DOI https://doi.org/10.58442/2218-7650-2023-24(53)-138-152
УДК 378.6:37].091.12.011.3-051:004.56:34

Петренко Лариса Михайлівна,
доктор педагогічних наук, професор,
завідувач відділу педагогічної освіти і освіти дорослих
Інституту педагогічної освіти і освіти дорослих
імені Івана Зязюна НАПН України.
Київ, Україна.
https://orcid.org/0000-0002-7604-7273
laravipmail@gmail.com

ЦИФРОВА БЕЗПЕКА В ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ МАЙБУТНІХ ВИКЛАДАЧІВ ПЕДАГОГІЧНИХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ

Анотація. Автором розглянуто низку нормативних, організаційних, інструктивних та інформаційних документів з питань цифрової безпеки суспільства, особи і держави, прийнятих на міжнародному і державному рівнях, систематизовано їх в хронологічному порядку, схарактеризовано в контексті підготовки майбутніх викладачів педагогічних закладів вищої освіти для професійної діяльності в цифровому суспільстві. Виявлено і висвітлено основні положення розподілу відповідальності за забезпечення кібербезпечної цифрової 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 медіа-контенту і соціальних мереж, хейтинг та безліч інших питань; доведено необхідність формування навичок цифрової безпеки у суб'єктів освітнього процесу. Висвітлено структуру цифрової безпеки в складі цифрової 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. Розкрито можливості використання представлених у статті документів з політики цифрової безпеки для професійної підготовки майбутніх викладачів педагогічних закладів вищої освіти: проектування політики (на рівні закладу вищої освіти) із цифрової

https://doi.org/10.58442/2218-7650-2023-24(53)

безпеки інформаційно-освітнього середовища; створення програм навчання, тренінгів, воркшопів з формування навичок цифрової безпеки майбутніх викладачів педагогічних закладів вищої освіти; тестування інформаційної системи закладу вищої освіти; різні позааудиторні заходи: семінари, конференції, олімпіади, конкурси, аналітичні звіти, просвітницька діяльність в регіоні тощо.

Ключові слова: майбутній викладач, педагогічний заклад вищої освіти, цифрова безпека, цифрова компетентність, нормативно-правове забезпечення, кіберзагрози, кіберзлочинність, інформаційна війна.

ВСТУП / INTRODUCTION

Постановка проблеми. В умовах розвитку цифрового суспільства, особливо під час повномасштабної війни, ландшафт загроз постійно розширюється та постають нові виклики, які вимагають адаптованих та інноваційних відповідей. У зв’язку з цим та усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується, актуальності набуває формування навичок цифрової безпеки усіх громадян, в тому числі майбутніх викладачів закладів педагогічної вищої освіти у процесі професійної підготовки, що обґрунтовано в низці документів, прийнятих як на міжнародному, так і на державному рівні в Україні.

Аналіз останніх досліджень та публікацій. Проблеми інформаційної безпеки тривалий час були у центрі наукових інтересів вітчизняних учених і науково-педагогічних працівників військових вищих закладів освіти, а їх результати та досвід формування й розвитку навичок інформаційної безпеки не оприлюднювались. Проте з розширенням доступу до Інтернету, експоненціальним зростанням обсягів інформації (друга половина ХХ століття) питання інформаційної безпеки, а пізніше – цифрової безпеки у галузі освіти почали привертати увагу учених-педагогів. Особливо ця тема актуалізувалась з початком російської агресії в Україну в 2014 році. З часом її дослідження активізувалось у зв’язку з переходом на дистанційне і змішане навчання в період пандемії SARS-CoV2 (COVID-19) [1].

За останні 20 років українськими ученими здійснено дослідження різних наукових тем з проблем інформаційної безпеки в різних галузях. Одержані результати відображені в 142 дисертаційних роботах (за даними пошуку з використанням ключових слів «інформаційна безпека» в Національному репозиторію академічних текстів). Такі дослідження в

https://doi.org/10.58442/2218-7650-2023-24(53)

галузі знань 01 Освіта/Педагогіка здійснили: С. Воскобойніков (2016), Ю. Іванчук (2013), М. Коляда (2012), Л. Конопленко (2016), О. Синекоп (2011), В. Ковальчук (2012).

Тема цифрової безпеки в професійній діяльності викладачів педагогічних закладів вищої освіти порушується у 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 вчителя в 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. Прокофєвої 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.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Метою статті є огляд законодавчих документів, прийнятих на вітчизняному і міжнародному рівнях, як нормативно-правового забезпечення та організаційно-методичного супроводу формування навичок цифрової безпеки у майбутніх викладачів педагогічних закладів вищої освіти.

Відповідно до зазначеної мети у статті поставлено такі ***завдання***:

- Проаналізувати документи (конвенції, стратегії, доктрини, резолюції, рекомендації, звіти, інформаційні бюлетені тощо) з питань політики цифрової безпеки, прийняті Європарламентом.
- Узагальнити і систематизувати документи (концепції, доктрини, стратегії, плани тощо) з питань політики цифрової безпеки, прийняті на державному рівні; здійснити опис основних положень у контексті підготовки майбутніх викладачів педагогічних закладів вищої освіти.
- Схарактеризувати можливості використання представлених у статті документів з політики цифрової безпеки для професійної підготовки майбутніх викладачів педагогічних закладів вищої освіти.

https://doi.org/10.58442/2218-7650-2023-24(53)

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ / THE THEORETICAL BACKGROUNDS

Дане дослідження ґрунтується на основних ідеях теорії інформації, теорії розвитку інформаційного суспільства [1], [3], ідеях цифровізації вищої освіти [2], основних нормативно-правових засадах цифрової безпеки суспільства [7]–[14], методологічних підходах професійного розвитку молоді й студенів [15], принципах протидії кіберзагрозам [4], [6].

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

Досягнення мети дослідження уможливлено внаслідок застосування комплексу методів: пошуку інформації з використанням пошукових систем, інформаційних урядових і парламентських платформ, баз даних і вебсайтів за ключовими словами; контент-аналіз нормативно-правових документів, аналітичних матеріалів, інструктивних й інформаційних матеріалів та їх формалізації, узагальнення і розроблення пропозицій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESULTS OF THE RESEARCH

Розвиток цифрової компетентності майбутніх викладачів закладів вищої педагогічної освіти є важливим завданням, про що йдеться у схваленій Кабінетом Міністрів України Стратегії розвитку вищої освіти на 2022–2032 роки [0]. Вважаємо доцільним акцентувати увагу на тому, що у цьому документі цифровізація визначена одним із пріоритетних напрямів прискорення розвитку ефективних цифрових освітніх екосистем. Для їх розвитку передбачається подальше створення розвинутої інфраструктури, зв’язку і цифрового обладнання, ефективного планування та використання цифрового потенціалу, який включає «сучасні організаційні можливості, підготовлених наукових, науково-педагогічних та педагогічних працівників, які володіють цифровими компетентностями» та здатні використовувати високоякісне освітнє наповнення, інструменти і безпечні платформи, що «відповідають стандартам приватності та етики та є зручними для користувачів», допоміжні технології для осіб з інвалідністю; спроможні розвивати цифрові компетентності для цифрової трансформації [2].

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

https://doi.org/10.58442/2218-7650-2023-24(53)

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 удвічі – з 2,18 мільярда на початку 2012 року до 4,95 мільярда на початку 2022 року. Це призводить 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 упродовж 2021 року з'явилося 424 мільйона нових користувачів [3].

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 телефонних номерів, міське населення частіше використовує Інтернет, ніж сільське, відсоток активних користувачів Інтернетом зменшується зі зростанням віку. Також виявлено, що чим вища освіта в українця/ки, тим частіше він/вона користується Інтернетом, а найчастіше використовують Інтернет українці віком від 18 до 49 років. Слід зазначити, що опитування проводилось з дорослими (у віці 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) [4].

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

https://doi.org/10.58442/2218-7650-2023-24(53)

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. Портал освітян України (https://www.pedrada.com.ua/article/2614-bezpechne-osvtn-seredovishche-zakladu-osvti) [5], 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 не обмеженим. Сьогодні не має сенсу доводити серйозний вплив інформаційного середовища на інтелектуальний, фізичний та психічний розвиток шкільної і студентської молоді. З однієї сторони забезпечення доступу до інформаційних ресурсів, впровадження 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'явились 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, як «за останні роки загрози порушення інтересів людей, самої держави й у 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» [6].

Державами-членами Ради Європи та іншими країнами у 2001 році підписано Конвенцію про кіберзлочинність, яка була ратифікована Верховною Радою України в 2005 році [7].

З кожним роком кількість кібератак лише зростає, дедалі вони стають все більш складнішими і надходять з широкого кола джерел. З метою підвищення стійкості до кіберзагроз та забезпечення отримання громадянами та бізнесом вигоди від надійних цифрових технологій в ЄС розроблено і прийнято Стратегію кібербезпеки. У цьому документі розділено відповідальність за забезпечення кібербезпечної цифрової

https://doi.org/10.58442/2218-7650-2023-24(53)

трансформації між урядами, підприємствами та громадянами [8].

В іншому документі – Європейській Декларації о цифрових правах і принципах цифрового десятиліття [9] наголошується на тому, що цифрова трансформація торкається усіх аспектів життя людей – розширення можливостей для покращення якості їхнього життя, впровадження інновацій, значне економічне зростання і сталість. В 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-світі [8].

Зважаючи на широкий, швидкий і екстенсивний 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. [10]. На наш погляд, на особливу увагу менеджерів освітнього процесу в педагогічних закладах вищої освіти заслуговує комплекс інформаційних бюлетенів ЄС, представлений на сайті Європейського парламенту, який розглядає питання, пов'язані із створенням безпечних цифрових просторів і послуг, створення рівних умов для цифрових ринків із великими платформами та зміцнення цифрового суверенітету Європи, одночасно сприяючи досягненню європейської мети кліматичної нейтральності до 2050 р. [10]. Ознайомлення з означеною інформацією уможливить випереджальне розроблення навчальних програм і контенту навчальних дисциплін для підготовки фахівців, для формування у них і 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» [6]. 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 прийнято рішення про схвалення проєкту Стратегії кібербезпеки України. Її основною метою є «створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [11].

З метою протистояння загрозам, спрямованим на свідомість громадян, розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом,

https://doi.org/10.58442/2218-7650-2023-24(53)

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» [12].

Нові виклики (розвиток інформаційних технологій та їх конвергенція з технологіями штучного інтелекту; визнання кіберпростору разом з іншими фізичними просторами 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, впливу 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, не передбачені загрози; пандемія COVID-19, яка очевидно матиме довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних тощо) та швидко змінюваний 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» [13].

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, громадські об'єднання та окремих громадян України. Прогнозується розроблення Загальнонаціональної програми кіберграмотності. Вона має спрямовуватися на підвищення рівня цифрової грамотності населення

https://doi.org/10.58442/2218-7650-2023-24(53)

України, зокрема, шляхом включення питань до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти» з формування цифрових навичок, кіберобізнаності відносно сучасних кіберзагроз та протидії ним (Про Стратегію кібербезпеки України, 2021). Основні положення цього документу конкретизовано Планом реалізації Стратегії кібербезпеки України, схваленим 30 грудня 2022 року [14].

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 удосконалена 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» [15].

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

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

https://doi.org/10.58442/2218-7650-2023-24(53)

громадянина. Ґрунтуючись на аналізі нормативно-правових, організаційних, інструктивних та інформаційних документів, розроблених на міжнародному і державному рівнях, уявляється вірогідним проектування 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 нашим переконанням важливим вбачається створення програми навчання, тренінгів, воркшопів з 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» [6]. 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.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ / CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

За результатами теоретичного аналізу встановлено низку 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 і державному рівнях, схарактеризовано 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 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

https://doi.org/10.58442/2218-7650-2023-24(53)

та безліч інших питань; доведено необхідність формування навичок цифрової безпеки у суб'єктів освітнього процесу; схарактеризовано можливості використання представлених у статті документів з політики цифрової безпеки для професійної підготовки майбутніх викладачів педагогічних закладів вищої освіти.

Перспективи подальших досліджень вбачаємо в діагностиці рівнів сформованості навичок цифрової безпеки у майбутніх викладачів педагогічних закладів вищої освіти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Л. М. Петренко, «Аналітичний огляд запиту на публікації з питань професійного розвитку педагогічних і науково-педагогічних працівників», на *III Всеукр. відкр. наук.-практ. онлайн-форумі, Інноваційні трансформації в сучасній освіті: виклики, реалії, стратегії.* Київ, Нац. центр «Мала академія наук України». 2021, с. 132–135.

[2] Кабінет Міністрів України. (2022, Лют. 23). *Розпорядження № 286-р «Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 рр.».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

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

[4] О. Черьомухіна, Користування інтернетом серед українців: результати телефонного опитування, проведеного 13–18 травня 2022 року. [Електронний ресурс]. Доступно: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1115&page=1 Дата звернення: Квіт. 01, 2023.

[5] Педрада. Портал освітян України. Безпечне освітнє середовище закладу освіти. [Електронний ресурс]. Доступно: https://www.pedrada.com.ua/article/2614-bezpechne-osvtn-seredovishche-zakladu-osvti Дата звернення: Квіт. 01, 2023.

[6] І. Р. Мальцева, Ю. О. Черниш, Р. М. Штонда, «Аналіз деяких кіберзагроз в умовах війни», *Кібербезпека: освіта, наука, техніка*, № 4(16), с. 37–44, 2022. https://doi.org/10.28925/2663-4023.2022.16.3744

[7] Верховна Рада України (2005. Верес. 07). *Конвенція про кіберзлочинність № 994_575 (чинний), поточна редакція.*

[Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/994_575#Text

[8] Europe's Digital Decade: digital targets for 2030. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en Дата звернення: Квіт. 01, 2023.

[9] European Declaration on Digital Rights and Principles. 2023. [Online]. Available: European Declaration on Digital Rights and Principles | Shaping Europe's digital future (europa.eu) Дата звернення: Квіт. 01, 2023.

[10] Digital Agenda for Europe. 2020. [Online]. Available: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe Дата звернення: Квіт. 01, 2023.

[11] Верховна Рада України. (2016, Берез. 15). *Указ Президента України № 96/2016 від 27 січня 2016 року «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/96/2016#Text

[12] Верховна Рада України. (2017, Лют. 25). *Указ Президента України № 47/2017 від 29 грудня 2016 року «Про рішення Ради національної безпеки і оборони України "Про Доктрину інформаційної безпеки України"».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/47/2017#Text

[13] Верховна Рада України. (2021, Серп. 26). *Указ Президента України № 447/2021 від 14 травня 2021 року «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[14] Верховна Рада України. (2022, Лют. 01). *Указ Президента України № 37/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України".* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/37/2022#Text

[15] Опис рамки цифрової компетентності для громадян України. 2021. [Електронний ресурс]. Доступно: 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 Дата звернення: Квіт. 01, 2023.

Вісник післядипломної освіти. Випуск 24(53) Серія «Педагогічні науки» (Категорія «Б»)
Bulletin of Postgraduate education. Issue 24(53) Educational Sciences Series (Category «B»)
https://doi.org/10.58442/2218-7650-2023-24(53)

DIGITAL SECURITY IN PROFESSIONAL ACTIVITIES OF FUTURE TEACHERS OF PEDAGOGICAL INSTITUTIONS OF HIGHER EDUCATION: REGULATORY AND LEGAL ASPECT

Larysa Petrenko,
Dr. hab. of Pedagogical Sciences, Full Professor,
head of the Department of Theory and Practice of Pedagogical Education
Ivan Ziaziun Institute of Pedagogical and Adult Education
of the National Academy of Educational Sciences of Ukraine.
Kyiv, Ukraine.
https://orcid.org/0000-0002-7604-7273
laravipmail@gmail.com

Abstract. The author reviewed a number of normative, organizational, instructional and informational documents on the digital security of society, the individual and the state, adopted at the international and state levels, systematized them in chronological order and characterized them in the context of training of the future teachers of pedagogical institutions of higher education for professional activities in a digital society. The main provisions of the distribution of responsibility for ensuring the cybersafe digital transformation between governments, enterprises and citizens have been identified and highlighted; the new risks and threats for all participants of the educational process were outlined, in particular: erosion of the cultural component of the educational process, the growth of Internet addiction (Internet dependence), the possibility of unauthorized access to personal data, cybermobbing, filling media content and social networks with fakes, hating and many other issues; the necessity of forming digital security skills among the subjects of the educational process has been proven. The structure of digital security as part of digital competence is covered: device protection and secure connection to the Internet; protection of personal data and privacy, Internet security; protection of consumer's personal rights against fraud and abuse; protection of health and well-being; environmental protection. The possibilities of using the digital security policy documents, presented in the article for professional training of future teachers of pedagogical institutions of higher education are revealed, i.e.: policy design (at the level of a higher education institution) on digital security of the information and educational environment; creation of training programs, trainings, workshops for the formation of digital security skills of future teachers of pedagogical institutions of higher education; testing of the information

system of the institution of higher education; various extracurricular activities: seminars, conferences, olympiads, competitions, analytical reports, educational activities in the region, etc.

Keywords: future teacher; pedagogical institution of higher education; digital security; digital competence; regulatory and legal support; cyber threats; cyber crime; information war.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] L. M. Petrenko, «Analitychnyi ohliad zapytu na publikatsii z pytan profesiinoho rozvytku pedahohichnykh i naukovo-pedahohichnykh pratsivnykiv», na III Vseukr. vidkr. nauk.-prakt. onlain-forumi, Innovatsiini transformatsii v suchasnii osviti: vyklyky, realii, stratehii. Kyiv, Nats. tsentr «Mala akademiia nauk Ukrainy». 2021, s. 132–135.

[2] Kabinet Ministriv Ukrainy. (2022, Liut. 23). Rozporiadzhennia № 286-r «Pro skhvalennia Stratehii rozvytku vyshchoi osvity v Ukraini na 2022-2032 rr.». [Elektronnyi resurs]. Dostupno: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

[3] Didgital 2022: Global Overview Report. [Online]. Available: https://datareportal.com/reports/digital-2022-global-overview-report Data zvernennia: Kvit. 01, 2023.

[4] O. Cheromukhina, Korystuvannia internetom sered ukraintsiv: rezultaty telefonnoho opytuvannia, provedenoho 13–18 travnia 2022 roku. [Elektronnyi resurs]. Dostupno: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1115&page=1 Data zvernennia: Kvit. 01, 2023.

[5] Pedrada. Portal osvitian Ukrainy. Bezpechne osvitnie seredovyshche zakladu osvity. [Elektronnyi resurs]. Dostupno: https://www.pedrada.com.ua/article/2614-bezpechne-osvtn-seredovishche-zakladu-osvti Data zvernennia: Kvit. 01, 2023.

[6] I. R. Maltseva, Yu. O. Chernysh, R. M. Shtonda, «Analiz deiakykh kiberzahroz v umovakh viiny», Kiberbezpeka: osvita, nauka, tekhnika, № 4(16), s. 37–44, 2022. https://doi.org/10.28925/2663-4023.2022.16.3744

[7] Verkhovna Rada Ukrainy (2005. Veres. 07). Konventsiia pro kiberzlochynnist № 994_575 (chynnyi), potochna redaktsiia. [Elektronnyi resurs]. Dostupno: https://zakon.rada.gov.ua/laws/show/994_575#Text

[8] Europe's Digital Decade: digital targets for 2030. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-

https://doi.org/10.58442/2218-7650-2023-24(53)

2030_en Data zvernennia: Kvit. 01, 2023.

[9] European Declaration on Digital Rights and Principles. 2023. [Online]. Available: European Declaration on Digital Rights and Principles | Shaping Europe's digital future (europa.eu) Data zvernennia: Kvit. 01, 2023.

[10] Digital Agenda for Europe. 2020. [Online]. Available: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe Data zvernennia: Kvit. 01, 2023.

[11] Verkhovna Rada Ukrainy. (2016, Berez. 15). Ukaz Prezydenta Ukrainy № 96/2016 vid 27 sichnia 2016 roku «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy"». [Elektronnyi resurs].
Dostupno: https://zakon.rada.gov.ua/laws/show/96/2016#Text

[12] Verkhovna Rada Ukrainy. (2017, Liut. 25). Ukaz Prezydenta Ukrainy № 47/2017 vid 29 hrudnia 2016 roku «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Doktrynu informatsiinoi bezpeky Ukrainy"». [Elektronnyi resurs].
Dostupno: https://zakon.rada.gov.ua/laws/show/47/2017#Text

[13] Verkhovna Rada Ukrainy. (2021, Serp. 26). Ukaz Prezydenta Ukrainy № 447/2021 vid 14 travnia 2021 roku «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy"». [Elektronnyi resurs].
Dostupno: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[14] Verkhovna Rada Ukrainy. (2022, Liut. 01). Ukaz Prezydenta Ukrainy № 37/2022 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku "Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy". [Elektronnyi resurs].
Dostupno: https://zakon.rada.gov.ua/laws/show/37/2022#Text

[15] Opys ramky tsyfrovoi kompetentnosti dlia hromadian Ukrainy. 2021. [Elektronnyi resurs].
Dostupno: 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 Data zvernennia: Kvit. 01, 2023.

Стаття надійшла до редакції
03 квітня 2023 року