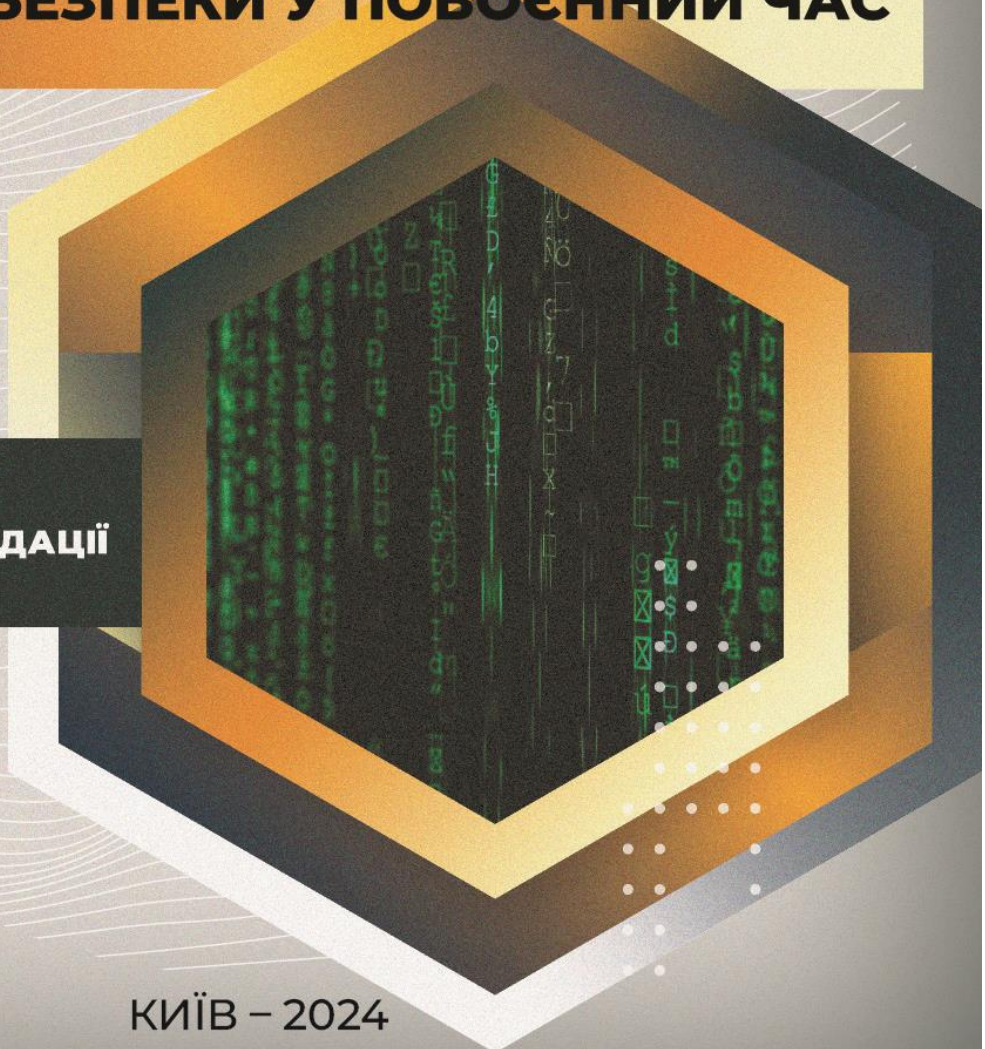
НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ ПЕДАГОГІЧНОЇ ОСВІТИ І ОСВІТИ ДОРОСЛИХ
ІМЕНІ ІВАНА ЗЯЗЮНА

Відділ теорії і практики педагогічної освіти

ПЕТРЕНКО Л.М., СУЛТАНОВА Л.Ю.

ПІДГОТОВКА ВИКЛАДАЧА ЗАКЛАДУ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ ДО ЦИФРОВОЇ БЕЗПЕКИ У ПОВОЄННИЙ ЧАС



МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

КИЇВ – 2024

НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ ПЕДАГОГІЧНОЇ ОСВІТИ І ОСВІТИ ДОРОСЛИХ
ІМЕНІ ІВАНА ЗЯЗЮНА

Відділ теорії і практики педагогічної освіти

ПЕТРЕНКО Л.М., СУЛТАНОВА Л.Ю.

ПІДГОТОВКА ВИКЛАДАЧА ЗАКЛАДУ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ ДО ЦИФРОВОЇ БЕЗПЕКИ У ПОВОЄННИЙ ЧАС

Методичні рекомендації

Київ
ТОВ «Юрка Любченка»
2024

УДК 378:373.3/.5.091.12.011.3-051]:[37.011.2:004.056]"364/366"(072)

Рекомендовано до друку
вченою радою Інституту педагогічної освіти і освіти дорослих імені
Івана Зязюна НАПН України (протокол № 18 від 28 грудня 2023 року)

П-30 Петренко Л. М., Султанова Л. Ю. Підготовка викладача закладу вищої педагогічної освіти до цифрової безпеки у повоєнний час: методичні рекомендації / Київ: Вид-во ТОВ «Юрка Любченка», 2024. Електронне видання. 71 с.

ISBN 978-617-7221-96-7

Рецензенти:
Артюшина М.В., доктор педагогічних наук, професор;
Карташова Л. А., доктор педагогічних наук, професор.

Авторами розкрито багатоаспектність цифрового потенціалу університету та його роль у розвитку ефективних цифрових освітніх екосистем для імплементації інноваційних моделей та педагогічних технологій професійного розвитку науково-педагогічних кадрів; узагальнено нормативно-правові засади, які становлять основу для розроблення політики цифрової безпеки в закладах педагогічної вищої освіти. Обґрунтовано структуру і зміст компетентностей з цифрової безпеки як складової цифрової компетентності викладачів закладів вищої педагогічної освіти; висвітлено дані з діагностування рівня володіння здобувачами вищої освіти компетентностями із цифрової безпеки, спрогнозовано напрями підготовки викладачів закладів вищої педагогічної освіти до цифрової безпеки у повоєнний час.

Для здобувачів закладів вищої освіти, а також магістрантів, аспірантів, науково-педагогічних працівників – усіх, хто цікавиться питаннями цифрової безпеки в сучасному суспільстві та прагне сформувати й удосконалити її в процесі професійної підготовки, підвищення кваліфікації та в системі безперервної освіти і освіти дорослих.

УДК 378:373.3/.5.091.12.011.3-051]:[37.011.2:004.056]"364/366"(072)

ISBN 978-617-7221-96-7

ЗМІСТ

ПЕРЕДМОВА

Другий рік поспіль на території України триває війна за незалежність та територіальну цілісність. Від рук агресора гине й цивільне населення. Росія нищить українську культуру та руйнує наші міста і села. Локальні, регіональні та глобальні наслідки цієї війни трансформують усталений світоустрій, діяльність соціальних інститутів, життя кожного українця. Війна змінила та обмежила умови функціонування національної освітньої системи, вразливої до зовнішніх чинників – соціально-економічних, політичних, правових тощо.

Нині під час воєнних дій, коли продовжується реформування освітньої галузі, тема підготовки майбутніх викладачів закладу вищої педагогічної освіти є дуже актуальною і водночас складною для вивчення. Від початку оголошення воєнного стану проведено низку науково-практичних конференцій, методологічних семінарів з виданням матеріалів на цю тему, опубліковано монографії і посібники, статті в наукових журналах, проте не вистачає ґрунтовних теоретичних досліджень, для проведення яких недостатньо часу.

Разом з цим, сьогодні маємо прогнозувати підготовку майбутніх викладачів закладу вищої педагогічної освіти в інших умовах – у повоєнний час. У цьому плані заслуговують на увагу висновки вчених – фахівців Світового банку, зроблені на основі вивчення досвіду різних країн, які пережили воєнні конфлікти у період 1994 – 2002 рр. Такий досвід висвітлений у наукових працях Т. Шульц (Schultz, 1961)[1], Ч. Р. Кіндлебергер (Kindleberger, 1967)[2], Е. А. Ханушек та Д. Д. Кімко (Hanushek, Kimko, 2000)[3], Е. Мейсон, М. Д. Кім. Д. Перкінс та ін. (Mason, Kim M., Perkins, Kim, K., & Cole, 1980)[4] та інших зарубіжних авторів. Його цінність для України безумовна, і він свідчить про одностайність думки дослідників відносно того, що драйвером економічного зростання після війни є освіта, яка має відповідати технологічному рівню економіки (Buckland, 2005, p. 79–81)[5].

На наш погляд, відповіді на виклики, що постануть перед науково-педагогічними колективами закладів вищої педагогічної освіти, також слід шукати в наукових працях вітчизняних учених з історії педагогіки, в яких висвітлюється практика підготовки майбутніх викладачів у різні повоєнні періоди, зокрема: Р. Вінничук[6], Р. Євсовича[7], Т. Скорик[8], І. Таможської[9] та ін.

---

[1] Schultz, T. W. (1961). Investment in Human Capital. *The American Economic Review*, 51(1). 1–17.

[2] Kindleberger, C. P. (1967). *Europe's postwar growth: The role of labor supply.* Harvard University Press. https://doi.org/10.4159/harvard.9780674498181

[3] Hanushek, E. A., & Kimko, D. D. (2000). Schooling, labor force quality, and the growth of nations. *American Economic Review*, 90. No. 5 (December). 1184–1208.

[4] Mason, E. S., Kim, M. J., Perkins, D. H., Kim, K. S., & Cole, D. C. (1980). *The Economic and Social Modernization of the Republic of Korea.* Cambridge, MA: Harvard University Press.

[5] Buckland, P. (2005). *Reshaping the future: Education and postconflict reconstruction*. World Bank Publications.

[6] Винничук, Р. В. (2023). *Система професійної підготовки магістрів гуманітарної галузі на аксіологічних засадах*. [Дис. д-ра. пед. наук, Полтавський національний педагогічний університет імені В. Г. Короленка]. URL: http://pnpu.edu.ua/wp-content/uploads/2023/10/dysertacziya_vynnychuk_26.10.pdf

Певну цінність для трансформації підготовки майбутніх викладачів закладів вищої педагогічної освіти в післявоєнний період можуть мати результати дослідження сучасного зарубіжного досвіду, представленого в рукописах дисертацій Н. Долінської[10], О. Юзик[11], С. Черкашина[12] тощо.

Проблему підготовки викладачів закладу вищої педагогічної освіти на сьогодні маємо розглядати крізь призму причин і наслідків російської агресії проти України, відновлення країни і реформування освітньої системи, євроінтеграції та інтернаціоналізації, розвитку національної ідентичності і патріотизму, цифровізації суспільства. Сучасна педагогічна наука повинна розвиватися «на нових методологічних основах, що має привести до появи нового покоління досліджень, які розглядають Україну в структурі європейського та світового освітніх просторів»[13].

Ідея підготовки майбутніх викладачів закладу вищої педагогічної освіти до цифрової безпеки у повоєнний час зумовлена постійними змінами в сучасній освіті, поширенням практики застосування цифрових засобів навчання, різних навчальних платформ, соціальних мереж, пошукових систем для знаходження інформації, що пов'язано з інформаційною безпекою і кіберзагрозами, кількість і різноманітність яких важко передбачити.

Пропоновані методичні рекомендації підготовлені в рамках виконання теми наукового дослідження «Теорія і практика підготовки майбутнього викладача закладу вищої педагогічної освіти до професійної діяльності в умовах цифровізації суспільства». Автори розкривають багатоаспектність цифрового потенціал університету (основні складові) та його роль у розвитку ефективних цифрових освітніх екосистем для імплементації інноваційних моделей та педагогічних технологій професійного розвитку науково-педагогічних кадрів. Нормативно-правові засади, представлені в методичних рекомендаціях, становлять основу для розроблення політики цифрової безпеки в закладі педагогічної вищої освіти, дають уявлення про розподіл відповідальності за забезпечення кібербезпечної цифрової трансформації між урядами, підприємствами та громадянами. Обґрунтовані структуру і зміст

---

[7] Євсович, Р. В. (2021). *Гуманізація та гуманітаризація вищої освіти України кінця XX початку XXI століть (1985–2012 рр.)*. [Дис. канд. пед. наук, Рівненський державний гуманітарний університет]. URL: https://www.rshu.edu.ua/images/afto/disert_evsovich_rv.pdf

[8] Скорик, Т. В. (2021). *Теорія і практика професійної успішності майбутнього вчителя у закладах вищої освіти України (друга половина XX – початок XXI століття)*. [Дис. д-ра пед. наук, Комунальний вищий навчальний заклад "Херсонська академія неперервної освіти" Херсонської обласної ради].

[9] Таможська, І. В. (2020). *Теоретичні і методичні засади підготовки науково-педагогічних кадрів в університетах України (друга половина XIX– початок XX століття).* [Дис. д-ра пед. наук, Харківський національний університет імені В.Н. Каразіна]. URL: https://uacademic.info/ua/document/0520U101620

[10] Долінська, Н. В., 2019. *Педагогічна складова у системі підготовки викладачів в університетах США*. [Дис. канд. пед. наук, Львівський національний університет імені Івана Франка].

[11] Юзик, О. П., 2022. *Теоретичні та методичні засади підготовки вчителя інформатики у Польщі (друга половина XX – поч. XXI ст.)*. [Дис. д-ра пед. наук, Рівненський обласний інститут післядипломної педагогічної освіти].

[12] Черкашин, С. В. (2021). *Розвиток університетської освіти Німеччини (XX – початок XXI століть)*. [Дис. д-ра пед. наук, Харківський національний педагогічний університет імені Г. С. Сковороди].

[13] Пуховська, Л. (2011). Теоретичні засади професійного розвитку вчителів: рух до концептуальної карти. *Порівняльна професійна педагогіка.* (1), 97-106. URL: http://hdl.handle.net/20.500.12424/371290.

компетентності з цифрової безпеки як складової цифрової компетентності викладачів закладів вищої педагогічної освіти доцільно використовувати при плануванні освітнього процесу, добору змісту навчання з цифрової безпеки для майбутніх фахівців різних спеціальностей. Автори вважали за необхідне висвітлити дані з діагностування рівнів володіння магістрів закладів вищої освіти з цифрової безпеки для визначення «прогалин» у знаннях і прийняття рішень для подальшого розгортання досліджень із заявленої проблеми – цифрової безпеки.

Ці методичні рекомендації мають на меті допомогти гарантам освітньо-професійних і освітньо-наукових програм, науково-педагогічним працівникам підвищити якість підготовки майбутніх викладачів закладів вищої педагогічної освіти для їхньої професійної діяльності в умовах цифровізації суспільства, розвиток якого буде незупинним у повоєнний час. Тому прогнозування підготовки цих фахівців у повоєнний час є доцільним, окреслює широкий спектр їхньої діяльності в суспільстві (наприклад, заклад освіти – локальний рівень, громада – регіональний рівень, органи влади – державний рівень), де навички з цифрової безпеки будуть завжди в нагоді.

Автори висловлюють сподівання, що структурна організація методичних рекомендацій, логічний взаємозв'язок між різними формами відтворення інформативного змісту дасть змогу використовувати їх для професійного розвитку, самоосвіти і самовдосконалення як бакалаврам та магістрам, так і аспірантам, науково-педагогічним працівникам, здобувачам освіти, слухачам курсів підвищення кваліфікації.

ВИКОРИСТАННЯ ЦИФРОВОГО ПОТЕНЦІАЛУ В ПІДГОТОВЦІ МАЙБУТНІХ ВИКЛАДАЧІВ ЗАКЛАДІВ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ

Підготовка майбутніх викладачів закладу вищої педагогічної освіти тривалий час знаходиться в центрі уваги науковців не тільки тому, що відбувається реформування національної системи освіти, але й тому, що саме йому належить бути носієм високої професійно-педагогічної культури, прикладом профактивності і державницького ставлення до створення інтелектуального і духовного потенціалу нації, творчих пошуків найкращих моделей професійного розвитку[14]. На них державою покладається відповідальність за підготовку тих, хто нині будує Нову українську школу (НУШ) і формує особистість, її громадянську позицію та моральні якості[15].

[14] Петренко, Л. М. (2023). Професійна підготовка майбутнього викладача педагогічного вищого закладу освіти у руслі світоглядних ідей Івана Зязюна. *Фундатор «педагогіки добра» і добротворення в педагогіці: збірник матеріалів до 85-річчя з дня народження Івана Зязюна,87-91*. Київ: Вид-во ТОВ «Юрка Любченка». URL: https://lib.iitta.gov.ua/735208/1/fundator-sity_11.05.2023.pdf

[15] Про схвалення Концепції реалізації державної політики у сфері реформування загальної середньої освіти «Нова українська школа» на період до 2029 року. Розпорядження Кабінет Міністрів України від 14.12.2016 р. № 988-р URL: https://www.kmu.gov.ua/npas/249613934

У закладі вищої педагогічної освіти здійснюють підготовку вчителів до реалізації головних компонентів концепції НУШ (рис. 1).

Рис. 1. Цільові орієнтири підготовки сучасного викладача закладу вищої педагогічної освіти[16]

Постійні зміни, що відбуваються в сучасному світі потребують від учителів постійного розвитку, а це, відповідно, підвищує рівень відповідальності викладачів закладу вищої педагогічної освіти в їхній професійній діяльності, у безперервному розвитку нових компетентностей. Вочевидь, що нові компетентності мають бути пов'язані із завданнями, які їм належить виконувати у процесі своєї викладацької діяльності, а тому необхідно вміти їх виокремлювати – осмислити і виявити. З огляду на ті реформи, які нині відбуваються в Україні, навіть під час війни з російським агресором, актуальними, на наш погляд, будуть три великі взаємозалежні категорії завдань, які наводить Ф. Імбернон (F. Imbernon):

учитель і громада – вимагає від учителя глибоких знань про навколишнє середовище, спільноту в громаді, щоб запроваджувати надбані культурні цінності та традиції у своїй практиці через розроблення проєктів навчальних програм і, відповідно, створення унікальних посібників, спрямованих на навчання за будь-яких обставин, включення локальних контекстуальних змінних у планування та управління процесом викладання і навчання;

учитель і школа як інституція – стосується знань, якими необхідно володіти вчителю про освітню систему, інтеграцію та адаптацію для досягнення повного розвитку, що вказує на доцільність формування низки таких компетентностей, як: культурологічна, технічна і технологічна, адміністративна і організаційна спроможність, здатність до критичного аналізу, рефлексії, адаптації, командної роботи та співпраці, адміністративна компетентність;

[16] Інститут модернізації змісту освіти. Нова українська школа. URL: http://surl.li/gyjiz.

учитель – учень і класний колектив – це найважливіша категорія завдань, що об'єднує знання учнів для полегшення адаптації педагогічних утручань і впливів до рівня зрілості, їхніх потреб та інтересів, вибору моделі оцінювання освітнього процесу і педагогічної практики студентів[17].

З нашої точки зору, названі категорії завдань можуть слугувати науково-педагогічним працівникам певним вектором у розробленні навчальних програм, змісту навчальних дисциплін, формулюванні тем курсових і дипломних робіт, тематики науково-дослідної роботи та проєктів. Водночас заклади вищої освіти в умовах розвитку інформаційного (знаннєвого) суспільства наближаються до регіональних місцевих громад, які сьогодні мають усі можливості для гнучкого і невідкладного реагування на виклики і потреби місцевих галузей, підприємств і суспільних груп для їх забезпечення фахівцями з необхідних професій, інноваційними розробками, програмами, проєктами тощо[18].

Трансформація вищої освіти у післявоєнну добу відбуватиметься в умовах цифровізації суспільства[19]. У Стратегії розвитку вищої освіти України на 2022–2032 роки цифровізація визначена одним з пріоритетних напрямів та інструментом підвищення ефективності професійної підготовки фахівців для відновлення національної економіки в повоєнні часи[20]. До основних орієнтирів розбудови вищої освіти віднесено прискорення розвитку ефективних цифрових освітніх екосистем (рис. 2), що потребує наявності розвинутої інфраструктури, зв'язку і цифрового обладнання та ефективного планування і розвитку цифрового потенціалу, який складається з: 1) сучасних організаційних можливостей; 2) підготовлених наукових, науково-педагогічних та педагогічних працівників, які володіють цифровими компетентностями; 3) високоякісного освітнього наповнення, інструментів і безпечних платформ, що відповідають стандартам приватності й етики та є зручними для користувачів; 4) допоміжних технологій для осіб з інвалідністю, що відповідають стандартам приватності й етики та є зручними для користувачів; 5) допоміжних технологій для осіб з інвалідністю, що спроможні розвивати цифрові компетентності для цифрової трансформації; 6) цифрових умінь і компетентностей для цифрової трансформації, підготовка більшої кількості фахівців у цій сфері, зокрема з урахуванням гендерного балансу[21].

---

[17] Imbernon, F. (1989). *La formación permanente del profesorado.* Col. Cuadernos de Pedagogía. Laia. Barcelona.

[18] Петренко, Л.М. (2019). Академічна свобода як фундаментальна цінність. *Розвиток професійної культури майбутніх фахівців: виклики. досвід, стратегії і перспективи: збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції, 107-110.* Ірпінь: Ірпінський державний коледж економіки та права. URL: https://api-ir.dpu.edu.ua/server/api/core/bitstreams/2a2792ac-a1dd-4061-a95f-f0b0c59f25e6/content

[19] Національна рада з відновлення України від наслідків війни. (2022). *Проект плану відновлення України. Матеріали робочої групи «Освіта і наука».* URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/education-and-science.pdf

[20] Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 рр. Розпорядження Кабінету Міністрів України від 23.02.2022 р. № 286-р. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

[21] Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 рр. Розпорядження Кабінету Міністрів України від 23.02.2022 р. № 286-р. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

Рис. 2. Розвиток ефективних цифрових освітніх екосистем: компоненти цифрового потенціалу

Кожний із названих компонентів може бути реалізований за умови грамотно підібраних і запроваджених цифрових інструментів. Наприклад, для реалізації сучасних організаційних можливостей (компонент 1) широко використовується LMS Moodle (Modular Object-Oriented Dynamic Learning Environment, вимовляється «Мудл») – модульне об'єктно-орієнтоване динамічне навчальне середовище, яке називають також системою управління навчанням (Learning Management System). LMS Moodle – одна із найпопулярніших навчальних систем, яка застосовується не тільки закладами освіти різних типів, але і в корпоративному навчанні, і в підвищенні кваліфікації. Вона включає організаційні методи, пов’язані із жорстким розподілом функцій між виконавцями, які діють на основі чіткої регламентації і контролю, та забезпечує організаційно-методичну підтримку освітнього процесу. Її використовують не тільки при дистанційному або змішаному навчанні, але й при традиційній організації освітнього процесу, оскільки LMS Moodle сприяє вдосконаленню педагогічного менеджменту, переводить діяльність усіх суб’єктів навчання у більш продуктивний режим, оскільки чітко її організує в просторі і часі[22]. У ролі такої організуючої моделі може бути і Office 365 Education, що включає Word, Excel, PowerPoint, OneNote, Microsoft Teams та додаткові інструменти для навчання (рис. 3), якими можна користуватися на всіх пристроях[23].

[22] Петренко, Л. (2018). Організаційні методи дистанційного навчання в закладах професійної (професійно-технічної) освіти. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми.* (50), 151-156. https://vspu.net/sit/index.php/sit/article/view/4777

[23] Office 365 Education. URL: http://surl.li/awfx

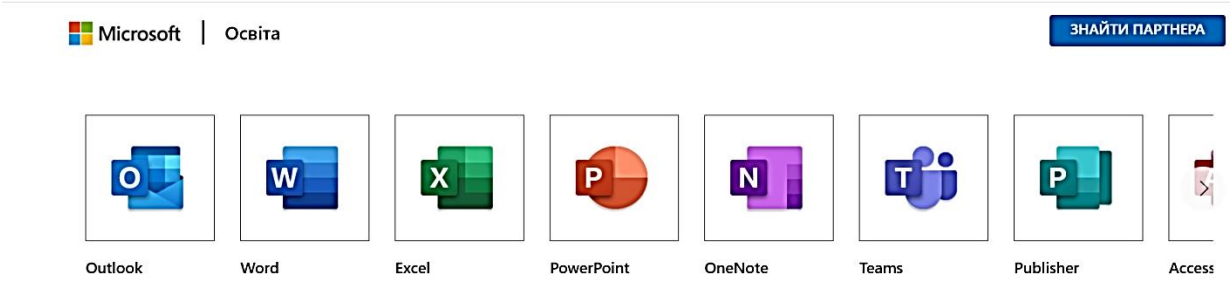


Рис. 3. Інструменти Office 365 Education

До переваг LMS відносять:

–зниження витрат і підвищення ефективності;

–культуру безперервного навчання;

–упровадження хмарних технологій та видимість рентабельності інвестицій;

–забезпечення відповідності нормативним вимогам;

–професійний розвиток та підвищення ефективності роботи персоналу;

–підвищення залученості здобувачів освіти[24].

У багатьох українських закладах вищої освіти використовують LMS, але дуже часто не весь її потенціал працює на якість організації освітнього процесу. Однією з причин є недостатня підготовленість науково-педагогічного персоналу до використання всіх її функцій, а іншою – зазначена система потребує постійної підтримки адміністратора, що не завжди забезпечується з боку адміністрації закладу вищої освіти. Потрібно зазначити, що при використанні LMS можна додатково застосовувати різні цифрові інструменти, відповідно до мети певного виду діяльності, – лекції, семінарського або практичного заняття, самостійної роботи або науково-дослідної діяльності.

Наукові, науково-педагогічні та педагогічні працівники, які володіють цифровими компетентностями (компонент 2), – є важливою педагогічною умовою використання цифрового потенціалу повною мірою в професійній підготовці майбутніх викладачів закладів педагогічної вищої освіти. Безумовно, опанування цифровою компетентністю потребує від кожного викладача певного часу і зусиль, і одного семінару (вебінару або майстер-класу) буде недостатньо. Це постійний процес, оскільки кожного року з'являється нове програмне забезпечення, нові хмарні технології, цифрові інструменти. Цифрові уміння і навички, цифрова компетентність розвиваються тільки в практичній діяльності. У зарубіжних закладах вищої освіти часто в їх структуру включають відділи із інформаційного супроводу освітнього процесу і діяльності викладачів. Вони мають різні назви, але дуже подібні функції.

Саме від якості цих двох компонентів – сучасних організаційних можливостей і підготовлених наукових, науково-педагогічних та педагогічних працівників, які володіють цифровими компетентностями, – залежить повнота і якість застосування інших чотирьох, показаних на рис. 2.

[24] Що таке система управління навчанням (LMS)? URL: http://surl.li/pfckp

Ефективне використання цифрового потенціалу для розвитку університетів можливе за умови входження в Європейський освітній простір вищої освіти, впровадження проєктної діяльності та продовження інтернаціоналізації, що передбачає активний розвиток національного простору освіти, тобто системи закладів освіти та взаємодії «всіх суб'єктів освітнього простору в межах національної держави щодо вироблення та реалізації єдиної стратегії розвитку освіти на єдиних когнітивних засадах» (Якимчук, 2015)[25].

Під філософсько-когнітивними основами розвитку освіти О. Якимчук пропонує розуміти «комплекс світоглядно-духовних характеристик, що узагальнюють уявлення людей» стосовно «значення освіти в житті суспільства», перспектив її розвитку «в межах держави та визначають специфіку мислення і пізнавальної діяльності суб'єктів освіти (Якимчук, 2015, с. 7)[26]. Ґрунтуючись на основних положеннях її дисертаційної роботи, маємо акцентувати увагу на необхідності подолання «відголосків централізованої адміністративної системи», які проявляються у «посттоталітарних освітніх практиках», «посттоталітарній свідомості», впливають на взаємовідносини в системі «викладач-студент» залишаються суб'єкт-об'єктними, монологічними тощо. Цілком погоджуємося з автором у тому, що оновленню світоглядного фундаменту освіти й «остаточному викоріненню посттоталітарних підходів організації мислення і пізнання з освітнього простору» сприятиме:

упровадження сучасних педагогічних моделей, розроблених на демократичних принципах організації освітнього процесу в закладах вищої освіти;

продуктивне оновлення когнітивних, світоглядних засад освітньої діяльності, що базуються на нелінійних пізнавальних підходах, завдяки яким мислення може реалізувати свій потенціал в якості гнучкого (флексибільного, творчого, дивергентного тощо) інструментів пізнання та аналізу отриманих знань;

вивчення рідної мови, історії державотворення, особливостей природи, розкриття досягнень культури (як духовної, так і матеріальної) народу, традицій та звичаїв, народних ремесел, регіональних традицій використовувати як важливий інструмент утвердження національного освітнього простору, посилення світоглядної компоненти, що забезпечує національну самобутність освіти та ресурс розвитку системи;

трансформація моделей пізнання та мислення у бік гармонізації з європейськими аналогами, побудованих на потребі демократизації взаємин між усіма суб'єктами освіти, на визнанні толерантності як ключового світоглядного орієнтиру уможливить здійснення низки кроків для максимізації ефективності процесів розвитку українського освітнього простору, зокрема у вищій школі,

---

[25] Якимчук, О.І. (2015). *Філософсько-когнітивні засади розвитку національного простору освіти* [Дис. канд. наук філософ. наук, Національний педагогічний університет імені М. П. Драгоманова]. URI: http://enpuir.npu.edu.ua/handle/123456789/41031

[26] Якимчук, О.І. (2015). *Філософсько-когнітивні засади розвитку національного простору освіти* [Дис. канд. наук філософ. наук, Національний педагогічний університет імені М. П. Драгоманова]. URI: http://enpuir.npu.edu.ua/handle/123456789/41031

яка є найбільш вираженою ареною трансформаційних процесів, орієнтованих на європейську перспективу (Якимчук, 2015, с. 8-10)[27].

Таким чином, справжнім драйвером упровадження інноваційних моделей та педагогічних технологій професійного розвитку майбутніх викладачів закладів вищої педагогічної освіти стала цифровізація освітнього простору, яка набула масштабного поширення з початком пандемії COVID-19 і продовжує свій розвиток нині, під час воєнних дій і, безумовно, буде невід'ємною складовою у повоєнний період. Це дає змогу швидко реагувати на нові зовнішні виклики і змінювати структуру освітнього процесу відповідно до нових завдань.

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЦИФРОВОЇ БЕЗПЕКИ В ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ВИКЛАДАЧІВ ЗАКЛАДІВ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ

Освіта є одним із базових елементів цифрових інновацій та цифрової економіки загалом, а вища освіта покликана постійно збільшувати підготовку фахівців, які володіють новими технологіями, необхідними для досягнення конкурентної переваги у цифровому світі. Наразі важко уявити собі організацію освітнього процесу в будь-якому закладі освіти без використання електронних освітніх ресурсів, платформ і сервісів для дистанційного та змішаного навчання. До речі, інтернет-простір широко використовується всіма верствами населення для пошуку різної інформації. За останні десять років кількість користувачів інтернету збільшилась майже вдвічі – з 2,18 мільярда на початку 2012 року до 4,95 мільярда на початку 2022 року. Це приводить до сукупного річного темпу зростання (CAGER) на рівні 8,6 % за останнє десятиліття в цілому, однак річні темпи зростання суттєво коливалися. У січні 2022 року налічувалось 62.2022 мільярда користувачів соціальних мереж, що становить 58,4 % від загальної чисельності населення планети, хоча доцільно зазначити, що користувачі соціальних мереж можуть не бути постійними. Чисельність постійних користувачів соціальних мереж зросла більше, ніж на 10 % за останні 12 місяців, тобто впродовж 2021 року з'явилося 424 мільйона нових користувачів[28].

За даними Укрінформ, близько 78% українців щодня чи майже щодня користуються інтернетом. За результатами всеукраїнського опитування громадської думки «Омнібус», яке провів Київський міжнародний інститут соціології (КМІС) 13–18 травня 2022 року методом телефонних інтерв'ю з використанням комп'ютера на основі випадкової вибірки мобільних

[27] Якимчук, О.І. (2015). *Філософсько-когнітивні засади розвитку національного простору освіти* [Дис. канд. наук філософ. наук, Національний педагогічний університет імені М. П. Драгоманова]. URI: http://enpuir.npu.edu.ua/handle/123456789/41031

[28] Didgital 2022: Global Overview Report. Дата звернення: Квіт. 01, 2023. [Online]. URL: https://datareportal.com/reports/digital-2022-global- overview-report

телефонних номерів, міське населення частіше використовує інтернет, ніж сільське, відсоток активних користувачів ним зменшується зі зростанням віку. Також виявлено, що чим вища освіта в українця/ки, тим частіше він/вона користуються інтернетом, а найчастіше використовують інтернет українці віком від 18 до 49 років.

Слід зазначити, що опитування проводилося з дорослими (віком 18 років і старше) громадянами України, які на момент опитування проживали на території України (у межах, які контролювалися владою України до 24 лютого 2022 року)[29]. За даними MarTech-агентство Newage, яке здійснює щорічне дослідження інтернет-трендів України, встановлено, що станом на травень-червень 2022 року на неокупованій території знаходилось ~ 22,1 млн. громадян у віці 14–70 років, з яких близько 19 млн. користувались інтернетом. І якщо значна частина цих користувачів у березні читали більше новини на семи із 20 найбільш популярних сайтах, до яких відносяться суспільно-політичні ЗМІ та «умовно-новинні» Телеграм і Youtube, то в квітні-травні 2022 р. ситуація змінилась. Трафік новинних сайтів почав падати, натомість більше уваги користувачі стали приділяти ecommerce-сайтам, та значно зріс інтерес до освітніх сайтів – «На урок» та Brainly (Znanija.com).

Нині спостерігається активний розвиток національної системи автоматизованого інформаційного комплексу освітнього менеджменту з використанням різних онлайн-інструментів, наприклад, для закладів освіти – «Педрада»[30], що зумовлює необхідність вивчення питання створення безпекового цифрового середовища. Доступ до інтернету є фундаментальним правом кожної людини, зокрема учасників освітнього процесу, і користування цим відкритим вільним простором, у якому відбувається обмін ідеями, інформацією та знаннями, соціальна взаємодія і спілкування людей, залишається необмеженим.

Сьогодні немає сенсу доводити серйозний вплив інформаційного середовища на інтелектуальний, фізичний та психічний розвиток шкільної і студентської молоді. Він цілком зрозумілий. З однієї сторони, забезпечення доступу до інформаційних ресурсів, упровадження інтерактивних технологій, застосування електронних освітніх ресурсів, різних форматів надання інформації уможливлює суттєве підвищення якості професійної підготовки фахівців для різних галузей економіки, а з іншої – з'явилися нові ризики та загрози для всіх учасників освітнього процесу. Їх перелік достатньо різноманітний: ерозія культурної складової освітнього процесу, зростання інтернет-адикації (інтернет-залежності), можливість несанкціонованого доступу до персональних даних, кібер-мобінг, наповнення фейками інтернет-медіа і соціальних мереж, хейтинг та безліч інших питань, які актуалізують інформаційну проблематику, зокрема цифрову безпеку в громадянському суспільстві. Ми є свідками того, як «за останні роки загрози

[29] Черьомухіна, О. (2022). *Користування інтернетом серед українців: результати телефонного опитування, проведеного 13–18 травня 2022 року.* Пресреліз. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1115&page=1

[30] Педрада. Портал освітян України. Безпечне освітнє середовище закладу освіти. URL: https://www.pedrada.com.ua/article/2614-bezpechne-osvtn- seredovishche-zakladu-osvti

порушення інтересів людей, самої держави й в цілому людства в кіберпросторі перейшли із потенційних та гіпотетичних на цілком реальні. Тож протистояння їх поширенню стало пріоритетним завданням на національному рівні урядів та міжнародної спільноти»[31]. Підтвердженням цьому є дані Cybersecurity Ventures: у 2023 році на боротьбу з кіберзлочинністю світ витратив 8 трил. доларів. У 2022 році середня вартість витоку даних склала 4,35 млн доларів. Саме цим пояснюється щорічне зростання інвестицій у кібербезпеку та потреби кадрів у сфері кібербезпеки – 3,5 млн незаповнених вакансій у всьому світі до 2025 року[32].

Державами-членами Ради Європи та іншими країнами у 2001 році підписано Конвенцію про кіберзлочинність, яка була ратифікована Верховною Радою України в 2005 році[33]. Як зазначалось вище, з кожним роком кількість кібератак лише зростає, дедалі вони стають все більш складнішими і надходять із широкого кола джерел. З метою підвищення стійкості до кіберзагроз та забезпечення отримання громадянами й бізнесом вигоди від надійних цифрових технологій, в ЄС розроблено і прийнято Стратегію кібербезпеки. У цьому документі розділено відповідальність за забезпечення кібербезпечної цифрової трансформації між урядами, підприємствами та громадянами[34].

В іншому документі – Європейській Декларації про цифрові правах і принципи цифрового десятиліття[35] – наголошується на тому, що цифрова трансформація торкається усіх аспектів життя людей: розширення можливостей для покращення якості їхнього життя, впровадження інновацій, значного економічного зростання і сталості. У ній також сформульовано нові завдання для структури, безпеки і стабільності національних суспільств і економік. Основною метою зазначеної Декларації є роз'яснення (визначення правил) щодо дотримання європейських цінностей і основних прав людини в онлайн-освіті[36].

Зважаючи на широкий і швидкий розвиток платформ цифрових послуг, а також дебати щодо загальнодоступних просторів даних і нових технологій, таких як штучний інтелект, що впливають на всі сфери нашого суспільства, Європейською Комісією прийнято Цифровий порядок денний на 2020–2030 рр.[37]. На наш погляд, особливої уваги менеджерів освітнього процесу в педагогічних закладах вищої освіти заслуговує комплекс

---

[31] Мальцева, І. Р., Черниш, Ю. О., Штонда, Р. М. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 4(16), 37– 44. DOI: https://doi.org/10.28925/2663-4023.2022.16.3744

[32] Yoshitaka, S. (2023). Top 10 Digital Transformation Trends for 2023. URL: https://www.upwork.com/resources/top-digital-transformation-trends.

[33] Конвенція про кіберзлочинність Міжнародний документ від 23.11.2001 № 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

[34] Europe's Digital Decade: digital targets for 2030. https://commission.europa.eu/strategy-and-policy/priorities-019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets- 2030_en.

[35] European Commission. Shaping Europe's digital future. European Declaration on Digital Rights and Principles. 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-principles

[36] Europe's Digital Decade: digital targets for 2030. https://commission.europa.eu/strategy-and-policy/priorities-019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets- 2030_en.

[37] Fact Sheets on the European Union. Digital Agenda for Europe. 2020. URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digit al-agenda-for-europe.

інформаційних бюлетенів ЄС, представлений на сайті Європейського парламенту, який розглядає питання, пов'язані зі створенням безпечних цифрових просторів і послуг, створенням рівних умов для цифрових ринків з великими платформами та зміцнення цифрового суверенітету Європи, одночасно сприяючи досягненню європейської мети кліматичної нейтральності до 2050 р. Ознайомлення з означеною інформацією уможливить випереджальне розроблення навчальних програм і контенту навчальних дисциплін з підготовки фахівців, спрямованих на формування в них та науково-педагогічних працівників цифрової компетентності.

Війна в інформаційному просторі України, яка продовжується вже тривалий час, «завдає не меншої шкоди, аніж війна на полі бою. І це без жодних перебільшень»[38]. Аналіз адміністративно-правових основ кібербезпеки показав, що у відповідь на застосування російською федерацією технологій гібридної війни, Радою національної безпеки і оборони України в січні 2016 року було ухвалено рішення щодо проєкту Стратегії кібербезпеки України. Її основною метою є «створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави»[39]. З метою протистояння загрозам, спрямованим на свідомість громадян, розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, що перетворило інформаційну сферу на ключову арену протиборства, була прийнята Доктрина інформаційної безпеки України. Одним із пріоритетів державної політики в інформаційній сфері визначено «підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності»[40].

Нові виклики (розвиток інформаційних технологій та їх конвергенція з технологіями штучного інтелекту; визнання кіберпростору разом з іншими фізичними просторами є одним з можливих театрів воєнних дій; деструктивна активність російської федерації – вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури; зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі; постійне вдосконалення та розроблення нових інструментів та механізмів реалізації кіберзагроз; посилення тенденції щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, вплив на виборчі процеси; перехід на 5G-мережі, функціонування яких кардинальним чином залежить від коректної роботи програмного забезпечення, що за рахунок новизни технології може мати нові, непередбачені загрози; пандемія COVID-19, яка очевидно матиме довготривалий вплив на світовий порядок, посилюючи роль електронних

[38] Мальцева, І. Р., Черниш, Ю. О., Штонда, Р. М. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 4(16), 37– 44. DOI: https://doi.org/10.28925/2663-4023.2022.16.3744

[39] Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Указ Президента України № 96/2016 від 27.01.2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

[40] Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України». Указ Президента України № 47/2017 від 29.12.2016 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних тощо) та швидкозмінюваний цифровий світ зумовили «формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя»[41].

Серед пріоритетів національних інтересів, окреслених у Стратегії кібербезпеки України (2021), слід акцентувати увагу на створенні умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Цим документом передбачається залучення широкого кола учасників до вирішення завдань у сфері кібербезпеки, у тому числі суб'єктів господарювання, громадських об'єднань та окремих громадян України. Прогнозується розроблення Загальнонаціональної програми кіберграмотності. Вона має спрямовуватися на підвищення рівня цифрової грамотності населення України, зокрема шляхом включення питань до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти з формування цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним. Основні положення цього документа конкретизовано Планом реалізації Стратегії кібербезпеки України, схваленим 30 грудня 2022 року[42].

Варто зазначити, що питання формування цифрових навичок у громадян України розглядається на державному рівні. На основі європейської концептуально-еталонної Рамки цифрових компетентностей для громадян ЄС та рекомендацій (DigComp 2.1: The Digital Competence Framework for Citizens) щодо формування цифрових компетентностей від європейських та міжнародних інституцій Міністерством цифрової трансформації України в 2021 році було розроблено Рамку цифрової компетентності для громадян України. Ця рамка обговорена та вдосконалена в експертному середовищі із залученням представників експертно-консультативного Комітету з цифрових технологій при Міністерстві освіти і науки, експертів мережі eSkills Програми EU4 Digital в Україні та експертів Комітету з питань цифрових навичок Української національної цифрової «Коаліції цифрової трансформації»[43].

Рамка містить 4 виміри, 6 сфер, 30 компетентностей та 6 рівнів володіння цифровими компетентностями. Безпека у цифровому середовищі є однією із шести сфер компетентностей, визначених у першому вимірі. До її структури

[41] Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Указ Президента України № 447/2021 від 14.05.2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[42] Про рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України». Указ Президента України № 37/2022 від 30.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text

[43] Опис рамки цифрової компетентності для громадян України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/20 21/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya- gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf

віднесено такі компетентності: захист пристроїв та безпечне підключення до мережі Інтернет; захист персональних даних та приватності, безпека в Інтернеті; захист особистих прав споживача від шахрайства і зловживань; захист здоров'я та благополуччя; захист навколишнього середовища. Принагідно зазначимо, що на основі національного тесту на цифрову грамотність «Цифрограм» (https://osvita.diia.gov.ua/digigram) розроблено окремий тест на діагностування рівня сформованості цифрової компетентності вчителів (додаток 1).

Таким чином, в Україні створено нормативно-правову і організаційну основу для розвитку безпечного інформаційно-освітнього середовища та цифрової компетентності педагогічних працівників. З нашого погляду, імплементація основних положень, описаних вище конвенцій, стратегій, доктрин – справа керівників закладів вищої освіти і науково-педагогічної спільноти. Але зволікати з вирішенням питання розвитку навичок цифрової безпеки сьогодні не можна, оскільки це стосується кожного громадянина. Ґрунтуючись на аналізі нормативно-правових, організаційних, інструктивних та інформаційних документів, розроблених на міжнародному і державному рівнях, уявляється вірогідним проєктування локальної політики (на рівні закладу вищої освіти) із цифрової безпеки інформаційно-освітнього середовища. Одним із її напрямів має бути діагностика рівнів сформованості навичок цифрової безпеки у суб'єктів освітнього процесу. За нашими переконаннями, важливим вбачається створення програми навчання, тренінгів, воркшопів із формування навичок цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти. Думається, що варто використовувати потенціал різних громадських організацій та волонтерів (фахівців з кібербезпеки) для тестування інформаційної системи закладу вищої освіти. Наприклад, нині активно діє «неофіційний громадський рух кіберопору ворогові, так звана «КіберАрмія». Звичайні люди, поряд із професіоналами сфери ІТ, наносять нищівний удар, атакуючи ворога у кіберпросторі, завдають йому збитків та зривають плани»[44]. Під час війни кожний (студент, викладач) знаходиться в зоні кіберризику, а тому не зайвими будуть різні позааудиторні заходи: семінари, конференції, олімпіади, конкурси, аналітичні звіти, просвітницька діяльність в регіоні й т. ін., спрямовані на розвиток навичок цифрової безпеки.

Таким чином, результати теоретичного аналізу уможливили встановлення низки нормативних, організаційних, інструктивних та інформаційних документів, основні положення яких можуть становити основу для розроблення політики цифрової безпеки в закладі педагогічної вищої освіти. Дані документи розроблено і прийнято на міжнародному й державному рівнях, охарактеризовано в контексті підготовки майбутніх викладачів педагогічних закладів вищої освіти для професійної діяльності в цифровому суспільстві, систематизовано у хронологічному порядку. Виявлено і висвітлено основні положення розподілу відповідальності за забезпечення кібербезпечної цифрової

[44] Мальцева, І. Р., Черниш, Ю. О., Штонда, Р. М. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 4(16), 37– 44. DOI: https://doi.org/10.28925/2663-4023.2022.16.3744

трансформації між урядами, підприємствами та громадянами; з'ясовано нові ризики та загрози для всіх учасників освітнього процесу, зокрема: ерозія культурної складової освітнього процесу, зростання інтернет-адикації (інтернет-залежності), можливість несанкціонованого доступу до персональних даних, кібер-мобінг, наповнення фейками інтернет-медіа і соціальних мереж, хейтинг та безліч інших питань; доведено необхідність формування навичок цифрової безпеки у суб'єктів освітнього процесу; охарактеризовано можливості використання представлених документів з політики цифрової безпеки для професійної підготовки майбутніх викладачів педагогічних закладів вищої освіти. Зазначені положення можуть бути використані при розробленні безпечного освітньо-інформаційного простору закладу вищої педагогічної освіти.

ЦИФРОВА БЕЗПЕКА ЯК КОМПОНЕНТ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ВИКЛАДАЧІВ ЗАКЛАДІВ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ: СУТНІСНІ ХАРАКТЕРИСТИКИ І СТРУКТУРА

Освіта є одним із базових елементів цифрових інновацій та цифрової економіки загалом, а вища освіта покликана постійно збільшувати підготовку фахівців, які володіють новими технологіями, потрібними для досягнення конкурентної переваги в цифровому світі. Нині важко уявити собі організацію освітнього процесу в будь якому закладі освіти без використання електронних освітніх ресурсів, платформ і сервісів для дистанційного та змішаного навчання.

Аналіз наукових досліджень з використанням Національного репозиторію академічних текстів (НРАТ) показав, що проблема інформаційної безпеки тривалий час була в центрі наукових інтересів вітчизняних учених і науково-педагогічних працівників військових вищих закладів освіти, а оприлюднення їх результатів та досвіду формування й розвитку навичок інформаційної безпеки було досить обмеженим. Проте з розширенням доступу до інтернету, експоненціальним зростанням обсягів інформації (друга половина XX століття), питання інформаційної безпеки, а пізніше – цифрової безпеки в галузі освіти почали привертати увагу учених-педагогів. Особливо ця тема актуалізувалася з початком російської агресії в Україну в 2014 році. Із часом її дослідження активізувалось у зв'язку з переходом на дистанційне і змішане навчання в період пандемії SARS-CoV2 (COVID-19)[45]. За останні 20 років українськими вченими здійснено дослідження різних наукових тем з проблем інформаційної безпеки в різних галузях.

[45] Петренко, Л. М. (2021). Аналітичний огляд запиту на публікації з питань професійного розвитку педагогічних і науково-педагогічних працівників. *Інноваційні трансформації в сучасній освіті: виклики, реалії, стратегії: матеріали III Всеукраїнського відкрого науково-практичного онлайн-форуму, 132–135*. Київ: Національний центр «Мала академія наук України».

Одержані результати відображені в 142 дисертаційних роботах (за даними пошуку з використанням поняття «інформаційна безпека»), які розміщені в НРАТ. Нами виявлено, що такі дослідження в галузі знань 01 Освіта/Педагогіка здійснили: С. Воскобойников (2016), Ю. Іванчук (2013), М. Коляда (2012), Л. Конопленко (2016), О. Синекоп (2011), В. Ковальчук (2012).

Аналіз результатів пошуку в базі даних OUCI – пошукова система і база даних наукових цитувань, які надходять від усіх видань, що використовують сервіс Cited-by від Crossref та підтримують Initiative for Open Citations, тема цифрової безпеки в професійній діяльності викладачів педагогічних закладів вищої освіти порушується в наукових публікаціях вітчизняних учених. Так, В. Бондаренко (2019) дослідив умови та засоби формування навичок інформаційної безпеки майбутніх учителів; О. Будник (2020) вивчала особливості формування цифрової грамотності вчителів у контексті безпеки в цифровому суспільстві. Цифрову безпеку педагогів як складову їхньої цифрової компетентності досліджували Г. Генсерук (2021), Л. Канішевська (2022), В. Плаксієнко (2020). У науковій публікації М. Друшляк, яка вивчала інфомедійну грамотність педагогів та обґрунтувала її характеристики, також йдеться про необхідність володіння суб'єктами освітнього процесу навичками цифрової безпеки. У дослідженні М. Прокоф'євої та Л. Султанової (2022) представлено результати опитування студентів та викладачів закладів вищої освіти щодо дотримання ними умов цифрової безпеки, запропоновано шляхи їх вирішення та здійснено фрагментарний аналіз основних документів, які регламентують формування навичок цифрової безпеки у громадян України.

На сьогодні в педагогічній спільноті й у колі науковців звичним стало використання понять «інформатизація освіти» та «цифровізація освіти». Однак синхронне застосування цих наукових категорій, на наш погляд, потребує пояснення. Тому вважаємо доречним зауважити, що ці поняття вживаються «як синоніми з тотожним лексичним значенням»[46]. Поширене використання поняття «цифровий» в останні роки пояснюється заміною більшої частини аналогових систем (сфер) на цифрову альтернативу, тобто «переведення у цифровий формат тих аналогових систем, розвиток та підтримка яких є очевидно невигідними та неефективними»[47].

Масовий перехід національних освітніх систем на дистанційне та змішане навчання в період суворого карантину з березня 2020 р., який було оголошено у зв'язку з початком пандемії COVID-19, зумовив необхідність активного опанування цифровими навичками і вміннями науково-педагогічних і педагогічних працівників, аби відреагувати на зміни реальності: виникла потреба в короткий проміжок часу організувати освітній процес у нових умовах – повної ізоляції. У зв'язку з цим виявилися суперечності між необхідністю

[46] Яцишин, А. В. (2020). *Цифрові відкриті системи у підготовці аспірантів і докторантів:* монографія. Київ: ЦП «Компринт».

[47] Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України № 67-р. від 17.01.2018 р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

дотримуватися цифрової безпеки в процесі педагогічної, науково-педагогічної діяльності та недостатньою розробленістю й обґрунтуванням сутнісних характеристик і структури компетентності з цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти. Розв'язання цієї проблеми актуалізувалось у зв'язку з початком широкомасштабної російської агресії, необхідністю релокації 29 закладів вищої освіти та їх структурних підрозділів, масовою еміграцією за кордон населення України та тимчасовою окупацією частини територій.

Пошук шляхів вирішення зазначеної суперечності було спрямовано на вивчення зарубіжного та вітчизняного досвіду, результати якого показали, що структура компетентності з цифрової безпеки відображена в Цифровій рамці компетентностей (DigCompEdu) та рекомендаціях у сфері цифрових компетентностей від європейських та міжнародних інституцій[48]. Вона широко використовується як в Україні, так і в багатьох європейських країнах.

Зазначена Рамка має 4 виміри, 6 сфер, 30 компетентностей і 6 рівнів володіння цифровими компетентностями. Однією із шести сфер компетентностей, визначених у першому вимірі, є безпека в цифровому середовищі, яку можна зобразити у вигляді парасольки (рис. 4).

Рис. 4. Структура компетентності з цифрової безпеки майбутніх викладачів закладу вищої педагогічної освіти

Ця сфера охоплює комплекс компетентностей, який можна розглядати як структуру компетентності майбутнього викладача закладу вищої педагогічної освіти з цифрової безпеки, зокрема: захист пристроїв і безпечне підключення до мережі Інтернет; захист персональних даних і приватності, безпека в Інтернеті; захист особистих прав споживача від шахрайства і зловживань; захист здоров'я та благополуччя; захист довкілля. Безпека в цифровому середовищі віднесена до п'ятої сфери (С4), що охоплює п'ять компетентностей: наявність умінь захищати пристрої та цифровий контент, розуміння ризиків та загроз у цифровому середовищі; наявність знань про заходи безпеки та захисту, враховуючи при цьому питання надійності й приватності.

[48] Опис рамки цифрової компетентності для громадян України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf

Переш ніж висвітлити істотні характеристики компетентності з цифрової безпеки майбутнього викладача закладу педагогічної вищої освіти, на наш погляд, необхідно сформулювати визначення феномену «цифрова безпека організації». Аналіз наукових публікацій уможливлює висновок:

Цифрова безпека організації – це тривалий і безперервний процес, який має починатися з аудиту цифрової безпеки для виявлення ризиків і розуміння захищеності від них та необхідності технічної підтримки.

Цифрова безпека складається із трьох компонентів – технологій, людей і процесів.

Розкриємо зміст кожної з компетентностей.

Захист пристроїв і безпечне підключення до мережі Інтернет.

У закладі освіти тема цифрової (інформаційної) безпеки є актуальною у зв'язку із широким використанням завантажених на смартфони, планшети та комп'ютери різних застосунків (наприклад, ігри), які не завжди проходять перевірку в онлайн-магазинах. Відносно захисту пристроїв та цифрового контенту, розуміння ризиків та загроз у цифровому середовищі доцільно акцентувати увагу на особливій небезпеці тих застосунків, що завантажуються з Інтернету/торентів. Вони містять потенційні загрози і можуть розповсюджуватися через локальну мережу закладів освіти (університети), які мають, зазвичай, слабкий рівень безпекових налаштувань, саме тому можуть бути одним з місць розповсюдження шкідливого програмного забезпечення[49]. В Україні створений і працює Ситуаційний центр забезпечення кібербезпеки, що «моніторить події в режимі реального часу та дає змогу аналізувати стан інформаційної безпеки, щоб оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі»[50]. Потрібно зазначити, що, за даними Держслужби спеціального зв'язку та захисту інформації, упродовж 2022 року щотижня в Україні блокувалось у середньому до 50 тисяч кібератак на державні інформаційні ресурси.

Захист персональних даних і приватності безпеки в Інтернеті.

Для громадського сектору найбільш поширеними загрозами є: фішинг (один із методів соціальної інженерії, відомий як скам, або звичайне шахрайство в Інтернеті, який використовують здебільшого для наживи – виманювання грошей), а тому не рекомендується:

[49] Лахно, В., Каламан, Є., Ягалієва Б., Криворучко, О., Десітко, А., Цюцюра, С., & Цюцюра, М. (2022). Модель захисту локальної мережі навчального закладу серверної системи віртуалізації. *Кібербезпека: освіта, наука, техніка: електронне фахове наукове видання*. 2 (18), 6–23. DOI: https://doi.org/10.28925/2663-4023.2022.18.623

[50] Мальцева, І., Черниш, Ю., & Штонда, Р. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка:* електронне фахове наукове видання. 4 (16), 37–44. DOI: https://doi.org/10.28925/2663-4023.2022.16.3744

- користуватись одним паролем на різних сайтах (повторне використання паролів);
- скидати пароль на пошту, прив'язану до акаунта, оскільки може статися блокування акаунтів (збільшилось під час війни, коли користувачі розміщують чутливу інформацію про воєнні події, адже правила соцмереж не пристосовані до воєнного часу).

Найчастіше користувачі стикаються саме із *комерційними фішингами*.

Найбільш поширеними залишаються такі низькотехнологічні методи, як *фішинг* та *компроментація* ділової електронної пошти. Зазначимо, що одержані фішингові електронні листи не відрізняються від звичайних, які адресату надходять щодня від установ, організацій, керівників та довірених осіб. Шкідливе програмне забезпечення, що відкриває доступ до критично важливих мереж, завантажується при переході за посиланнями. Наведемо декілька прикладів рисунки 5-6.

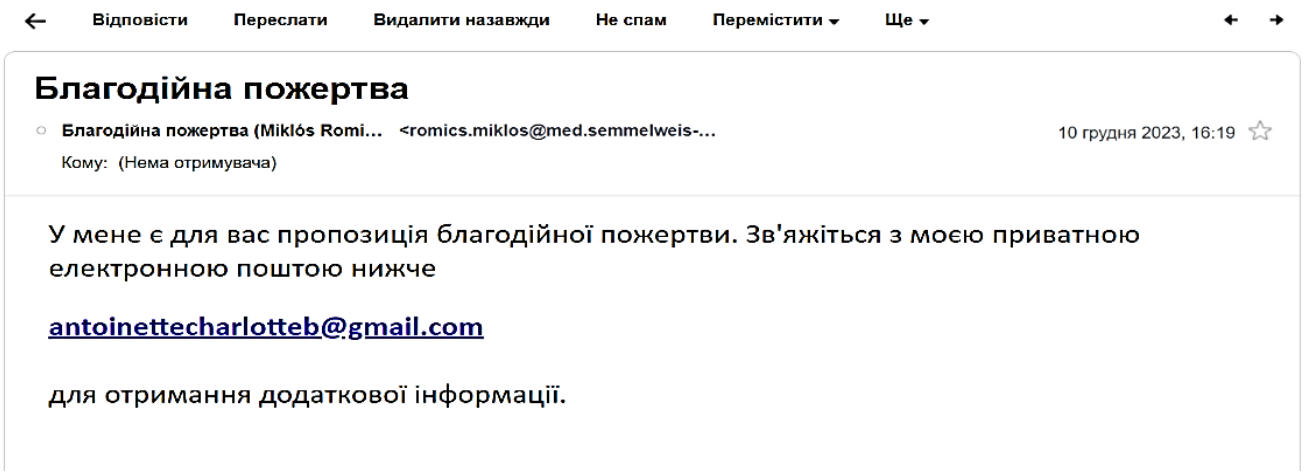


Рис. 5. Фішинг електронний лист із пропозицією благодійної пожертви

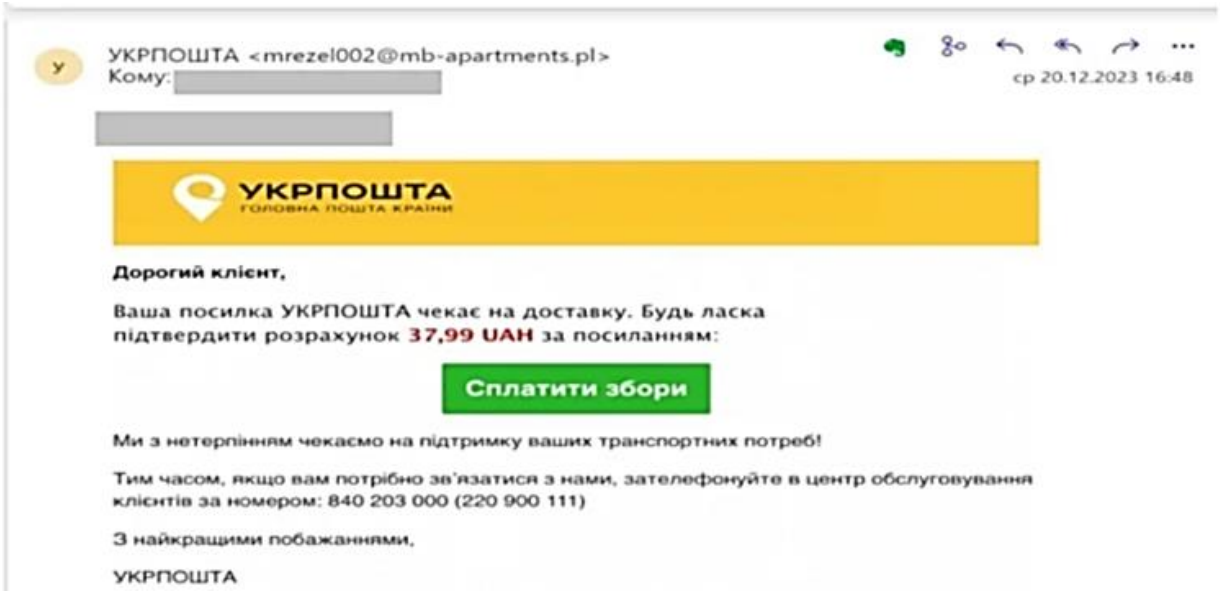


Рис. 6. Фішинг електронний лист про оплату з Укрпошти

На запит щодо розсилки таких листів є коментар керівництва відомого поштового оператора «Укрпошти»: «Такі повідомлення розсилаються шахраями, які використовують бренд компанії Укрпошта. Є висока ймовірність, що в такий спосіб ошуканці можуть незаконно отримати ваші персональні та фінансові дані: ПІБ, номери телефонів та номери карт і, як наслідок, незаконно заволодіти вашими особистими коштами».

Важливо! Якщо ви отримали подібне підозріле повідомлення – видаляйте його, не відкриваючи. Ні в якому разі не відповідайте на такі SMS-повідомлення та не переходьте за посиланням. Є великий ризик того, що ваш телефон буде зламано.

У випадку, якщо ви все ж таки ввели свої особисті дані та/або дані своїх платіжних пластикових карт на фішингових сайтах, радимо негайно звернутися до технічної підтримки вашого банку»[51].

Майбутнім викладачам закладів педагогічної вищої освіти варто взяти до уваги той факт, що такі хмарні сервіси, як Gmail та Office 365, не можуть адекватно захистити персональні конфіденційні дані. Тому виникає необхідність вживати додаткові заходи захисту електронної пошти. Для цього потрібно: використовувати тільки складні паролі; підтверджену авторизацію за допомогою мобільного телефону (двоетапна перевірка); не вказувати свою поштову адресу без необхідності; не використовувати сервіси для перевірки пошти на злом; обов'язково встановити на комп'ютері надійну антивірусну програму[52].

Щодо *захисту особистих прав споживача від шахрайства і зловживань в Інтернеті*, то, насамперед, потрібно уважно ознайомитися з інформацією на сайті Інтернет-магазину, яка має містити: повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи – підприємця; адресу підприємства або місце реєстрації та місце фактичного проживання ФОП; адресу електронної пошти; ідентифікаційний код для юридичної або фізичної особи – підприємця; якщо діяльність передбачає отримання ліцензії, то зазначити відомості про таку ліцензію, зокрема: серію, номер, строк дії та дату видачі; порядок формування кінцевої вартості товару щодо включення (не включення) певних податків у вартість товару; інформацію про вартість доставки. Такі дані мають бути і при розсиланні потенційним споживачам електронних повідомлень (емейл-розсилки) з комерційними пропозиціями для налагодження належної взаємодії, при необхідності[53].

О. Бондарєв зазначає, що всі «найбільш дієві види шахрайства будуються за одним і тим же принципом, починаючись з того, що вам роблять дуже важливу послугу в умінні захищати пристрої та цифровий контент, розумінні ризиків та загроз у цифровому середовищі; знання про заходи безпеки та захисту, враховуючи при цьому питання надійності й приватності, –

[51] Суспільний кореспондент. (2023, 25 грудня) Шахраї розсилають листи від Укрпошти. URL: https://www.sknews.net/shakhrai-rozsylaiut-lysty-vid-ukrposhty/

[52] Комп'ютерна допомога. URL: http://surl.li/oxkpwl

[53] Безоплатна правова допомога. (Б. р.). URL: http://surl.li/oxkqn

привабливу пропозицію. Найчастіше – це отримати безкоштовно те, що коштує значних грошей»[54]. Наприклад, чудодійні ліки, нігерійські листи щастя, онлайн-продажі (це може бути портал онлайн-оголошень OLX), фішинг, підроблена банківська карта, допомога другові, робота вдома, підроблений вірус).

А. Апетик та І. Купчинська наголошують, що цифрова безпека стосується кожного, оскільки активність українських громадян в інформаційному просторі зростає щомісячно, а розвиток національної системи автоматизованого інформаційного комплексу освітнього менеджменту, який активно формується з використанням різних онлайн-інструментів, зумовлює необхідність вивчення питання створення безпекового цифрового середовища[55].

З початком повномасштабної війни в Україні ця проблема набула ще більшої значущості: жертвами шахраїв з початку повномасштабного вторгнення стали 11% українців. Найчастіше – це потерпілі від купівлі чи продажу товарів в інтернеті[56]. Пам'ятаємо, що «Кожен і кожна є бійцем інформаційного фронту сьогодні»[57].

Розглядаючи зміст цифрової безпеки як складника цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти, вважаємо за необхідне звернути увагу на дотримання певних *рекомендацій*, аби не стати жертвою шахрайства в мережі:

1) стежити за тим, щоб ваші особисті дані не були у відкритому доступі;

2) періодично змінювати ПІН-код банківської картки;

3) користуватися банківською карткою з чіпом;

4) перевіряти продавця, для чого промоніторити його мобільний в мережі;

5) завжди ігнорувати дзвінки і SMS з проханням зателефонувати на якийсь номер або оплатити відправку вашого виграшу;

6) здійснювати платежі в Інтернеті тільки через авторитетні сайти;

7) ніколи не вводьте дані своєї карти, якщо надійшов такий запит після оновлення на смартфоні[58].

8) не вкладайте власні гроші за роботу в інтернеті та не сплачуйте жодних послуг, щоб працевлаштуватися.[59]

---

[54] Бондарєв, О. (2015). Кидали-онлайн. Названо найбільш поширені способи інтернет-шахрайства. URL: https://techno.nv.ua/ukr/gadgets/kidali-onlajn-nazvano-najbilsh-poshireni-sposobi-internet-shahrajstva75741.htm

[55] Петренко, Л. М. (2023). Цифрова безпека у професійній діяльності майбутнього викладача педагогічної *освіти. Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій: матеріали ІІІ Всеукраїнської науково-практичної конференції, 291-294.* Глухів: Глухівський НПУ ім. О. Довженка. URL: https://lib.iitta.gov.ua/735042/

[56] Віноградова, У. (2023, 25 грудня). *Варто бути обережним – українцям розповіли про популярну схему шахраїв.* Новини.LIVE. URL: https://news.novyny.live/varto-buti-oberezhnimi-ukrayintsiam-rozpovili-pro-populiarnu-skhemu-shakhrayiv-140424.html

[57] Апетик, А., Купчинська, І. (2022, 29 серпня). *Як захистити себе онлайн? Поради від експертки з цифрової безпеки.* UNDP. URL: https://www.undp.org/uk/ukraine/blog/yak-zakhystyty-sebe-onlayn-porady-vid-ekspertky-z-tsyfrovoyi-bezpeky

[58] Безоплатна правова допомога. (Б. р.). URL: http://surl.li/oxkqn

[59] Віноградова, У. (2023, 25 грудня). *Варто бути обережним – українцям розповіли про популярну схему шахраїв.* Новини.LIVE. URL: https://news.novyny.live/varto-buti-oberezhnimi-ukrayintsiam-rozpovili-pro-populiarnu-skhemu-shakhrayiv-140424.html

На наш погляд, важливо акцентувати увагу на дефініції «особисті (персональні) дані» в контексті цифрової безпеки[60]:

Особисті (персональні) дані – це вся та інформація, що може конкретно ідентифікувати особу: повне ім’я, номер телефону, адреса електронної пошти та проживання, номер і марка автомобіля, номер банківського рахунку, банківської картки і строк її дії, інформація про особисті доходи, про членів сім'ї, фото, біометричні дані, ідентифікаційний код, підпис, історія хвороб, дані про групу крові та національність, політичні або релігійні погляди і сексуальну орієнтацію; інформація про місце перебування, IP-адреса та онлайн-ідентифікатор.

Важливими навичками й уміннями у змісті компетентності з цифрової безпеки є *захист здоров’я та благополуччя в процесі роботи з комп’ютером (смартфоном).* На жаль, в освітньо-інформаційному середовищі вищої освіти це питання дуже рідко порушується. Проте можливості і блага, які отримало людство в зв’язку з безперервним доступом до інформації межує з неусвідомлюваними до кінця ризиками для здоров’я як окремих представників суспільства, так і громадського здоров’я суспільства в цілому. Оскільки уникнути впливу цифровізації на суспільне здоров'я неможливо, адже «технологічний прогрес задає параметри соціальної реальності, змушуючи людину адаптуватися до нових умов, насамперед, до тотальної комп'ютеризації, до перенесення соціальної комунікації у віртуальне середовище, до появи нових культурних практик»[61], то виникає необхідність вивчення впливу цього явища на здоров’я людини, окремих професійних спільнот.

Ученими зроблено перші узагальнення відносно впливу цифрового середовища на людську психіку. Це виникнення:

психічних розладів унаслідок активного використання цифрових пристроїв;

негативного впливу на когнітивний, вербальний і соціально-емоційний розвиток дитячої вікової групи;

когнітивних порушень у дорослих – синдрому розсіяної уваги, хронічного стресу та втоми;

інформаційної «перевантаженості» людини, що виявляється у її нездатності цілісно сприймати та аналізувати інформацію, вибудовувати логічні зв'язки між окремими фактами та приходити до аргументованих висновків;

---

[60] Апетик, А., Купчинська, І. (2022, 29 серпня). *Як захистити себе онлайн? Поради від експертки з цифрової безпеки.* UNDP. URL: https://www.undp.org/uk/ukraine/blog/yak-zakhystyty-sebe-onlayn-porady-vid-ekspertky-z-tsyfrovoyi-bezpeky

[61] Пуліч, О. А. & Москальов, М. В. (2023). Стрес і перевантаження від постійного з'єднання з інтернетом та технологіями. *Професійний розвиток в умовах цифровізації суспільства: сучасні тренди*: тези доповідей IV науково-практичної конференції з нагоди 70-річчя заснування Університету менеджменту освіти. Київ: ДЗВО «Університет менеджменту освіти». URL: http://surl.li/pqubm

синдрому розсіяної уваги, що не дозволяє людині сконцентруватися на необхідній інформації, «розпорошуючи» її увагу;

номофобії – побоювання втратити важливу особисту/виробничу інформацію (дані контактів, фото, відео тощо), острах опинитися навіть на короткий час в інформаційному вакуумі (пропустити актуальну інформацію в режимі реального часу); страх повної ізоляції (самотності)[62].

Також серед загроз здоров'ю викладача виокремлюють: наслідки електромагнітного випромінювання; проблеми із зором; проблеми із м'язами і суглобами. Існує прямопропорційна залежність ступеня ризику від того часу, який фахівець проводить за комп'ютером. Окрім цього, в людини розвивається гіподинамія, з'являється швидке втомлення, дратівливість. Від постійної напруги погіршується зір, а під час тривалої роботи за комп'ютером втрачається концентрація уваги. Кисті рук знаходяться в постійній напрузі, оскільки здійснюються однотипні рухи, що призводить до стійкого стомлення м'язів рук і виникає біль у суглобах, порушення кровообігу. Під час тривалої роботи за комп'ютером посилюється навантаження на шийний відділ хребта, від чого порушується кровопостачання мозку і з'являється ймовірність кисневого голодування, що проявляється в головних болях[63].

Профспілка працівників освіти і науки України розробила 6 правил роботи з комп'ютером, які представлено на рис. 7. Фахівці наголошують на основній пораді – слухати своє тіло, відпочивати, коли втомилися, прислухатися до потреб організму, і він вам віддячить гарним почуттям і добрим здоров'ям[64].

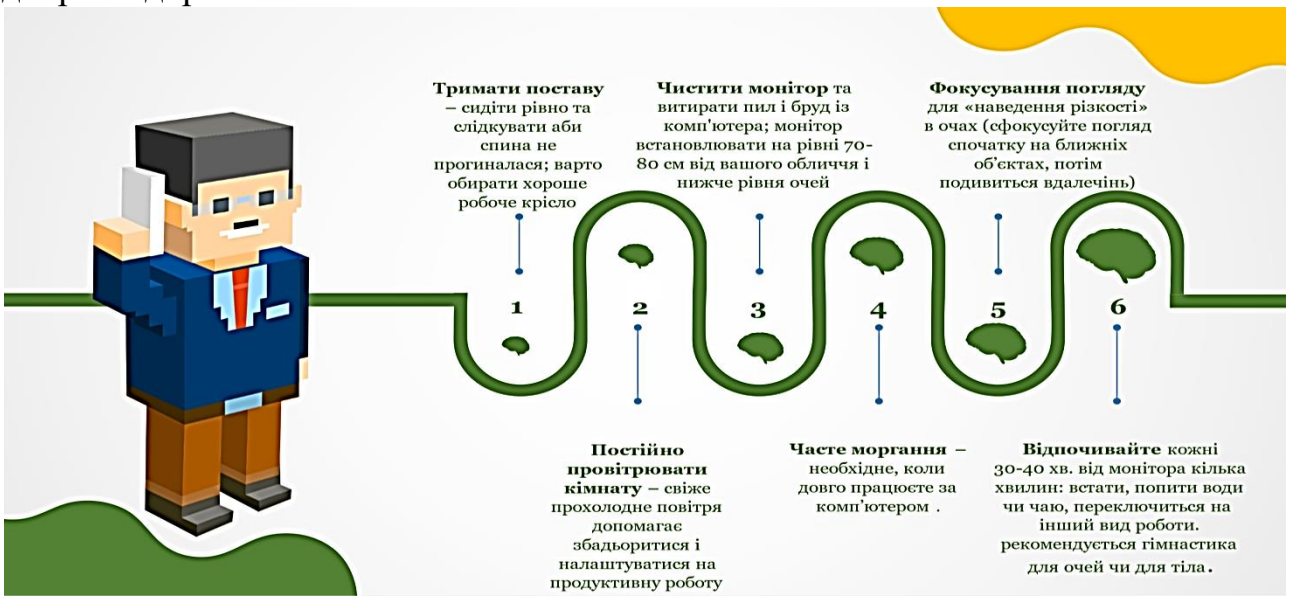


Рис. 7. Правила роботи за комп'ютером

[62] Пуліч, О. А. & Москальов, М. В. (2023). Стрес і перевантаження від постійного з'єднання з інтернетом та технологіями. *Професійний розвиток в умовах цифровізації суспільства: сучасні тренди*: тези доповідей IV науково-практичної конференції з нагоди 70-річчя заснування Університету менеджменту освіти. Київ: ДЗВО «Університет менеджменту освіти». URL: http://surl.li/pqubm

[63] Інтернет. Шкода здоров'ю. URL: http://surl.li/oxlum

[64] Профспілка працівників освіти і науки України. (2017, 5 вересня). *6 правил роботи за комп'ютером без шкоди для здоров'я.* URL: http://surl.li/bnegy

Ще одним складником компетентності з цифрової безпеки визначають *захист навколишнього середовища*. У вільному тлумачному словнику наведено декілька дефініцій, пов'язаних із поняттям «довкілля»:

1) навколишнє середовище у відношенні до особи чи групи осіб, які в ньому перебувають;

2) природне навколишнє середовище, сукупність усіх живих і неживих об'єктів, що зустрічаються в певному регіоні без впливу людини;

3) оточуючі люди щодо особи[65].

У контексті нашого дослідження під навколишнім середовищем доцільно розуміти перший варіант трактування зазначеного поняття як «право на безпечне для життя і здоров'я довкілля», визначення якому найбільш широко наведено у ст. 293 Цивільного кодексу України: «довкілля – це все, з чим стикається людина в процесі свого існування: природне середовище, предмети використання та вжитку, умови повсякденного існування тощо». У поточній редакції ст. 293 «Право на безпечне для життя і здоров'я довкілля» сформульована в такому трактуванні: «Фізична особа має право на безпечне для життя і здоров'я довкілля, право на достовірну інформацію про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її збирання та поширення… Фізична особа має право на належні, безпечні і здорові умови праці, проживання, навчання тощо»[66]. В Академічному тлумачному словнику окремо наведено визначення слів «середовище» та «живильне середовище». Суть слова «середовище» трактується як «речовина, тіла, що заповнюють який-небудь простір і мають певні властивості; сфера», а суть живильного середовища має такі тлумачення: сукупність природних умов, у яких проходить життєдіяльність якого-небудь організму; соціально-побутові умови, в яких проходить життя людини; оточення; сукупність людей, зв'язаних спільністю життєвих умов, занять, інтересів і т. ін.[67]. Отже, результати аналізу словникової літератури уможливлюють висновок, що під поняттям «навколишнє середовище» в контексті цифрової безпеки майбутнього викладача педагогічного закладу вищої освіти необхідно розуміти:

1) навколишнє середовище у відношенні до особи чи групи осіб, які в ньому перебувають;

2) соціально-побутові умови, в яких проходить життя людини;

3) оточення;

4) сукупність людей, зв'язаних спільністю життєвих умов, занять, інтересів. Право на належні, безпечні і здорові умови праці, проживання, навчання їм забезпечується законодавством України.

---

[65] Вільний тлумачний словник. Новітній онлайновий словник української мови. 2013-2018. URL: http://sum.in.ua/f/dovkillja

[66] Кодекс України «Кодекс цивільного захисту України» від 02.10.2012 р. № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17

[67] Словник української мови. Академічний тлумачний словник (1970-1980). URL: http://sum.in.ua/s/seredovyshhe/

Ґрунтуючись на цьому тлумаченні, розглянемо основні рекомендації експертів щодо захисту навколишнього середовища. У процесі вивчення зазначеного питання ми виходили з розуміння захисту навколишнього середовища сукупності людей, зв'язаних спільністю життєвих умов, занять, інтересів у контексті цифровізації. Для закладу педагогічної вищої освіти навколишнім середовищем може бути кафедра, аудиторія, лабораторія або будь-яке інше приміщення, в якому працюють фахівці або навчаються студенти. Нині ці приміщення мають приладдя, які забезпечують використання інформаційних технологій в освітньому процесі, в організації діяльності педагогічного і науково-педагогічного колективу, а саме: комп'ютери, принтери, багатофункціональні пристрої, інтерактивні дошки тощо; матеріали – папір, тонер та ін., функціонування яких впливає на навколишнє середовище. Тому необхідно звертати увагу на їх технічні характеристики, від чого залежить екостійкість навколишнього середовища[68]. На жаль, у сучасних закладах вищої освіти увага цим питанням цифрової безпеки майже зовсім не приділяється. Більше того, деякі кафедри та інші приміщення, в яких працюють викладачі, іноді перетворюються у складські приміщення, в яких зберігається непрацююча техніка в очікуванні її списання.

Підсумовуючи сказане, зазначимо, що заявленій проблемі в галузі знань 01 Освіта/Педагогіка приділяється, на жаль, недостатньо уваги. У наявних дисертаційних дослідженнях висвітлено результати вивчення питання професійної підготовки майбутніх фахівців інформаційної безпеки до захисту інформації. Публікації, що знаходяться у відкритому доступі, відображають загальні питання формування цифрової компетентності у майбутніх учителів. З'ясовано, що добір і обґрунтування змістового компонента компетентності з цифрової безпеки як складника цифрової компетентності майбутніх викладачів педагогічної вищої освіти залишається поза увагою вітчизняних учених. Встановлено, що, відповідно до Рамки цифрової компетентності для громадян України, структуру компетентності з цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти складає комплекс компетентностей: захист пристроїв і безпечне підключення до мережі Інтернет; захист персональних даних і приватності, безпека в Інтернеті; захист особистих прав споживача від шахрайства і зловживань[69]; захист здоров'я та благополуччя; захист навколишнього середовища. На основі вивчення результатів наукових досліджень, експертних оцінок визнаних експертів з проблем цифрової безпеки та практичного досвіду визначено й обґрунтовано зміст кожної окремої компетентності.

[68] Створення екостійкого офісу. Xerox. URL: https://www.xerox.com/uk-ua/about/ehs/green-office

[69] Петренко, Л. (2023). Цифрова безпека в стуктурі цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти: змістовий компонент. *Освіта дорослих: теорія, досвід, перспективи*. 23(1), 98-109. DOI: https://doi.org/10.35387/od.1(23).2023.98-109

РЕЗУЛЬТАТИ ДІАГНОСТУВАННЯ РІВНІВ ВОЛОДІННЯ КОМПЕТЕНТНОСТЯМИ З ЦИФРОВОЇ БЕЗПЕКИ СТУДЕНТАМИ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Результати опитування студентів та викладачів закладів вищої освіти щодо дотримання ними умов цифрової безпеки висвітлено в публікаціях М. Прокоф'євої і Л. Султанової[70] та запропоновано шляхи їх вирішення. Ними також здійснено фрагментарний аналіз основних документів, які регламентують формування навичок цифрової безпеки у громадян України.

Ураховуючи масштаби та рівень проблеми інформаційної безпеки в освіті, варто звернути особливу увагу на формування медіакомпетентності, розвиток критичного мислення, цифрової обізнаності та доброчесності в процесі здобуття вищої освіти. Йдеться про так звану «fake-free-освіту», тобто сучасну цифрову освіту, яка базується на принципах визнання знань найвищою цінністю суспільства, доброчесності та критичного мислення[71].

Основою такої освіти є вміння розпізнавати фейкові освітні ресурси. Однак це стає майже неможливим для пересічного користувача Інтернету чи здобувача вищої освіти. Фейкова інформація – це наслідок, а причина – низький рівень ерудиції, критичного мислення та медіакомпетентності. Отже, метою fake-free-освіти є протидія поширенню фейкової інформації на макрорівні та розвитку вмінь критичного відбору інформації на мікрорівні, а також у формуванні світогляду з орієнтацією на цінність достовірної інформації в процесі здобуття вищої освіти.

З метою визначення рівня медіаграмотності та академічної доброчесності здобувачів вищої освіти та викладачів закладів вищої освіти у сфері цифрової безпеки М. Прокоф'євою та Л. Султановою було розроблено опитувальник. Опитування здійснюється в рамках реалізації проєкту «Fake-free-освіта» громадської організації «Українська асоціація дослідників освіти».

Опитувальник складався з трьох розділів, кожен з яких містив 6 запитань.

Розділ І. Інформація про респондента.

Розділ ІІ. Медіаграмотність.

Розділ ІІІ. Академічна доброчесність.

В опитуванні взяли участь 361 респондент. З них 59% – студенти закладів вищої освіти, 41% – викладачі. Опитуванням було охоплено респондентів з міста Києва (37,7%), Івано-Франківської області (23,5%), Дніпропетровської області (10,5%), Хмельницької області (7,2%), Запорізької області (6,1%), а також інших (18) областей України (рис. 8).

[70] Султанова, Л. & Прокоф'єва, М. (2022). Цифрова безпека в галузі вищої освіти. *Освіта дорослих: теорія, досвід, перспективи.* 21 (1), 106- 117. DOI: https://doi.org/10.35387/od.1(21).2022.106-117.

[71] Султанова, Л.Ю. & Прокоф'єва, М. (2022). *Цифрова безпека в галузі вищої освіти: аналітичні матеріали*. Кропивницький: Імекс-ЛТД.

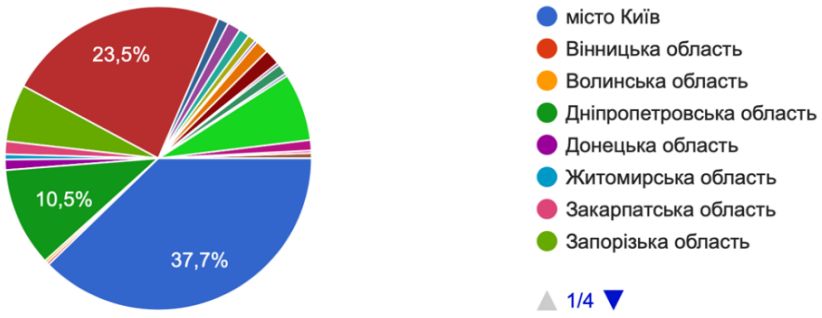


Рис. 8. Регіон навчання або роботи (n=361)

Більше половини респондентів (51,5%) становила вікова категорія від 18 до 30 років. Переважна більшість респондентів (89,5%) – це жінки. Значна частина респондентів (66,9%) за своєю спеціальністю належала до галузі освіти, зокрема гуманітарних наук.

Аналіз результатів діагностування.

Із запропонованих запитань найскладнішим виявилось запитання про те, в якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації? На це запитання більшість респондентів (майже 60%) дали неправильну відповідь.

За результатами опитування виявлено, що більшість респондентів знає, як діяти в ситуації погроз у соціальних мережах (96,7%); який пароль є надійним для власного акаунту (92,8%); що таке фішинг (82%). Однак значна частина респондентів не розуміє, де і як краще зберігати паролі (51,2%), а також плутається у поняттях «фішинг», «спамінг» та «тролінг» (біля 27%) (рис. 9).

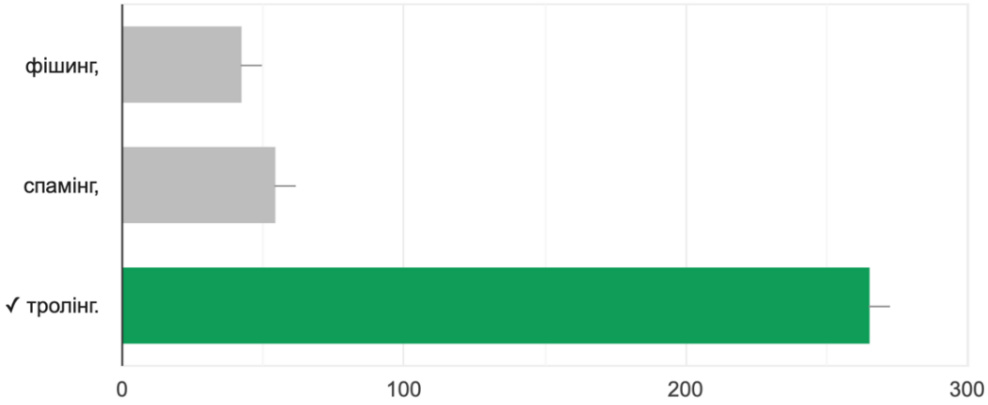


Рис. 9. Диференціація розуміння понять «фішинг», «спамінг» та «тролінг» у відповідях респондентів (n=361)

Щодо запитань, пов’язаних з академічною доброчесністю, то результати аналізу відповідей показали, що респонденти є досить обізнаними. Переважна більшість (91,1%) розуміє різницю між авторським правом, академічною доброчесністю й інтелектуальною власністю. А також знає, що надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації не є різновидом академічного плагіату (85,3% правильних відповідей). Практично

всі респонденти (95,6%) знають, що дотримання академічної доброчесності учасниками освітнього процесу передбачає самостійне виконання навчальних завдань поточного та підсумкового контролю.

Дещо складнішою виявилася диференціація понять: «плагіат», «фабрикація» та «фальсифікація». Розрізняють ці поняття лише 57,1% респондентів (рис. 10). Також майже 40% респондентів не знають, які наслідки має порушення академічної доброчесності.

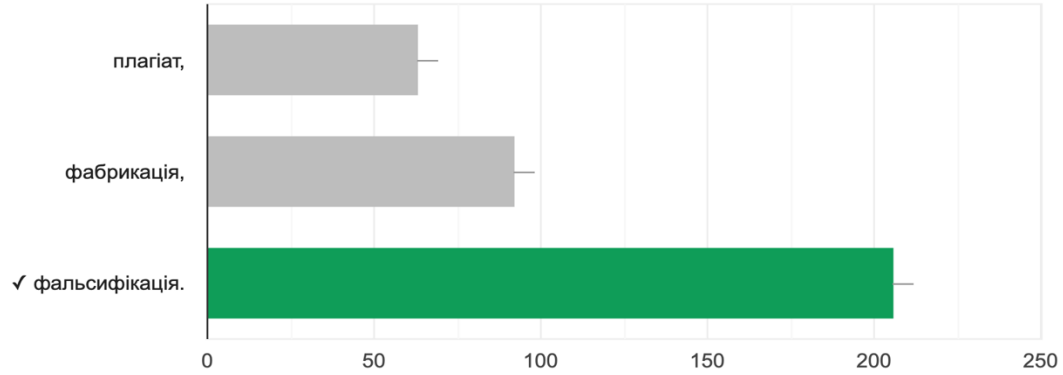


Рис. 10. Диференціація відповідей респондентів у розумінні понять: «плагіат», «фабрикація» та «фальсифікація» (n=361).

Анкетування готовності майбутніх викладачів закладів вищої педагогічної освіти до професійної діяльності в умовах цифровізації суспільства здійснювалось на початку 2023 року з використанням кількісного методу дослідження – онлайн-опитування, для якого було розроблено і запропоновано п’ять онлайн-анкет, створених за допомогою GoogleForms. Анкети розроблялись на основі Опису рамки цифрової компетентності для педагогів України. Запитання онлайн-анкети були відкритими, з варіантами відповідей, що дали можливість визначити рівень компонентного складу готовності, на основі яких визначався загальний рівень готовності майбутніх викладачів закладів вищої педагогічної освіти.

Анкета складалась із п’яти розділів:

Розвиток цифрової компетентності учнів:

- інформаційна та медіаграмотність;
- відповідальне використання цифрових технологій та сервісів;
- розв'язання проблем за допомогою цифрових технологій та сервісів.

Навчання та оцінювання учнів:

- організація та управління освітнім процесом учнів;
- інтерактивне та активне навчання учнів. Організація співпраці учнів;
- індивідуалізація навчання та диференціація;
- інклюзивне навчання;
- Аналіз та інтерпретація цифрових даних. Забезпечення зворотного зв'язку й оцінювання учнів. Організація самоконтролю учнів.

Використання та аналіз цифрових ресурсів:

- добір цифрових ресурсів;
- створення та модифікація цифрових освітніх ресурсів;
- управління та спільне використання цифрових освітніх ресурсів;
- захист цифрових ресурсів.

Професійний розвиток:

- професійна комунікація;
- професійна співпраця;
- рефлексія розвитку цифрової компетентності;
- безперервний професійний розвиток.

Учитель у цифровому суспільстві:

- цифрове суспільство;
- електронне урядування;
- електронна школа;
- електронне навчання;
- безпека в цифровому суспільстві.

Для проведення онлайн-анкетування використано простий випадковий відбір – відбір одиниць у вибіркову сукупність, під час якого, ще до його здійснення, кожна одиниця основи вибірки має визначену, заздалегідь задану (однакову) імовірність бути включеною до вибірки. Заповнення онлайн-форми анкети відбувалось за власним бажанням.

В анкетуванні взяли участь 64 магістри – майбутні викладачі закладів вищої педагогічної освіти із 4-ох закладів вищої педагогічної освіти та з 8-и закладів вищої освіти різних регіонів: 90,6% (58 осіб) здобувачів вищої освіти за другим (магістри) і першим (бакалаври) рівнями.

У контексті теми підготовки викладачів закладу вищої педагогічної освіти до цифрової безпеки у повоєнний час варто звернути увагу на результати опитування щодо рівнів сформованості компетентності «безпека у цифровому суспільстві». У цій частині анкети сформульовано три запитання із запропонованими відповідями:

У якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації?

У соціальній мережі ви отримали погрози від якогось користувача. Якими будуть ваші дії у відповідь?

Олена Сергіївна Іванова викладає математику та хоче використовувати надійний пароль до власного акаунту. Який із наведених паролів є надійнішим для неї?

Аналіз отриманих результатів опитування показав, що 34,4% респондентів знають, у якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації (рис. 11).

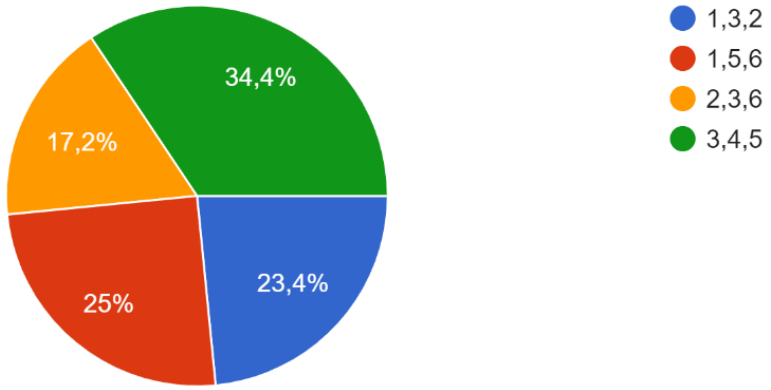


Рис. 11. Використання резервних способів підтвердження під час подвійної автентифікації (n = 64).

Розуміння правильних дій у соціальній мережі у відповідь на отримані погрози від якогось користувача має переважна більшість опитуваних – 84,4% (рис. 12).

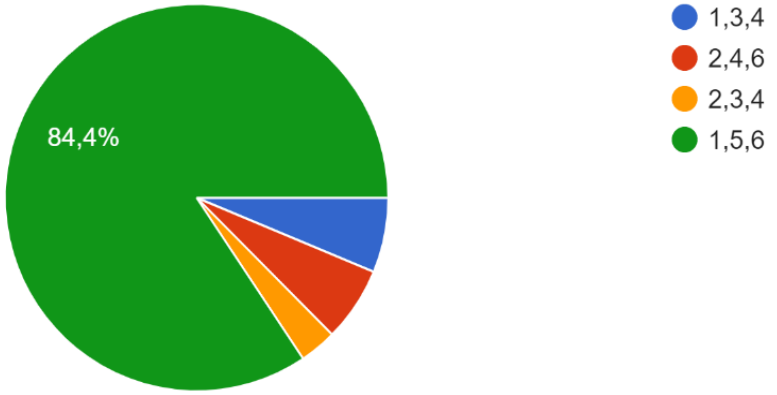


Рис. 12. Дії у соціальній мережі у відповідь на отримані погрози (n = 64).

Думки респондентів відносно найнадійніших паролів майже співпадають – 85,9% і вказують на варіант 3. B&h28Pz# (рис. 13).

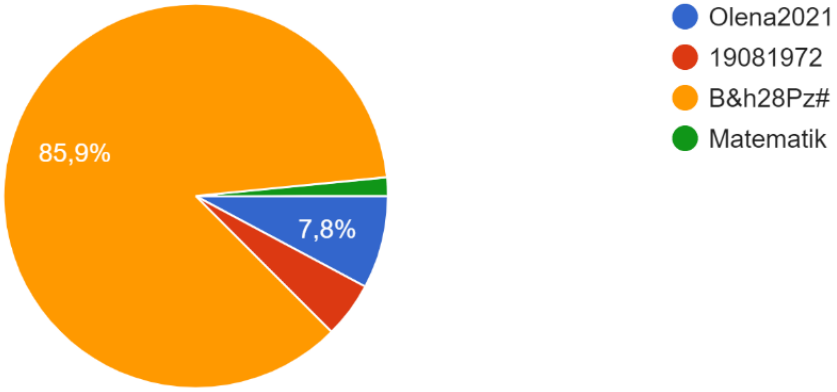


Рис. 13. Найнадійніші паролі до власного акаунту (n = 64).

Компетентність «Безпека у цифровому суспільстві» є складовою компетентності «Учитель у цифровому суспільстві». Рівень її сформованості визначався за трьома критеріями (вони визначаються як компетенції у «Цифрограм»): використання резервних способів підтвердження під час подвійної автентифікації; дії у соціальній мережі у відповідь на отримані погрози; найнадійніші паролі до власного акаунту (табл. 1). Критеріально-рівнева характеристика подана вище. Для зручності обчислення рівнів сформованості компетентності з цифрової безпеки використано числове визначення критеріїв:

Критерії оцінювання мають визначення:

$0{,}10 < K_{ц.к.} \leq 0{,}50$ – низький рівень;

$0{,}50 < K_{ц.к.} \leq 0{,}75$ – середній рівень;

$0{,}75 < K_{ц.к.} \leq 1{,}00$ – високий рівень.

Таблиця 1

Результати діагностики рівнів сформованості компетентності з цифрової безпеки у майбутніх викладачів закладів вищої педагогічної освіти на початку конструктивно-емпіричного етапу науково-дослідної роботи (n = 64, %)

Назва компетентності/ компетенції	Рівні						Примітки
	Високий		Середній		Низький		
	Абс.	%	Абс.	%	Абс.	%	
Здатність до використання резервних способів підтвердження під час подвійної автентифікації	-	-	-	-	22	34,4	
Здатність до застосування дій у соціальній мережі у відповідь на отримані погрози	54	84,4	-	-	-	-	
Здатність до використання найнадійніших паролів до власного акаунту	55	85,9	-	-	-	-	

Аналіз отриманих даних показав, респонденти демонструють високий рівень сформованості тих компетенцій, які вони застосовують у своїй повсякденній життєдіяльності, тобто ті, що сьогодні їх можна віднести до функціональної грамотності (дії у соціальній мережі у відповідь на отримані погрози; найнадійніші паролі до власного акаунту). Принагідно звернемо увагу на те, що зазначене поняття почало розроблятися ЮНЕСКО з 1957 року, а в 1965 р. дефініція «функціональна грамотність» було закріплено Конгресом міністрів просвіти з питань викорінення безграмотності, коли вперше розвели поняття «грамотність» і «функціональна грамотність». Цей концепт тлумачився як форма підготовки людини до виконання нею соціальної, громадянської та економічної ролі в суспільстві (1978 р.) і визнавався важливим для

особистісного зростання і розвитку соціуму[72]. Аналіз наукового доробку вказує на багатоаспектність дослідження функціональної грамотності у представників різних професій, школярів, студентів. При цьому слід зауважити, що визначення суті цього поняття залежить від контексту його вивчення: розвитку інформаційного суспільства, безперервної освіти, акмеології, нової грамотності, дослідження компетенції тощо[73].

Водночас більше ніж третина опитуваних показали низький рівень сформованості компетенції «Здатність до використання резервних способів підтвердження під час подвійної автентифікації», яку сьогодні слід віднести до професійної компетентності майбутнього викладача. Адже основними засобами навчання в закладах вищої освіти в сучасних умовах є цифрові.

Таким чином, проведене опитування дало можливість з'ясувати необхідність розвитку цифрової компетентності як викладачів, так і студентів закладів вищої освіти. Наразі освітній процес у закладах вищої освіти більшою мірою зорієнтований на фундаментальну фахову підготовку. Однак сучасні виклики потребують від здобувачів освіти інформаційно-технологічної готовності виконувати свої професійні функції. Насамперед, це: знання інформаційних і цифрових засобів, технологій та вміння їх використовувати; вміння збирати, оцінювати і використовувати інформацію; пристосовуватися до нових умов праці (здатність до адаптивності); усвідомлення необхідності самоосвіти і потреба в регулярному підвищенні кваліфікації тощо).

Для цього доречними є посилення цифрової складової освіти (спецкурси з медіаграмотності, фактчекінгу, розвиток критичного мислення, консультації ІТ-фахівців, створення міждисциплінарних курсів на основі цифрових навчальних платформ) тощо. Освітній процес необхідно спланувати таким чином, щоб у результаті здобувачі вищої освіти могли захистити свої пристрої та безпечно підключалися до мережі Інтернет, тобто йдеться про низький рівень сформованості компетентності з цифрової безпеки: здатність визначити прості способи захисту своїх пристроїв та цифрового контенту; диференціювати прості ризики та загрози в цифрових середовищах; вибрати прості заходи безпеки та гарантії; визначити прості способи належного врахування надійності та конфіденційності; обирати прості способи захисту своїх приладів та цифрового контенту; дотримуватися простих заходів безпеки.

На середньому рівні сформованості компетентності з цифрової безпеки – передбачається можливість самостійно вказати чітко визначені і рутинні способи захисту своїх пристроїв та цифрового контенту; диференціювати чітко визначені і рутинні ризики та загрози в цифрових середовищах; обрати чітко визначені і рутинні заходи безпеки та гарантії; вказати чітко визначені і рутинні способи належного врахування надійності та

[72] UNESCO. (1978). *Revised Recommendation concerning the International Standardization of Educational Statistics.* In: General Conference of UNESCO. Paris: UNESCO. Дата звернення: 08.04.2020. URL: http://portal.unesco.org/en/ev.phpURL_ID=13136&URL_DO=DO_TOPIC&URL_ SECTION=201.html

[73] Петренко, Л. М. (2020). Функціональна грамотність у контексті трансформації професійного розвитку фахівців. *Актуальні проблеми технологічної і професійної освіти*: тези доповідей ІІ міжнародної науково-практичної конференції, 56-58. Глухів: Глухівський НПУ ім. О. Довженка.

конфіденційності; вирішити чітко визначені і нестандартні проблеми, організувати способи захисту своїх пристроїв та цифрового контенту.

Високий рівень сформованості компетентності з цифрової безпеки передбачає можливість, окрім допомоги іншим, застосовувати різні способи захисту своїх пристроїв та цифрового контенту; диференціювати низку ризиків та загроз у цифрових середовищах; застосовувати заходи безпеки та гарантії; використовувати різні способи належного врахування надійності та конфіденційності. А також у складних контекстах, відповідно до власних потреб та потреб інших людей, можливість вибрати найбільш відповідний захист пристроїв та цифрового контенту; дискримінувати ризики та загрози в цифрових середовищах; вибрати найбільш відповідні заходи безпеки та гарантії; оцінити найоптимальніші способи належного врахування надійності та конфіденційності.

Отже, розвиток інформаційного суспільства, яке характеризується розвиненими інфраструктурами, високим рівнем інформаційних технологій, наявністю інформаційних ресурсів і можливостей доступу до інформації, зумовлює зміну парадигми освіти. Завдяки інформаційним технологіям уможливлюється створення освітніх спільнот, до яких долучаються як студенти, так і викладачі, а також фахівці обраної сфери діяльності – професійної спільноти. Така співпраця забезпечує доступ до освітніх матеріалів і необхідних ресурсів. Зважаючи на викладене вище, постає потреба в розробці та впровадженні методик нового покоління у процес підготовки майбутніх викладачів закладів вищої педагогічної освіти.

ПРОГНОЗУВАННЯ ПІДГОТОВКИ ВИКЛАДАЧІВ ЗАКЛАДІВ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ ДО ЦИФРОВОЇ БЕЗПЕКИ У ПОВОЄННИЙ ЧАС

Прогнозування соціальних процесів, зокрема розвитку вищої освіти, є важливим етапом в її реформуванні і формуванні стратегії, а також являється складовою у розробленні стратегічних планів соціально-економічного розвитку держави, регіонів і громад. Нині існує багато обґрунтованих у науковій літературі моделей і методів прогнозування розвитку освітньої політики, однак в умовах турбулентності, що характеризує сучасний період розвитку України, вони потребують суттєвого коригування. Водночас не виключено, що воєнні події, які розгорнулись на теренах української держави, знову-таки потребуватимуть коригування цих прогнозів, тому що ситуація невизначеності притаманна кожній миті сьогодення.

З огляду на існуючі методичні підходи щодо прогнозування соціально-економічного розвитку України на середньостроковий період (5 років), правовими основами прогнозування є законодавча база, яка включає:

– Закон України «Про державне прогнозування та розроблення програм економічного і соціального розвитку України»;
– Закон України «Про Національний банк України»;
– Закон України «Про державні цільові програми»;
– Закон України «Про стимулювання розвитку регіонів»;
– Закон України «Про наукову і науково-технічну діяльність»[74].

Основоположні принципи Стратегії розвитку вищої освіти (2022р.)[75], План Відновлення України (2022 р.)[76], спрямований на прискорення стійкого економічного зростання, узгоджені з такими програмними документами:

Цілі сталого розвитку України на період до 2030 року (ціль 4 щодо забезпечення всеохоплюючої і справедливої якісної освіти та заохочення можливості навчання впродовж усього життя для всіх);

Стратегія людського розвитку (за напрямом 20 «Якість життя);

Національна економічна стратегія до 2030 року;

Стратегія розвитку медичної освіти в Україні;

Пріоритетні напрями та завдання (проєкти) цифрової трансформації на період до 2023 року.

З першими формулюваннями перспектив розвитку системи освіти України після повномасштабного вторгнення російської армії можна ознайомитись в інформаційно-аналітичному збірнику[77], які потім були доопрацьовані і покладені в основу низки Національних програм з розвитку освіти[78]. Зокрема у системі вищої освіти виокремлено цілі, спрямовані на поетапне вирішення низки таких проблем:

неефективне використання ресурсів у системах вищої і фахової передвищої освіти;

несистемне сприйняття, недовіра до інституційних механізмів забезпечення якості вищої освіти;

низький рівень доступності вищої освіти для окремих верств населення;

низький рівень інтеграції вищої освіти в сучасні глобалізаційні процеси;

низький рівень привабливості закладів вищої освіти для навчання та академічної кар'єри;

втрати людського потенціалу (викладачі, науковці, потенційні вступники) та руйнування інфраструктури фахової передвищої і вищої освіти України під час воєнного стану.

---

[74] Завгородній, К. В. (2023). Прогнозування в системі управління національною економікою. *Ефективна економіка*. 3. DOI: http://doi.org/10.32702/2307-2105.2023.3.44

[75] Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 рр. Розпорядження Кабінету Міністрів України від 23.02.2022 р. № 286-р. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

[76] План Відновлення України. (2022). URL: https://recovery.gov.ua/

[77] МОН України. (2022). *Освіта України в умовах воєнного стану: інформаційно-аналітичний збірник.* Київ: Інститут освітньої аналітики. URL: http://surl.li/cxswm.

[78] Національна рада з відновлення України від наслідків війни. (2022). *Проект плану відновлення України. Матеріали робочої групи «Освіта і наука».* 145. URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/education-and-science.pdf

У розв'язку із зазначеними проблемами було розроблено низку цілей і передбачено заходи з їх поетапною реалізацією (І етап: червень 2022 р. – кінець 2022 р.; ІІ етап: січень 2023 р. – грудень 2025 р.; ІІІ етап: січень 2026 р. – грудень 2032 р.). Також чітко окреслено терміни, сформульовано ризики досягнення цілей, визначено вимірюваний показник і загальний розмір потреби у фінансових ресурсах для досягнення кожної цілі[79].

Аналіз суті цих проблем свідчить про те, що жодна з них не може бути розв'язана без ефективного використання цифрового інструментарію, потенціал якого дає змогу створити безпечне й ефективне освітнє середовище, підвищити якість освітнього процесу, стимулювати індивідуальні освітні траєкторії здобувачів вищої освіти, формувати «нульову» толерантність учасників освітнього процесу до корупції, дискримінації за різними ознаками та академічної недоброчесності тощо. Відтак реалізація кожного завдання потребує використання цифрової компетентності майбутнього викладача вищого педагогічного закладу освіти та компетентності з цифрової безпеки як її складової.

Проілюструємо яскравими прикладами ті завдання, які необхідно розв'язувати в процесі цифрової трансформації освіти і науки:

запровадження використання електронних підручників у межах реформування загальної середньої освіти «Нова українська школа», дистанційних курсів для учнів 5-11(12) класів;

сприяння автоматизації освітніх та управлінських процесів, включаючи запровадження ведення електронних журналів та щоденників, електронної звітності, обліку здобувачів освіти, педагогічних працівників та суб'єктів підвищення кваліфікації на базі державних інформаційних систем;

залучення інших освітніх інформаційних систем, створення в рамках Єдиної державної електронної бази з питань освіти реєстрів здобувачів освіти всіх рівнів, педагогічних та інших працівників закладів освіти;

автоматизація вступної кампанії;

організація набору та навчання (стажування) іноземців та осіб без громадянства;

замовлення документів про освіту та додатків до них європейського зразка;

запровадження електронного ліцензування;

модернізація Єдиної державної електронної бази з питань освіти;

створення та модернізація єдиної електронної системи моніторингу працевлаштування випускників;

створення інформаційної системи, призначеної для конкурсного фінансування наукових досліджень;

створення електронної системи доступу до існуючих інформаційних ресурсів наукового призначення, електронної науково-інформаційної системи;

створення реєстру українських дослідницьких інфраструктур;

розвиток українського індексу наукового цитування;

---

[79] Національна рада з відновлення України від наслідків війни. (2022). *Проект плану відновлення України. Матеріали робочої групи «Освіта і наука».* 147-154. URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/education-and-science.pdf

створення електронної системи присудження наукових ступенів та присвоєння вчених звань;

модернізація систем подання документів та проведення державної атестації наукових установ і закладів вищої в частині провадження ними наукової діяльності;

забезпечення розвитку репозиторію академічних текстів та підключення до нього локальних репозиторіїв.[80]

Для прогнозування підготовки викладачів закладів вищої педагогічної освіти до цифрової безпеки у повоєнний час можна запропонувати схематичний процес формування моделей соціально економічного розвитку національної економіки, представлений в науковій праці К. Завгороднього[81]. Водночас педагогічна наука має значний арсенал методів прогнозування і моделювання розвитку різних систем. На наше переконання, для управлінських кадрів закладів вищої освіти буде доречним ознайомитися з деякими з них.

Наприклад, Д. Пузіковим представлено освітньо-педагогічне прогнозування розвитку загальної середньої освіти[82]. Розроблена ним теоретична модель розглядається як «інструмент оптимізації реформування вітчизняної системи загальної середньої освіти» і охоплює шість основних компонентів: управлінський, інформаційний, процесуально-діяльнісний, методичний, ресурсний, результативний[83]. Зміст кожного компонента розкривається через певний алгоритм дій: процесуально-діяльнісний має десять послідовних етапів прогнозування розвитку загальної середньої освіти: підготовчо-програмний, аналітико-діагностувальний, прогнозного фону, базової моделі, пошукового прогнозу, нормативного прогнозу, верифікації, обговорення, результативний, коригувальний. Зазначена модель виконує низку функцій спрямованих на забезпечення оптимального здійснення прогнозування розвитку загальної середньої освіти (гносеологічна, методологічна, методична, інформаційна, освітня, організаційна, координувальна).

Проблему прогнозування розвитку системи освіти в контексті підвищення ефективності його впливу на практику підготовки фахівців та наукову діяльність у педагогічній галузі в цілому вивчає В. Ковальчук. Він указує на багатоаспектність прогнозування в освіті, яке «передбачає дослідження назріваючих проблем шляхом екстраполяції спостережуваних тенденцій, закономірностей розвитку, визначення шляхів вирішення цих проблем через нормативну розробку (оптимізацію) таких тенденцій» (Ковальчук, 2016, с. 113)[84]. Ґрунтуючись на тому, що прогноз – це оцінка майбутніх результатів і шляхів розвитку системи освіти, ресурсів й

[80] Пріоритетні напрями та завдання (проєкти) цифрової трансформації на період до 2023 року. Розпорядження Кабінету Міністрів України від 17.02.2021 р. № 365-р. URL: https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#n14

[81] Завгородній, К. В. (2023). Прогнозування в системі управління національною економікою. *Ефективна економіка*. 3. DOI: http://doi.org/10.32702/2307-2105.2023.3.44

[82] Пузіков, Д. О. (2017). Теоретична модель прогнозування загальної середньої освіти. *Український педагогічний журнал.* 4, 128-137.

[83] Пузіков, Д. О. (2017). Теоретична модель прогнозування загальної середньої освіти. Український педагогічний журнал. 4, 135.

[84] Ковальчук, В. І. (2016). Прогнозування розвитку системи освіти. *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Педагогіка, психологія, філософія*. (233), 112-120.

організаційних заходів, необхідних для його здійснення, необхідно дотримуватися таких методичних принципів:

системності (розглядати об'єкт прогнозування і прогнозний фон як систему взаємозв'язків і співвідношень);

оптимальності (розроблення точних і достовірних прогнозів при мінімальних витратах);

аналогічності (використання випереджальної інформації про розвиток аналізованого об'єкта як джерела знання про траєкторії розвитку подібних об'єктів);

комплексності (забезпечує всебічний опис об'єкта прогнозування);

специфічності (передбачає обов'язковий облік відмінних, характерних особливостей і ознак, притаманних тільки аналізованому об'єкту) (Ковальчук, 2016, с. 114)[85].

Зважаючи на цілі прогнозування підготовки викладачів закладів вищої педагогічної освіти до цифрової безпеки у повоєнний час, визначений низкою законодавчих і нормативних документів, висвітлених раніше, гарантам освітньо-професійних та освітньо-наукових програм насамперед варто обрати тип прогнозування, сформулювати цілі, відповідно до яких здійснити добір змісту. Для цього пропонуємо скористатися класифікацією, запропонованою В. Ковальчуком, у якій узагальнено найпоширеніші типи прогнозування різних освітніх процесів, а саме:

дослідний прогноз, в основу якого покладається пізнання тенденцій і закономірностей, накопичення досвіду конкретних наук, що уможливлює виявлення і формування (на другому (магістерському) етапі вищої освіти) нових можливостей і перспективних напрямів розвитку науки, освіти й техніки;

програмний прогноз – у своїй основі має пізнання суспільних потреб, тенденцій і закономірностей розвитку, покликаний сформувати програму можливих підходів, методів і заходів, створення умов для досягнень науки і техніки;

організаційний прогноз – використовує дані дослідницького і програмних прогнозів для формулювання обґрунтованої гіпотези розвитку комплексу організаційних аспектів науки, оцінювання ресурсів і перспектив зростання наукового потенціалу країни;

комплексний прогноз – охоплює елементи, зміст пошукового і нормативного прогнозу, які має в своїй основі;

системний прогноз – застосовує системні уявлення щодо предмета прогнозування (Ковальчук, 2016, с. 115)[86].

Принагідно зазначимо, що підготовка викладачів закладів вищої педагогічної освіти до цифрової безпеки у повоєнний час у будь-якому разі потребує прогнозування, оскільки цифрові інструменти розвиваються дуже

[85] Ковальчук, В. І. (2016). Прогнозування розвитку системи освіти. *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Педагогіка, психологія, філософія*. (233), 112-120.

[86] Ковальчук, В. І. (2016). Прогнозування розвитку системи освіти. *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Педагогіка, психологія, філософія*. (233), 112-120.

швидко. І чим швидше відбувається цей розвиток, тим більше може виникнути невиявлених небезпек у їх використанні, а тому викладач має знати хоча б основні їх прояви і шляхи уникнення, попередження чи захисту.

Мета прогнозування включає комплекс методів і підходів, її суть в тому, як найефективніше використовувати накопичені знання про процес прогнозування для вибору пріоритетних напрямів його науково-інноваційного розвитку.

Повертаючись до назви методичних рекомендацій, маємо акцентувати увагу на основних питаннях, яким необхідно приділити увагу в процесі підготовки викладачів закладів вищої педагогічної освіти до цифрової безпеки у повоєнний час.

Розвиток освітнього простору закладу вищої педагогічної освіти в системі інформаційної безпеки держави.

Насамперед звернемося до поняття освітнього простору як важливої характеристики освітнього процесу. Його смислове поле, виявлення структури і механізмів формування, зважаючи на сучасний контекст розуміння, вивчала А. Цимбалару. Базуючись на багатомірності й різноплановості істотних характеристик феномена «освітній простір» та залежно від підходів до його розуміння, вчена акцентує увагу на двох аспектах:

інституційному (освітній простір як певна частка соціуму, де створені умови для розвитку особистості; нормована освітня діяльність; глобальний (світовий) освітній простір, міжнародний освітній простір, європейський освітній простір, освітній простір регіону (округу), університету, академічної групи тощо);

субстанційному або індивідуальному (освітній простір як можливість і наявність формування особистісного простору суб'єкта освітнього процесу), під яким слід розуміти освітній простір особистості не лише як «наявність можливостей, а й ефективність результатів їх реалізації»[87].

Нормативне закріплення поняття «освітній простір» і пов'язаних з ним термінів «освітнє середовище», «освітній процес», їх смислові акценти в контексті основних педагогічних категорій розглядає С. Цюра та А. Терзалова. За результатами аналізу нормативного закріплення та розмежування цих термінів у Законах України в сфері освіти (кінець XX – початок XXI ст.), вони дійшли висновку, що зазначені поняття, їх співвідношення у контексті основних педагогічних категорій в україномовній педагогічній термінології вже зафіксовано державним регулятором в основних документах про освіту. Наприклад, у Законі України «Про загальну середню освіту» поняття «освітнє середовище» і «освітній простір» вживаються як синонімічні (ст. 9. Забезпечення рівного доступу до здобуття повної загальної середньої освіти). Починаючи з кінця XX століття в науковий обіг теорії і методики професійної освіти, загальної педагогіки введено такі феномени, як: «освітньо-інформаційний простір», «мережний освітній простір», «електронний освітній простір», «Інтернет-простір» тощо.

[87] Цимбалару, А. Д. (2016). Освітній простір: сутність, структура і механізми створення. *Український педагогічний журнал*. 1, 41-50.

Н. Петренко вивчає освітній простір інформаційного суспільства в контексті становлення глобального інформаційно-медійного простору, під впливом основних чинників якого (інформатизація і глобалізація) виникає «новий тип освітньої реальності, відмінний від традиційного» (Петренко, 2016, с. 36)[88]. У зв'язку з цим особливої уваги, на думку автора, потребують проблеми та ризики для розвитку особистості в освітньому просторі інформаційного суспільства, який достатньо швидко трансформується і відповідно зумовлює необхідність нового розуміння завдань освіти XXI століття.

З точки зору Н. Петренко, з однієї сторони, відкритий освітній простір на відміну від освітніх систем, створює умови для особистісного розвитку людини, демонструє різні можливості для її саморозвитку, забезпечує її «суб'єктний статус» в освіті у «вигляді можливості створювати власні реальні освітні форми» (Петренко, 2016, с. 37)[89], а з іншої – існують потенційні ризики цього процесу, зокрема системні ризики:

системні соціальні зміни, пов'язані з інформаційною та технологічними революціями, вплив яких позначається на її основних характеристиках освіти: гнучкість, динамічність, варіативність, стабільність, адаптивність, наступність, цілісність, прогностичність (зокрема динамічність як швидкість реагування освіти на вимоги часу зумовлює «ризик того, що випереджаюча реакція може видати результат, який не буде затребуваний через кілька років»; прогностичність пов'язана з ризиками, що «характеризують складності в тій сфері, яка відповідає за рівень успішної застосованості здобутих у системі освіти знань і міри їх відповідності передбачуваній соціальній системі хоча б найближчого майбутнього»);

соціокультурні наслідки формування сучасного медіапростору, вплив якого на сучасну культуру є невідворотнім, що виражається у складному переході до префігуративної культури як культурної норми, коли молодим поколінням не сприймається модель життя батьків, у зв'язку з чим виникають розбіжності в «розумінні змістів, цілей, цінностей і завдань освіти»;

комодифікація освіти, що проявляється в перетворенні освіти в різновидність товару з усіма притаманними йому властивостями (якість, асортимент, вартість, конкурентність тощо), і може призвести до втрати «статусу освіти як основи національно-культурного розвитку», «суспільного блага», суспільного ресурсу, доступного всім верствам населення;

втрата темпоральних, комунікативних, етичних рис, властивих освіті як феномену і водночас можливість її переміщувати, володіти нею, «не опікуючись підтриманням її життєдіяльності», може спричинити втрату «наукових шкіл і традицій освіти, які забезпечували наступність їх розвитку»;

[88] Петренко, Н. В. (2016). Освітній простір інформаційного суспільства як простір ризику для розвитку людини. *Науково-теоретичний альманах Грані*. *19*(5), 35-40. DOI: https://doi.org/10.15421/171606

[89] Петренко, Н. В. (2016). Освітній простір інформаційного суспільства як простір ризику для розвитку людини. *Науково-теоретичний альманах Грані*. *19*(5), 35-40. DOI: https://doi.org/10.15421/171606

проникнення кліпової свідомості («кліпове мислення»), що заснована на нескінченному і безконтрольному миготінні інформаційних відрізків[90] з медіакультури у сутнісні засади освіти;

створення нового виду комунікації – мережного співтовариства, яке веде до серйозного розриву між поколіннями, пропонує учасникам «множинність вирішень та ілюзію індивідуальної ніші переживання й світовлаштування» без опори на узагальнену раціональну картину світу», яка формується на традиційному засвоєнні знань;

контекстуальна залежність у межах сучасного освітнього медіапростору, що спричиняє звуження комунікації індивіда до обмеженого поля взаємодії, інформації, способів переживання дійсності, хоча й «перебуває в ілюзії власної присутності» у світовій комунікаційній мережі, що може викликати «якісні, глибинні зміни в особистості, часто негативного характеру» (Петренко, 2016, с. 37-38)[91].

Відтак, наукова категорія «інформаційна безпека» має досить широкий смисл і пов'язана із забезпеченням гарантованих Конституцією умов існування і розвитку людини, всього суспільства та держави[92]. Це – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій[93].

Важливо звернути увагу на те, що об'єктами інформаційної безпеки є свідомість, психіка людей; інформаційно-технічні системи різного масштабу і призначення. Саме вони на сьогодні є основними цілями інформаційної війни, яку вже тривалий час веде росія проти українського народу. До соціальних об'єктів інформаційної безпеки відносять: особистість, колектив, суспільство, державу, світове співтовариство.

Для розуміння відповідальності за забезпечення інформаційної безпеки необхідно виокремити суб'єктів:

громадяни України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства;

Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;

---

[90] Преса. (2021, 20 травня). *Кліпова свідомість: опис поняття, плюси і мінуси мислення*. URL: https://presa.com.ua/psykholohiia/klipova-svidomist-opis-ponyattya-plyusi-i-minusi-mislennya.html

[91] Петренко, Н. В. (2016). Освітній простір інформаційного суспільства як простір ризику для розвитку людини. *Науково-теоретичний альманах Грані*. *19*(5), 35-40. DOI: https://doi.org/10.15421/171606

[92] Кормич, Б. А. (2003). Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література.

[93] Концепція інформаційної безпеки України (проєкт). URL: https://ips.ligazakon.net/document/NT1607

засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;

наукові установи, освітні і навчальні заклади України, які здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності в галузі інформаційної безпеки[94],[95].

У зв'язку з цим виходить, що заклади вищої педагогічної освіти України, які здійснюють підготовку педагогічних кадрів і викладачів закладів вищої освіти, наукові дослідження також, є суб'єктами забезпечення інформаційної безпеки. Відповідно до Законів України «Про освіту» (ст. 7), «Про функціонування української мови як державної», які закріплюють українську мову як єдину державну в Україні, обов'язкову для органів державної влади і публічних сфер на всій території країни, використання в освітній та медичній сферах, у трудових відносинах та у сфері обслуговування споживачів, у публічних заходах, рекламі та інших сферах[96], вони є активними учасниками процесу українізації культурного простору України. За висновками І. Парфенюка, «роль українізації в системі інформаційної безпеки не зводиться лише до розуміння її як засобу поширення української культури – це фактор національної безпеки України та єдності нації»[97].

На завершення зробимо висновки.

1. Для підготовки викладача закладу вищої педагогічної освіти у повоєнний час необхідним є створення нового освітнього простору як безпечного та доступного освітнього середовища із застосуванням сучасних інформаційно-комунікаційних засобів, для чого мають упроваджуватися новітні технології енергоефективності, дизайну, архітектури будівель, споруд та територій закладів освіти.

2. Освітній простір підготовки викладача закладу вищої педагогічної освіти у повоєнний час має постійно розвиватися в контексті українізації культурного простору України в системі національної інформаційної безпеки.

3. Майбутньому викладачеві закладу вищої педагогічної освіти у повоєнний час необхідно володіти компетентністю з цифрової безпеки як складовою цифрової компетентності, що визнана на міжнародному рівні ключовою в умовах четвертої промислової революції. Рівень її сформованості (A_1, A_2, B_1, B_2, C_1, C_2) може підтверджуватися електронним сертифікатом про проходження тестування на національній онлайн-платформі «Дія. Освіта».

---

[94] Остроухов, В., Петрик, В. (2008). До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 4, 135-141. URL: http://jnas.nbuv.gov.ua/article/UJRN-0000734254

[95] Паш, Б. В. (2017). Складові інформаційної безпеки держави: постановка питання. *Закарпатські правові читання.* 1, 509–512. URL: http://surl.li/pwqdd

[96] Закон України «Про забезпечення функціонування української мови як державної» № 2704-VIII. (2023, 31 грудня). https://zakon.rada.gov.ua/laws/show/2704-19#Text

[97] Парфенюк І. (2019). Українізація культурного простору України в системі інформаційної безпеки держави. Український інформаційний простір. 2(4), 63-72. DOI: https://doi.org/10.31866/2616-7948.2(4).2019.186926

4. Розвиток компетентностей з цифрової безпеки у складі цифрової компетентності викладача закладу вищої педагогічної освіти має здійснюватися в процесі реалізації всіх компонентів освітньої програми через виконання завдань до самостійної роботи, включення до плану проходження практики, участь у дослідницькій діяльності та науково-масових заходах, виконання магістерських проєктів тощо. При цьому вбачається важливим оволодіння методиками захисту індивідуальної і суспільної свідомості від негативних інформаційних впливів («інформаційного шуму», «інформаційного перенавантаження», «інформаційно-психологічних операцій»), оволодіння емоційним інтелектом як здатністю розпізнавати свої переживання, розуміти стан і мотивацію свого оточення, мати стійку самооцінку, адекватно визначати небезпечності й регулювати свою поведінку.

Таким чином, розвиток компетентності з цифрової безпеки майбутнього викладача закладу вищої педагогічної освіти є одним з результатів готовності до професійної діяльності в повоєнний період, що уможливить його участь у створенні безпечного освітнього середовища для розвитку особистості й системи національної безпеки України.

ВИСНОВКИ

Майбутнім викладачам закладів вищої педагогічної освіти належить бути носіями високої професійно-педагогічної культури, прикладом профактивності і державницького ставлення до створення інтелектуального й духовного потенціалу нації, творчих пошуків найкращих моделей професійного розвитку. Тому державою на них покладається відповідальність за підготовку тих, хто нині будує НУШ і формує особистість, її громадянську позицію та моральні якості, що потребує безперервного розвитку нових компетентностей. Очевидним є те, що вони, у свою чергу, мають бути пов’язані із завданнями, які їм належить виконувати у процесі своєї викладацької діяльності, а тому актуалізуються уміння їх виокремлювати, тобто осмислити і виявити як на державному, так і на регіональному рівні для гнучкого і невідкладного реагування на виклики і потреби місцевих галузей, підприємств та суспільних груп з метою їх забезпечення фахівцями з необхідних професій, інноваційними розробками, програмами, проєктами тощо.

Цифровізація освітнього простору є невід’ємною складовою упровадження інноваційних моделей та педагогічних технологій професійного розвитку майбутніх викладачів закладів вищої педагогічної освіти під час російської агресії в Україні й, безумовно, далі набуватиме масштабного поширення в повоєнний період, що уможливлює швидке реагування на нові зовнішні виклики і спонукає змінювати структуру освітнього процесу відповідно до нових завдань.

Серйозний вплив інформаційного середовища на інтелектуальний, фізичний та психічний розвиток шкільної і студентської молоді, дорослого населення сьогодні є цілком зрозумілий. Він проявляється, з однієї сторони, у

забезпеченні доступу до інформаційних ресурсів, упровадженні інтерактивних технологій, застосуванні електронних освітніх ресурсів, різних форматів надання інформації, що уможливлює суттєве підвищення якості професійної підготовки фахівців для різних галузей економіки, а з іншої – з'явилися нові ризики та загрози для всіх учасників освітнього процесу. Очевидними є: ерозія культурної складової освітнього процесу, зростання інтернет-адикації (інтернет-залежності), можливість несанкціонованого доступу до персональних даних, кібер-мобінг, наповнення фейками інтернет-медіа і соціальних мереж, хейтинг та безліч інших питань, які актуалізують інформаційну проблематику, зокрема цифрову безпеку в громадянському суспільстві. Ці загрози перейшли із потенційних та гіпотетичних на цілком реальні, тож протистояння їх поширенню стало пріоритетним завданням на національному рівні урядів та міжнародної спільноти. У зв'язку з цим, як в Україні, так і на міжнародному рівні, прийнято низку нормативно-правових документів, подальший процес гармонізації яких знаходиться в постійній динаміці.

В управління закладом вищої освіти, освітнім процесом у ньому доцільно взяти до уваги: Конвенцію про кіберзлочинність; європейську стратегію «Цифрове десятиліття Європи: цифрові цілі до 2030 року»; європейську Декларацію про цифрові права і принципи цифрового десятиліття; Цифровий порядок денний на 2020–2030 рр., прийнятий Європейською Комісією; Стратегію кібербезпеки України; Доктрину інформаційної безпеки України; План реалізації Стратегії кібербезпеки України; Рамку цифрової компетентності для громадян України (зокрема для вчителів).

Імплементацію основних положень конвенцій, стратегій, доктрин можливо здійснювати через проєктування локальної політики (на рівні закладу вищої освіти) із цифрової безпеки інформаційно-освітнього середовища: діагностику рівнів сформованості навичок цифрової безпеки у суб'єктів освітнього процесу; створення програм навчання, тренінгів, воркшопів із формування навичок цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти. Для цього варто використовувати потенціал різних громадських організацій та волонтерів (фахівців з кібербезпеки).

Поняття «інформатизація освіти» та «цифровізація освіти» в колі науковців використовуються синхронно, оскільки в останні роки відбувається заміна більшої частини аналогових систем (сфер) на ефективніший цифровий формат, що зумовило необхідність активного опанування цифровими навичками та вміннями науково-педагогічних і педагогічних працівників, аби відреагувати на зміни реальності. У зв'язку з цим виявилися суперечності між необхідністю дотримуватися цифрової безпеки в процесі педагогічної, науково-педагогічної діяльності та недостатньою розробленістю й обґрунтуванням істотних характеристик і структури компетентності з цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти.

Структура компетентності з цифрової безпеки відображена в Цифровій рамці компетентностей (DigCompEdu) та рекомендаціях у сфері цифрових компетентностей від європейських та міжнародних інституцій. Це комплекс

компетентностей, які можна розглядати як структуру компетентності майбутнього викладача закладу вищої педагогічної освіти з цифрової безпеки, зокрема: захист пристроїв і безпечне підключення до мережі Інтернет; захист персональних даних і приватності, безпека в Інтернеті; захист особистих прав споживача від шахрайства і зловживань; захист здоров'я та благополуччя; захист довкілля. На основі вивчення результатів наукових досліджень, експертних оцінок визнаних експертів з проблем цифрової безпеки та практичного досвіду визначено й обґрунтовано зміст кожної окремої компетентності.

Аналіз отриманих даних показав: респонденти демонструють високий рівень сформованості тих компетенцій, які вони застосовують у своїй повсякденній життєдіяльності, тобто ті, що сьогодні можна віднести до функціональної грамотності (дії у соціальній мережі у відповідь на отримані погрози; найнадійніші паролі до власного акаунту). Водночас більше ніж третина опитуваних продемонстрували низький рівень сформованості компетентності «здатність до використання резервних способів підтвердження під час подвійної автентифікації», яку сьогодні слід віднести до професійної компетентності майбутнього викладача. Адже основними засобами навчання у закладах вищої освіти в сучасних умовах є цифрові.

Отже, сучасні виклики потребують від здобувачів освіти інформаційно-технологічної готовності виконувати свої професійні функції. Насамперед, йдеться про: знання інформаційних і цифрових засобів, технологій та вміння їх використовувати; уміння збирати, оцінювати і використовувати інформацію; пристосовуватися до нових умов праці (здатність до адаптивності); усвідомлення необхідності самоосвіти і потреба в регулярному підвищенні кваліфікації тощо.

Для цього доречними є посилення цифрової складової освіти (спецкурси з медіаграмотності, фактчекінгу, розвиток критичного мислення, консультації ІТ-фахівців, створення міждисциплінарних курсів на основі цифрових навчальних платформ) тощо. Освітній процес необхідно спланувати таким чином, щоб у результаті здобувачі вищої освіти могли захистити свої пристрої та безпечно підключалися до мережі Інтернет, тобто володіти здатністю визначити прості способи захисту своїх пристроїв та цифрового контенту; диференціювати прості ризики та загрози в цифрових середовищах; вибрати прості заходи безпеки та гарантії; визначити прості способи належного врахування надійності та конфіденційності; дотримуватися простих заходів безпеки.

ЛІТЕРАТУРА

Buckland, P. (2005). *Reshaping the future: Education and postconflict reconstruction*. World Bank Publications.

Didgital 2022: Global Overview Report. [Online]. Дата звернення: Квіт. 01, 2023. URL: https://datareportal.com/reports/digital-2022-global- overview-report

Europe's Digital Decade: digital targets for 2030. URL: https://commission.europa.eu/strategy-and-policy/priorities-019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets- 2030_en

European Commission. Shaping Europe's digital future. European Declaration on Digital Rights and Principles. 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-principles

Fact Sheets on the European Union. Digital Agenda for Europe. 2020. URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digit al-agenda-for-europe

Hanushek, E. A., & Kimko, D. D. (2000). Schooling, labor force quality, and the growth of nations. *American Economic Review*, 90. No. 5 (December). 1184–1208.

Imbernon, F. (1989). *La formación permanente del profesorado.* Col. Cuadernos de Pedagogía. Laia. Barcelona.

Kindleberger, C. P. (1967). *Europe's postwar growth: The role of labor supply.* Harvard University Press. DOI: https://doi.org/10.4159/harvard.9780674498181

Mason, E. S., Kim, M. J., Perkins, D. H., Kim, K. S., & Cole, D. C. (1980). *The Economic and Social Modernization of the Republic of Korea.* Cambridge, MA: Harvard University Press.

Office 365 Education. URL: http://surl.li/awfx

Schultz, T. W. (1961). Investment in Human Capital. *The American Economic Review*, 51(1). 1–17.

UNESCO. (1978). *Revised Recommendation concerning the International Standardization of Educational Statistics.* In: General Conference of UNESCO. Paris: UNESCO. Дата звернення: 08.04.2020. URL: http://portal.unesco.org/en/ev.phpURL_ID=13136&URL_DO=DO_TOPIC&URL_ SECTION=201.html

Yoshitaka, S. (2023). Top 10 Digital Transformation Trends for 2023. URL: https://www.upwork.com/resources/top-digital-transformation-trends.

Апетик, А., Купчинська, І. (2022, 29 серпня). *Як захистити себе онлайн? Поради від експертки з цифрової безпеки.* UNDP. URL: https://www.undp.org/uk/ukraine/blog/yak-zakhystyty-sebe-onlayn-porady-vid-ekspertky-z-tsyfrovoyi-bezpeky

Безоплатна правова допомога. (Б. р.). URL: http://surl.li/oxkqn

Бондарєв, О. (2015). Кидали-онлайн. Названо найбільш поширені способи інтернет-шахрайства. URL: https://techno.nv.ua/ukr/gadgets/kidali-onlajn-nazvano-najbilsh-poshireni-sposobi-internet-shahrajstva75741.htm

Винничук, Р. В. (2023). *Система професійної підготовки магістрів гуманітарної галузі на аксіологічних засадах*. [Дис. д-ра. пед. наук, Полтавський національний педагогічний університет імені В. Г. Короленка]. URL: http://pnpu.edu.ua/wp-content/uploads/2023/10/dysertacziya_vynnychuk_26.10.pdf

Вільний тлумачний словник. Новітній онлайновий словник української мови. 2013-2018. *URL:* http://sum.in.ua/f/dovkillja

Віноградова, У. (2023, 25 грудня). *Варто бути обережним – українцям розповіли про популярну схему шахраїв.* Новини.LIVE. URL: https://news.novyny.live/varto-buti-oberezhnimi-ukrayintsiam-rozpovili-pro-populiarnu-skhemu-shakhrayiv-140424.html

Долінська, Н. В., 2019. *Педагогічна складова у системі підготовки викладачів в університетах США*. [Дис. канд. пед. наук, Львівський національний університет імені Івана Франка].

Євсович, Р. В. (2021). *Гуманізація та гуманітаризація вищої освіти України кінця XX початку XXI століть (1985–2012 рр.)*. [Дис. канд. пед. наук, Рівненський державний гуманітарний університет]. URL: https://www.rshu.edu.ua/images/afto/disert_evsovich_rv.pdf

Завгородній, К. В. (2023). Прогнозування в системі управління національною економікою. *Ефективна економіка*. 3. DOI: http://doi.org/10.32702/2307-2105.2023.3.44

Закон України «Про забезпечення функціонування української мови як державної» № 2704-VIII. (2023, 31 грудня). https://zakon.rada.gov.ua/laws/show/2704-19#Text

Інститут модернізації змісту освіти. Нова українська школа. URL: http://surl.li/gyjiz.

Інтернет. *Шкода здоров'ю. URL: http://surl.li/oxlum*

Ковальчук, В. І. (2016). Прогнозування розвитку системи освіти. *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Педагогіка, психологія, філософія*. (233), 112-120.

Кодекс України «Кодекс цивільного захисту України» від 02.10.2012 р. № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17

Комп'ютерна допомога. URL: http://surl.li/oxkpwl

Конвенція про кіберзлочинність Міжнародний документ від 23.11.2001 № 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

Концепція інформаційної безпеки України (проєкт). URL: https://ips.ligazakon.net/document/NT1607

Кормич, Б. А. (2003). Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література.

Лахно, В., Каламан, Є., Ягалієва Б., Криворучко, О., Десітко, А., Цюцюра, С., & Цюцюра, М. (2022). Модель захисту локальної мережі навчального закладу серверної системи віртуалізації. *Кібербезпека: освіта, наука, техніка: електронне фахове наукове видання*. 2 (18), 6–23. DOI: https://doi.org/10.28925/2663-4023.2022.18.623

Мальцева, І. Р., Черниш, Ю. О., Штонда, Р. М. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 4(16), 37– 44. DOI: https://doi.org/10.28925/2663-4023.2022.16.3744

МОН України. (2022). *Освіта України в умовах воєнного стану: інформаційно-аналітичний збірник.* Київ: Інститут освітньої аналітики. URL: http://surl.li/cxswm.

Національна рада з відновлення України від наслідків війни. (2022). *Проект плану відновлення України. Матеріали робочої групи «Освіта і наука».* URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/education-and-science.pdf

Опис рамки цифрової компетентності для громадян України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/20 21/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf

Остроухов, В., Петрик, В. (2008). До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 4, 135-141. URL: http://jnas.nbuv.gov.ua/article/UJRN-0000734254

Парфенюк І. (2019). Українізація культурного простору України в системі інформаційної безпеки держави. Український інформаційний простір. 2(4), 63-72. DOI: https://doi.org/10.31866/2616-7948.2(4).2019.186926

Паш, Б. В. (2017). Складові інформаційної безпеки держави: постановка питання. *Закарпатські правові читання.* 1, 509–512. URL: http://surl.li/pwqdd.

Педрада. Портал освітян України. Безпечне освітнє середовище закладу освіти. URL: https://www.pedrada.com.ua/article/2614-bezpechne-osvtn-seredovishche-zakladu-osvti

Петренко, Л. (2018). Організаційні методи дистанційного навчання в закладах професійної (професійно-технічної) освіти. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми.* (50), 151-156. https://vspu.net/sit/index.php/sit/article/view/4777

Петренко, Л. (2023). Цифрова безпека в структурі цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти: змістовий компонент. *Освіта дорослих: теорія, досвід, перспективи*. 23(1), 98-109. DOI: https://doi.org/10.35387/od.1(23).2023.98-109

Петренко, Л. М. (2021). Аналітичний огляд запиту на публікації з питань професійного розвитку педагогічних і науково-педагогічних працівників. *Інноваційні трансформації в сучасній освіті: виклики, реалії, стратегії*: матеріали ІІІ Всеукраїнського відкрого науково-практичного онлайн-форуму. Київ: Національний центр «Мала академія наук України». 132–135.

Петренко, Л. М. (2023). Професійна підготовка майбутнього викладача педагогічного вищого закладу освіти у руслі світоглядних ідей Івана Зязюна. *Фундатор «педагогіки добра» і добротворення в педагогіці:*

збірник матеріалів до 85-річчя з дня народження Івана Зязюна. 87-91. Київ: Вид-во ТОВ «Юрка Любченка». URL: https://lib.iitta.gov.ua/735208/1/fundator-sity_11.05.2023.pdf

Петренко, Л. М. (2023). Цифрова безпека у професійній діяльності майбутнього викладача педагогічної освіти. Р*озвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій:* матеріали ІІІ Всеукраїнської науково-практичної конференції. Глухів: Глухівський НПУ ім. О. Довженка. 291-294. URL: https://lib.iitta.gov.ua/735042/

Петренко, Л. М. *(2020). Функціональна грамотність у контексті трансформації професійного розвитку фахівців. Актуальні проблеми технологічної і професійної освіти: тези доповідей ІІ міжнародної науково-практичної конференції, 56-58. Глухів: Глухівський НПУ ім. О. Довженка.*

Петренко, Л.М. (2019). Академічна свобода як фундаментальна цінність. *Розвиток професійної культури майбутніх фахівців: виклики. досвід, стратегії і перспективи*: збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції. Ірпінь: Ірпінський державний коледж економіки та права. 107-110. URL: https://api-ir.dpu.edu.ua/server/api/core/bitstreams/2a2792ac-a1dd-4061-a95f-f0b0c59f25e6/content

Петренко, Н. В. (2016). Освітній простір інформаційного суспільства як простір ризику для розвитку людини. *Науково-теоретичний альманах Грані*. *19*(5), 35-40. DOI: https://doi.org/10.15421/171606

План Відновлення України. (2022). URL: https://recovery.gov.ua/

Преса. (2021, 20 травня). *Кліпова свідомість: опис поняття, плюси і мінуси мислення*. URL: https://presa.com.ua/psykholohiia/klipova-svidomist-opis-ponyattya-plyusi-i-minusi-mislennya.html

Пріоритетні напрями та завдання (проєкти) цифрової трансформації на період до 2023 року. Розпорядження Кабінету Міністрів України від 17.02.2021 р. № 365-р. URL: https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#n14

Про рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України». Указ Президента України № 37/2022 від 30.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text

Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Указ Президента України № 447/2021 від 14.05.2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України». Указ Президента України № 47/2017 від 29.12.2016 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Указ Президента України № 96/2016 від 27.01.2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

Про схвалення Концепції реалізації державної політики у сфері реформування загальної середньої освіти «Нова українська школа» на період до 2029 року. Розпорядження Кабінет Міністрів України від 14.12.2016 р. № 988-р URL: https://www.kmu.gov.ua/npas/249613934

Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України № 67-р. від 17.01.2018 р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 рр. Розпорядження Кабінету Міністрів України від 23.02.2022 р. № 286-р. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

Профспілка працівників освіти і науки України. *(2017, 5 вересня). 6 правил роботи за комп'ютером без шкоди для здоров'я. URL:* http://surl.li/bnegy

Пузіков, Д. О. (2017). Теоретична модель прогнозування загальної середньої освіти. Український педагогічний журнал. 4, 127-138.

Пуліч, О. А. & Москальов, М. В. (2023). *Стрес і перевантаження від постійного з'єднання з інтернетом та технологіями. Професійний розвиток в умовах цифровізації суспільства: сучасні тренди*: тези доповідей IV науково-практичної конференції з нагоди 70-річчя заснування Університету менеджменту освіти. Київ: ДЗВО «Університет менеджменту освіти». URL: http://surl.li/pqubm

Пуховська, Л. (2011). Теоретичні засади професійного розвитку вчителів: рух до концептуальної карти. *Порівняльна професійна педагогіка.* (1), 97-106. URL: http://hdl.handle.net/20.500.12424/371290

Скорик, Т. В. (2021). *Теорія і практика професійної успішності майбутнього вчителя у закладах вищої освіти України (друга половина XX – початок XXI століття)*. [Дис. д-ра. пед. наук, Комунальний вищий навчальний заклад "Херсонська академія неперервної освіти" Херсонської обласної ради].

Словник української мови. Академічний тлумачний словник (1970-1980). URL: http://sum.in.ua/s/seredovyshhe/

Створення екостійкого офісу. Xerox. URL: https://www.xerox.com/uk-ua/about/ehs/green-office

Султанова, Л. & Прокоф'єва, М. (2022). Цифрова безпека в галузі вищої освіти. *Освіта дорослих: теорія, досвід, перспективи.* 21 (1), 106- 117. DOI: https://doi.org/10.35387/od.1(21).2022.106-117.

Султанова, Л.Ю. & Прокоф'єва, М. *(2022). Цифрова безпека в галузі вищої освіти: аналітичні матеріали. Кропивницький: Імекс-ЛТД.*

Суспільний кореспондент. (2023, 25 грудня). Шахраї розсилають листи від Укрпошти. URL: https://www.sknews.net/shakhrai-rozsylaiut-lysty-vid-ukrposhty/

Таможська, І. В. (2020). *Теоретичні і методичні засади підготовки науково-педагогічних кадрів в університетах України (друга половина XIX–початок XX століття).* [Дис. д-ра. пед. наук, Харківський національний

університет імені В.Н. Каразіна]. URL: https://uacademic.info/ua/document/0520U101620

Цимбалару, А. Д. (2016). *Освітній простір: сутність, структура і механізми створення*. *Український педагогічний журнал*. 1, 41-50.

Черкашин, С. В. (2021). *Розвиток університетської освіти Німеччини (XX – початок XXI століть)*. [Дис. д-ра. пед. наук, Харківський національний педагогічний університет імені Г. С. Сковороди].

Черьомухіна, О. (2022) *Користування інтернетом серед українців: результати телефонного опитування, проведеного 13–18 травня 2022 року.* Пресреліз. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1115&page=1

Що таке система управління навчанням (LMS)? URL: http://surl.li/pfckp

Юзик, О. П., 2022. *Теоретичні та методичні засади підготовки вчителя інформатики у Польщі (друга половина XX – поч. XXI ст.)*. [Дис. д-ра. пед. наук, Рівненський обласний інститут післядипломної педагогічної освіти].

Якимчук, О.І. (2015). *Філософсько-когнітивні засади розвитку національного простору освіти* [Дис. канд. наук філософ. наук, Національний педагогічний університет імені М. П. Драгоманова]. URI: http://enpuir.npu.edu.ua/handle/123456789/41031

Яцишин, А. В. (2020). *Цифрові відкриті системи у підготовці аспірантів і докторантів:* монографія. Київ: ЦП «Компринт».

ДОДАТКИ

Тест побудований на основі національного тесту на цифрову грамотність «Цифрограм». (https://osvita.diia.gov.ua/digigram)

ТЕСТ
КОМПЕТЕНЦІЯ: УЧИТЕЛЬ У ЦИФРОВОМУ СУСПІЛЬСТВІ

ЦИФРОВЕ СУСПІЛЬСТВО

1. Ви бажаєте оплатити комунальні послуги онлайн. Яким способом це можна зробити?
Оберіть одну правильну відповідь.
1. Звернутися до касира у відділенні банку
2. Скористатися онлайн-банкінгом
3. Зателефонувати до комунальної установи
4. Написати в чат спільноти

2. У закладі освіти проводиться фотоконкурс, переможці якого будуть визначені за кількістю вподобайок під фото в тематичному пості. Як допомогти закладу здобути перемогу чесним та найбільш результативним шляхом?
Оберіть одну правильну відповідь.
1. Поширити інформацію серед аудиторії, яка підтримає
2. Створити декілька фейкових акаунтів у соціальній мережі та вподобати фото
3. Поділитися постом декілька разів у соціальній мережі
4. Зателефонувати всім знайомим і друзям

3. Ви плануєте сімейну подорож під час літньої відпустки. Який із перелічених сервісів допоможе вам спланувати маршрут і переглянути об'єкти для відвідування?
Оберіть одну правильну відповідь.
1. Google Карти
2. Google Expedition
3. Google Pay
4. Google Earth

ЕЛЕКТРОННЕ УРЯДУВАННЯ

4. Оберіть твердження, яке характеризує поняття «відкриті державні дані»:
Оберіть одну правильну відповідь.
1. публічна інформація, що надається органами влади в машиночитному форматі з обмеженнями щодо подальшого використання

2. публічна інформація, що надається органами влади у машиночитному форматі без обмежень щодо подальшого використання
3. конфіденційна інформація, що надається органами влади в машиночитному форматі без обмежень щодо подальшого використання
4. публічна інформація, що надається органами влади на запит без обмежень щодо подальшого використання

5. Установіть відповідність між сервісами, які допомагають отримувати освітні послуги дистанційно, та категоріями замовників:
1. Кабінет учасника єдиного фахового вступного випробування. 2. Регіональні центри оцінювання якості освіти. 3. Кабінет учасника сертифікації педагогічних працівників. 4. Перевірка достовірності учнівських робіт та студентських квитків. A. Учасники ЗНО. B. Педагогічні працівники. C. Абітурієнти. D. Здобувачі освіти.
1. 1-A, 2-C, 3-B, 4-D
2. 1-D, 2-B, 3-C, 4-A
3. 1-B, 2-C, 3-A, 4-D
4. 1-C, 2-A, 3-B, 4-D

6. Оберіть, що з перерахованого відповідає концепції відкритих даних:
Оберіть одну правильну відповідь.
1. відкрита ліцензія, відкритий доступ
2. відкрита взаємодія, відкриті технології
3. відкритий доступ, відкриті технології
4. відкриті технології, відкрита ліцензія

ЕЛЕКТРОННА ШКОЛА

7. Установіть відповідність між онлайн-ресурсами закладу освіти та цільовими групами користувачів:
1. сторінка з публічною інформацією на сайті закладу. 2. сторінка з інформацією для вступу на сайті закладу. 3. електронний журнал класу. 4. сайт педагогічного працівника з навчальними матеріалами. A. батьки. B. педагогічні працівники. C. громадськість. D. здобувачі освіти.
1. 1-B, 2-B, 3-C, 4-A
2. 1-A, 2-C, 3-B, 4-D
3. 1-C, 2-A, 3-B, 4-D
4. 1-D, 2-B, 3-C, 4-A

8. Установіть правильну відповідність функції електронного класного журналу та дії педагогічного працівника в ньому:
1. уведення структури навчального року. 2. уведення відмітки про відвідування. 3. уведення теми заняття та домашнього завдання. 4. уведення поточної оцінки. A. формування звіту про відвідування. B. формування запису в електронному

щоденнику. C. формування дат проведення занять. D. формування прогнозованої оцінки за тему.
1. 1-C, 2-A, 3-B, 4-D
2. 1-B, 2-C, 3-A, 4-D
3. 1-A, 2-B, 3-C, 4-D
4. 1-D, 2-B, 3-A, 4-C

9. У педагогічного працівника в браузері дуже багато закладок на різні освітні ресурси. Для зручної роботи він хоче впорядкувати їх за темами. У який спосіб він може це зробити?
Оберіть одну правильну відповідь.
1. розподілити закладки по папках, використати сервіс закладок
2. використати сервіс закладок, переписати всі закладки в робочий блокнот
3. створити документ, у якому переписати всі закладки, розподілити закладки по папках
4. розподілити закладки по папках, переписати всі закладки в робочий блокнот

ЕЛЕКТРОННЕ НАВЧАННЯ

10. Поставте у відповідність види навчання із можливими результатами навчання:
1. Ознайомитися з можливостями цифрового інструменту. 2. Навчитися працювати з цифровим інструментом під керівництвом тренера. 3. Навчитися працювати з цифровим інструментом самостійно за наданими матеріалами та звертаючись за консультацією в разі потреби. 4. Навчитися працювати з цифровим інструментом, повторюючи дії тренера під час демонстрації. A. Онлайн-курс. B. Вебінар. C. Тренінг. D. Майстер-клас.
1. 1-B, 2-C, 3-A, 4-D
2. 1-D, 2-C, 3-B, 4-A
3. 1-C, 2-A, 3-D, 4-B
4. 1-A, 2-D, 3-C, 4-B

11. Для підвищення цифрової компетентності ви бажаєте пройти онлайн-курси та шукаєте організацію, що пропонує такі послуги. Які ознаки свідчать про надання цією організацією якісної освіти?
1. позитивні відгуки користувачів — учасників онлайн-курсів. 2. наявність офіційного сайту організації. 3. низька ціна онлайн-курсів або надання безкоштовних послуг. 4. наявність офіційної сторінки в соціальних мережах. 5. позитивний відгук від знайомого/знайомої. 6. наявність детальної інформації про курси.
1. 1, 3, 5
2. 1, 2, 6
3. 2, 3, 4
4. 2, 4, 5

12. Педагогічний працівник підготував онлайн-тест для здобувачів освіти, але бажає зробити його засобом формувального оцінювання, а не контролю. Які параметри слід установити педагогічному працівнику?
Оберіть одну правильну відповідь.
1. показувати правильні відповіді, показувати час проходження тесту
2. показувати не зараховані відповіді, показувати кількість спроб
3. показувати час проходження тесту, показувати кількість спроб
4. показувати кількість балів, показувати не зараховані відповіді

БЕЗПЕКА У ЦИФРОВОМУ СУСПІЛЬСТВІ

13. У якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації?
1. відновити доступ до акаунту, якщо ви придбали телефон. 2. відновити доступ до акаунту, якщо треба змінити пароль. 3. відновити доступ до акаунту, якщо ви забули до нього пароль. 4. відновити доступ до акаунту, якщо ви загубили телефон. 5. увійти в свій обліковий запис, якщо доступ до вашого робочого комп'ютеру мають інші користувачі. 6. увійти в свій обліковий запис на надійному пристрої.
1. 1, 3, 2
2. 1, 5, 6
3. 2, 3, 6
4. 3, 4, 5

14. У соціальній мережі ви отримали погрози від якогось користувача. Якими будуть ваші дії у відповідь?
1. заблокувати цього користувача. 2. написати подібну відповідь користувачу. 3. видалити свою сторінку в соціальній мережі. 4. запросити друзів написати цьому користувачу погрози. 5. подати скаргу на користувача адміністрації мережі. 6. зафіксувати повідомлення та звернутися до спеціальних служб.
1. 1, 3, 4
2. 2, 4, 6
3. 2, 3, 4
4. 1, 5, 6

15. Олена Сергіївна Іванова викладає математику та хоче використовувати надійний пароль до власного акаунту. Який із наведених паролів є надійнішим для неї?
Оберіть одну правильну відповідь.
1. Olena2021
2. 19081972
3. B&h28Pz#
4. Matematik

КОМПЕТЕНЦІЯ: ПРОФЕСІЙНИЙ РОЗВИТОК

ПРОФЕСІЙНА КОМУНІКАЦІЯ

16. Ви отримали лист з прикріпленими об'єктами. Яку дію потрібно обрати, щоб поділитися вмістом листа з іншими людьми?
Оберіть одну правильну відповідь.
1. відповісти
2. відповісти всім
3. переслати
4. переслати всім

17. Для дистанційного навчання в закладі освіти використовується Google Клас. Установіть відповідність між способом зворотного зв'язку та його реалізацією в Google Клас.
1. Уточнення щодо виконання завдання. 2. Оголошення для всіх здобувачів освіти. 3. Опис допущених помилок. 4. Відповідь на коментар здобувача освіти в «Потоці». A. Коментар до завдання. B. Коментар до повідомлення в «Потоці». C. Приватний коментар до роботи здобувача освіти. D. Розміщення повідомлення в «Потоці».
1. 1-C, 2-A, 3-D, 4-B
2. 1-B, 2-A, 3-D, 4-C
3. 1-A, 2-D, 3-C, 4-B
4. 1-A, 2-C, 3-B, 4-D

18. Батьки класу хочуть висловлювати власну думку та обговорювати важливі питання, використовуючи цифрові інструменти. Які інструменти доцільно використати для цього?
Оберіть одну правильну відповідь.
1. створити закриту групу батьків у соціальній мережі або групу в месенджері
2. створити відкриту групу батьків у соціальній мережі
3. створити сторінку на сайті закладу освіти для спілкування батьків
4. організувати відеоконференцію батьків

ПРОФЕСІЙНА СПІВПРАЦЯ

19. Для обміну дидактичними та методичними матеріалами з колегами доцільно використовувати:
Оберіть одну правильну відповідь.
1. електронну пошту, хмарні сховища
2. месенджери, персональні сайти
3. соціальні мережі, електронну пошту
4. форуми, месенджери

20. Ви викладаєте навчальний предмет у класі та хочете запросити класного керівника приєднатися до створеного вами електронного курсу (віртуального класу) з метою налагодження взаємодії. Що для цього вам слід зробити?
Оберіть одну правильну відповідь.
1. запросити його приєднатися до освітнього середовища в ролі студента
2. запросити його приєднатися до освітнього середовища в ролі викладача
3. запросити його приєднатися до освітнього середовища в ролі опікуна
4. запросити його приєднатися до освітнього середовища в ролі адміністратора

21. Ви створили документ Google для спільної роботи та бажаєте, щоб з документом працювали лише ті колеги, яких ви запросили як співавторів. Як заборонити запрошеним співавторам долучати інших осіб до редагування цього документа?
Оберіть одну правильну відповідь.
1. У вікні спільного доступу натиснути «Отримати посилання для спільного доступу», обрати варіант доступу, натиснути «Готово»
2. У вікні «Надайте доступ користувачам» праворуч угорі обрати позначку з шестернею, поставити відповідний прапорець. Натиснути «Готово»
3. У вікні спільного доступу вписати до відповідного поля реальні адреси користувачів, натиснути «Надіслати»
4. Такої можливості не існує

РЕФЛЕКСІЯ РОЗВИТКУ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ

22. Для визначення рівня власної цифрової компетентності можна скористатися такими ресурсами:
Оберіть одну правильну відповідь.
1. https://osvita.diia.gov.ua/digigram/
2. https://thedigital.gov.ua/
3. https://teachfromanywhere.google/
4. https://prometheus.org.ua/

23. Оберіть ціль національної онлайн-платформи з цифрової грамотності Дія. Цифрова освіта:
Оберіть одну правильну відповідь.
1. вільне навчання цифрової грамотності
2. використання цифрових технологій у професійній діяльності
3. поширення інформації про навчання цифрової грамотності
4. рекламування курсів щодо набуття спеціалізованих цифрових навичок

24. Оберіть цифрові платформи, завдяки ресурсам яких педагогічний працівник може підвищити власний професійний рівень:
1. https://osvita.diia.gov.ua/. 2. https://prometheus.org.ua/. 3. http://osvita.ua/. 4. https://www.online.ua/. 5. https://www.coursera.org/. 6. https://www.udemy.com/. 7. https://www.education.ua/.
1. 1, 2, 4, 5
2. 1, 2, 5, 6
3. 2, 4, 6, 7
4. 1, 2, 3, 7

НЕПЕРЕРВНИЙ ПРОФЕСІЙНИЙ РОЗВИТОК

25. Ви хочете зберегти адресу знайденої вебсторінки з цікавою інформацією для подальшого використання. Як це можна зробити?
1. створити закладку в браузері. 2. додати скопійоване посилання до нотатки. 3. додати закладку на комп'ютер. 4. створити нову вкладку в браузері. 5. зберегти в менеджері закладок. 6. зберегти в спеціальному документі.
1. 1, 2, 4, 5
2. 1, 2, 3, 4
3. 1, 2, 5, 6
4. 3, 4, 5, 6

26. Оберіть варіант, у якому вказані інструменти планування власної діяльності:
Оберіть одну правильну відповідь.
1. календар, сайт, блог
2. портфоліо, сайт, план
3. календар, щоденник, план
4. нотатка, портфоліо, план

27. Які ресурси може використати педагогічний працівник для створення систематизованого каталога власних інтерактивних навчальних та методичних розробок щодо вивчення предмета?
Оберіть одну правильну відповідь.
1. Вебсайт, блог, документ з гіперпосиланнями
2. Блог, електронна пошта, хмарне сховище
3. Презентація, електронна пошта, канал на YouTube
4. Канал на YouTube, хмарне сховище, месенджер

КОМПЕТЕНЦІЯ: ВИКОРИСТАННЯ ТА АНАЛІЗ ЦИФРОВИХ РЕСУРСІВ

ДОБІР ЦИФРОВИХ РЕСУРСІВ

28. Ви відкрили на комп'ютері в браузері Google Chrome/Microsoft Edge/Mozilla Firefox статтю. Як знайти ту частину статті, у якій трапляється потрібне вам слово або словосполучення?
Оберіть одну правильну відповідь.
1. В адресному рядку сторінки набрати «find» і слово для пошуку
2. В адресному рядку сторінки набрати «go» і слово для пошуку
3. Натиснути Ctrl+F
4. Натиснути Ctrl+A

29. Педагогічний працівник часто використовує у своїй роботі іноземні джерела. Оберіть послідовність дій для встановлення доповнення браузера з перекладу іншомовних сторінок:
1. відкрити налаштування браузера та обрати пункт «Розширення». 2. відкрити вебмагазин та в полі пошуку вписати назву, наприклад «Google Перекладач». 3. у переліку знайдених обрати потрібне розширення та натиснути кнопку «Додати в Chrome». 4. підтвердити свій вибір і закріпити кнопку автоматичного перекладу.
1. 2, 1, 3, 4
2. 4, 1, 2, 3
3. 1, 2, 3, 4
4. 4, 1, 2, 3

30. Ви встановили нову програму на свій комп'ютер та хочете ознайомитись із довідником щодо роботи програми. Виберіть дію, яка допоможе відкрити довідник.
Оберіть одну правильну відповідь.
1. У вікні програми знайти розділ «Довідка» або натиснути кнопку F1
2. Пошукати необхідні матеріали в інтернеті
3. Дослідити папку зі встановленою програмою
4. Знайти файл з назвою програми на комп'ютері

СТВОРЕННЯ ТА МОДИФІКАЦІЯ ЦИФРОВИХ ОСВІТНІХ РЕСУРСІВ

31. Педагогічний працівник потрібно зробити скриншот екрана комп'ютера (ноутбука). Оберіть способи, якими він може це зробити:
1. використати спеціальну програму зі стандартних. 2. використати програму «Скриншот» на своєму комп'ютері. 3. натиснути клавішу PrintScreen/PrtSc на клавіатурі. 4. натиснути клавішу Insert на клавіатурі. 5. встановити спеціальну програму для створення скриншотів.

1. 1, 2, 4
2. 1, 2, 3
3. 1, 3, 5
4. 2, 4, 5

32. Педагогічний працівник на своєму робочому комп'ютері має календарний план на поточний навчальний рік. Як йому на основі наявного зробити календарний план на наступний навчальний рік, не втративши поточний?

1. зробити копію файлу. 2. редагувати наявний файл. 3. скопіювати його та вставити в цей документ нижче. 4. зберегти файл під новим ім'ям. 5. скопіювати все і вставити в новий документ.

1. 1, 2, 4
2. 1, 2, 3
3. 1, 4, 5
4. 2, 4, 6

33. Ви хочете зберегти зміни у відкритому документі в іншому файлі. Яку команду потрібно обрати?

Оберіть одну правильну відповідь.

1. Зберегти
2. Зберегти як...
3. Зберегти копію
4. Зберегти зміни

УПРАВЛІННЯ ТА СПІЛЬНЕ ВИКОРИСТАННЯ ЦИФРОВИХ ОСВІТНІХ РЕСУРСІВ

34. Вам потрібно надіслати папку з документами та відео, що має обсяг понад 25 Мб, декільком колегам. Який спосіб буде найефективнішим для цього?

Оберіть одну правильну відповідь.

1. записати копії папки на CD/DVD-диски та надіслати колегам Новою поштою
2. розмістити папку в хмарному сховищі та надіслати колегам посилання на електронну скриньку
3. прикріпити папку до електронного листа та надіслати
4. надіслати кожен файл окремим електронним листом

35. За допомогою яких цифрових інструментів можна ефективно організувати власний інформаційний простір?

Оберіть одну правильну відповідь.

1. електронна пошта, хмарне сховище, онлайн-календар, сервіс нотаток
2. груповий чат, хмарне сховище, онлайн-календар, канал YouTube
3. сайт, електронна пошта, хмарне сховище, відеоконференції

4. онлайн-календар, відеоконференції, сервіс нотаток, блог

36. Педагогічні працівники, які викладають у кількох класах один предмет, вирішили об'єднати свої зусилля та створити банк планів до уроків. Як їм швидко реалізувати цю ідею?
1. створити групу в соціальній мережі та завантажити плани уроків у групу. 2. створити спільний документ із календарним планом і додати посилання на плани уроків. 3. завантажити плани уроків у спільну папку й узагальнити їхні назви у спільному документі. 4. створити сайт із посиланнями на плани уроків.
1. 1, 2, 3
2. 1, 2, 4
3. 1, 3, 4
4. 2, 3, 4

ЗАХИСТ ЦИФРОВИХ РЕСУРСІВ

37. Батьки здобувача освіти просять ознайомити їх із успішністю за поточний місяць. Ваші дії.
Оберіть одну правильну відповідь.
1. Сфотографувати сторінку журналу та надіслати в месенджер
2. Запросити на зустріч та надати журнал для ознайомлення
3. Відксерити сторінку журналу та вкласти в щоденник здобувача освіти
4. Запропонувати батькам підключитися до електронного щоденника

38. Готуючи добірку матеріалів для здобувачів освіти, педагогічний працівник скопіював статтю з журналу, декілька прикладів із антології та оповідання обсягом 15 сторінок іншого автора. У кінці добірки він склав повну бібліографію використаних джерел. Чи дотримано норми захисту їх авторського права?
Оберіть одну правильну відповідь.
1. так
2. ні, потрібно отримати дозвіл на публікацію статті з журналу
3. ні, потрібно отримати дозвіл на публікацію оповідання
4. ні, потрібно отримати дозвіл на публікацію всіх зазначених джерел
Повернутись назад

39. Установіть порядок оформлення посилання на електронний ресурс, розміщений в інтернеті:
1. [Електронний ресурс]. 2. Назва ресурсу чи сторінки сайту. 3. Режим доступу: посилання на ресурс. 4. Автор ресурсу.
1. 2, 1, 4, 3
2. 2, 3, 4, 3
3. 1, 2, 4, 3
4. 4, 3, 1, 2

КОМПЕТЕНЦІЯ: НАВЧАННЯ ТА ОЦІНЮВАННЯ УЧНІВ

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ УЧНІВ

40. Педагогічний працівник не встигає опублікувати завдання здобувачам освіти на початку асинхронного уроку в Google Класі. Виберіть з переліку, що допоможе розв'язати проблему:
Оберіть одну правильну відповідь.
1. запланувати публікацію завдання у визначений час
2. опублікувати завдання раніше визначеного часу
3. використовувати планувальник завдань
4. запланувати подію в календарі публікацій

41. Здобувачі освіти працюють над створенням спільного проєкту, результати роботи буде розміщено на Google Сайті. Установіть послідовність дій для надання доступу здобувачам освіти для розміщення матеріалів на сайті.
1. Праворуч угорі знайти іконку «Надати доступ іншим». 2. Натиснути кнопку «Готово». 3. У полі «Додайте користувачів і групи» ввести електронну адресу здобувача освіти. 4. Праворуч від електронної адреси обрати «Може редагувати».
1. 1, 2, 3, 4
2. 1, 3, 4, 2
3. 1, 2, 4, 3
4. 3, 4, 1, 2

42. Оберіть цифрові інструменти для презентації роботи групи у проєкті:
1. онлайн-редактор. 2. сайт/блог. 3. електронна пошта. 4. месенджер. 5. соціальна мережа. 6. відеофільм.
1. 1, 3, 5
2. 1, 2, 3
3. 1, 2, 6
4. 3, 4, 5

ІНТЕРАКТИВНЕ ТА АКТИВНЕ НАВЧАННЯ УЧНІВ. ОРГАНІЗАЦІЯ СПІВПРАЦІ УЧНІВ

43. Ви плануєте організувати спільну роботу здобувачів освіти в одному документі для накопичення та візуалізації ідей із певного питання. Який сервіс із запропонованих не дозволить це зробити?
Оберіть одну правильну відповідь.
1. Електронна пошта
2. Онлайн-дошка

3. Google Документ
4. Інтелект-карти

44. Ви вирішили організувати свято та провести попереднє дослідження сімейних традицій класу. Установіть правильну відповідність між інструментами та їх застосуванням для проведення дослідження:
1. Онлайн-дошка. 2. Google Форма. 3. Текстовий (графічний) редактор. A. отримання відповідей на питання анкети, узагальнення результатів опитування. B. розміщення інформації про дослідження, зображення, посилання на анкету з питаннями. C. створення оголошення про свято, запрошення для гостей.
1. 1-B, 2-A, 3-C
2. 1-A, 2-B, 3-C
3. 1-C, 2-B, 3-A
4. 1-C, 2-A, 3-B

45. Установіть відповідність між цифровими інструментами та їх можливим використанням в освітньому процесі:
1. для спілкування. 2. для обміну матеріалами. 3. для планування спільної роботи. 4. для презентації результатів. A. хмарне сховище. B. календар. C. сайт. D. месенджер.
1. 1-A, 2-B, 3-D, 4-C
2. 1-A, 2-C, 3-D, 4-B
3. 1-C,2-D, 3-B, 4-A
4. 1-D, 2-A, 3-B, 4-C

ІНДИВІДУАЛІЗАЦІЯ НАВЧАННЯ ТА ДИФЕРЕНЦІАЦІЯ

46. Педагогічний працівник бажає відстежувати алгоритм міркування здобувачів освіти під час опрацювання певного матеріалу. Які цифрові сервіси найдоцільніше для цього використати?
Оберіть одну правильну відповідь.
1. сервіси онлайн-тестування
2. ментальні карти
3. інтерактивні робочі аркуші
4. сервіси для створення закладок

47. Якими цифровими засобами педагогічний працівник може забезпечити індивідуалізацію освітнього процесу?
1. надавати навчальні матеріали в цифровому вигляді. 2. пропонувати здобувачам освіти для виконання завдання із застосуванням цифрових інструментів. 3. перевіряти рівень засвоєння матеріалу здобувачів освіти одразу після заняття. 4. пропонувати здобувачам освіти різнорівневі завдання. 5.

дозволити здобувачам освіти самостійно обирати цифрові інструменти для виконання завдань.
1. 1, 2, 5
2. 1, 2, 4
3. 1, 4, 5
4. 3, 4, 5

48. Який цифровий сервіс може використати педагогічний працівник для диференціації навчання здобувачів освіти?
Оберіть одну правильну відповідь.
1. відео на YouTube
2. інтерактивні робочі аркуші
3. сервіс відеоконференцій
4. миттєве опитування

ІНКЛЮЗИВНЕ НАВЧАННЯ

49. Цифрові технології в інклюзивному навчанні не можна використати як:
Оберіть одну правильну відповідь.
1. компенсаторний засіб
2. комунікаційний засіб
3. дидактичний засіб
4. інклюзивний засіб
Повернутись назад

50. До асистивних (допоміжних) технологій належать:
1. пристрої для читання з екрану. 2. клавіатури зі спеціальними можливостями. 3. персональні комп'ютери. 4. програми для голосового введення. 5. аудіогарнітура.
1. 1, 2, 3
2. 1, 2, 4
3. 1, 4, 5
4. 3, 4, 5

51. У класі навчаються здобувачі освіти з порушенням зору. Які додатки може використати на уроці педагогічний працівник, щоб допомогти здобувачам освіти навчатися?
1. Voice Dream Reader. 2. Екранний диктор. 3. Media Player. 4. FineReader. 5. Екранна лупа.
1. 1, 2, 5
2. 1, 2, 3
3. 1, 4, 5
4. 3, 4, 5

АНАЛІЗ ТА ІНТЕРПРЕТАЦІЯ ЦИФРОВИХ ДАНИХ. ЗАБЕЗПЕЧЕННЯ ЗВОРОТНОГО ЗВ'ЯЗКУ І ОЦІНЮВАННЯ УЧНІВ. ОРГАНІЗАЦІЯ САМОКОНТРОЛЮ УЧНІВ

52. Який символ потрібно використати в сучасних цифрових ресурсах (месенджери, ФБ, спільні документи Гугл та інші), щоб адресувати повідомлення конкретній людині?
Оберіть одну правильну відповідь.
1. @
2. #
3. *
4. $

53. Під час організації спілкування зі здобувачами освіти педагогічний працівник вагається з вибором засобів. Установіть відповідність між сервісами для спілкування та їх можливим використанням:
1. Viber. 2. Discord. 3. Facebook.4. Zoom. A. Кімната для аудіоконсультацій. B. Чат для оголошень та сповіщень. C. Кімната для відеоконференцій. D. Група для спілкування.
1. 1-A, 2-C, 3-B, 4-D
2. 1-B, 2-A, 3-D, 4-C
3. 1-B, 2-C, 3-A, 4-D
4. 1-A, 2-B, 3-D, 4-C

54. Вашим здобувачам освіти подобається працювати з QR-кодами. Який сервіс можна використати для проведення оцінювання здобувачів освіти з QR-кодами?
Оберіть одну правильну відповідь.
1. plickers
2. kahoot
3. quizizz
4. quizlet

КОМПЕТЕНЦІЯ: РОЗВИТОК ЦИФРОВОЇ КОМПЕТЕНТНОСТІ

ІНФОРМАЦІЙНА ТА МЕДІАГРАМОТНІСТЬ

55. У соціальній мережі ви побачили оголошення. Ваші дії:
З метою запобігання поширенню коронавірусу COVID-19, забезпеченню безпечних умов навчання для здобувачів освіти, керуючись рішенням Державної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій від 20.03.2021 Кабінет Міністрів України постановляє заборонити відвідування закладів освіти здобувачами освіти з

01.04.2021 по 31.05.2021 та перенести освітній процес на червень-липень 2021 року.
1. поширю цю інформацію, адже дописувач спирається на офіційні документи, тож це правдива інформація
2. перевірю інформацію в офіційних джерелах, у разі підтвердження поширю
3. запитаю про достовірність інформації в директора (завуча, методиста), у разі підтвердження поширю
4. перевірю достовірність на освітніх форумах

56. Відома та правдива інформація, яка подана в такий спосіб, щоб ввести в оману, – це:
Оберіть одну правильну відповідь.
1. фейк
2. маніпуляція
3. дезінформація
4. упередження

57. Ви прочитали інформацію, що викликає певні сумніви в її правдивості. Яку послідовність дій вам слід виконати, щоб її перевірити? Установіть відповідність:
1. Відшукати першоджерело походження інформації. 2. Проаналізувати надійність першоджерела походження інформації. 3. Перевірити факти на достовірність та об'єктивність. 4. Виокремити факти.
1. 1, 2, 3, 4
2. 2, 3, 1, 4
3. 1, 2, 4, 3
4. 4, 1, 2, 3

ВІДПОВІДАЛЬНЕ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА СЕРВІСІВ

58. Явище залякування особистості для її повного підпорядкування своїм інтересам, компрометації називається:
Оберіть одну правильну відповідь.
1. фішинг
2. спамінг
3. булінг
4. тролінг

59. Оберіть фактори, що не належать до загроз інформаційної безпеки:
Оберіть одну правильну відповідь.
1. пожежа в серверній кімнаті
2. пошкодження пристроїв інформаційної системи
3. несанкціоноване отримання особистих даних іншого користувача

4. знищення та спотворення даних

60. Для безпечної роботи відстань від очей до екрану монітора має становити:
Оберіть одну правильну відповідь.
1. 30-40 см
2. 50-60 см
3. 60-70 см
4. близько 1 м

ВИРІШЕННЯ ПРОБЛЕМ ЗА ДОПОМОГОЮ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА СЕРВІСІВ

61. Педагогічний працівник бажає показати здобувачам освіти відео, що збережене в нього на флешці, але на комп'ютері в класі під час запуску відео з'явилося повідомлення «Не вдалося відтворити файл. Формат не підтримується». Що потрібно зробити?
1. Змінити формат файлу, використовуючи програму-конвертор. 2. Перейменувати файл, змінивши розширення. 3. Встановити на комп'ютер іншу програму відтворення відео. 4. Встановити програму-кодек відеофайлів. 5. Завантажити файл на комп'ютер.
1. 1, 4, 5
2. 1, 2, 5
3. 1, 3, 4
4. 5, 4, 3

62. Ви вирішили видалити з комп'ютера програму, якою не користуєтесь. Яку послідовність дій для цього потрібно зробити?
1. відкрити панель керування операційної системи. 2. обрати «Програми та компоненти». 3. відкрити меню «Пуск». 4. обрати програму, яку потрібно видалити. 5. натиснути кнопку «Видалити».
1. 1, 2, 3, 4, 5
2. 2, 3, 4, 4, 5
3. 5, 4, 1, 3, 2
4. 3, 1, 2, 4, 5

63. Виберіть правильні твердження, пов'язані з роботою у спеціальній програмі для інтерактивної дошки:
Оберіть одну правильну відповідь.
1. результат роботи можна зберегти в декількох форматах
2. результатом роботи можна зберегти виключно у графічному форматі
3. результат роботи зберігається частково, лише те, що вміщується
4. результат роботи зберігається автоматично на комп'ютер

Виробничо-практична продукція

ПІДГОТОВКА ВИКЛАДАЧА ЗАКЛАДУ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ ДО ЦИФРОВОЇ БЕЗПЕКИ У ПОВОЄННИЙ ЧАС:

методичні рекомендації

(електронне видання)

Літературний редактор: Гуменна Л.С.
Технічний редактор: Майборода Л. А.

Гарнітура Times New Roman.
Обл.-вид. арк. 5,67.

Видано ТОВ «Юрка Любченка»
e-mail: u19-07@ukr.net
тел. 098-444-06-68
м. Київ, просп. Берестейський, 50.
Свідоцтво суб'єкта видавничої справи ДК № 4685 від 06.03.2014