УДК 378.011.2:004.056].011.33
DOI: https://doi.org/10.35387/od.1(23).2023.98-109

Петренко Лариса Михайлівна *– доктор педагогічних наук, професор, завідувач відділом теорії і практики педагогічної освіти Інституту педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України*

Petrenko Larysa *– Dr. hab. of Pedagogical Sciences, Full Professor, Head of the Department of Theory and Practice of Pedagogical Education of the Ivan Ziaziun Institute of Pedagogical and Adult Education of the National Academy of Educational Sciences of Ukraine*

ORCID iD: http://orcid.org/0000-0002-7604-7273
E-mail: laravipmail@gmail.com

ЦИФРОВА БЕЗПЕКА В СТУКТУРІ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ МАЙБУТНЬОГО ВИКЛАДАЧА ПЕДАГОГІЧНОГО ЗАКЛАДУ ВИЩОЇ ОСВІТИ: ЗМІСТОВИЙ КОМПОНЕНТ

Анотація. *У статті здійснено аналіз наукових праць з проблеми формування компетентності з цифрової безпеки майбутніх фахівців. Виявлено суперечності, що існують між необхідністю дотримуватися цифрової безпеки в процесі педагогічної, науково-педагогічної діяльності та недостатньою розробленістю й обґрунтуванням змісту компетентності з цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти. Акцентовано увагу на необхідності визначення структури і змісту компетентності з цифрової безпеки майбутніх викладачів педагогічної вищої освіти як складника їхньої цифрової компетентності, що зумовлено інтенсивністю кібератак у національному кіберпросторі під час повномасштабної війни проти російської навали, та актуалізовано потребою у фахівцях із сформованою цифровою компетентністю для відновлення і технологічного розвитку країни у післявоєнний період. Установлено, 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; захист здоров'я та благополуччя; захист довкілля. На основі вивчення результатів наукових досліджень, експертних оцінок визнаних експертів з проблем цифрової безпеки, практичного досвіду визначено й обґрунтовано зміст кожної окремої компетентності. Одержані результати можуть використовуватись для розроблення навчальних дисциплін в рамках освітньо-професійних програм галузі знань 01 Освіта/педагогіка,*

спеціальності 011 Освітні, педагогічні науки, окремих модулів, а також для саморозвитку викладачів закладів вищої освіти та ін.

Ключові слова: *цифрова компетентність; компетентність з цифрової безпеки; майбутній викладач; педагогічний заклад вищої освіти; зміст; структура; професійна підготовка.*

Petrenko Larysa

DIGITAL SECURITY WITHIN THE STRUCTURE OF DIGITAL COMPETENCE OF THE FUTURE TEACHER OF A PEDAGOGICAL INSTITUTION OF HIGHER EDUCATION: CONTENT COMPONENT

Abstract*. The article analyzes scientific works on the problem of forming competence in digital security of future specialists. The contradictions that exist between the need to observe digital security in the process of pedagogical and scientific-pedagogical activities as well as the insufficient development and justification of the content of digital security competence of future teachers of pedagogical institutions of higher education, have been revealed. Attention is focused on the need to determine the structure and content of the digital security competence of future teachers of pedagogical higher education as a component of their digital competence, which is caused by the intensity of cyberattacks in the national cyberspace during the full-scale war against the Russian invasion, and actualized by the need for specialists with formed digital competence to restore and technological development of the country during the post-war period. It was found out that, according to the Digital Competence Framework for citizens of Ukraine, the structure of digital security competence of future teachers of pedagogical institutions of higher education consists of a set of competencies: protection of devices and secure connection to the Internet; protection of personal data and privacy, safety on the Internet; protection of consumer's personal rights against fraud and abuse; protection of health and well-being; environmental Protection. Based on the study of the results of scientific research, expert evaluations of recognized experts on digital security issues and practical experience, the content of each individual competence was determined and substantiated. The obtained results can be applied for the development of educational disciplines within the educational and professional programs of the field of knowledge 01 Education/pedagogy, speciality 011 Educational, pedagogical sciences, individual modules, as well as for the self-development of teachers of higher education institutions and others.*

Key words: *digital competence; digital security competence; future teacher; pedagogical institution of higher education; content; structure; professional training.*

Постановка проблеми, її актуальність. Громадяни України набувають унікальний досвід жити і діяти в умовах війни, протистояти фізичним загрозам та інформаційним атакам і спецопераціям. Зважаючи

на масштаби означеної проблеми, актуалізується необхідність формування навичок цифрової безпеки в професійній діяльності майбутнього викладача педагогічного закладу вищої освіти (Султанова & Прокоф'єва, 2022) як в умовах ведення воєнних дій проти російського агресора, так і в повоєнний час, оскільки відновлення національної економіки й подальша цифровізація суспільства, темпи якої зростають, потребують фахівців зі сформованою цифровою компетентністю, здатних протистояти різним викликам глобального світу.

Аналіз актуальних досліджень і публікацій. Аналіз бази даних Національного репозиторію академічних текстів (НРАТ) дав змогу виявити за останні 20 років 142 дисертаційні роботи з різних галузей науки і 31-ї спеціальності за ключовою термосполукою «інформаційна безпека», з них шість дисертацій – у галузі знань 01 Освіта/Педагогіка – присвячені проблемам: професійної підготовки майбутніх фахівців інформаційної безпеки (С. Воскобойніков, Ю. Іванчук, М. Коляда, Л. Конопленко, О. Синекоп); забезпечення інформаційної безпеки старшокласників у комп'ютерно орієнтованому навчальному середовищі (В. Ковальчук). Публікації, що знаходяться у відкритому доступі, здебільшого висвітлюють результати досліджень у галузі знань: 12 Інформаційні технології; 25 Воєнні науки, національна безпека, безпека державного кордону; 26 Цивільна безпека. Водночас необхідно звернути увагу на те, що з використанням терміносполуки «цифрова безпека» в базі даних НРАТ виявлено лише дві дисертаційні роботи: в одній з них відображаються результати вивчення проблеми економічної безпеки підприємницької діяльності в умовах розвитку цифрової економіки (О. Онофрійчук), в іншій – моделювання та управління інформаційною безпекою підприємства в умовах цифрової трансформації (О. Урденко). Проте цифрова безпека представлена в них контекстно.

Однак з початком пандемії COVID-19 та переходом на дистанційне і змішане навчання з березня 2020 року питання цифрової безпеки актуалізувалось в галузі вищої освіти (Sultanova, Milto, and Zheludenko, 2021, p. 132-147), а з початком воєнного стану посідають пріоритетне місце на національному рівні. Свідченням цьому є прийняття на державному рівні низки документів стратегічного характеру: «Про Стратегію кібербезпеки України» (2016; 2021); «Про Доктрину інформаційної безпеки України» (2017); «Про План реалізації Стратегії кібербезпеки України» (2022). У них здійснено розподіл відповідальності за забезпечення кібербезпечної цифрової трансформації між урядом, підприємствами та громадянами; охарактеризовано нові ризики та загрози для всіх учасників освітнього процесу (Петренко, 2023).

Необхідно зазначити, що Радою Європи та іншими країнами світу приділяється значна увага кібербезпеці. Так, прийнято і підписано Конвенцію про кіберзлочинність; Політичну програму Цифрового десятиліття з конкретними цілями та завданнями до 2030 року, спрямовану на цифрову трансформацію Європи; Декларацію про цифрові права та принципи, в якій представлено зобов'язання ЄС щодо безпечної та стійкої

цифрової трансформації; Цифровий порядок денний на 2020-2030 рр., спрямований на створення безпечних цифрових просторів і послуг, зміцнення цифрового суверенітету Європи.

Вивченню проблеми цифрової компетентності фахівців різних галузей економіки та її розвитку приділяють увагу вітчизняні учені: С. Баценко, І. Гадяк, А. Зелінська, Н. Куриленко, С. Лавриненко, В. Павленко, О. Семеног, Т. Семигіна, Л. Тарасович, В. Федюк та ін. Науковий інтерес для цього дослідження становлять роботи Ф. Олайя, (F. Olayah), Е.А. Анаам (E. A. Anaam), М.А. Бахтан (M.A. Bakhtan), Дж. Портільо (J. Portillo), У. Гарай (U. Garay), Е. Техада (E. Tejada) та ін.

Відтак тема інформаційної безпеки залишається актуальною для вчених різних галузей знань і спеціальностей. Крім цього, цифрова безпека у професійній діяльності освітян як педагогічна проблема розглядається в наукових публікаціях В. Бондаренко (умови та засоби формування навичок інформаційної безпеки майбутніх учителів), Г. Генсерук (міжнародні рамки цифрової компетентності майбутніх учителів), В. Олексюка та О. Олексюк (стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики), В. Плаксієнко (проєктування рамки цифрової компетентності майбутніх економістів), М. Прокоф'євої та Л. Султанової (цифрова безпека в галузі вищої освіти). Принагідно зауважимо, що в цих публікаціях висвітлюються лише загальні питання формування цифрової компетентності й обґрунтовано необхідність забезпечення цифрової безпеки у закладах вищої освіти. Водночас публікації, в яких здійснюється аналіз стану сформованості компетентностей з інформаційної безпеки майбутніх учителів, свідчать про необхідність цілісного вивчення заявленої проблеми. Безумовно, «зазначений процес повинен бути безперервним і здійснюватися упродовж усього життя» (Олексюк & Олексюк, 2017), а відтак добір і обґрунтування змістового компонента цифрової безпеки як складника цифрової компетентності майбутніх викладачів педагогічної вищої освіти наразі потребує окремого вивчення.

Мета статті полягає у визначенні та обґрунтуванні змісту цифрової безпеки у структурі цифрової компетентності майбутніх викладачів педагогічної вищої освіти.

Виклад основного матеріалу дослідження. Період суворого карантину з березня 2020 р., який було оголошено у зв'язку з початком пандемії COVID-19, зумовив перехід національних освітніх систем на дистанційне навчання. Це, в свою чергу, спонукало педагогічні спільноти до активного опанування цифровими навичками і вміннями, аби відреагувати на зміни реальності, адже необхідно було в короткий проміжок часу організувати відповідний освітній процес. У зв'язку з цим виявилися суперечності між необхідністю дотримуватися цифрової безпеки в процесі педагогічної, науково-педагогічної діяльності та недостатньою розробленістю й обґрунтуванням змісту компетентності з цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти. Постала проблема з необхідністю розроблення ключових аспектів DigCompEdu – Цифрової рамки компетентностей, в основу якої було покладено

європейську концептуально-еталонну модель цифрових компетентностей для громадян DigComp 2.1: The Digital Competence Framework for Citizens та рекомендації у сфері цифрових компетентностей від європейських та міжнародних інституцій (Опис рамки цифрової компетентності для громадян України, 2021).

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. Ця сфера охоплює комплекс компетентностей, який можна розглядати як структуру компетентності 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 (C_4), 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 (Опис рамки цифрової компетентності для громадян України, 2021; Султанова & Прокоф'єва, 2022, с. 110). У національному тесті «Цифрограм» (https://osvita.diia.gov.ua/digigram) окремим блоком виділено положення про безпеку в цифровому суспільстві, що стосуються, насамперед, цифрової грамотності вчителів. Розглядаються питання: в 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? Пропонується вибрати відповідь із наведених варіантів, поданих під кожним питанням. На наш погляд, ці питання в Цифрограмі відображають зміст включених компетентностей до сфери C_4 не повною мірою. У зв'язку з цим і відповідно до зазначеної теми дослідження маємо визначити зміст компетентностей, що входять до сфери «безпека у цифровому суспільстві».

У наукових публікаціях учені підкреслюють, що 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. Водночас завжди необхідно мати на увазі, що цифрова безпека складається із трьох компонентів – технологій, людей і процесів. Майбутні викладачі педагогічних закладів вищої освіти використовують у процесі навчання та у професійній діяльності інформаційні (цифрові) технології, що зумовлює необхідність визначення рівня сформованості в них умінь і навичок цифрової безпеки.

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,* то 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 (Лахно, Каламан, Ягалієва, Криворучко, Десітко, Цюцюра & Цюцюра, 2022).

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» (Мальцева, Черниш & Штонда, 2022). 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.

Для громадського сектора 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); повторне використання паролів (не рекомендується користуватись одним паролем на різних сайтах); скидання паролю на пошту, прив'язану до акаунта; 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 з комерційними фішингами. Як зазначають експерти, найбільш поширеними низько-технологічними методами залишаються 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. 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 (Комп'ютерна допомога, 2023).

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 (Безоплатна правова допомога, 2023).

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, – привабливу пропозицію. Найчастіше – це отримати безкоштовно те, що коштує значних грошей» (Бондарєв, 2023). 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 (Петренко, 2023). З початком повномасштабної війни в Україні ця проблема набула ще більшої значущості, адже: «Кожен і кожна є бійцем інформаційного фронту сьогодні», – наголошує експертка з цифрової безпеки А. Апетик (Як захистити себе онлайн? Поради від експертки з цифрової безпеки, 2023).

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 у 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 вводити дані своєї карти, якщо надійшов такий запит після оновлення на смартфоні (Безоплатна правова допомога, 2023).

На наш погляд, важливо акцентувати увагу на дефініції «особисті (персональні) дані» в контексті цифрової безпеки. За визначенням експерток А. Апетик та І. Купчинської, особистими (персональними) даними, за якими

полюють злочинці, є вся та інформація, що може конкретно ідентифікувати особу. Це: 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. До персональних даних також належить інформація про місце перебування, IP-адреса та онлайн-ідентифікатор.

Важливими навичками й уміннями у змісті цифрової безпеки є *захист здоров'я та благополуччя* в процесі роботи з комп'ютером (смартфоном). Здебільшого ця тема висвітлюється відносно загрози здоров'ю дітей при роботі з комп'ютером. Оскільки комп'ютер сьогодні сприймається не тільки як робоче пристосування, але й як «права рука» фахівця в галузі 011 Освіта, педагогіка, то питання наслідків постійного контактування з комп'ютером є актуальним, зокрема наразі, коли викладач, починаючи з 2020 року й донині працює щодня онлайн. Вважається, що із застосуванням комп'ютера, як і з іншими приладами, пов'язані потенційні загрози для нашого здоров'я. Серед них 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 (Інтернет. Шкода здоров'ю, 2023).

Ще одним складником 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 у певному регіоні без впливу людини; 3) оточуючі люди щодо особи (Вільний тлумачний словник, 2013-2018). 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» (Цивільний кодекс України, 2023).

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. (Словник української мови, 1970-1980).

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 (ст. 293 Цивільного кодексу України). 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 (Створення екостійкого офісу. Xerox, 2023). На жаль, у сучасних закладах вищої освіти увага цим питанням цифрової безпеки майже зовсім не приділяється.

Висновки і перспективи подальших досліджень. Підсумовуючи сказане, зазначимо, що заявленій проблемі в галузі знань 01 Освіта/Педагогіка приділяється 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, що зумовлює необхідність здійснення окремого дослідження. 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; 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.

Перспективи подальших досліджень розглядаємо в розробці технологій навчання цифровій безпеці майбутніх викладачів педагогічних закладів вищої освіти.

Список використаних джерел

Безоплатна правова допомога. (Б. р.). URL: https://wiki.legalaid.gov.ua/index.php/Шахрайство_при_покупках_і_продажах_в_мережі_Інтернет

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-shahrajstva-75741.html

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

Інтернет. Шкода здоров'ю. URL: https://sites.google.com/view/bezpecnyj-internet/загрози-в-інтернеті/шкода-здоровю

Комп'ютерна допомога. URL: http://pro-computer.pp.ua/177-yak-zahistiti-elektronnu-poshtu-vd-zlomu-5-prostih-porad.html

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., 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.

Олексюк В.П., Олексюк О.Р. (2017). Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики. *Інформаційні технології і засоби навчання*, *62*(6), 277–291. DOI: https://doi.org/10.33407/itlt.v62i6.1906.

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.

Петренко, Л.М. (2023). Цифрова безпека в професійній діяльності майбутніх викладачів педагогічних закладів вищої освіти: нормативно-правовий аспект. *Вісник післядипломної освіти. Серія «Педагогічні науки»*, 24 (53), 138-152. DOI https://doi.org/10.58442/2218-7650-2023-24(53)-138-152.

Петренко, Л.М. (2023). Цифрова безпека у професійній діяльності майбутнього викладача педагогічної освіти. Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій: матеріали III Всеукраїнської науково-практичної конференції (7 квітня 2023, Глухів, Україна), 291-294. URL: https://lib.iitta.gov.ua/735042/.

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.

Цивільний кодекс України. Документ 435-IV, чинний, ред. від 22.05.2023 р. URL: https://zakon.rada.gov.ua/laws/show/435-15?find=1&text=%D1%81%D1%82+293#Text.

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.

Sultanova, L., Milto, L. and Zheludenko, M. (2021). The Impact of the Covid-19 Pandemic on the Development of Higher Education, *Acta Paedagogica Vilnensia*, 46, 132-147. DOI: 10.15388/ActPaed.46.2021.9.

References (translated and transliterated)

Bezoplatna pravova dopomoha. Shakhraistvo pry pokupkakh i prodazhakh v merezhi Internet [Free legal assistance. Internet shopping and selling fraud]. WikiLegalAid. [in Ukrainian].

Bondariev, O. Kydaly-onlain. Nazvano naibilsh poshyreni sposoby internet-shakhraistva [Kydali-online. The most common methods of Internet fraud are named]. NV [in Ukrainian].

Internet. Shkoda zdoroviu [Internet. It's bad for your health]. [in Ukrainian].

Kompiuterna dopomoha. Yak zakhystyty elektronnu poshtu vid zlomu – 5 prostykh porad. [in Ukrainian].

Lakhno, V., Kalaman, Ye., Yahaliieva B., Kryvoruchko, O., Desitko, A., Tsiutsiura, S., & Tsiutsiura, M. (2022). Model zakhystu lokalnoi merezhi navchalnoho zakladu servernoi systemy virtualizatsii [The model of protection of the local network of the educational institution of the virtualization server

system]. *Kiberbezpeka: osvita, nauka, tekhnika: elektronne fakhove naukove vydannia – Cybersecurity: education, science, technology: electronic professional scientific publication*, 2 (18), 6–23 [in Ukrainian].

Maltseva, I., Chernysh, Yu., & Shtonda, R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny [Analysis of some cyber threats in the conditions of war]. *Kiberbezpeka: osvita, nauka, tekhnika: elektronne fakhove naukove vydannia – Cybersecurity: education, science, technology: electronic specialized scientific publication,* 4 (16), 37–44 [in Ukrainian].

Oleksiuk, V.P., Oleksiuk, O.R. (2017). Stan sformovanosti kompetentnostei z informatsiinoi bezpeky maibutnikh uchyteliv informatyky [The state of formation of information security competencies of future computer science teachers]. *Informatsiini tekhnolohii i zasoby navchannia – Information technologies and teaching aids*, 62 (6), 277–291 [in Ukrainian].

Opys ramky tsyfrovo kompetentnosti dlia hromadian Ukra ny [Description of the framework of digital competence for citizens of Ukraine]. 2021. [in Ukrainian].

Petrenko, L.M. (2023). Tsyfrova bezpeka u profesiinii diialnosti maibutnoho vykladacha pedahohichnoi osvity [Digital security in the professional activity of the future teacher of pedagogical education]. Rozvytok pedahohichnoi maisternosti maibutnoho pedahoha v umovakh osvitnikh transformatsii: materialy III Vseukrayins'koyi naukovo-praktychnoyi konferentsiyi (7 kvitnia 2023, Hlukhiv, Ukraina), 291-294 [in Ukrainian].

Petrenko, L.M. (2023). Tsyfrova bezpeka v profesiinii diialnosti maibutnikh vykladachiv pedahohichnykh zakladiv vyshchoi osvity: normatyvno-pravovyi aspekt [Digital security in the professional activity of future teachers of pedagogical institutions of higher education: regulatory and legal aspect]. *Visnyk pisliadyplomnoi osvity - Bulletin of postgraduate education*. Seriia «Pedahohichni nauky», 24 (53), 138-152 [in Ukrainian].

Slovnyk ukrainskoi movy. Akademichnyi tlumachnyi slovnyk (1970-1980) [Dictionary of the Ukrainian language. Academic explanatory dictionary]. [in Ukrainian].

Stvorennia ekostiikoho ofisu [Creating an eco-friendly office]. Xerox [in Ukrainian].

Sultanova L., Milto L., & Zheludenko M. (2021). «The Impact of the Covid-19 Pandemic on the Development of Higher Education», Acta Paedagogica Vilnensia, 46, 132-147 [in English].

Sultanova, L. & Prokofieva, M. (2022). Tsyfrova bezpeka v haluzi vyshchoi osvity [Digital security in higher education]. *Osvita doroslykh: teoriia, dosvid, perspektyvy – Adult education: theory, experience, perspectives*, 21 (1), 106-117 [in Ukrainian].

Tsyvilnyi kodeks Ukrainy [The Civil Code of Ukraine]. Dokument 435-IV, chynnyi, red. vid 22.05.2023 r. [in Ukrainian].

Vilnyi tlumachnyi slovnyk. Novitnii onlainovyi slovnyk ukrainskoi movy 2013-2018 [Free explanatory dictionary. The newest online dictionary of the Ukrainian language 2013-2018]. dovkillia – Vilnyi tlumachnyi slovnyk ukrainskoi movy (sum.in.ua) [in Ukrainian].

Yak zakhystyty sebe onlain? Porady vid ekspertky z tsyfrovoi bezpeky [How to protect yourself online? Tips from a digital security expert]. UNDP. [in Ukrainian].