DOI: https://doi.org/10.32782/2524-0072/2021-30-30

УДК 331.103.2:349.2+004

ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНО-ТРУДОВІЙ СФЕРІ: ВИКЛИКИ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

INFORMATION SECURITY IN THE SOCIAL AND LABOR SPHERE: CHALLENGES OF ECONOMY DIGITALIZATION

Новікова Ольга Федорівна
доктор економічних наук, професор, заступник директора,
Інститут економіки промисловості Національної академії наук України
ORCID: https://orcid.org/0000-0002-8263-1054

Азьмук Надія Анатоліївна
доктор економічних наук, доцент, провідний науковий співробітник,
Інститут економіки промисловості Національної академії наук України
ORCID: https://orcid.org/0000-0002-6650-328X

Novikova Olga, Azmuk Nadiya
Institute of Industrial Economics, National Academy of Sciences of Ukraine

У статті досліджено концептуальні та правові засади становлення інформаційної безпеки у соціально-трудовій сфері в умовах переходу до цифрової економіки. Визначено основні передумови зниження інформаційної безпеки: розрив у цифрових навиках носіїв людського капіталу та недостатній рівень цифрової культури. Обґрунтовано виокремлення двох площин інформаційної безпеки у соціально-трудовій сфері: результат праці у цифровій формі та персональні дані. Основними ризиками у першій площині є незаконне заволодіння результатами праці та порушення авторських прав працівника, або виконавця замовлення. Друга площина характеризується неправомірним використанням персональних даних. Обґрунтовано необхідність виокремлення захисту персональних даних зайнятих через цифрові трудові платформи. Запропоновано стратегічні напрямки посилення інформаційної безпеки у сфері соціально-трудових відносин в умовах цифровізації національної економіки.

Ключові слова: інформаційна безпека, інформаційна безпека у соціально-трудовій сфері, цифрові компетенції, цифрова культура, зайнятість через платформи, персональні дані.

В статье исследованы концептуальные и правовые основы становления информационной безопасности в социально-трудовой сфере в условиях перехода к цифровой экономике. Определены основные предпосылки снижения информационной безопасности: разрыв в цифровых навыках носителей человеческого капитала и недостаточный уровень цифровой культуры. Обоснованно выделение двух плоскостей информационной безопасности в социально-трудовой сфере: результат работы в цифровой форме и персональные данные. Основными рисками в первой плоскости являются незаконное завладение результатами труда и нарушения авторских прав. Вторая плоскость характеризуется неправомерным использованием персональных данных сотрудника или исполнителя заказа. Обоснована необходимость выделения защиты персональных данных занятых через цифровые трудовые платформы. Предложены стратегические направления усиления информационной безопасности в сфере социально-трудовых отношений в условиях цифровизации национальной экономики.

Ключевые слова: информационная безопасность, информационная безопасность в социально-трудовой сфере, цифровые компетенции, цифровая культура, занятость через платформы, персональные данные.

The introduction of digital technologies in business has radically changed the workplace, having transformed the content, nature, work process and forms of its organization, as well as the interaction between the subjects of social and labor relations. It has made the issue of information security in the social and labor sphere acute. The purpose of the article is to study the conceptual, legal basis for the implementation of information security in the social and labor sphere in the formation of national digital economy and substantiate strategic directions for minimizing information threats in the social and labor sphere. The article examines the features of the formation and implementation of information security in the social and labor sphere in the transition of the national economy to digital form. The main causes that result in reducing information security in the context of economy digitalization are identified. A gap in the digital competencies of human capital carriers is revealed. The imbalance is considered to be the result

of mismatch between skill levels that shape digital competence. Insufficient level of digital culture among population is identified as a threat to information security. The expansion of digital culture components is offered. The separation of two planes of information security in the social and labor sphere is substantiated. The first one is the protection of personal data of employees as well as the work platform entities, with the latter having a higher level of danger. The second one is the protection of information data, such as the result of work in the form of information and intellectual property rights. The main risks in the first plane are illegal seizure of work results and infringement of employee's or executor's copyrights. The second plane is characterized by the misuse of employees' or executors' personal data. Strategic directions of strengthening information security in the field of social and labor relations under the conditions of national economy digitalization are offered. The main directions of improving information security are identified: minimization of imbalance in skills that constitute digital competence; formation of digital culture in the field of social and labor relations; standardization of the status of labor platform subjects; regulation of compliance with intellectual property rights created in digital form.

Keywords: information security, information security in the social and labor sphere, digital competencies, digital culture, employment through platforms, personal data.

Постановка проблеми. Впровадження цифрових технологій значно випереджає за темпами інституційний, соціальний, правовий розвиток суспільства, тим самим формуються умови для зниження інформаційної безпеки, насамперед у сфері соціально-трудових відносин.

Впровадження роботехніки, штучного інтелекту, бездротового зв'язку та інших технологій в бізнес та виробничі процеси змінили підходи до організації праці. Бізнес-процеси у цифровій формі вийшли за фізичні межі підприємств та перемістилися в Інтернет-простір. Цифровізація бізнесу докорінним чином змінила трудову сферу, трансформував зміст, характер, процес праці та форми її організації, а також взаємодію між суб'єктами соціально-трудових відносин. Це загострило питання забезпечення інформаційної безпеки у соціально-трудовій сфері.

Серед проблем, які зумовлені цифровізацією бізнес-процесів та потребують розв'язання у соціально-трудовій сфері зазначимо такі: недостатній рівень цифрової компетенції представників робочої сили; необізнаність працівників щодо цифрової безпеки; нерозвиненість цифрової культури, зокрема корпоративної.

Виникає потреба дослідження двох напрямів інформаційної безпеки у соціально-трудовій сфері. Перша – це захист персональних даних працівників підприємств та суб'єктів трудових платформ. Де останні мають вищий рівень небезпеки. Друга – захист інформаційних даних, таких як результат праці в інформаційному вигляді та права інтелектуальної власності.

Аналіз останніх досліджень і публікацій. У центрі уваги сучасних науковців знаходяться питання цифровізації економіки та соціально-трудової сфери зокрема. Значна кількість публікацій вітчизняних та закордонних науковців присвячена дослідженню впливу цифрових технологій на сферу праці та пошуку шляхів мінімізації їх деструктивного впливу. В рамках нашого дослідження доцільно виокремити наступні праці. Роботу Краус Н., Краус К., Маслова А. (2021), в якій представлено результати вивчення відцифрованого інтелектуального капіталу. Автори представляють рамку «цифрової людини» через визначення «генетичного коду» цифрового підприємництва [1]. Ґрунтовно вивчають формування нової парадигми праці 4.0 в умовах цифрових трансформацій Колот А., Герасименко О. (2020) [2]. Дослідники (Zysman, J., & Kenney, M., 2018) визначають тренди цифровізації та вивчають цифрові виклики у трудовій сфері. Автори акцентують на залежності майбутнього робочої сили від соціально-політичних рішень національних регуляторів. Такі рішення обумовлюють траєкторію розвитку та використання людського капіталу: або заміщення людської праці інтелектуальними інструментами, або навпаки розширення та збагачення навичок персоналу [3].

Загрозливий характер, з точки зору інформаційної безпеки у соціально-трудовій сфері, має поширення зайнятості через трудові платформи. Окремі аспекти особливостей зайнятості через платформи в Україні висвітлено у дослідженні КМІС «Зайнятість через цифрові платформи в Україні. Проблеми і стратегічні перспективи» (2018), яке було проведено на замовлення Міжнародної організації праці [4].

В умовах цифровізації особливої актуальності набувають питання правового врегулювання платформної праці. Авторські дослідження цієї проблематики представлено у роботі [5]. Інформаційні загрози у цій сфері зумовлені таким: невизначеність статусу суб'єктів трудових платформ (виконавці – працівники, замовники – роботодавці, провайдери – власники трудових платформ); відсутність, або недотримання правил, норм

процедур цифрової безпеки у сфері взаємодії названих суб'єктів.

Питанням захисту персональних даних присвячені праці Легкої О. (2021), Пилипчука В., Брижка В. (2017) [6–7]. Дзьобань О., Соснін О. (2015) акцентують увагу на вивченні загроз у сфері інформаційної безпеки, що зумовлені розвитком інформаційно-комп'ютерних технологій [8]. У роботі Воронкової В., Капітаненко Н., Нікітенко В. (2019) досліджено умови захисту інтелектуальної власності в умовах цифровізації [9].

Водночас обмаль досліджень присвячених питанням інформаційної безпеки саме у соціально-трудовій сфері в умовах цифровізації економіки.

Метою статті є дослідження концептуальних, правових засад реалізації інформаційної безпеки в соціально-трудовій сфері в умовах становлення національної цифрової економіки та обґрунтування стратегічних напрямків мінімізації інформаційних загроз у соціально-трудовій сфері.

Виклад основного матеріалу. Впровадження цифрових технологій у всі сфери життєдіяльності людини актуалізує питання пов'язані з інформаційною безпекою. Розвиток інформаційно-комунікаційних технологій випереджає за темпами опанування цифрових компетенцій переважною кількістю носіїв людського капіталу. Це зумовлює зростання загроз у сфері забезпечення цифрової безпеки особи, підприємства та держави в цілому.

За даними ресурсу Internet World Stat станом на 31 березня 2021 р. 65,6% населення світу користувалися інтернетом. Для Європи цей показник станом на 31 грудня 2020 р. становив 87,7%. Щодо України частка користувачів Інтернету від загальної кількості населення становила 94,9% [9]. За кількістю користувачів серед країн Європи Україна входить в ТОР-10 та посідає 8 позицію.

Зростання доступу населення до інформації обумовлює збільшення рівня інформаційних загроз. «І особистість, і суспільство, і держава постійно знаходяться в стані інформаційної небезпеки. Їм постійно загрожують у будь-якій формі заподіяти фізичної, моральної або матеріальної шкоди їх інтересам» [8].

Особливої актуальності ця теза набуває в суспільстві, де з одного боку, *переважна частина населення має доступ до Інтернету*, водночас *не має достатніх цифрових навичок*, а головне, *не має усвідомлення та розуміння цифрових ризиків.*

До таких країн і належить Україна, яка характеризується *доступним Інтернетом*, зокрема мобільним та його широким використанням. Серед 230 країн світу Україна посіла 31 сходинку за доступністю мобільного Інтернету з середньою вартістю одного гігабайта 0,75 дол. США у 2021 р. Найнижча середня вартість гігабайта в Ізраїлі (0,05 дол. США), найвища у найменш розвинутих країнах, де сягає позначки 49,67 дол. США у Гвінеї, острівних країнах: Фолклендські острови – 44,56 дол. США, Острів Святої Єлени – 39,87 дол. США. Середня вартість гігабайта у розвинутих країнах коливається від 0,27 дол. США в Італії до 5,81 дол. США у Норвегії [10].

Водночас в Україні є понад 17 тис. населених пунктів, що не охоплені оптичними мережами жодного оператора. Понад 4 млн українців мешкають у селах, де немає якісного фіксованого інтернету [11]. Попри це, Україна належить до країн з розвинутим та доступним Інтернетом.

Щодо *цифрових навичок* населення, то за результатами дослідження Міністерства цифрових трансформацій України 37,9% серед опитаних у віці від 18 до 70 років мають цифрові навички нижче базових, 15,1% взагалі не володіють ними, що становить разом 53,0%. В ході дослідження було опитано 1800 осіб [12].

Водночас, населення Україні вирізняється високим рівнем володіння *інформаційними* (пошук, перегляд, опрацювання цифрової інформації) та *комунікаційними* (взаємодія і спілкування у мережах) навичками. Частка респондентів, які володіють *просунутими інформаційними навичками* становить 74,4% в середньому по країні, 76,1% – серед молоді 10-17 років [12].

На увагу заслуговує факт значної частки населення, яка опанувала *просунуті комунікаційні навички* у цифровому середовищі. Частка таких осіб в Україні складає 75,3%, а серед молоді 10-17 років – 86,2% [12].

Наведені результати дослідження свідчать про значний ***розрив у навичках***, які мають доповнювати одна одну та складати єдину цифрову компетенцію. Частка населення з просунутими інформаційними та комунікаційними навичками перевищує частку населення з просунутими цифровими навичками майже в 3 рази. *Такий дисбаланс у навичках, необхідних для життя і роботи у цифровому середовищі створює передумови для* ***формування загроз цифровій безпеці населення.***

Позитивним у цій сфері є затвердження Концепції розвитку цифрових компетентностей та затвердження плану її реалізації [13]. Ця концепція передбачає реалізацію комп-

лексу завдань, спрямованих на розвиток цифрових компетентностей носіїв людського капіталу, правового регулювання цієї сфери та підвищення обізнаності щодо небезпек в Інтернеті.

Ця ситуація посилюється ще й тим, що українському суспільстві не розвинутою є соціальна відповідальність та цифрова культура, що обумовлює низький рівень дотримання порядку, правил та процедур. Це певним чином зумовлює нехтування правилами безпеки та вимагає поряд з навчанням людського капіталу цифровим навичкам запроваджувати заходи щодо формування та розвитку ***цифрової культури***.

Цифрова культура суспільства є базовою засадою інформаційної безпеки. До складових цифрової культури включають: раціональне споживання інформації, критичне мислення, цифрова грамотність, IT-волонтерство, «зелене використання» ІКТ [14]. Цей перелік доцільно доповнити такими компонентами: безпекова обізнаність (кіберкультура) та розуміння і усвідомлення відповідальності за дії, вчинені особою у віртуальному просторі.

Важливою складовою цифрової культури є кіберкультура. Елементи глобальної кіберкультури визначено у резолюції 57/239 Генеральної асамблеї ООН, а саме: обізнаність; відповідальність; вчасне реагування; етика; демократія; оцінка ризику; проектування і впровадження засобів забезпечення безпеки; управління забезпеченням безпеки; переоцінка [15].

Забезпечення реалізації елементів визначених складових є невід'ємною частиною інформаційної безпеки країни. В умовах цифровізації економіки цифрова культура стає частиною національної культури.

Цифровізація бізнес-процесів трансформує процес праці та потребує нових форм організації праці. Усталені форми організації праці є обтяжливими та неефективними, оскільки ієрархічні структури є занадто повільними, з ускладненою комунікацією всередині та довгим ланцюгом передання команд. Нова форма передбачає гнучку структуру із залученням фрілансерів до тимчасових проєктних груп. При цьому залучення людської праці відбуватися у віртуальний спосіб.

Цифрова організація праці за допомогою ІКТ забезпечує ефективне функціонування системи «людина – техніка – знання – середовище» [16]. Ключовими напрямками, які визначають сутнісні аспекти цифрової організації праці є: мережева взаємодія через корпоративні мережі та трудові платформи; цифрова мобільність / цифрова міграція; цифрові інструменти (сервіси), які дозволяють в режимі «реального часу» працювати спільно над проектами; цифрові системи оплати праці; законодавчі норми та правила цифрової зайнятості, цифрової безпеки.

Така організація праці стала можлива через перенесення процесу праці та соціально-трудових відносин у віртуальний простір. Основними формами цифрової організації праці є цифрові трудові платформи та корпоративні ресурси.

Цифрові трудові платформи виступають як посередники між замовниками послуг (роботодавцями) та виконавцями (працівниками) та встановлюють правили та стандарти взаємодії. Поряд з цим, цифрові трудові платформи не несуть жодної відповідальності за дотримання авторських та суміжних прав на інтелектуальну власність; гарантування оплати праці виконавця за виконане замовлення; дотримання норм часу на працю та відпочинок; поширення нелегальної трудової зайнятості тощо.

За даними опитування МОП в Україні серед респондентів 11% мають тривалість робочого тижня 35-49 годин; 14% – 50-85 годин; 7% – більше ніж 86 годин. Окремою проблемою є непоодинокі випадки не оплати вже наданих послуг, з такими випадками стикалися 32% респондентів [4].

Ще однією вадою діяльності трудових платформ у національному вимірі є масштабування тіньової зайнятості та прихованих трудових відносин у віртуальному (цифровому) просторі. Оскільки доступ до отримання завдань та їх оплати після виконання відбувається у цифровий спосіб, здебільшого це відбувається без укладання трудової або цивільно-правової угоди. За результатами опитування МОП 48% [4] респондентів не мають офіційного статусу зайнятої, або самозайнятої особи, тобто є фактично неформально зайнятими.

Відбувається формування віртуального середовища, яке знаходиться фактично поза зоною дії та моніторингу національного регулятора. За відсутності практики регулювання соціально-трудових відносин на платформі формується середовище з високим ризиком інформаційних загроз щодо витоку інформації, її крадіжки та неправомірного використання. Тут доцільно виокремити ***дві безпекові площини***: цифровий результат праці та персональні дані.

Основними ризиками у першій площині є *незаконне заволодіння результатами праці у цифровій формі* без належної оплати, або отриманням неправомірної вигоди у сфері порушення авторських прав. Інформаційні ризики зумовлені відсутністю регламентації соціально-трудових відносин на платформах та невизначеністю правового статусу суб'єктів домовленості, що створює сприятливі умови для неправомірних дій.

Друга площина це *неправомірне використання персональних даних*. Використання платформ для пошуку замовлень (роботи) актуалізувало питання захисту персональних даних користувачів. За збереження персональних даних мають нести відповідальність провайдери, в цьому випадку власники трудових платформ. Проте кожен провайдер має власні правила щодо використання отриманої від користувачів інформації, які не завжди гарантують належне збереження та виключають використання з комерційною метою.

Ще однією формою організації праці у цифровій економіці є корпоративні ресурси, які забезпечують одночасний доступ працівників компанії до виконання проєктних завдань. Основні загрози полягають у слабкому програмному захисті корпоративної інформації в тому числі персональних даних працівників, об'єктів інтелектуальної власності, новітніх розробок у цифровій формі.

Поза увагою залишився *трудовий аспект*, а саме регламентація обробки персональних даних, які надають користувачі провайдерам – трудовим платформам. «Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [17]. Чіткий перелік інформації, яка належить до персональних даних в законі не наведено.

Персональними даними у випадку ***зайнятості через платформи*** є: прізвище, ім'я користувача, запис зображень (фото, відео), інформація про освіту і кваліфікацію, номер мобільного телефону, електрона адреса, електронні ідентифікаційні дані (трафік, IP-адреса), дані про геолокацію, дані про транспортний засіб (у випадку з Глово, Убер, Уклон, Болт тощо), дані банківської карти тощо. Ці та інші дані користувач трудової платформи надає при реєстрації, або заповненні акаунту та, як правило, автоматично дає згоду на їх обробку. Можна стверджувати, що власники трудових платформ збирають, накопичують персональні дані своїх користувачів та формують базу персональних даних. «База персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних» [17].

«Володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом» [17]. Власники трудових цифрових платформ є володільцями та, як правило, розпорядниками персональних даних, якщо право бути розпорядником не передано іншій фізичній чи юридичній особі.

На відміну від соціальних мереж та інших ресурсів для користувача трудової платформи надання правдивих персональних даних є обов'язковою вимогою для отримання замовлення (роботи). У соціальній мережі користувач може використовувати вигадане ім'я, не розміщувати особисті фото та відео та не має надавати дані банківської карти. Водночас провайдер – трудова платформа не бере на себе повну відповідальність за належне збереження, використання та вчасне знищення отриманої інформації. Ці та інші аспекти оговорюються у політиці конфіденційності та захисту даних.

Такий стан справ зумовлений тим, що статус самого виконавця (користувача) з точки зору трудового права є невизначеним, так само як і статус власника трудової платформи. Виконавцями на платформах можуть бути як самозайняті особи, так і особи без статусу зайнятої особи. Платформи позиціонують себе лише як майданчики, які створюють умови для взаємодії та відмовляються від будь-яких гарантій.

У сфері інформаційної безпеки відкритими залишаються питання ***захисту результату праці*** під час його передачі від виконавця до замовника у цифровій формі. У цифровому виробництві, результат праці набуває нематеріальної форми та має вигляд інформації. Поряд з іншими результатами цифрового виробництва це обумовлює додатковий захист.

Ще однією сферою, яка потребує уваги щодо інформаційної безпеки є *право на інтелектуальну власність*. За даними Компанії «Gartner» починаючи з 2018 року, лише 3D-друк призведе до щорічних глобальних втрат у сфері інтелектуальної власності на суму понад 100 мільярдів доларів» [18].

Питання інформаційної безпеки у цифровому виробництві постає гостро та поряд з цим

вимагає *дотримання суб'єктами соціально-трудових відносин майнових та немайнових прав на інтелектуальну власність*.

Аргументованими є висновки М. Гудмана, що «правовий захист інтелектуальної власності у цифровому суспільстві вимагає формування нової правової системи», яка включає «норми, правила, очікування, цілі, інструкції та стимули, що трансформували спосіб створення правових цінностей та цілковито змінили світ» [18].

Ці питання є надзвичайно важливими та потребують нагального вирішення, особливо за умов поширення зайнятості через цифрові платформи. Взаємодія між замовником та виконавцем ґрунтується на довірі, як правило суб'єкти платформ не укладають письмових угод, провайдер захищає лише свої інтереси.

Визначені проблеми інформаційної безпеки у соціально-трудовій сфері за умов цифрових трансформацій не знайшли місця у проекті Стратегії інформаційної безпеки України [19] ні серед інформаційних загроз, ні серед 8 стратегічних цілей та шляхів їх досягнення.

Наведені вище обґрунтування обумовили розробку пропозицій до проекту Стратегії інформаційної безпеки України.

Пропонується врахувати такі основні напрями підвищення інформаційної безпеки у соціально-трудовій сфері:

1. Зменшення розриву між цифровими та інформаційними, між цифровими та комунікаційними навичками.

2. Формування цифрової культури у сфері соціально-трудових відносин.

3. Унормування статусу суб'єктів трудових платформ.

4. Забезпечення дотримання прав на інтелектуальну власність, створену у цифровій формі.

До кожного визначеного напряму посилення інформаційної безпеки у соціально-трудовій сфері необхідно визначити та реалізувати заходи, які повинні знайти відповідне місце у Плані заходів з реалізації Стратегії інформаційної безпеки.

Висновки.

1. Передумовами виокремлення інформаційної безпеки соціально-трудової сфери з загальної безпекової царини є перенесення соціально-трудових відносин у віртуальний простір.

2. У сфері інформаційної безпеки соціально-трудових відносин доцільно виокремити дві площини: перша стосується захисту персональних даних, друга – захисту результатів праці у цифровій формі та права на інтелектуальну власність.

Особливої гостроти набуває захист персональних даних для зайнятих через трудові платформи, вразливість яких зумовлена насамперед невизначеністю статусу.

Результатом цифрового виробництва є цифровий продукт, який переважно не має уречевленої форми є об'єктом інформаційної безпеки як і права інтелектуальної власності.

3. Стратегічними напрямами підвищення інформаційної безпеки у соціально-трудовій сфері є:

– зменшення розриву між цифровими та інформаційними, між цифровими та комунікаційними навичками;

– формування цифрової культури у сфері соціально-трудових відносин;

– унормування статусу суб'єктів трудових платформ;

– забезпечення дотримання прав на інтелектуальну власність, створену у цифровій формі.

4. Розв'язання питання щодо розриву у навичках носіїв людського потенціалу полягає:

– в оновленні та модернізації наявних програм у сфері цифрової грамотності в закладах освіти з врахуванням вимог рамки цифрових компетенцій для громадян України;

– впроваджені програм «Цифрова грамотність для дорослих», «Заснування власного бізнесу з використанням переваг цифрових технологій» для підготовки осіб, які мають статус безробітних;

– заснування цифрових хабів в рамках співпраці між закладами вищої, професійної освіти і бізнес-структурами.

5. Підвищення рівня інформаційної безпеки у сфері праці вимагає формування цифрової культури у суб'єктів соціально-трудової сфери. Важливим заходом щодо посилення інформаційної безпеки на трудових платформах є запровадження тристороннього електронного договору, форма якого має бути визначення на законодавчому рівні, як і його обов'язковість.

6. Унормування статусу суб'єктів трудових платформ як сторін соціально-трудових відносин дозволить вивести такі відносини у правове поле та забезпечить значно вищий рівень інформаційної безпеки щодо збереження персональних даних, результату праці у цифровій формі та прав інтелектуальної власності. Це потребує оновлення трудового законодавства та закону щодо захисту прав інтелектуальної власності.

7. Ефективність становлення концептуальних, правових та стратегічних засад забезпечення інформаційної безпеки в соціально-трудовій сфері за умов цифровізації економіки залежить від збалансованості дій інститутів державної виконавчої влади, які несуть відповідальність за інформаційну, трудову та цифрову політику. Але інституційне забезпечення подолання інформаційних небезпек у соціально-трудовій сфері при цифрових трансформаціях не відбувається. Запропоновані стратегічні засади будуть сприяти збалансованості управлінських рішень щодо інформаційного, трудового та цифрового розвитку на принципах безпеки. Їх доцільно врахувати при доопрацюванні проекту Стратегії інформаційної безпеки України та Плану заходів з її реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Краус Н.М., Краус К.М., Маслов А.О. Інституціонально-еволюційні фрейми ментальності «цифрової людини» як «генетичного коду» цифрового підприємництва. *Ефективна економіка*. 2021. № 3. URL: http://www.economy.nayka.com.ua/?op=1&z=8734 DOI: https://doi.org/10.32702/2307-2105-2021.3.4

2. Колот А.М., Герасименко,О.О. Концепт "Праця 4.0": теоретико-прикладні засади формування та розвитку. *Економіка і прогнозування.* 2020. № 1. С. 7–31. DOI: https://ir.kneu.edu.ua:443/handle/2010/34494

3. Zysman, J., & Kenney, M. The next phase in the digital revolution: intelligent tools, platforms, growth, employment. *Communications of the ACM*. 2018. 61(2), 54–63. DOI: https://doi.org/10.1145/3173550

4. Зайнятість через цифрові платформи в Україні. Проблеми і стратегічні перспективи. МОП. 2018. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_635371.pdf

5. Азьмук Н.А. Зайнятість через цифрові платформи – нова реальність сучасної економіки: виклики та стратегії адаптації. *Економічний простір*. 2019. № 152. С. 66–80. DOI: https://doi.org/10.32782/2224-6282/152-6

6. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Міжнародне право.* 2021. № 2(31). URL: http://biblio.umsf.dp.ua/jspui/handle/123456789/4358 DOI: https://doi.org/10.32836/2521-6473.2021-2.15

7. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*. 2017. № 3. С. 36–50. URL: http://visnyk.kh.ua/web/uploads/journals_pdf/323242422.pdf#page=36

8. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. *Гуманітарний вісник Запорізької державної інженерної академії*. 2015. № 61. С. 24–34. URL: http://vestnikzgia.com.ua/article/view/47745

9. Internet usage statistics. *Internet World Stat.* 2021. URL: https://www.internetworldstats.com/stats.htm

10. Worldwide mobile data pricing 2021. *Cable.co.uk.* 2021. URL: https://www.cable.co.uk/mobiles/worldwide-data-pricing/

11. Федоров М. Понад 5,5 млн. українців не можуть отримати якісний фіксований інтернет. *Українська правда*. 2020. URL: https://www.pravda.com.ua/columns/2020/07/30/7261199/

12. Цифрова грамотність населення України. *Міністерство цифрової трансформації України*. 2019. URL: https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf

13. Концепція розвитку цифрових компетенцій. Розпорядження КМУ від 03.03.2021 № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

14. Літвінова К. Про компоненти цифрової культури. *Digitle Blog*. URL: https://digitle.wordpress.com/2016/10/04/12499875/

15. Создание глобальной культуры кибербезопасности (2003) : Резолюция Генеральной Ассамлеии ООН. URL: https://www.un.org/ru/documents/decl_conv/conventions/elements.shtml

16. Савельева Е.А. Цифровая организация труда: направления, принципы, подходы. *Экономика труда*. 2018. № 5(4). С. 935–950. URL: https://www.elibrary.ru/download/elibrary_37111715_84842660.pdf

17. Про захист персональних даних : Закон України, 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

18. Гудмен М. Злочини майбутнього. Харків : Вид-во «Ранок» : Фабула, 2019. 592 с.

19. Стратегія інформаційної безпеки: проект. *Міністерство культури та інформаційної політики України.* 2021. URL: https://mkip.gov.ua/files/pdf/45698712365.pdf

REFERENCES:

1. Kraus N., Kraus K., Maslov A. (2021) Instytutsionalno-evoliutsiini freimy mentalnosti “tsyfrovoi liudyny” yak “henetychnoho kodu” tsyfrovoho pidpryiemnytstva [Institutional-evolutionary frames of the mentality of “digital man” as a “genetic code” of digital entrepreneurship”]. *Efektyvna ekonomika*, [Online], vol. 3. Available at: http://www.economy.nayka.com.ua/?op=1&z=8734 DOI: https://doi.org/10.32702/2307-2105-2021.3.4 (in Ukrainian)

2. Kolot A., Herasymenko O. (2020) Kontsept "Pratsia 4.0": teoretyko-prykladni zasady formuvannia ta rozvytku [Labor 4.0 Concept theoretical-applicable principles of formation and development]. *Ekonomika i prohnozuvannia*, vol. 1. Available at: https://ir.kneu.edu.ua:443/handle/2010/34494 (in Ukrainian)

3. Zysman, J., & Kenney, M. (2018) The next phase in the digital revolution: intelligent tools, platforms, growth, employment. *Communications of the ACM*, 61(2), 54–63. Available at: https://dl.acm.org/doi/fullHtml/10.1145/3173550 DOI: https://doi.org/10.1145/3173550

4. Zainiatist cherez tsyfrovi platformy v Ukraini. Problemy i stratehichni perspektyvy (2018) ILO. Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_635371.pdf (in Ukrainian)

5. Azmuk N. (2019) Zainiatist cherez tsyfrovi platformy–nova realnist suchasnoi ekonomiky: vyklyky ta stratehii adaptatsii [Digital employment platform as a new reality of modern economy: challenges and adaptation strategies]. *Ekonomichnyi prostir*, 152, 66–80. DOI: https://doi.org/10.32782/2224-6282/152-6 (in Ukrainian)

6. Lehka O. V. (2021) Current issues of personal data protection: domestic and international experience. *Mizhnarodne pravo,* 2(31). Available at: http://biblio.umsf.dp.ua/jspui/handle/123456789/4358 DOI: https://doi.org/10.32836/2521-6473.2021-2.15 (in Ukrainian)

7. Pylypchuk V., Bryzhko V. (2017) Transformatsiia systemy zakhystu personalnykh danykh ta pryvatnosti v konteksti yevrointehratsii Ukrainy [Transformation of the Personal Data and Privacy Protection System in the Context of European Integration of Ukraine]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy,* 3, 36–50. Available at: http://visnyk.kh.ua/web/uploads/journals_pdf/323242422.pdf#page=36 (in Ukrainian)

8. Dzoban A., Sosnin A. (2015) Transformatsiia systemy zakhystu personalnykh danykh ta pryvatnosti v konteksti yevrointehratsii Ukrainy [Information security: new dimensions threats related information and communication sphere]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, 61, 24–34. Available at: http://vestnikzgia.com.ua/article/view/47745 (in Ukrainian)

9. Internet usage statistics. *Internet World Stat.* 2021. Available at: https://www.internetworldstats.com/stats.htm

10. Worldwide mobile data pricing 2021. *Cable.co.uk.* 2021. URL: https://www.cable.co.uk/mobiles/worldwide-data-pricing/

11.Fedorov M. (2020) Ponad 5,5 mln. ukraintsiv ne mozhut otrymaty yakisnyi fiksovanyi internet. *Ukrainska pravda*. Available at: https://www.pravda.com.ua/columns/2020/07/30/7261199/ (in Ukrainian)

12. Tsyfrova hramotnist naselennia Ukrainy (2019) Ministerstvo tsyfrovoi transformatsii Ukrainy. Available at: https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf (in Ukrainian)

13. Kontseptsiia rozvytku tsyfrovykh kompetentsii. Rozporiadzhennia KMU vid 03.03.2021 № 167-r. Available at: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text (in Ukrainian)

14. Litvinova K. Pro komponenty tsyfrovoi kultury. *Digitle Blog*. Available at: https://digitle.wordpress.com/2016/10/04/12499875/ (in Ukrainian)

15. Creation of a global culture of cybersecurity: Resolution adopted by the General Assembly 57/239 (2003) United Nations. Available at: https://digitallibrary.un.org/record/482184

16. Saveleva E.A. (2018) Tsyfrovaia orhanyzatsyia truda: napravlenyia, pryntsypy, podkhody [Digital organization of labor: directions, principles, approaches]. *Ekonomika truda*, 5(4), 935–950. Available at: https://www.elibrary.ru/download/elibrary_37111715_84842660.pdf (in Russian)

17. Pro zakhyst personalnykh danykh : Zakon Ukrainy. 01.06.2010 r. № 2297-VI. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (in Ukrainian)

18. Hudmen M. (2019) Zlochyny maibutnoho [Crimes of the future]. Kharkiv: Vyd-vo «Ranok»: Fabula, 592 p. (in Ukrainian)

19. Stratehiia informatsiinoi bezpeky: proekt (2021) Ministerstvo kultury ta informatsiinoi polityky Ukrainy. Available at: https://mkip.gov.ua/files/pdf/45698712365.pdf (in Ukrainian)