DOI https://doi.org/10.30525/978-9934-26-647-8-20

ІНФОРМАЦІЙНА БЕЗПЕКА ПРОЦЕСІВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ У СФЕРІ ОСВІТИ

Шопіна І. М.

ВСТУП

Цифрова трансформація всіх сфер суспільної діяльності значним чином впливає на особливості здійснення процесів управління, виробничих процесів, підготовку кадрів, контроль за якістю їх діяльності та інші сфери суспільної активності. Однією з таких сфер є сфера освіти, яка у будь-якій державі є надзвичайно чутливою, адже в ній зосереджена квінтесенція позитивного досвіду у науковій сфері, кращі здобитки розвитку сфери управлінських відносин, відомості про новітні технології, які змінюють обличчя сучасного світу. Ця інформація слугує фундаментом освітніх процесів і дозволяє формувати особистість фахівців майбутнього, тому від наповненості освітніх процесів об'єктивною та достовірною інформацією, яка відповідала б усім етичним вимогам і до сфери освіти, і до тих сфер суспільних відносин, в яких будуть працювати випускники університетів, залежить якість підготовки здобувачів освіти.

Однак сучасні реалії світової безпеки свідчать, що інформація в освітніх процесах деяких держав активно використовується для формування зручного для держави типу особистості з некритичним мисленням і несформованою відповідальністю за свої дії, що робить його зручним об'єктом для маніпуляцій. Класичним прикладом такої ситуації є функціонування російської системи освіти, в якій вміння аналізувати підміняється пропагандистськими гаслами. Необхідність формування особистості професіонала з розвиненими ціннісними, мотиваційними та когнітивними якостями, який мав би необхідні для успішної роботи в умовах інформаційного суспільства знання, вміння та навички, обумовлює потребу у постійній ревізії всього масиву освітньої інформації, що, у свою чергу, утворює ризики заміни базової для кожного професіонала сукупності знань на непідтверджені гіпотези, які згодом можуть бути скасовані як недоказові.

Іншим чинником важливості інформаційної безпеки освітніх систем є їх наповненість персональними даними значної кількості громадян, що вимагає здійснення низки заходів у сфері захисту цієї інформації. Захист персональних даних у сфері освіти ускладнюється необхідністю

додержуватися низки вимог правових актів щодо оприлюднення різноманітних списків здобувачів освіти, ведення інституційних депозитаріїв, наявністю вимог щодо розміщення персональних даних укладачів методичних матеріалів. Отже, університети мають постійно балансувати між вимогами до публічності наукової та освітньої діяльності та обмеженнями, пов'язаними з охороною чутливої персональної інформації.

Штучний інтелект, використання якого набуває все більш широкомасштабного характеру, теж впливає на процеси інформаційної безпеки систем освіти, вимагаючи знаходити найкращі варіанти додержання вимог академічної доброчесності в умовах розвитку інформаційних технологій, наслідком яких є підвищення рівня цифровізації сфери освітньої діяльності як в Україні, так і в інших демократичних державах.

Окремий аспект інформаційної безпеки сфери освіти пов'язаний з убезпеченням здобувачів освіти від деструктивного впливу проросійської ідеології. На жаль, існують непоодинокі приклади, коли викладачі провідних національних університетів України мали змогу транслювати свою проросійську позицію здобувачам освіти. Цікавість молоді до новинок розважальних жанрів активно використовується російським агресором для впливу на юнацьку аудиторію за допомогою музичних творів, кінофільмів, комп'ютерних ігор, в яких містяться антиукраїнські імперські наративи. Отже, ефективна протидія інформаційно-психологічним російським операціям є стратегічним пріоритетом для збереження незалежності освітньої сфери.

Вказане вимагає комплексного перегляду освітньої політики та впровадження ефективних механізмів захисту інформаційного простору, що є надзвичайно важливим для формування особистості свідомих та відповідальних громадян демократичного суспільства. При цьому інформаційна безпека освітніх систем в умовах цифрової трансформації має розглядатися як ключовий компонент національної безпеки і важлива складова національної інформаційної політики.

1. Сутність та особливості інформаційної безпеки цифрової трансформації

Конституція України у ст. 17 визначила, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу[1]. Особливу важливість уявляє

[1] Конституція України: офіц. текст. ІПС ЛІГА Закон Прайм. URL: https://ips.ligazakon.net/

собою забезпечення інформаційної безпеки процесів цифрової трансформації, які активно здійснюються в українському суспільстві.

Як справедливо зауважує І. Арістова, інформаційна сфера є системоутворюючим елементом досягнення цілей сталого розвитку України, забезпечуючи технологічну основу для економічного зростання, соціальної інклюзії та екологічної безпеки. Цифрові технології оптимізують використання ресурсів та підвищують ефективність різних секторів економіки, а інформаційне право створює правову основу для регулювання цифрового середовища. В умовах воєнного стану цифровізація набуває особливого значення, підтримуючи економічну стабільність і сприяючи післявоєнному відновленню, що підкріплюється Стратегією цифрового розвитку України до 2030 року та євроінтеграцією[2]. Динамічний технологічний розвиток в інформаційній сфері докорінно трансформує всі структури суспільних відносин. Ця глобальна зміна спричинена комплексом об'єктивних факторів. Серед ключових чинників слід назвати скорочення часових витрат на здійснення виробничих робочих процесів завдяки автоматизації виробничих циклів, зростання швидкості збору та поліпшення якості аналізу відомостей і даних, необхідних для ухвалення управлінських рішень. Крім того, спостерігаються значні зрушення у структурі зайнятості громадян: певні професії, типові для доцифрової епохи, поступово зникають, тоді як зміст інших галузей людської діяльності зазнає суттєвої видозміни. Ці обставини вимагають обов'язкового врахування феномену цифровізації на всіх щаблях прогнозування (від загальнонаціонального рівня до планування індивідуальної кар'єри). Не менш важливим є досягнення відповідності між поточним рівнем розвитку інформаційних технологій та правовим забезпеченням їх використання. Проте, темпи прогресу технологій, зокрема цифрових, набагато випереджають розвиток системи інформаційно-правового регулювання. Відтак, першочерговим завданням правової науки в цих умовах є формування термінологічної та методологічної основи для розуміння і супроводу цифрової трансформації[3].

Інформаційна безпека як чинник і умова успішності цифрової трансформації є більш усталеною науковою категорією і вже кілька

[2] Арістова І. В. Роль інформаційної сфери та науки «інформаційне право» у досягненні цілей сталого розвитку в умовах цифрової трансформації в Україні. *Аналітично-порівняльне правознавство*. 2025. Вип. 4. Ч. 2. С. 96. DOI https://doi.org/10.24144/2788-6018.2025.04.2.14

[3] Шопіна І.М., Грищук А.Б. Поняття, напрями та суб'єкти цифрової трансформації: правові аспекти. *Правовий часопис Донбасу*. 2022. № 4. С. 167–170. DOI https://doi.org/10.32782/2523-4269-2022-81-4-1-167-170

десятиліть привертає активну увагу науковців і практиків. Проблеми забезпечення інформаційної безпеки в Україні набули особливої актуальності ще у 2014 році, із початком збройної російської агресії проти нашої держави. Постійне проведення противником інформаційно-психологічних операцій продовжується і після набуття збройною агресією держави-терориста повномасштабного характеру. Нині ціна помилки в інформаційній сфері є надзвичайно високою – будь-які відомості та дані активно використовуються противником для розвідування позицій підрозділів Збройних Сил України та інших військових формувань, проведення шантажу на основі компрометуючої інформації, здійснення терористичних актів проти цивільного населення та об'єктів критичної інфраструктури[4]. Особливо вразливою групою є діти та молодь, які активно вербуються російською розвідкою через соціальні мережі та месенджери і використовуються для збору інформації про військові об'єкти, об'єкти критичної інфраструктури, для знищення автомобілів, що належать військовослужбовцям та військовим частинам, і навіть для здійснення терористичних актів.

Слід сказати, що перед початком повномасштабної російської збройної агресії наша держава знаходилася на піку розвитку цифровізації процесів взаємодії громадянина і держави, а також діяльності органів публічної влади. Не зважаючи на певні недоліки системи «Дія», а також єдиних та державних реєстрів (переважно пов'язаних із їх вразливістю до витоку персональних та інших даних), можна констатувати, що Україна вийшла на одне з перших місць в Європі у сфері цифрової трансформації органів публічного адміністрування. Єдина судова інформаційно-телекомунікаційна система, яка включає у тому числі й підсистему «Електронний суд», дозволила зробити великий крок уперед на шляху підвищення доступності правосуддя. Цифровізація сфери публічних послуг підвищила зручність та інклюзивність користування ними для громадян, а також сприяла зниженню корупційних ризиків у найбільш чутливих сферах правовідносин. Навіть після 2022 року цифровізація відносин між громадянином і державою не стала на паузу: за рейтингом Online services Index, міжнародного дослідження E-Government Development Index, що оцінює 193 країни світу та розробляється ООН, Україна займає 5 місце за рівнем розвитку цифрових державних послуг. У 2018-му році Україна була в цьому рейтингу на 102-му місці. Так

[4] Шопіна І.М. Інформаційна безпека цифрової трансформації. *Вісник ЛьвДУВС*. 2023. № 1. С. 28–35. DOI https://doi.org/10.32782/2311-8040/2023-1-4

за шість років країна перетнула 97 позицій і посіла 5 місце[5]. У теперішній час, не зважаючи на те, що об'єкти енергетичної інфраструктури України зазнали значних руйнувань, в Україні активно продовжуються процеси цифрової трансформації, інформаційна безпека яких є предметом нашого розгляду.

Значущість категорії інформаційної безпеки настільки загальновизнана й деталізована у наукових дослідженнях, що деякі вчені вважають цей феномен навіть не інститутом, а підгалуззю інформаційного права[6]. Не вдаючись до дискусій з приводу відмінностей між підгалузями та інститутами права, які точаться багато десятиліть, зауважимо, що важливість інформаційної безпеки як правового феномену підтверджується, на нашу думку, двома основними факторами: її практичною роллю для підтримання життєдіяльності держави (саме прогалини у сфері інформаційної безпеки сприяли швидкому і безперешкодному відновленню влади Талібана в Афганістані[7]), а також її ґрунтовним теоретичним осмисленням у багатьох науках (інформаційному, адміністративному, кримінальному, фінансовому, цивільному праві, праві національної безпеки та військовому праві тощо).

Існує декілька підходів до структури інформаційної безпеки. Так, її розглядають як відносини, що складаються в інформаційній сфері і включають: суспільні відносини, що забезпечують реалізацію права на інформацію і на охорону інформації від незаконного втручання; суспільні відносини, що забезпечують безпеку інформаційних ресурсів; суспільні відносини, що забезпечують безпеку використання інформаційно-телекомунікаційних технологій[8]. Безумовно, будь-яке правове явище пов'язано з суспільними відносинами, оскільки право виступає їх універсальним регулятором, водночас це лише один із аспектів, в якому можна розглядати інформаційну безпеку. Багатогранність цього феномену обумовлює необхідність його розгляду з використанням широкого арсеналу методів наукового пізнання, як правових, так і запозичених в інших галузях наукових знань.

---

[5] Кінша Д. Україна посідає 5 місце у світі за розвитком цифрових держпослуг. URL: https://surl.li/payofz.

[6] Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. № 2(25). С. 73-85. URL: http://ippi.org.ua/sites/default/files/9_8.pdf.

[7] The Fall of Afghanistan and the Taliban Victory of 2021: Was it really an Intelligence Failure? National Security Journal. 2024. Volume 6, Issue 2. https://doi.org/10.36878/nsj20241103.07

[8] Малашко О. Є., Ковалів М. В. Теоретична конструкція поняття «інформаційна безпека». *Інтернаука. Серія: «Юридичні науки».* 2020. № 10. С. 20–33. URL: https://doi.org/10.25313/2520-2308-2020-10-6350.

У діяльнісному аспекті інформаційна безпека розглядається як феномен, що включає до себе: інформаційне забезпечення діяльності; захист інформаційного ресурсу; протидію негативному інформаційному впливу[9]. Діяльнісний підхід, запозичений правовими науками у методологічному апараті загальної психології, дуже ефективно використовується у правничих дослідженнях. Разом з тим не зовсім зрозуміло, як співвідносять між собою захист і протидія, адже ці терміни є близькими за змістом, на наш погляд, захист включає у тому числі протидію, втім, ці питання потребують окремих досліджень.

Адміністративно-правовий підхід до структури інформаційної безпеки передбачає наділення цього феномену адміністративно-правовими властивостями та включення його до всіх рівнів структури адміністративно-правового регулювання. Відповідно до вказаного підходу структуру інформаційної безпеки ототожнюють з її адміністративно-правовим регулюванням і розглядають як сукупність наступних елементів: 1) фізичні та юридичні особи, суспільство, держава, які є носіями прав, свобод і законних інтересів у сфері інформаційної безпеки та охороняються адміністративно-правовими засобами і способами; 2) охоронювані адміністративно-правовими засобами, визначеними у Конституції України та інших нормативно-правових актах інформаційні права, свободи і законні інтереси громадян (об'єктами безпеки у сфері адміністративно-правового регулювання); 3) позначені типізовані умови (ситуації), що виникають та стають шкідливими і небезпечними у сфері адміністративно-правового регулювання інформаційних відносин та їх забезпечення (адміністративно дозволені дії (діяльність) фізичних та юридичних осіб; адміністративно заборонені дії (бездіяльність); адміністративно-правові казуси). При цьому критерієм, що визначає структуру адміністративно-правового регулювання відносин у сфері інформаційної безпеки особи, суспільства і держави, виступають формально закріплені у нормативно-правових актах носії адміністративно охоронюваних законних інтересів, на підставі чого існує потреба у виокремленні наступних видів інформаційної безпеки – безпека особи, суспільна/національна безпека і державна безпека[10]. Погоджуючись з наведеним науковцями критеріями поділу елементів інформаційної безпеки на три категорії залежно від їх носіїв,

[9] Мохнюк А. М., Скорук О. В. Організація та управління інформаційною безпекою на підприємстві: конспект лекцій. Луцьк : ПП «Поліграфія», 2017. С. 31.

[10] Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2021. № 3 (31). С. 172–173. URL: http: //doi.org/10.23939/law2021.31.167.

зауважимо однак, що повне ототожнення структури інформаційної безпеки зі структурою адміністративно-правового регулювання уявляється нам не зовсім можливим з огляду на поєднання у структурі інформаційної безпеки приватноправових та публічно-правових відносин. При цьому в наукових дослідженнях, присвячених проблемам інформаційної безпеки, і у програмах інвестицій, спрямованих на безпосереднє забезпечення інформаційної безпеки, найбільша увага приділяється саме приватним аспектам досліджуваного явища (це цілком логічно, адже провідну роль серед замовників наукових досліджень та технологічних рішень у сфері інформаційної безпеки займають великі міжнародні корпорації, бюджети яких перевищують розміри бюджетів багатьох держав світу).

Найбільш розгалужений підхід до структури інформаційної безпеки включає низку її різнопланових критеріїв. Так, у широкому аспекті інформаційна безпека класифікується: а) за джерелом походження повноважень щодо здійснення заходів із забезпечення інформаційної безпеки (природні права і свободи людини, Конституція України, закони України, підзаконні правові акти); б) за видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності); в) за ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки: основна (для спеціально уповноважених органів публічної влади та військових формувань); факультативна (для інших органів публічної влади); делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами; необов'язкова (для громадян і суб'єктів громадянського суспільства). У вузькому аспекті інформаційна безпека включає наступні види: а) за критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, органів державної влади та місцевого самоврядування, громадянського суспільства і держави в цілому); б) за критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо); в) за критерієм досягнутих результатів (досконала і недосконала інформаційна безпека)[11]. Цей підхід вбачається нам таким, що враховує максимальну кількість аспектів

[11] Онопрієнко С. Класифікація видів інформаційної безпеки як правової категорії. *Вісник Київського національного університету імені Тараса Шевченка. Серія: «Військово-спеціальні науки».* 2022. № 1 (49). С. 61–62.

досліджуваного явища, разом з тим хотілося б згадати про позицію О. Золотар, яка наголошує на некоректності ототожнення інформаційної безпеки людини з її забезпеченням. Це, на думку дослідниці, є методологічною помилкою, оскільки забезпечення (щодо інформаційної безпеки людини) стосується більшою мірою заходів (технічних, організаційних, правових, кадрових тощо), а сама безпека – суб'єктивного переживання людиною, що відображає активний зміст її свідомості, яка здатна прогнозувати, передбачити і уявити небезпеки, а також своєчасно і адекватно на них відреагувати. Наступною дилемою, що має місце в правових (і не лише) дослідженнях інформаційної безпеки вчена називає протиставлення її як стану і процесу. На її думку, у самому загальному вигляді під інформаційною безпекою людини можна розуміти її здатність зберігати свої істотні властивості, і забезпечувати власне існування і розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Тобто, не слід обмежуватись розумінням її як «стану», а найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем[12]. Отже, розгляд інформаційної безпеки у динаміці дозволяє з'ясувати не лише притаманні їй закономірності та ризики, а й визначити ступінь впливу на неї кожного з них. Тому структура інформаційної безпеки має включати й розмежування залежно від перманентності або дискретності впливу на неї зовнішніх та внутрішніх факторів, а також залежно від того, статичні чи динамічні особливості узяті дослідником, законотворцем або представником публічної адміністрації як основоположні.

Структура інформаційної безпеки відображує сучасні особливості розвитку науки інформаційного права, а також завдання, які постають перед дослідником у кожному конкретному випадку. Крім того, заслуговує на увагу розмежування між інформаційною безпекою як ідеальним конструктом, що відображується у свідомості суб'єкта та має суб'єктивний характер, інформаційною безпекою як метою, рівень досягнення якої вимірюється за допомогою конкретних (кількісних) показників, і інформаційною безпекою як діяльністю або процесом (у даному випадку доречним є використання терміну «забезпечення інформаційної безпеки»). Це не означає відмову від розмежування між видами інформаційної безпеки за суб'єктами, змістом, джерелами повноважень чи загроз, однак ці критерії, на нашу думку, носять

[12] Золотар О.О. Правові основи інформаційної безпеки людини: дис. …докт. юрид. наук: 12.00.07. Київ, 2018. С. 70–71.

вторинний характер. Методологічно вірним було б, на нашу думку, спочатку визначити, який саме (моделюючий, телеологічний чи діяльнісний) підхід буде найбільше відповідати цілям дослідника, а вже потім розгалужувати один з вказаних підходів, будуючи власну класифікацію.

Цифрова трансформація, яку ми розуміємо як оптимізацію організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій, може розглядатися у двох аспектах: телеологічному, як мета органів публічного адміністрування, і в діяльнісному, як сукупність дій, спрямованих на реалізацію функцій, методів, заходів, що є частиною управлінської системи підприємства, установи, організації або органу публічної влади. Прикладом телеологічного розуміння може бути відображення у проєкті Рішення Європейського Парламенту та Ради 2021/0293 про запровадження Політичної програми до 2030 року «Шлях до цифрового десятиліття цілей цифрового розвитку до 2030 року, до яких віднесено: 1) населення з цифровими навичками та висококваліфіковані професіонали з цифрових технологій: принаймні 80% осіб у віці 16-74 років мають принаймні базові цифрові навички; щонайменше 20 мільйонів зайнятих у сфері інформації та зв'язку працюють як спеціалісти з технологій із конвергенцією між жінками і чоловіками; 2) безпечні, продуктивні та стійкі цифрові інфраструктури: усі європейські домогосподарства охоплені гігабітною мережею з усіма населеними пунктами, охопленими 5G; виробництво передових та стійких напівпровідників у Європейському Союзі становить не менше 20% світового виробництва у вартісному вираженні; розгорнуто принаймні 10000 кліматично нейтральних високозахищених «граничних вузлів» в Європейському Союзі, розповсюджених у спосіб, який гарантує доступ до послуг даних з низькою затримкою (кілька мілісекунд) незалежно від того, де розташовані підприємства; до 2025 року в Європейському Союзі з'явиться перший комп'ютер із квантовим прискоренням, прокладаючи шлях до того, щоб Європейський Союз був на передньому краї квантових технологічних можливості до 2030 року; 3) цифрова трансформація бізнесу: принаймні 75% підприємств Європейського Союзу взяли на себе: послуги хмарних обчислень; великі дані; штучний інтелект; охоплення понад 90% малих і середніх підприємств Союзу принаймні базовим рівнем цифрової інтенсивності; Європейський Союз нарощує коло своїх інноваційних масштабів і вдосконалюється доступ до фінансування, що призведе до принаймні подвоєння кількості

підприємств з високим рівнем капіталізації активів; 4) цифровізація державних послуг: 100% доступне онлайн надання ключових державних послуг для громадян та підприємств Європейського Союзу; 100% громадян Союзу мають доступ до своїх медичних записів (електронні медичні картки (EHR)); принаймні 80% громадян Союзу використовують рішення цифрової ідентифікації (ID)[13]. Діяльнісне розуміння цифрової трансформації базується на здобутках теорії управління та соціальної психології, і передбачає структурування дій суб'єктів суспільних відносин, дотичних до впровадження інформаційних технологій у процеси функціонування та життєдіяльності фізичних та юридичних осіб.

Хронологічно вироблення телеологічного підґрунтя цифрової трансформації має передувати розробці її діяльнісних аспектів: за відсутності цілей, формалізованих і доведених до відома всіх суб'єктів, планування їх конкретних дій уявляється марним. Втім, в національній практиці таке спостерігалося неодноразово: як приклад, можна навести таке декларативне завдання Національної програми інформатизації, як «застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України»[14], простежити ступінь реалізації якого не уявляється можливим.

Отже, можливість досягнення поставленої мети залежить від коректності її формулювання, що, у випадку з інформаційною безпекою цифрової трансформації, потребує використання кількісних критеріїв, які дозволяють порівнювати між собою різні сфери суспільних відносин, різні проміжки часу тощо.

Успішна діяльність з цифрової трансформації залежить також від правильного вибору тих сфер суспільних відносин, стосовно яких можна прогнозувати зростання інформаційних ризиків. Однією з таких сфер в Україні є сфера освіти, цифрова трансформація якої з моменту встановлення карантинних обмежень внаслідок пандемії коронавірусної хвороби COVID-19 розвивалася надзвичайно швидкими темпами, які не загальмувалися навіть після початку повномасштабної російської агресії.

Як свідчить досвід технологічно розвинених держав, нині спостерігається посилення основних типів кіберзагроз для сфери вищої освіти. Це значні фінансові втрати, спричинені програмами-вимагачами

[13] Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

[14] Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27-28. Ст. 181.

або знищеними даними. Хоча кібератаки університетів за допомогою програм-вимагачів не є новим явищем, однак протягом останніх кількох років їх стрімко зросла, причому швидше, ніж в інших секторах, особливо після пандемії COVID-19[15]. Наприклад, протягом перших девяти місяців 2025 року дослідниками компанії Comparitech зафіксувано 180 атак на сектор освіти. Це на шість відсотків більше, ніж у 2024 році за той самий період. Багато з цих підтверджених атак на сектор освіти призвели до простоїв системи, що спричинило перебої в роботі мереж та скасування занять на кілька днів, якщо не тижнів. Найчастіше хакери крадуть дані в процесі, в середньому за атаку викрадається 2,6 ТБ. Середня вимога викупу за всі атаки складає приблизно 444 тис. доларів. Так, наприклад, невідомі хакери здійснили атаку на японський університет Токай у квітні 2025 року, спричинивши масштабні порушення. Пізніше університет підтвердив, що внаслідок подальшого витоку даних постраждали майже 43 500 осіб[16] .Серед найбільш значущих прикладів – Маастрихтський університет у Нідерландах заплатив 220 000 доларів як викуп у 2019 році[17]. Той факт, що вища освіта стає прибутковою мішенню для кіберзлочинців, викликає особливу тривогу, враховуючи внесок сектора у ВВП. На додаток до їхніх прямих деструктивних наслідків у формі порушення конфіденційності студентів і співробітників, переривання навчальних процесів, спричинення фінансових втрат і крадіжки прав інтелектуальної власності, кіберінциденти проти освіти можуть також призвести до репутаційних збитків, вплинути на потенціал грантів та іноземних інвестицій та підірвати довіру до сектору загалом. Імовірність таких деструктивних наслідків експоненційно зростає, враховуючи складний цифровий слід освітніх установ, їхню культуру відкритості та їхню відносно обмежену готовність до кібербезпеки порівняно з іншими секторами[18].

[15] Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*. 2021. № 6(2). P. 137–154. DOI: 10.1080/23738871.2021.1973526.

[16] Moody R. Education Ransomware Roundup: Q1-Q3 2025 stats on attacks, ransoms, and data breaches. URL: https://www.comparitech.com/news/education-ransomware-roundup-q1-q3-2025-stats-on-attacks-ransoms-and-data-breaches/

[17] Reuters. University of Maastricht Says It Paid Hackers 200,000-Euro Ransom (2020). URL: https://uk. reuters.com/article/us-cybercrime-netherlands-university-idUKKBN1ZZ2HH. Цит. за: Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

[18] Top Cyber Threats to Educational Institutions in 2025. URL: https://blog.blackbaud.com/top-cyber-threats-to-educational-institutions.

Заслуговує на увагу, що за деякими кібератаками стоїть цілеспрямована державна політика деяких тоталітарних країни Так, Група Lazarus, ідентифікована у 2014 році, але активна щонайменше з 2009 року, як зазначається у низці розслідувань, пов'язана з Генеральним бюро розвідки Північної Кореї. Lazarus, відома своїми складними кібератаками, спрямованими на фінансову вигоду, шпигунство та руйнування, використовує різноманітні спеціальні шкідливі програми та тактики. У травні 2017 року кілька університетів США, зокрема Массачусетський технологічний інститут (MIT), Трініті-коледж, Вашингтонський університет та Університет штату Північна Дакота, повідомили про зараження внаслідок атаки «Lazarus Wannacry». Ці установи зазнали збоїв у роботі, оскільки WannaCry шифрував файли та вимагав викуп у біткоїнах[19].

Отже, активізація процесів цифрової трансформації потребує більш активного застосування заходів інформаційної безпеки, що обумовлено зростанням кількості та інтенсивності інформаційних загроз у тих сферах суспільних відносин, в яких вказана трансформація здійснюється особливо швидкими темпами. Ці процеси перебувають у нерозривному взаємозв'язку: ефективність інформаційної безпеки обумовлює досягнення цілей цифрової трансформації, тоді як активізація процесів цифрової трансформації викликає необхідність застосування, розвитку та вдосконалення засобів забезпечення інформаційної безпеки.

Отже, інформаційна безпека цифрової трансформації – це ідеальна модель позбавленого інформаційних загроз середовища, в якому динамічно відбувається впровадження інформаційних (цифрових) технологій у всі сфери функціонування та життєдіяльності фізичних та юридичних осіб з метою найбільш повної реалізації ними своїх інформаційних та інших прав, свобод та інтересів. Розуміння сутності цієї моделі можливо або через суб'єктивне сприйняття суб'єктів інформаційних правовідносин, або через систему кількісних критеріїв, які характеризують досягнення цілей цифрової трансформації.

Від інформаційної безпеки цифрової трансформації слід відрізняти забезпечення цього явища. Забезпечення інформаційної безпеки цифрової трансформації – це сукупність дій органів публічного адміністрування, правоохоронних, правозахисних органів та військових формувань, судів, підприємств, установ, організацій всіх форм власності, інститутів громадянського суспільства та окремих громадян, спрямована на оптимізацію організації, управління, функцій та методів діяльності,

[19] Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*. 2021. № 6(2). P. 137–154. DOI: 10.1080/23738871.2021.1973526.

підвищення рівня інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних (цифрових)технологій.

2. Принципи цифрової трансформації освітньої сфери в умовах євроінтеграції

Повномасштабна російська збройна агресія проти України не зупинила процеси правового та технологічного розвитку нашої держави. Руйнування державою-агресором об'єктів української інфраструктури обумовлює необхідність їх відновлення на основі сучасних технологій і з урахуванням тих напрацювань, які накопичені нині державами-членами Європейського Союзу. У листопаді 2022 року держави-члени, Європейський Парламент та Європейська Комісія завершили переговори про цінності ЄС у цифровому світі, результатом яких має стати підписання Європейської декларації про цифрові права та принципи цифрового десятиліття (*European declaration on digital rights and principles for the digital decade*). Цей документ має ознаменувати центрування уваги на правах і потребах людини та громадянина, що слугує закономірним результатом попереднього розвитку інформаційного права та законодавства Європейського Союзу. Враховуючи активізацію євроінтеграційних прагнень України в умовах консолідації всіх європейських демократичних сил для протидії державі, визнаній Європейським Парламентом спонсором тероризму, аналіз досвіду Європейського Союзу у сфері розбудови цифрового суспільства уявляється вельми актуальним.

Масштабні завдання, які постають перед сучасною правовою демократичною державою, яка розбудовує інформаційне суспільство, у галузі цифрової трансформації, вимагають наявності правового та методологічного підґрунтя. У Європейському Союзі рух до сучасного розуміння цінностей цифрового світу ознаменувався прийняттям таких важливих документів, як Європейський кодекс електронних комунікацій (European Electronic Communications Code, 2018), Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЕС (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), Директива (ЄС) 2016/1148 Європейського парламенту та Ради від 6 липня 2016 р. щодо заходів щодо забезпечення високого загального рівня безпеки мережевих та

інформаційних систем на території Союзу (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) та низки інших актів[20].

Важливе місце серед правових актів Європейського Союзу у досліджуваній сфері займає Регламент (ЄС) 2021/694 Європейського Парламенту і Ради від 24 квітня 2021 року про створення програми «Цифрова Європа» та скасування Регламенту (ЄС) 2015/2240 (Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240). Цілі Програми полягають у підтримці цифрової трансформації промисловості та у сприянні більш ефективному використанню просування політики в галузі інновацій, досліджень та технологічного розвитку на благо громадян та підприємств Європейського Союзу, включаючи його найвіддаленіші регіони та її економічні неблагополучні райони. Програма включає конкретні цілі, що відображають ключові галузі політики, а саме: високопродуктивні обчислення; штучний інтелект; кібербезпека та довіра; просунуті цифрові навички; розгортання та використання цифрових можливостей та функціональної сумісності. Програма також має бути спрямована на краще узгодження політики Європейського Союзу і держав-членів та вимагає підтримки приватних та промислових ресурсів для збільшення інвестицій та розвитку. Крім того, Програма має підвищити результативність Союзу та його економіки. Заслуговує на увагу, що п'ять цілей програми «Цифрова Європа» знаходяться у тісному взаємозв'язку. Так, кібербезпека є важливою для високопродуктивних обчислень, що знаходить своє відображення у оволодінні цифровими навичками, тощо. Взаємозалежність між рівнем розвитку елементів соціальних систем знаходить своє вираження і у підходах, які у досліджуваному документі пропонуються для суб'єктів підприємницької діяльності. У Програмі наголошується на необхідності підтримки малих та середніх підприємств, які мають намір використовувати цифрову трансформацію у своїх виробничих процесах. Така підтримка забезпечує високий внесок цих підприємств у зростання європейської економіки з допомогою раціонального використання ресурсів. Разом з тим центральна роль у реалізації програм відводиться центрам цифрових інновацій, які мають стимулювати широке впровадження передових цифрових технологій у промисловості та інших організаціях, у яких зайнято до 3000 осіб,

[20] Шопіна І.М. Принципи цифрової трансформації України крізь призму досвіду Європейського Союзу. *Південноукраїнський правничий часопис. Тематичний випуск з питань євроінтеграції.* 2022. № 4. С. 29–34. DOI https://doi.org/10.32850/sulj.2022.4.3.6

громадських організацій та академічних спільнот. Наголошується, що мережа європейських центрів цифрових інновацій потребує широкого географічного охоплення всієї Європи та глобального охоплення найвіддаленіших регіонів у єдиному цифровому ринку, системи кібербезпеки, а також для звичайних технологій швидкого доступу. Низькі ціни в центрах інновацій мають бути перевірені технологічними процесами, а також мають відповідати міжнародним стандартам. Вони також повинні викликати зростання в сфері передових цифрових навичок, наприклад, з постачальниками освітніх послуг для отримання короткострокового навчання та стажувань для студентів[21]. Цей підхід, на нашу думку, вартий впровадження в Україні – не зважаючи на високий рівень цифровізації освітньої сфери, формування передових цифрових навичок у студентів під час проходження практики з використанням потенціалу позауніверситетських інноваційних інституцій ще не стало елементом національної системи вищої освіти.

У програмі «Цифрова Європа» підкреслюється важливість цифрової трансформації галузей, що становлять суспільний інтерес, таких, як охорона здоров'я, мобільність, правосуддя, охорона навколишнього середовища, безпека, енергетична інфраструктура, освіта та навчання, а також культура, що вимагає спостереження та розширення інфраструктури цифрових послуг, які роблять можливим транскордонний обмін даними. Координація між шістьма інфраструктурами цифрових послуг проголошується відкритою для використання синергії. Крім того, цифрова трансформація повинна дозволити громадянам безпечно отримувати доступ до своїх персональних даних, використовувати їх та керувати ними через кордони, незалежно від їхнього місцезнаходження чи місцезнаходження даних[22]. Варто згадати, що Україна на момент початку повномасштабної російської збройної агресії випереджала багато держав Європейського Союзу у сфері дистанційного надання адміністративних послуг (у тому числі у цифровому форматі) та розповсюдження у багатьох сферах діяльності довірчих електронних послуг.

Слід також звернути увагу на проєкт Рішення Європейського Парламенту та Ради 2021/0293 про запровадження Політичної програми до 2030 року «Шлях до цифрового десятиліття». Підготовці цього документа передувало повідомлення Європейської Комісії від 9 березня 2021 року «Цифровий компас 2030: європейський шлях для

[21] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. URL: https://eur--lex-europa-eu.translate.goog/legal-content/EN/TXT/?uri=CELEX:32021R0694 &qid=1669541141598&_x_tr_sl=auto&_x_tr_tl=uk&_x_tr_hl=uk&_x_

[22] Там само

цифрового десятиліття» («Цифровий компас комунікації»). У цьому повідомленні було представлено бачення, цілі та шляхи успішної цифрової трансформації Європейського Союзу до 2030 р. Ця трансформація, як відкреслюється у документі, також має вирішальне значення для досягнення переходу до кліматично нейтральної та стійкої економіки. Амбіції ЄС – бути цифровим сувереном у відкритому та взаємопов'язаному світі, а також проводити цифрову політику, яка розширює можливості людей і компаній, щоб затверджувати людиноцентричні, стійкі та процвітаючі цифрові технології майбутнього. Це включає усунення вразливостей і залежностей, а також прискорення залучення інвестицій[23].

Хотілося б сказати, що нам уявляється не зовсім реалістичним усунення залежностей у цифровій сфері – враховуючи особливості та розмір капіталовкладень при появи нових цифрових технологій, держава і суспільство завжди будуть відчувати помітний вплив на свою життєдіяльність власників ІТ-підприємств та володільців авторських прав на такі технології. Хоча, безумовно, підвищення рівня прозорості у відносинах таких суб'єктів з органами публічної влади сприяло б зменшенню можливих зловживань у досліджуваній сфері.

«Шлях до цифрового десятиліття» спрямований на те, щоб Європейський Союз досягнув своїх цілей щодо цифрової трансформації суспільства та економіки у відповідності з цінностями ЄС, зміцнюючи цифрове лідерство та просуваючи орієнтацію на людину, інклюзивну та стійку цифрову політику, яка розширює можливості громадян і бізнесу. Це передбачає здійснення цифрової трансформації ЄС відповідно до цього бачення шляхом встановлення чіткого, структурованого та спільного процесу для досягнення такого результату. З цією метою «Шлях до цифрового десятиліття» встановлює конкретні цифрові цілі, досягнення яких до 2030 року базується на чотирьох кардинальних моментах: цифрові навички, цифрова інфраструктура, цифровізація бізнесу та державних послуг. Спільні цілі інститутів Європейського Союзу та держав-членів включають наступне:

а) просувати орієнтоване на людину, інклюзивне, безпечне та відкрите цифрове середовище, в якому цифрові технології та послуги сприяють повазі та зміцненню принципів та цінностей Європейського Союзу;

б) підвищити колективну стійкість держав-членів і, зокрема, скоротити цифровий розрив, просуваючи базові та спеціалізовані

[23] Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

цифрові навички для всіх та сприяючи розробці високоефективних цифрових систем освіти та навчання;

в) забезпечити цифровий суверенітет, зокрема, за рахунок безпечної та доступної цифрової інфраструктури, здатної обробляти величезні обсяги даних, що дозволяє використовувати інші технологічні розробки, що підтримують конкурентоспроможність промисловості Європейського Союзу;

г) сприяти розгортанню та використанню цифрових можливостей, що забезпечують доступ до цифрових технологій та даних на легких та справедливих умовах для досягнення високого рівня цифровізації та інноваційності на підприємствах Європейського Союзу, особливо малих та середніх;

ґ) забезпечити, щоб демократичне життя, громадські послуги та служби охорони здоров'я та догляду були доступні в Інтернеті для всіх, зокрема для вразливих груп, включаючи осіб з обмеженими можливостями, пропонуючи їм інклюзивні, ефективні та персоналізовані послуги та інструменти з високими стандартами безпеки та конфіденційності;

д) забезпечити, щоб цифрові інфраструктури та технології стали більш стійкими, енергоефективними та ресурсоефективними, а також сприяти стійкій замкнутій та кліматично нейтральній економіці та суспільству відповідно до Європейського зеленого курсу;

е) сприяти створенню конвергентних умов для інвестицій у цифрову трансформацію у всьому Європейському Союзі, у тому числі шляхом посилення синергізму між Європейським Союзом та національними фондами, та розробка передбачуваних підходів до регулювання;

є) забезпечити, щоб всі політики та програми, що стосуються досягнення цифрових цілей, враховувалися скоординованим та послідовним чином, щоб повністю сприяти цифровій трансформації[24].

Для визначення досягнення рівня досягнення вказаних цілей має застосовуватися Індекс цифрової економіки та суспільства (*Digital Economy and Society Index*, або *DESI*), який означає річний набір аналізів і показники вимірювання, на основі яких Комісія здійснює моніторинг Європейського Союзу і загальної цифрової ефективності держав-членів у кількох вимірах політики, включаючи їхній прогрес у досягненні визначених вище цифрових цілей. Інституції Європейського Союзу та держави-члени співпрацюють для досягнення наступних показників досягнення цифрових цілей до 2030 року:

[24] Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

1) населення з цифровими навичками та висококваліфіковані професіонали з цифрових технологій: принаймні 80% осіб у віці 16–74 років мають принаймні базові цифрові навички; щонайменше 20 мільйонів зайнятих у сфері інформації та зв'язку працюють як спеціалісти з технологій із конвергенцією між жінками і чоловіками;

2) безпечні, продуктивні та стійкі цифрові інфраструктури: усі європейські домогосподарства охоплені гігабітною мережею з усіма населеними пунктами, охопленими 5G; виробництво передових та стійких напівпровідників у Європейському Союзі становить не менше 20% світового виробництва у вартісному вираженні; розгорнуто принаймні 10000 кліматично нейтральних високозахищених «граничних вузлів» в Європейському Союзі, розповсюджених у спосіб, який гарантує доступ до послуг даних з низькою затримкою (кілька мілісекунд) незалежно від того, де розташовані підприємства; до 2025 року в Європейському Союзі з'явиться перший комп'ютер із квантовим прискоренням, прокладаючи шлях до того, щоб Європейський Союз був на передньому краї квантових технологічних можливості до 2030 року.

3) цифрова трансформація бізнесу: принаймні 75% підприємств Європейського Союзу взяли на себе: послуги хмарних обчислень; великі дані; штучний інтелект; охоплення понад 90% малих і середніх підприємств Союзу принаймні базовим рівнем цифрової інтенсивності; Європейський Союз нарощує коло своїх інноваційних масштабів і вдосконалюється доступ до фінансування, що призведе до принаймні подвоєння кількості підприємств з високим рівнем капіталізації активів;

4) цифровізація державних послуг: 100% доступне онлайн надання ключових державних послуг для громадян та підприємств Європейського Союзу; 100% громадян Союзу мають доступ до своїх медичних записів (електронні медичні картки (EHR)); принаймні 80% громадян Союзу використовують рішення цифрової ідентифікації (ID)[25].

У Звіті Європейської Комісії «Стан цифрового десятиліття 2025» було запропоновано вичерпний огляд цифрової трансформації ЄС. Зокрема, було акцентовано увагу на тому, що колективна відповідальність усіх держав-членів за цілі та завдання «Цифрового десятиліття» є важливою для їх досягнення та забезпечення послідовної, ефективної та інклюзивної цифрової трансформації по всьому ЄС. Держави-члени проактивно впроваджують Програму цифрової політики на десятиліття, яка є, перш за все, спільною основою для держав-членів,

[25] Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

щоб працювати разом, узгоджувати та об'єднувати ресурси у сфері цифрової політики. Усі держави-члени розробили Національні стратегічні дорожні карти Цифрового десятиліття (Національні дорожні карти), що окреслюють політику, заходи та дії, які вживаються з 2024 року для просування цифрової трансформації ЄС з 2024 року. Ухвалення дорожніх карт є значною віхою, оскільки держави-члени колективно беруть на себе зобов'язання щодо загальної кількості 1 910 заходів із загальним обсягом інвестицій у 288,6 млрд євро, що включає 205,1 млрд євро з державних бюджетів (що еквівалентно 1,14% ВВП ЄС). Держави-члени виконали 57% із 306 рекомендацій, наданих Комісією на рівні країн у 2024 році, шляхом або впровадження значних політичних змін (12%), або внесення деяких змін (45%) за допомогою нових заходів. 19 держав-членів виконали принаймні половину своїх рекомендацій за допомогою нових заходів. Серед рекомендацій на рівні ЄС понад 45% демонструють або помітний (35%), або значний прогрес (10%), з вагомими результатами у сферах, пов'язаних із розвитком штучного інтелекту, орієнтованого на людину, та захистом цифрових прав і принципів. З іншого боку, 48% рекомендацій на рівні ЄС, виданих у 2024 році, досягли лише обмеженого прогресу, а 7% не продемонстрували жодного прогресу. Ця змішана картина підкреслює, що, хоча існує чіткий імпульс до досягнення деяких цілей та завдань «Цифрового десятиліття», залишається постійна потреба у структурованих та більш рішучих політичних діях для прискорення та покращення траєкторії ЄС у цьому Десятилітті[26].

Аналіз наведених вище, а також інших актів європейського законодавства у сфері цифрової трансформації, свідчить, що досягнення поставлених перед Європейським Союзом і державами-членами цілей пов'язується із додержанням європейських демократичних цінностей та принципів, які в цілому узгоджуються з нормами українського законодавства і відображені у Конституції України, Законах України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про електронні довірчі послуги», «Про Національну програму інформатизації» та інших. Однак перманентний розвиток інформаційних технологій обумовлює необхідність постійного руху національної науки та законотворчості у напрямі, обумовленому євроінтеграційними прагненнями нашої держави.

[26] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

Формулювання принципів цифрової трансформації, узгоджених з чинними та перспективними *acquis communautaire* Європейського Союзу, уявляється нині надзвичайно важливим, оскільки зупинення руху у напряму правового забезпечення досягнення цифрових цілей призведе до фатального відставання України у сфері цифрового розвитку. Тому нам уявляється важливим формулювання узгоджених з базовими правовими актами Європейського Союзу і відповідаючих українським правовим цінностям принципів цифрової трансформації.

По-перше, це принцип солідарності, який передбачає проведення заходів цифрової трансформації у межах та на основі консолідації її суб'єктів, до яких належать громадянське суспільство України та його інститути, органи публічної влади нашої держави, правоохоронні органи, військові формування, підприємства всіх форм власності, заклади освіти, наукові установи України, а також Європейський Союз, його держави-члени, міжнародні організації. Складність та багатоплановість цифрової трансформації обумовлює, на нашу думку, широке використання засобів так званого «м'якого права» («soft law»), які можуть не мати традиційних для жорсткого права інструментів реалізації, але, разом з тим, вельми ефективно впроваджуються у площину суспільних відносин на основі вільної згоди сторін. При цьому університети, в силу їх особливого статусу академічної платформи для збору, аналізу і розповсюдження передового досвіду і найкращих практик виступають ключовим організатором заходів, за допомогою яких консолідується суспільство.

По-друге, це принцип інклюзивності, який передбачає включення до процесів цифрової трансформації всіх суб'єктів, не зважаючи на початковий рівень їх цифрової грамотності, вік, стать, стан фізичного та психічного здоров'я, національність, регіони розташування, ведення діяльності або знаходження бажаних цифрових продуктів, форму власності суб'єктів господарювання, відомчу приналежність тощо. Виклики, пов'язані з інклюзивністю у сфері цифрової трансформації, стосуються нині цифрової нерівності, яка характеризує відмінності між мегаполісами та сільськими регіонами, молоддю та людьми похилого віку, та посилюється гендерною нерівністю, притаманною суспільству з домінуванням патріархальних цінностей. Знову-таки, саме університети мають особливу роль у сфері впровадження інклюзивності, що знаходить свій прояв у розповсюдженні знань про права осіб з різним статусом, а також про найкращі практики, спрямовані на подолання цифрової нерівності з урахуванням тих перешкод, які можуть при цьому виникати.

По-третє, це принцип вільного доступу до цифрових послуг, цифрової освіти, навчання та навичок, сутність якого полягає у можливості безперешкодно скористатися цифровими продуктами та технологіями для досягнення своїх особистих, освітніх, трудових, громадських, релігійних, фінансових та інших цілей. Рівень кваліфікованості і, відповідно, рівень конкурентоспроможності працівника на ринку праці вже нині значним чином залежить від його вміння оперативно скористатися цифровими технологіями, і можна прогнозувати, що у майбутньому така закономірність буде посилюватися. Пандемія коронавірусної хвороби COVID-19 з її обмеженнями пересування внаслідок карантинних заходів несподівано мала своїми наслідками подолання стереотипів, які заважали більш широкому впровадженню цифрових технологій. Держава-агресор, крім масового геноциду українського населення, руйнування населених пунктів та критичної інфраструктури, спричинила шкоду і вільному доступу до цифрових продуктів внаслідок руйнування об'єктів енергетики. Однак ми впевнені, що відновлення за допомогою держав-партнерів енергетичної інфраструктури дозволить нашій державі досить швидко вийти на рівень максимального задоволення суб'єктів інформаційних правовідносин можливістю доступу до цифрових послуг, цифрової освіти, навчання та навичок.

Принцип свободи вибору при взаємодії з алгоритмами та системами штучного інтелекту тісно пов'язаний з питанням етики застосування штучного інтелекту, щодо яких нині ведуться активні дискусії. З одного боку, існує позиція, відповідно до якої штучний інтелект не має використовуватися у таких видах діяльності, які потребують особистісного спілкування та емпатії (викладачів, лікарів, медсестер, доглядальниць літніх людей, працівників служби підтримки), а також у професіях, представники яких наділені правом здійснення правосуддя або застосування засобів примусу (судді, військовослужбовці, правоохоронці, працівники пенітенціарних служб). Прихильники іншого підходу вважають, що саме штучний інтелект дозволить подолати всі негативні наслідки спілкування у системі «людина-людина», як то корупція, булінг, формалізм під час виконання професійних обов'язків, низька ефективність внаслідок втоми чи стресу тощо). Поки ці питання не вирішені на рівні суспільної свідомості, користувач товарів чи послуг повинен мати право відмовитися від взаємодії зі штучним інтелектом. Однак слід зазначити, що Міністерством освіти України вже розроблено і поширено у закладах освіти Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти, в яких, зокрема, зазначається, що інструменти

штучного інтелекту можуть пробудити цікавість і сприяти командній роботі, пропонуючи унікальні ресурси чи досвід, що доцільно використовувати їх для спільних заходів, як-от генерування ідей або аналізу наборів даних у групових проєктах[27]. Безумовно, такому застосуванню має передувати ретельна підготовка, що включає у тому числі створення внутрішніх університетських стандартів роботи з інструментами штучного інтелекту.

Принцип безпеки цифрового середовища виступає наріжним каменем цифрової трансформації і потребує від суб'єктів інформаційних відносин високого рівня відповідальності під час створення цифрових продуктів або користування ними. На нашу думку, логічним розвитком цього принципу у сфері трудових відносин може стати юридична відповідальність працівника за шкоду, спричинену організації його необережними діями з цифровими продуктами, що актуалізує питання цифрової грамотності у мотиваційній структурі особистості. Цікаво, що стаття 363 Кримінального кодексу України, якою передбачено кримінальну відповідальність за порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, фактично не працює – за даними Єдиного державного реєстру судових рішень з 2004 по 2025 рік жодну особу не було засуджено за вчинення вказаних дій, натомість, за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж з 2010 по 2025 рр. винесено 268 вироків. Втім, вирішення проблеми забезпечення безпеки цифрового середовища слід, на нашу думку, шукати у позитивній юридичній відповідальності, яка полягає у інтеріоризації вимог інформаційної безпеки, усвідомленні їх важливості, і оволодінні на цій основі відповідними знаннями та навичками.

Процес цифрової трансформації України дещо уповільнився внаслідок повномасштабної російської збройної агресії Російської Федерації, однак масштабні здобутки нашої держави на шляху цифровізації сфери освіти дозволяє припустити можливість швидкого відновлення та розвитку. Такий розвиток, на нашу думку, має відбуватися з урахуванням векторів руху Європейського Союзу у напряму побудови стійкого цифрового суспільства, заснованого на людиноцентризмі. Принципи солідарності, інклюзивності, вільного

[27] Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти. URL: https://storage.thedigital.gov.ua/files/5/b5/1de422b38985d037d9ba8f9f6cb2ab58.pdf

доступу до цифрових послуг, цифрової освіти, навчання та навичок, свободи вибору при взаємодії з алгоритмами та системами штучного інтелекту та безпеки цифрового середовища мають бути покладені в основу процесу цифрової трансформації нашої держави.

3. Напрями удосконалення електронних публічних освітніх послуг в умовах цифрової трансформації

Розвиток інформаційних технологій спричинив кардинальні зміни у всіх сферах суспільних відносин. Особливо чутливою до інновацій є сфера освіти, в якій постійно відбуваються процеси вдосконалення процесів та технологій завдяки появі нових освітніх інструментів. Велику роль в упорядкуванні механізмів та інструмента здійснення освітньої діяльності займає правове регулювання. Однак, крім детально унормованої формальної освіти, в Україні активно розвиваються неформальна та інформальна, правове регулювання та методологічне забезпечення яких не привертало такої великої уваги дослідників, як сфера формальної освіти. При цьому велика кількість освітніх продуктів розробляється та розповсюджується нині за участю центральних органів виконавчої влади, а також підприємств, установ та організацій, які належать до їх сфери управління (Міністерство цифрової трансформації України, Міністерство освіти і науки України, Міністерство охорони здоров'я України, установа «Центр громадського здоров'я» та низка інших). Виникають численні цифрові освітні платформи, розміщення освітніх матеріалів на яких відбувається відповідно до різних правил, зміст яких найчастіше не оприлюднюється. Не завжди можна отримати інформацію про експертну оцінку освітніх продуктів, джерела фінансування їх створення, авторські права, відсутні єдині вимоги щодо сертифікатів про проходження освітніх курсів представників різних професій (відносно врегульованою є ситуація з вимогами до сертифікатів працівників освіти та сфери охорони здоров'я, але оприлюднені освітні продукти стосуються значно більшої сфери суспільної активності)[28]. Вказане обумовлює необхідність більш детального дослідження проблем розвитку електронних публічних послуг в сфері освіти.

Проблеми, пов'язані із правовим забезпеченням надання електронних публічних послуг в Україні ще недостатньо представлені у розглядали у вітчизняних правових дослідженнях. Серед науковців, які започаткували вивчення цієї проблематики, слід назвати Є. Щербину, який дослідив процедуру надання електронної послуги в

[28] Шопіна І.М. Проблеми розвитку електронних публічних послуг у сфері освіти. *Академічні візії.* 2024. № 30. https://academy-vision.org/index.php/av/article/view/1034. DOI: https://doi.org/10.5281/zenodo.10978140

системі публічних послуг в Україні як регламентовану правовими актами діяльність органів публічної адміністрації за допомогою сучасних інформаційних комунікаційних технологій з розгляду заяви фізичної або юридичної особи про видачу адміністративного акту (дозволу (ліцензії), посвідчення, сертифіката тощо), спрямованого на забезпечення її прав і законних інтересів та/або на виконання особою визначених законом обов'язків[29]. Є. Легеза констатував необхідність прийняти концепцію вдосконалення системи надання публічних послуг, яка спрямована на розбудову сервісної, демократичної держави, основним завданням якої є обслуговування потреб споживачів послуг, забезпечення реалізації ними своїх прав, свобод і законних інтересів, і яка містить загальні положення (основні терміни, які необхідно запровадити, та їх зміст); проблеми, на розв'язання якої спрямована зазначена концепція; мету і завдання; шляхи і способи розв'язання проблем, строки реалізації концепції; очікувані результати від реалізації зазначеної концепції; обсяг фінансових, матеріально-технічних, трудових ресурсів, необхідних для реалізації концепції[30]. І. Лопушинський, В. Клюцевський та О. Момоток зясували, що ухвалення Закону України «Про особливості надання публічних (електронних публічних) послуг» є важливим кроком в напрямку спрощення та цифровізації державних послуг та загалом має позитивну оцінку. Однак вказаний Закон наразі не регулює всі сторони процесу надання публічних послуг, особливо в умовах запровадження воєнного стану в Україні, а отже для його реалізації потрібно Кабінетом Міністрів України ухвалити відповідні підзаконні нормативно-правові акти, що частково вже було зроблено, і лише після цього можна буде говорити про можливість реалізації Закону на практиці[31].

А. Стрельников у колективній монографії «Адміністративістика в умовах цифровізації: теорія, правове регулювання, практика» вказує, що суб'єктивним публічним правом, реалізація якого зазнає суттєвих змін та трансформацій, у зв'язку із цифровізацією публічного управління, є право на освіту. Згідно Конституції України всі громадяни мають право на освіту, що безпосередньо передбачає можливість отримувати від держави освітні публічні послуги, у тому числі мова йде

[29] Щербина Є. М. Характеристика процедури надання електронних послуг в системі публічних послуг в Україні. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 4. С. 185-189.

[30] Легеза Є. Основні теоретичні положення концепції публічних послуг в Україні. *Підприємництво, господарство і право.* 2016. № 9. С. 81-85.

[31] Лопушинський І., Клюцевський В., Момоток О. Особливості надання публічних (електронних публічних) послуг в умовах воєнного стану в Україні. *Наукові інновації та передові технології*. 2023. № 4 (18). С. 110–123.

про електронну освіту, яка має на меті здобуття знань, умінь та навичок у дистанційній формі за допомогою використання інформаційно-комунікаційних технологій. Автор досліджує електронне навчання, яке він визначає як форму навчання з використанням комп'ютерних і телекомунікаційних технологій, які забезпечують інтерактивну взаємодію викладачів та здобувачів освіти на різних етапах навчання і самостійну роботу з матеріалами інформаційної мережі. На думку науковця, застосування «цифрових» технологій в освіті дозволяють не лише сприяти реалізації фізичними особами свого публічного права на освіту, але і інтенсифікувати освітній процес, збільшити швидкість та якість сприйняття, розуміння та засвоєння знань[32]. Однак правове регулювання електронних публічних послуг в сфері освіти ще не здобуло достатнього висвітлення на теоретико-методологічному рівні, що визначає вектори подальших наукових розвідок.

Як ми вже згадували вище, у сучасному українському суспільстві, як і в багатьох інших демократичних країнах з високим рівнем розвитку інформаційних технологій активно розвиваються процеси цифрової трансформації. Вони здійснюють вплив на всі сфери суспільних відносин, змінюють розуміння компетенції органів публічної влади, створюють нові стандарти забезпечення прав людини і громадянина. Цифрова трансформація – це процес кардинальної перебудови організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій. Основні напрями цифрової трансформації включають: а) підвищення ефективності технологічних процесів; б) оптимізацію структури організації, змісту її діяльності та системи підготовки, прийняття та виконання управлінських рішень; в) підвищення рівня інформаційної культури та інформаційної свідомості індивідуальних і колективних суб'єктів, включаючи громадянське суспільство; г) зменшення рівня корупції, суб'єктивності та міжрегіональних бар'єрів у системі публічної служби; г) зменшення частки неефективної рутинної праці у структурі зайнятості завдяки використанню штучного інтелекту; д) створення моделі цифрового розвитку, наслідування якої сприяє більш повному задоволенню потреб та інтересів фізичних та юридичних осіб[33]. Однак, разом із безсумнівними перевагами процесів цифрової трансформації, слід вказати і

[32] Адміністративістика в умовах цифровізації: теорія, правове регулювання, практика : монографія / С. В. Ківалов, Л. Р. Біла-Тіунова, Т. А. Латковська та ін. Одеса : Видавничий дім «Гельветика», 2022. 800 с.

[33] Шопіна І., Грищук А. Поняття, напрями та суб'єкти цифрової трансформації: правові аспекти. *Правовий часопис Донбасу*. 2022. № 4(81). Ч. 1. С. 167–170. URL: https://doi.org/10.32782/2523-4269-2022-81-4-1-167-170

на існування низки проблем, головна з яких пов'язана з відставанням управлінської та правової реальності від динамічних процесів розвитку інформаційних технологій.

Закріплення у ст. 53 Конституції України права людини і громадянина на освіту ознаменувало взяття на себе державою обов'язку забезпечити реалізацію такого права за допомогою різноманітних правових механізмів. У законах України «Про освіту», «Про повну загальну середню освіту», «Про професійну (професійно-технічну освіту», «Про фахову передвищу освіту», «Про вищу освіту» та низці інших вказані правові механізми знайшли своє закріплення, що дозволяє мільйонам осіб реалізовувати свої освітні траєкторії. Особливе місце серед Національна рамка кваліфікацій – системний і структурований за компетентностями опис кваліфікаційних рівнів, призначений для використання органами державної влади та органами місцевого самоврядування, установами та організаціями, закладами освіти, роботодавцями, іншими юридичними та фізичними особами з метою розроблення, ідентифікації, співвіднесення, визнання, планування і розвитку кваліфікацій. Національна рамка кваліфікацій передбачає вісім кваліфікаційних рівнів і запроваджена з метою гармонізації норм законодавства у сферах освіти і соціально-трудових відносин, сприяння національному та міжнародному визнанню кваліфікацій, здобутих в Україні, налагодження ефективної взаємодії сфери освіти і ринку праці[34].

Ч.1 ст.8 Закону України «Про освіту» визначає, що особа реалізує своє право на освіту впродовж життя шляхом формальної, неформальної та інформальної освіти. В аспекті правового регулювання освітніх публічних послуг нас перш за все цікавить неформальна освіта, яка здобувається, як правило, за освітніми програмами та не передбачає присудження визнаних державою освітніх кваліфікацій за рівнями освіти, але може завершуватися присвоєнням професійних та/або присудженням часткових освітніх кваліфікацій[35]. Слід сказати, що неформальна освіта в її дистанційній формі отримала поштовх для активного розвитку під час пандемії короновірусної хвороби COVID-19, а з початком повномасштабної російської збройної агресії здобула значне поширення у багатьох професійних сферах.

Однією зі сфер, в якій активно застосовують заходи неформальної освіти, є сфера підвищення кваліфікації педагогічних і науково-

[34] Національна рамка кваліфікацій: затверджена постановою Кабінету Міністрів України від 23 листопада 2011 р. № 1341. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.

[35] Про освіту: Закон України від 5 вересня 2017 року № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

педагогічних працівників, які зобов'язані постійно підвищувати свою кваліфікацію з метою професійного розвитку відповідно до державної політики у галузі освіти та забезпечення якості освіти. Формами підвищення кваліфікації є інституційна (очна (денна, вечірня), заочна, дистанційна, мережева), дуальна, на робочому місці, на виробництві тощо[36].

Електронна публічна послуга – це послуга, що надається органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями, які перебувають в їх управлінні, у тому числі адміністративна послуга (у тому числі в автоматичному режимі), яка надається з використанням інформаційно-телекомунікаційних систем на підставі заяви (звернення, запиту), поданої в електронній формі з використанням інформаційно-телекомунікаційних систем (у тому числі з використанням Єдиного державного веб-порталу електронних послуг), або без подання такої заяви (звернення, запиту)[37]. Виходячи із змісту вказаного визначення, яке знайшло своє відображення у Законі України «Про особливості надання публічних (електронних публічних) послуг» до суб'єктів, які уповноважені їх надавати, слід віднести органи державної влади, органи місцевого самоврядування, підприємства, установи, організації, які перебувають в їх управлінні.

Серед органів державної влади, які надають освітні публічні послуги, одне з провідних місць займає Міністерство цифрової трансформації України, яке створило національну освітню платформу Дія.Освіта, на якій міститися більш ніж 250 освітніх продуктів. З 2020 року, коли ця платформа була створена, нею скористалися більш ніж 2,1 млн користувачів, які отримали сукупно 3,1 млн сертифікатів. Функціонування освітньої платформи Дія.Освіта здійснюється відповідно до принципу Lifelong learning – різні за своїм соціальним статусом, віком, освітнім рівнем громадяни можуть знайти освітні продукти, які здатні задовольнити їх потреби та інтереси[38].

Так, освітній серіал «Антикорупційна робота в ОМС» має своєю метою налагодження ефективної антикорупційної роботи в органі місцевого самоврядування і включає такі теми, як аналіз потенційних контрагентів, захист викривачів, знання стандартів протидії корупції, менеджмент антикорупційної роботи, мінімізація корупційних ризиків,

[36] Порядок підвищення кваліфікації педагогічних і науково-педагогічних працівників: затверджено постановою Кабінету Міністрів України від 21 серпня 2019 р. № 800. URL: https://zakon.rada.gov.ua/laws/show/800-2019-%D0%BF#n57

[37] Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 року № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text

[38] Дія.Освіта – національна едьютейнмент освітня платформа актуальних знань та навичок. URL: https://osvita.diia.gov.ua/about

організація антикорупційного навчання, оцінювання корупційних ризиків, розробка антикорупційної політики. Його створено за спільної ініціативи Мінвідновлення, Мінцифри та Фундації інституційного розвитку для платформи Дія.Освіта в межах проєкту «Прозоре відновлення громад через управління ризиками та розвиток системи комплаєнсу», що реалізується за підтримки Антикорупційної ініціативи ЄС (EUACI) – провідної програми підтримки боротьби з корупцією в Україні, що фінансується ЄС, співфінансується та реалізується Міністерством закордонних справ Данії. Цей освітній продукт рекомендовано для публічних службовців і активних громадян[39]. Призначені для вчителів, державних службовців, медичних працівників та широкого кола громадян тести цифрової грамотності дозволяють диференціювати потреби та актуальні сфери застосування цифрових знань, вмінь та навичок залежно від сфери професійної діяльності і отримати сертифікат[40]. Симулятори кількох десятків професій дозволяють отримати уявлення про особливості типового робочого дня спеціалістів різних сфер, що може стати у нагоді під час першого професійного вибору або під час зміни професії та спеціальності[41].

В деяких цифрових освітніх продуктах поєднуються зусилля багатьох суб'єктів надання освітніх публічних послуг – так, освітній серіал «Школа без цькувань» покликаний запропонувати доказові підходи для протидії боулінгу, надати знання для роботи з дітьми з особливими освітніми потребами та створення інклюзивного середовища в школі. Цей курс було розроблено громадською організацією «Студена» за ініціативи Міністерства цифрової трансформації України для платформи «Дія.Цифрова освіта», за підтримки Міністерства освіти і науки України та проєкту «Дружній простір»[42].

До здобутків Міністерства освіти і науки у досліджуваній сфері слід також віднести Всеукраїнську школу онлайн-платформу для дистанційного та змішаного навчання учнів 5–11 класів та методичної підтримки вчителів. Мета Всеукраїнської школи онлайн – забезпечити кожному українському учневі та вчителю рівний, вільний і безоплатний доступ до якісного навчального контенту. Платформа містить відеоуроки, тести та матеріали для самостійної роботи з 18 основних предметів: українська література, українська мова, біологія, біологія та екологія, географія, всесвітня історія, історія України, математика, алгебра, алгебра і початки

[39] Антикорупційна робота в ОМС. URL: https://osvita.diia.gov.ua/courses/antikorupcijna-robota-v-oms

[40] Цифрограм. URL: https://osvita.diia.gov.ua/digigram

[41] Симулятори. URL: https://osvita.diia.gov.ua/simulators

[42] «Школа без цькувань»: серіал для освітян і батьків. URL: https://mon.gov.ua/ua/news/shkola-bez-ckuvan-serial-dlya-osvityan-i-batkiv

аналізу, геометрія, мистецтво, основи правознавства, природознавство, фізика, хімія, англійська мова та зарубіжна література[43].

Активну роботу в сфері надання освітніх публічних послуг проводить державна установа «Центр громадського здоров'я», яка є науково-практичною установою медичного профілю Міністерства охорони здоров'я України, що здійснює функції з забезпечення збереження і укріплення здоров'я населення, проведення соціально-гігієнічного моніторингу захворювань, епідеміологічного нагляду та біологічної безпеки, здійснення групової та популяційної профілактики захворюваності, боротьби з епідеміями, стратегічного управління з питань громадського здоров'я[44]. На офіційному вебсайті Центру розміщено більш ніж 90 курсів з таких тем, як психічне здоров'я та соціальна підтримка, замісна підтримувальна терапія, неінфекційні захворювання, організація та управління в громадському здоров'ї, епідемічний нагляд, лабораторна діагностика, ВІЛ-інфекція, туберкульоз, вірусні гепатити та ін. Курси охоплюють низку гостроактуальних проблем, які виникають у сфері охорони здоров'я. Так, курс «Забезпечення наукової чесності та захисту морально-етичних прав осіб, які виступають суб'єктами дослідження», проходження якого дозволяє набрати 6 кредитів ЄКТС, розрахований на всіх працівників сфери охорони здоров'я, включених до розділів «Керівники» (у разі наявності освіти у галузі знань 22 «Охорона здоров'я»), «Професіонали» та «Фахівці» Довідника кваліфікаційних характеристик професій працівників (випуск 78 «Охорона здоров'я»), затвердженого наказом МОЗ від 29 березня 2002 р. № 117. Програма курсу включає 11 лекцій, у тому числі: міжнародні документи та законодавство України щодо захисту морально-етичних прав учасників дослідження, огляд існуючих етичних комітетів в Україні, Порядок подання заяви до Комісії з питань етики ЦГЗ, види експертиз тощо[45].

Широкомасштабна збройна російська агресія проти України виявила проблему недостатності навичок надання екстренної домедичної і медичної допомоги. Вказане сприяло розробці численних відеокурсів з тактичної медицини, екстреної медичної допомоги та ін. Міністерство охорони здоров'я України також є одним із суб'єктів освітньої діяльності за вказаним напрямом. Так, наприклад, на освітній платформі Prometheus розміщено цикл онлайн-курсів «Надання

[43] Всеукраїнська школа онлайн. URL: https://lms.e-school.net.ua/about

[44] Про утворення державної установи «Центр громадського здоров'я Міністерства охорони здоров'я України»: наказ Міністерства охорони здоров'я від 18 вересня 2015 року № 604. URL: https://zakon.rada.gov.ua/rada/show/v0604282-15#n28

[45] Забезпечення наукової чесності та захисту морально-етичних прав осіб, які виступають суб'єктами дослідження. URL: https://courses.phc.org.ua/courses/course-v1:PHC+122+2024/about

екстреної медичної допомоги на догоспітальному етапі», який розроблено в рамках реалізації спільного зі Світовим банком проєкту Міністерства охорони здоров'я України, а його розробником виступив Тернопільський національний медичний університет імені І. Я. Горбачевського.

Курс розрахований на медичних працівників, які працюють в системі екстреної медичної допомоги, а також інших медичних працівників, студентів та інтернів, які хочуть поглибити свої знання з медицини невідкладних станів[46].

Як можна побачити з наведеного вище, центральні органи виконавчої влади виступають активними суб'єктами надання освітніх публічних послуг. Однак ч.2 ст.6 Конституції України визначає, що органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених цією Конституцією межах і відповідно до законів України[47]. Базовим законом, яким регламентовано організацію, повноваження та порядок діяльності центральних органів виконавчої влади України, є Закон України «Про центральні органи виконавчої влади», однак в ньому відсутні повноваження означених органів щодо здійснення освітньої діяльності для широкого кола осіб – компетенція звужена до невеликого сегменту організації підготовки, перепідготовки та підвищення кваліфікації державних службовців та інших працівників міністерств та інших центральних органів виконавчої влади[48]. Відсутні і положення щодо надання означеними структурами виконавчої влади публічних послуг, згадуються лише адміністративні, у той час як коло публічних послуг значно ширше за своїм змістом.

Проникнення інформаційних технологій у всі сфери людського життя обумовлює удосконалення багатьох процесів суспільної активності, у тому числі і в галузі освіти. Навіть збереження наявного рівня професіоналізму потребує сьогодні постійного ознайомлення з новими способами та стандартами здійснення своєї професійної діяльності, а бажання професійного зростання потребує безупинного навчання в рамках формальної, неформальної та інформальної освіти. Активну роль в організації такого навчання відіграють нині центральні органи виконавчої влади та установи, підприємства й організації, що перебувають в їх управлінні. Правові можливості здійснювати таку діяльність ці органи мають у межах електронних публічних послуг.

[46] Цикл онлайн-курсів «Надання екстреної медичної допомоги на догоспітальному етапі». URL: https://prometheus.org.ua/course/course-v1:Prometheus+TE_CYCLE101+2023_T3

[47] Конституція України: офіц. текст. ІПС ЛІГА Закон Прайм. URL: https://ips.ligazakon.net/

[48] Про центральні органи виконавчої влади: Закон України від 17 березня 2011 року № 3166-VI. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Tex

Однак Закон України «Про центральні органи виконавчої влади» не передбачає можливості здійснення вказаними суб'єктами освітньої діяльності щодо осіб, що не належать до кола їх персоналу. Іншою проблемою, яка виникає у зв'язку з неврегульованістю участі міністерств та інших органів державної влади у системі надання електронних публічних послуг в освітній сфері, є відсутність єдиних стандартів для їх надання. Так, деякі з освітніх продуктів унормовані відповідно до Європейської кредитної трансферно-накопичувальної системи, включаючи відповідну кількість балів (наприклад, освітні продукти Центру громадського здоров'я), а деякі – ні. Спостерігаються значні відмінності у наявності та формі сертифіката про проходження освітнього курсу, наявності рецензентів, кількості та складності тестових питань, за допомогою яких визначається опанування змістом освітньої програми. Не завжди вказані джерела фінансування освітніх фільмів та серіалів, підготовка яких вимагає значних витрат коштів.

Безсумнівною перевагою освітніх продуктів, підготовлених за участі органів державної влади, є їх гостра актуальність та практична спрямованість, а також можливість оперативно підходити до їх створення завдяки мінімізації бюрократичних бар'єрів (якщо фінансування та звітність бере на себе міжнародна або благодійна організація). Однак, на нашу думку, підвищення якості та науковості досліджуваних освітніх продуктів, а також зниження корупційних ризиків при їх виготовленні потребують унормування найбільш важливих аспектів цієї діяльності. Зокрема, це стосується визначення компетенції центральних органів виконавчої влади щодо надання електронних публічних послуг, особливостей проведення експертного оцінювання змісту освітніх продуктів, встановлення єдиних вимог для сертифікатів, відомостей про право інтелектуальності власності, а також обов'язкового оприлюднення інформації про фінансування таких освітніх проєктів.

Правове забезпечення електронних публічних послуг у сфері освіти уявляє собою сукупність правових інструментів, за допомогою яких людина і громадянин отримує змогу реалізувати своє конституційне право на освіту в формальній, неформальній та інформальній формі з використанням інформаційно-комунікаційних технологій. Розвиток правового забезпечення освітніх електронних публічних послуг відрізняється певною нерівномірністю. Формальна освіта і правовий статус закладів освіти, які належать до сфери управління органів державної влади, здобули досить детальне правове регулювання. Однак статус самих державних органів та відмінних від закладів освіти суб'єктів, які надають електронні освітні публічні послуги, має численні прогалини та потребує свого удосконалення.

Процеси поширення цифрових освітніх продуктів, створених за участі центральних органів виконавчої влади, розпочалися в останнє десятиліття, однак активізації ця діяльність досягла під час пандемії короновірусної хвороби COVID-19, коли карантинні вимоги унеможливлювали продовження навчання в очній формі, а також потребували проведення просвітницької антиепідемічної роботи у наочній формі, доступній для різних вікових груп. Початок широкомасштабної російської збройної агресії обумовив нові вимоги до безпеки учасників освітнього процесу внаслідок постійних терористичних атак противника проти мирного населення нашої держави. Нинішній етап поширення освітніх продуктів, створених за участі органів публічної влади, свідчить про намагання постійно збільшувати аудиторію дистанційних освітніх послуг, включаючи до неї не лише студентів та осіб, зайнятих на ринку праці, а й пенсіонерів та дітей дошкільного віку. У поєднанні з високою актуальністю тем освітніх матеріалів це дозволяє зробити висновок про високий рівень активності державних щодо задоволення освітніх потреб широких верств населення, а також їх убезпечення від загроз воєнного часу завдяки просвітницькій роботі.

Однак прогалини у правовому статусі органів центральної виконавчої влади щодо надання ними електронних освітніх публічних послуг та відсутність єдиного стандарту надання таких послуг обумовлюють різні підходи до якості освітніх продуктів. Ця проблема має вирішуватися шляхом доповнення Закону України «Про центральні органи виконавчої влади» вказівкою на надання публічних послуг як частини компетенції вказаних суб'єктів. Крім того, необхідно унормувати підходи до якості та структури освітніх продуктів, створених у системі неформальної освіти, зокрема, щодо їх фінансування, експертного оцінювання, авторського права, умов отримання сертифікату та його форми.

ВИСНОВКИ

Цифрова трансформація системи освіти ставить на порядок денний питання про забезпечення прав і свобод учасників освітніх відносин, важливе місце серед яких займають інформаційні права і свободи. Динамічні процеси цифрової трансформації в Україні потребують більш активного застосування заходів інформаційної безпеки, що обумовлено зростанням кількості та інтенсивності інформаційних загроз у тих сферах суспільних відносин, в яких вказана трансформація здійснюється особливо швидкими темпами. Ці процеси перебувають у нерозривному взаємозв'язку: ефективність інформаційної безпеки обумовлює досягнення цілей цифрової трансформації, тоді як активізація процесів

цифрової трансформації викликає необхідність застосування, розвитку та вдосконалення засобів забезпечення інформаційної безпеки.

Цифрова трансформація освітніх процесів має відбуватися з урахуванням векторів руху Європейського Союзу у напряму побудови стійкого цифрового суспільства, заснованого на людиноцентризмі. Принципи солідарності, інклюзивності, вільного доступу до цифрових послуг, цифрової освіти, навчання та навичок, свободи вибору при взаємодії з алгоритмами та системами штучного інтелекту та безпеки цифрового середовища мають бути покладені в основу процесу цифрової трансформації нашої держави.

Розвиток правового забезпечення електронних освітніх публічних послуг як один із напрямів цифрової трансформації системи освіти характеризується певною нерівномірністю. Це потребує ліквідації прогалин у правовому статусі органів центральної виконавчої влади щодо надання ними електронних освітніх публічних послуг та створення єдиного стандарту надання таких послуг, що дозволить покращити якість освітніх процесів та запобігти ризиків, пов'язаних із можливим наданням здобувачам неформальної та інформальної освіти суб'єктивної, не підкріпленої науковими дослідженнями інформації.

АНОТАЦІЯ

Визначено, що процеси цифрової трансформації в Україні потребують більш активного застосування заходів інформаційної безпеки, що обумовлено зростанням кількості та інтенсивності інформаційних загроз у тих сферах суспільних відносин, в яких вказана трансформація здійснюється особливо швидкими темпами. З'ясовано причини та умови чутливості сфери освіти до інформаційних ризиків. Досліджено тенденції зростання кібератак на заклади освіти. Встановлено, що ефективність інформаційної безпеки обумовлює досягнення цілей цифрової трансформації, тоді як активізація процесів цифрової трансформації викликає необхідність застосування, розвитку та вдосконалення засобів забезпечення інформаційної безпеки.

Аргументовано, що інформаційна безпека цифрової трансформації – це ідеальна модель позбавленого інформаційних загроз середовища, в якому динамічно відбувається впровадження інформаційних (цифрових) технологій у всі сфери функціонування та життєдіяльності фізичних та юридичних осіб з метою найбільш повної реалізації ними своїх інформаційних та інших прав, свобод та інтересів. Розуміння сутності цієї моделі можливо або через суб'єктивне сприйняття суб'єктів інформаційних правовідносин, або через систему кількісних критеріїв, які характеризують досягнення цілей цифрової трансформації.

Цифрова трансформація освітніх процесів має відбуватися з урахуванням векторів руху Європейського Союзу у напряму побудови стійкого цифрового суспільства, заснованого на людиноцентризмі. Принципи солідарності, інклюзивності, вільного доступу до цифрових послуг, цифрової освіти, навчання та навичок, свободи вибору при взаємодії з алгоритмами та системами штучного інтелекту та безпеки цифрового середовища мають бути покладені в основу процесу цифрової трансформації нашої держави.

Комплексний перегляд освітньої політики та впровадження ефективних механізмів захисту інформаційного простору є надзвичайно важливими для формування особистості свідомих та відповідальних громадян демократичного суспільства. При цьому інформаційна безпека освітніх систем в умовах цифрової трансформації має розглядатися як ключовий компонент національної безпеки і важлива складова національної інформаційної політики.

Література

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

2. Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*. 2021. № 6(2). P. 137–154. DOI: 10.1080/23738871.2021.1973526.

3. Moody R. Education Ransomware Roundup: Q1-Q3 2025 stats on attacks, ransoms, and data breaches. URL: https://www.comparitech.com/news/education-ransomware-roundup-q1-q3-2025-stats-on-attacks-ransoms-and-data-breaches/

4. Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

5. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. URL: https://eur--lex-europa-eu.translate.goog/legal-content/EN/TXT/?uri=CELEX:32021R0694&qid=1669541141598&_x_tr_sl=auto&_x_tr_tl=uk&_x_tr_hl=uk&_x_

6. Reuters. University of Maastricht Says It Paid Hackers 200,000-Euro Ransom (2020). URL: https://uk. reuters.com/article/us-cybercrime-netherlands-university-idUKKBN1ZZ2HH. Цит. за: Fouad N. S. Securing

higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

7. The Fall of Afghanistan and the Taliban Victory of 2021: Was it really an Intelligence Failure? National Security Journal. 2024. Volume 6, Issue 2. https://doi.org/10.36878/nsj20241103.07

8. Top Cyber Threats to Educational Institutions in 2025. URL: https://blog.blackbaud.com/top-cyber-threats-to-educational-institutions.

9. Адміністративістика в умовах цифровізації: теорія, правове регулювання, практика : монографія / С. В. Ківалов, Л. Р. Біла-Тіунова, Т. А. Латковська та ін. Одеса : Видавничий дім «Гельветика», 2022. 800 с.

10. Антикорупційна робота в ОМС. URL: https://osvita.diia.gov.ua/courses/antikorupcijna-robota-v-oms

11. Арістова І. В. Роль інформаційної сфери та науки «інформаційне право» у досягненні цілей сталого розвитку в умовах цифрової трансформації в Україні. *Аналітично-порівняльне правознавство*. 2025. Вип. 4. Ч. 2. С. 92–96. DOI: https://doi.org/10.24144/2788-6018.2025.04.2.14

12. Всеукраїнська школа онлайн. URL: https://lms.e-school.net.ua/about

13. Дія.Освіта – національна едьютейнмент освітня платформа актуальних знань та навичок. URL: https://osvita.diia.gov.ua/about

14. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дис.-курс. *Інформація і право*. 2018. № 2(25). С. 73–85. URL: http://ippi.org.ua/sites/default/files/9_8.pdf.

15. Забезпечення наукової чесності та захисту морально-етичних прав осіб, які виступають суб'єктами дослідження. URL: https://courses.phc.org.ua/courses/course-v1:PHC+122+2024/about

16. Золотар О.О. Правові основи інформаційної безпеки людини : дис. … докт. юрид. наук: 12.00.07. Київ, 2018. 479 с.

17. Кінша Д. Україна посідає 5 місце у світі за розвитком цифрових держпослуг. URL: https://surl.li/payofz.

18. Конституція України: офіц. текст. ІПС ЛІГА Закон Прайм. URL: https://ips.ligazakon.net/

19. Легеза Є. Основні теоретичні положення концепції публічних послуг в Україні. *Підприємництво, господарство і право.* 2016. № 9. С. 81–85.

20. Лопушинський І., Клюцевський В., Момоток О. Особливості надання публічних (електронних публічних) послуг в умовах воєнного стану в Україні. *Наукові інновації та передові технології*. 2023. № 4 (18). С. 110–123.

21. Малашко О. Є., Ковалів М. В. Теоретична конструкція поняття «інформаційна безпека». *Інтернаука. Серія: «Юридичні науки».* 2020. № 10. С. 20–33. URL: https://doi.org/10.25313/2520-2308-2020-10-6350.

22. Мохнюк А. М., Скорук О. В. Організація та управління інформаційною безпекою на підприємстві: конспект лекцій. Луцьк : ПП «Поліграфія», 2017. 99 с.

23. Національна рамка кваліфікацій: затверджена постановою Кабінету Міністрів України від 23 листопада 2011 р. № 1341. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.

24. Онопрієнко С. Класифікація видів інформаційної безпеки як правової категорії. *Вісник Київського національного університету імені Тараса Шевченка. Серія: «Військово-спеціальні науки».* 2022. № 1 (49). С. 60–62.

25. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2021. № 3 (31). С. 167–179. URL: http: //doi.org/10.23939/law2021.31.167.

26. Порядок підвищення кваліфікації педагогічних і науково-педагогічних працівників: затверджено постановою Кабінету Міністрів України від 21 серпня 2019 р. № 800. URL: https://zakon.rada.gov.ua/laws/show/800-2019-%D0%BF#n57

27. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. *Відомості Верховної Ради України.* 1998. № 27-28. Ст. 181.

28. Про освіту: Закон України від 5 вересня 2017 року № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

29. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 року № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text

30. Про утворення державної установи «Центр громадського здоров'я Міністерства охорони здоров'я України»: наказ Міністерства охорони здоров'я від 18 вересня 2015 року № 604. URL: https://zakon.rada.gov.ua/rada/show/v0604282-15#n28

31. Про центральні органи виконавчої влади: Закон України від 17 березня 2011 року № 3166-VI. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Tex

32. Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти. URL: https://storage.thedigital.gov.ua/files/5/b5/1de422b38985d037d9ba8f9f6cb2ab58.pdf

33. Симулятори. URL: https://osvita.diia.gov.ua/simulators

34. Цикл онлайн-курсів «Надання екстреної медичної допомоги на догоспітальному етапі». URL: https://prometheus.org.ua/course/course-v1:Prometheus+TE_CYCLE101+2023_T3

35. Цифрограм. URL: https://osvita.diia.gov.ua/digigram

36. «Школа без цькувань»: серіал для освітян і батьків. URL: https://mon.gov.ua/ua/news/shkola-bez-ckuvan-serial-dlya-osvityan-i-batkiv

37. Шопіна І., Грищук А. Поняття, напрями та суб'єкти цифрової трансформації: правові аспекти. Правовий часопис Донбасу. 2022. № 4(81). Ч. 1. С. 167–170. URL: https://doi.org/10.32782/2523-4269-2022-81-4-1-167-170

38. Шопіна І.М. Інформаційна безпека цифрової трансформації. *Вісник ЛьвДУВС*. 2023. № 1. С. 28–35. DOI https://doi.org/10.32782/2311-8040/2023-1-4

39. Шопіна І.М. Принципи цифрової трансформації України крізь призму досвіду Європейського Союзу. *Південноукраїнський правничий часопис. Тематичний випуск з питань євроінтеграції.* 2022. № 4. С. 29–34. DOI https://doi.org/10.32850/sulj.2022.4.3.6

40. Шопіна І.М. Проблеми розвитку електронних публічних послуг у сфері освіти. *Академічні візії.* 2024. № 30. https://academy-vision.org/index.php/av/article/view/1034.
DOI:https://doi.org/10.5281/zenodo.10978140

41. Щербина Є. М. Характеристика процедури надання електронних послуг в системі публічних послуг в Україні. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 4. С. 185–189.

Information about the author:
Shopina Iryna Mykolayivna,
Doctor of Law, Professor,
Professor at the Department of Administrative and Legal Disciplines
Lviv State University of Internal Affairs,
26, Horodotska Str., Lviv, 79000, Ukraine