність до деталей та відповідальне ставлення до цифрової безпеки. Важливо, що такі завдання може бути інтегровано у процес професійної іншомовної підготовки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Havrilova, L. H., & Topolnik, Y. V. (2017). Digital culture, digital literacy, digital competence as the modern educational phenomena. *Information Technologies and Learning Tools*, *61*(5), 1–14. DOI: https://doi.org/10.33407/itlt.v61i5.1744
2. Bawden, D. (2001). *Information and digital literacies: A review of concepts*. Journal of Documentation, 57(2), 218–259. DOI: https://doi.org/10.1108/EUM0000000007083
3. Belshaw, D. (2014). The essential elements of digital literacies (v1.0). URL: http://dougbelshaw.com/essential-elements-book.pdf
4. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1-upd1). National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-161r1-upd1
5. Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens. Publications Office of the European Union. DOI: https://doi.org/10.2760/38842
6. Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93–106.
7. Eshet-Alkalai, Y. (2012). Thinking in the digital era: A revised model for digital literacy. *Issues in Informing Science and Information Technology, 9*, 267–276. DOI: https://doi.org/10.28945/1621
8. Giese, T.G.; Wende, M.; Bulut, S.; Anderl, R. Introduction of Data Literacy in the Undergraduate Engineering Curriculum. In Proceedings of the 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 27–30 April 2020; pp. 1237–1245. URL: https://www.researchgate.net/publication/342457765_Introduction_of_Data_Literacy_in_the_Undergraduate_Engineering_Curriculum
9. Gilster, P. (1997). *Digital literacy*. Wiley & Sons.
10. Gümüş, M. M., Kukul, V., & Korkmaz, Ö. (2024). Relationships between middle school students' digital literacy skills, computer programming self-efficacy, and computational thinking self-efficacy. *Informatics in Education*, *23*(3), 571–592. DOI: https://doi.org/10.15388/infedu.2024.20
11. Herold, B. (2017). Student data privacy and security: Red flags in terms-of-service agreements. Education Week. URL: https://www.edweek.org/technology/student-data-privacy-and-security-red-flags-in-terms-of-service-agreements
12. La Trobe University. (2019). *Skills for a digital world: Digital literacies framework* (Rev. ed.). URL: https://www.latrobe.edu.au/__data/assets/pdf_file/0009/1248350/digital-literacies-framework.pdf
13. Lee, N. T., Resnick, P., & Barton, G. (2019). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. Brookings Institution. URL: https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/
14. Lüdorf, V., Meister, S., Mainz, A., Ehlers, J. P., Nitsche, J., & Busse, T. S. (2025). Developing a concept on ethical, legal and social implications (ELSI) for data literacy in health professions: A learning objective-based approach. *Healthcare, 13*(17), Article 2108. DOI: https://doi.org/10.3390/healthcare13172108

15. Monteiro, A., & Leite, C. (2021). Alfabetizaciones digitales en la educación superior: Habilidades, usos, oportunidades y obstáculos para la transformación digital. *Revista de Educación a Distancia* (RED), 21(65). DOI: https://doi.org/10.6018/red.438721
16. Ng, W. (2012). Can we teach digital natives digital literacy? URL: https://www.scirp.org/reference/referencespapers?referenceid=3344276
17. O'Brien, D., & Scharber, C. (2008). Digital literacies go to school: Potholes and possibilities. *Journal of Adolescent & Adult Literacy*, *52*(1), 66–68.
18. OECD. (2023). OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. OECD Publishing. DOI: https://doi.org/10.1787/c74f03de-en
19. Pakistan Journal of Engineering, Technology & Science. (2024). Ahmed, A., Qamar, R., Asif, R., Imran, M., Khurram, M., & Ahmed, S. Dead Internet Theory. *Pakistan Journal of Engineering, Technology & Science*, *12*(1), 37–48. DOI: https://doi.org/10.22555/pjets.v12i1.1077
20. Redecker, C. (2017). European Framework for the Digital Competence of Educators: DigCompEdu. Publications Office of the European Union. DOI: https://doi.org/10.2760/159770
21. Redecker, C., & Punie, Y. (2017). European framework for the digital competence of educators (DigCompEdu)
22. Sander, I. (2020). What is critical big data literacy and how can it be implemented? *Internet Policy Review, 9*(2), **1–22.** DOI: 10.14763/2020.2.1479. URL: https://policyreview.info/pdf/policyreview-2020-2-1479.pdf
23. Santos, S. (n.d.). List of OSINT exercises – Challenge yourself!. URL: https://gralhix.com/list-of-osint-exercises/
24. ShadowDragon. (2025). OSINT exercises: Ultimate guide to investigative skills. URL: https://shadowdragon.io/blog/osint-exercises/
25. UNESCO. (2018). *A global framework of reference on digital literacy skills for indicator 4.4.2*. URL: https://unesdoc.unesco.org/ark:/48223/pf0000265403
26. UNESCO. (2023). Digital Literacy Assessment [Background paper for the 2023 Global Education Monitoring Report]. UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000386202
27. University of Pennsylvania Carey Law School. (n.d.). Field guide to address bias in datasets. https://www.law.upenn.edu/live/files/11569-field-guide-to-address-bias-in-datasets
28. University of York. (n.d.). *Digital literacy*. URL: https://subjectguides.york.ac.uk/digital-literacy
29. Walton, G. (2016). Digital literacy (DL): Establishing the boundaries and identifying the partners. *New Review of Academic Librarianship*, 22(1), 1–4. DOI: https://doi.org/10.1080/13614533.2015.1137466
30. Wu, H., & Holmes, R. (2024). Identifying affected libraries and their ecosystems for open source vulnerability remediation. In Proceedings of the IEEE/ACM 46th International Conference on Software Engineering (ICSE '24). URL: https://chenbihuan.github.io/paper/icse24-wu-holmes.pdf

Автори заявляють про відсутність конфлікту інтересів щодо публікації цього рукопису.
Внесок авторів: *всі автори зробили рівний внесок у цю роботу.*
В роботі не використано ресурс штучного інтелекту

Отримано: 10.09.2025
Переглянуто: 18.10.2025
Прийнято: 25.10. 2025
Опубліковано: 30.11.2025

Oleksandr Pasichnyk
PhD in Education, Associate Professor, Department of Foreign Languages[1],
bez-nicka@ukr.net, https://orcid.org/0000-0002-0665-2099

Olena Pasichnyk
PhD in Education, Associate Professor, Department of Foreign Languages[1]
bez-nicka@ukr.net, https://orcid.org/0000-0003-0792-2406

[1]Khmelnytskyi National University Instytuts'ka str. 11, Khmelnytskyi, Ukraine, 29016

SHAPING DIGITAL LITERACY OF IT-STUDENTS IN THE PROCESS OF FOREIGN LANGUAGE ACQUISITION FOR PROFESSIONAL PURPOSE

The article elaborates on the problem of shaping digital literacy skills in students of IT majors in context of modern challenges. Based on the analysis of relevant scientific works, the concept of digital literacy is defined as an integral ability to consciously, critically, and safely apply digital technologies for information retrieval, interaction, content creation, and solving professional tasks.

A series of practical tasks adapted for English language classes in IT-groups is proposed. It is aimed at combining language training with the development of technical skills. These include: analysis of open sources (OSINT), assessment of one's cyber hygiene, identification of phishing messages, detection of biases in datasets, critical code review with emphasis on common vulnerabilities, analysis of licenses and security of software libraries, as well as work with user agreement terms. The proposed tasks involve the use of authentic materials, development of critical thinking, and the expansion of English-language technical terminology.

Practical orientation of the tasks is embedded in close-to-real-life situations that students encounter during their studies and future professional activities: risk assessment, working with data, understanding security policies, and communication in technical English. The acquired experience contributes to enhancing digital literacy, strengthening cybersecurity skills, and fostering responsible digital citizenship.

Keywords: *IT majors; English for professional purpose; digital literacy; learning content.*

REFERENCES

1. Havrilova, L. H., & Topolnik, Y. V. (2017). Digital culture, digital literacy, digital competence as the modern educational phenomena. *Information Technologies and Learning Tools*, 61(5), 1-14. DOI: https://doi.org/10.33407/itlt.v61i5.1744
2. Bawden, D. (2001). *Information and digital literacies: A review of concepts*. Journal of Documentation, 57(2), 218-259. DOI: https://doi.org /10.1108/EUM0000000007083
3. Belshaw, D. (2014). The essential elements of digital literacies (v1.0). URL:http://dougbelshaw.com/essential-elements-book.pdf
4. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1-upd1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1-upd1
5. Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens. Publications Office of the European Union. DOI: https://doi.org/10.2760/38842
6. Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13(1), 93-106.
7. Eshet-Alkalai, Y. (2012). Thinking in the digital era: A revised model for digital literacy. Issues in Informing Science and Information Technology, 9, 267-276. DOI: https://doi.org/10.28945/1621
8. Giese, T.G.; Wende, M.; Bulut, S.; Anderl, R. Introduction of Data Literacy in the Undergraduate Engineering Curriculum. In Proceedings of the 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 27–30 April 2020; pp. 1237-1245. https://www.researchgate.net/publication/342457765_Introduction_of_Data_Literacy_in_the_Undergraduate_Engineering_Curriculum
9. Gilster, P. (1997). *Digital literacy*. Wiley & Sons.
10. Gümüş, M. M., Kukul, V., & Korkmaz, Ö. (2024). Relationships between middle school students' digital literacy skills, computer programming self-efficacy, and computational thinking self-efficacy. *Informatics in Education*, 23(3), 571-592. DOI: https://doi.org/10.15388/infedu.2024.20
11. Herold, B. (2017). Student data privacy and security: Red flags in terms-of-service agreements. Education Week. URL: https://www.edweek.org/technology/student-data-privacy-and-security-red-flags-in-terms-of-service-agreements
12. La Trobe University. (2019). *Skills for a digital world: Digital literacies framework* (Rev. ed.). URL: https://www.latrobe.edu.au/__data/assets/pdf_file/0009/1248350/digital-literacies-framework.pdf
13. Lee, N. T., Resnick, P., & Barton, G. (2019). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. Brookings Institution. URL: https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/
14. Lüdorf, V., Meister, S., Mainz, A., Ehlers, J. P., Nitsche, J., & Busse, T. S. (2025). Developing a concept on ethical, legal and social implications (ELSI) for data literacy in health professions: A learning objective-based approach. Healthcare, 13(17), Article 2108. DOI: https://doi.org/10.3390/healthcare13172108
15. Monteiro, A., & Leite, C. (2021). Alfabetizaciones digitales en la educación superior: Habilidades, usos, oportunidades y obstáculos para la transformación digital. *Revista de Educación a Distancia* (RED), 21(65). DOI: https://doi.org/10.6018/red.438721
16. Ng, W. (2012). Can we teach digital natives digital literacy? URL: https://www.scirp.org/reference/referencespapers?referenceid=3344276
17. O'Brien, D., & Scharber, C. (2008). Digital literacies go to school: Potholes and possibilities. *Journal of Adolescent & Adult Literacy*, 52(1), 66-68.
18. OECD. (2023). OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. OECD Publishing. DOI: https://doi.org/10.1787/c74f03de-en

19. Pakistan Journal of Engineering, Technology & Science. (2024). Ahmed, A., Qamar, R., Asif, R., Imran, M., Khurram, M., & Ahmed, S. Dead Internet Theory. *Pakistan Journal of Engineering, Technology & Science*, 12(1), 37-48. DOI: https://doi.org/10.22555/pjets.v12i1.1077
20. Redecker, C. (2017). European Framework for the Digital Competence of Educators: DigCompEdu. Publications Office of the European Union. DOI: https://doi.org/10.2760/159770
21. Redecker, C., & Punie, Y. (2017). European framework for the digital competence of educators (DigCompEdu)
22. Sander, I. (2020). What is critical big data literacy and how can it be implemented? Internet Policy Review, 9(2), 1–22. DOI: https://doi.org/10.14763/2020.2.1479. https://policyreview.info/pdf/policyreview-2020-2-1479.pdf
23. Santos, S. (n.d.). List of OSINT exercises – Challenge yourself!. URL: https://gralhix.com/list-of-osint-exercises/
24. ShadowDragon. (2025). OSINT exercises: Ultimate guide to investigative skills. URL: https://shadowdragon.io/blog/osint-exercises/
25. UNESCO. (2018). *A global framework of reference on digital literacy skills for indicator 4.4.2*. URL: https://unesdoc.unesco.org/ark:/48223/pf0000265403
26. UNESCO. (2023). Digital Literacy Assessment [Background paper for the 2023 Global Education Monitoring Report]. UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000386202
27. University of Pennsylvania Carey Law School. (n.d.). Field guide to address bias in datasets. URL: https://www.law.upenn.edu/live/files/11569-field-guide-to-address-bias-in-datasets
28. University of York. (n.d.). *Digital literacy*. URL: https://subjectguides.york.ac.uk/digital-literacy
29. Walton, G. (2016). Digital literacy (DL): Establishing the boundaries and identifying the partners. *New Review of Academic Librarianship*, 22(1), 1-4. DOI: https://doi.org/10.1080/13614533.2015.1137466
30. Wu, H., & Holmes, R. (2024). Identifying affected libraries and their ecosystems for open source vulnerability remediation. In Proceedings of the IEEE/ACM 46th International Conference on Software Engineering (ICSE '24). URL: https://chenbihuan.github.io/paper/icse24-wu-holmes.pdf

The authors declare no conflict of interest regarding the publication of this manuscript.
Authors Contribution: *all authors have contributed equally to this work.*
The work does not use artificial intelligence resources

Submission received: 10.09.2025
Revised: 18.10.2025
Accepted: 25.10. 2025
Published: 30.11. 2025