

ТРУДОВЕ ПРАВО; ПРАВО СОЦІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ
LABOR LAW; THE RIGHT TO SOCIAL SECURITY

УДК 349.2

DOI: 10.26565/2075-1834-2021-32-02

ІНФОРМАЦІЙНА БЕЗПЕКА СУБ'ЄКТІВ ТРУДОВОГО ПРАВА

Шабанова С. О.,

кандидат юридичних наук,
асистентка кафедри трудового права
Національного юридичного університету
імені Ярослава Мудрого,
61024, вулиця Пушкінська, 77, Харків, Україна
e-mail: shabanovasophiya@gmail.com
orcid: <https://orcid.org/0000-0001-9813-8179>

Лазебна А. В.,

бакалавр права, студентка 5 курсу
факультету адвокатури
Національного юридичного університету
імені Ярослава Мудрого,
61024, вулиця Пушкінська, 77, Харків, Україна
e-mail: lazebnaya3003@gmail.com
orcid: <https://orcid.org/0000-0002-0475-5836>

АНОТАЦІЯ. *Вступ.* Процеси цифровізації бізнесу, запровадження нових форм організації виробництва і праці значно випереджають урегулювання таких інновацій у правничому середовищі.

Постановка проблеми. Архаїчність трудового законодавства порівняно з тенденціями розвитку цифрової економіки спричиняє виникнення підстав для зниження рівня інформаційної безпеки суб'єктів трудових правовідносин.

Актуальність обумовлена недосконалістю нормативного врегулювання основних засад інформаційної безпеки, застарілістю норм трудового законодавства, низьким рівнем цифрової культури населення України, внаслідок чого виникає нагальна потреба у дослідженні інформаційної безпеки суб'єктів трудового права.

Мета. Вивчення шляхів модернізації механізмів забезпечення інформаційної безпеки роботодавців та працівників, викликане тенденцією до поєднання трудових відносин з інформаційними технологіями.

Методи. Теоретичні та загальнонаукові (аналіз, синтез, систематизація), емпіричний метод (метод порівняння).

Основні результати дослідження. Міжнародно-правове регулювання значно випереджає розвиток національного законодавства щодо інформаційної безпеки. Український законодавець вбачає у цьому процесі ілюзорність, оминаючи масштабність технологічного розвитку та можливих «цифрових» проблем. Дедалі більше процес праці переміщується у віртуальний простір. Ця тенденція створила умови для успішного розвитку цифрових трудових платформ. Учасники трудових правовідносин в Україні потребують оновлення механізмів захисту від інформаційних загроз, пов'язаних з діджиталізацією діяльності, а також модернізації захисту трудових прав працівників. З метою створення належних умов праці, роботодавці повинні контролювати трудову діяльність робітників, але у способи, що не порушують їх основоположних прав і свобод.

Висновки. Обов'язок забезпечення невтручання до приватного життя необхідно здійснювати за допомогою єдиного загальнонаціонального нормативного регулятора. Органи державної влади уповноважені на забезпечення невтручання до приватного життя суб'єктів трудового права. Необхідно закріпити механізми захисту учасників трудових правовідносин від інформаційних загроз на рівні єдиного загальнообов'язкового нормативно-правового акту та врегулювати статус цифрових трудових платформ з метою забезпечення захисту прав інтелектуальної власності, гарантій оплати виконаної роботи, недопущення поширенню тіньової зайнятості працівників.

КЛЮЧОВІ СЛОВА: інформаційна безпека, персональні дані, трудові правовідносини, цифровізація, корпоративні ресурси, моніторинг працівників.

INFORMATION SECURITY OF LABOR LAW SUBJECTS

Sofia Shabanova,

Candidate of Law,
Assistant of the Department of Labor Law
of the Yaroslav the Wise National Law University,
61024, 77 Pushkinska Street, Kharkiv, Ukraine
e-mail: shabanovasophiya@gmail.com
orcid: <https://orcid.org/0000-0001-9813-8179>

Anna Lazebna,

Bachelor of Law, 5th year student
of the Faculty of Advocacy
of the Yaroslav the Wise National Law University,
61024, 77 Pushkinska Street, Kharkiv, Ukraine
e-mail: lazebna3003@gmail.com
orcid: <https://orcid.org/0000-0002-0475-5836>

ANNOTATION. *Introduction.* The processes of digitalization of business, the introduction of new forms of organization of production and labor are much ahead of the settlement of such innovations in the legal environment.

Formulation of the problem. The archaic nature of labor legislation in comparison with the trends of the digital economy gives rise to grounds for reducing the level of information security of the subjects of labor relations.

The relevance is due to the imperfection of the normative regulation of the basic principles of information security, the obsolescence of labor legislation, the low level of digital culture of the population of Ukraine, resulting in an urgent need to study the information security of labor law.

Goal. The study of ways to modernize the mechanisms of information security of employers and employees, caused by the tendency to combine labor relations with information technology.

Methods. Theoretical and general scientific (analysis, synthesis, systematization), empirical method (method of comparison).

The main results of the study. International legal regulation is significantly ahead of the development of national legislation on information security. The Ukrainian legislator sees this process as illusory, bypassing the scale of technological development and possible "digital" problems. Increasingly, the work process is moving into cyberspace. This trend has created the conditions for the successful development of digital work platforms. Participants in labor relations in Ukraine need to update the mechanisms of protection against information threats related to the digitalization of activities, as well as the modernization of protection of labor rights of employees. In order to create appropriate working conditions, employers must control the work of workers, but in ways that do not violate their fundamental rights and freedoms.

Conclusions. The obligation to ensure privacy must be exercised through a single national regulatory framework. Public authorities are authorized to ensure non-interference in the private life of subjects of labor law. It is necessary to establish mechanisms to protect labor relations participants from information threats at the level of a single mandatory legal act and regulate the status of digital labor platforms to protect intellectual property rights, guarantee payment for work performed, prevent the spread of shadow employment.

KEY WORDS: information security, personal data, labor relations, digitalization, corporate resources, employee monitoring.

Вступ. Постановка проблеми. Процеси цифровізації бізнесу, запровадження нових форм організації виробництва і праці значно випереджають урегулювання таких інновацій у правничому середовищі. Архаїчність трудового законодавства порівняно з тенденціями розвитку цифрової економіки спричиняє виникнення підстав для зниження рівня інформаційної безпеки суб'єктів трудових правовідносин.

Актуальність обраної теми обумовлена недосконалістю нормативного врегулювання основних засад інформаційної безпеки, застарілістю норм трудового законодавства, низьким рівнем цифрової культури населення України, внаслідок чого виникає нагальна потреба у дослідженні інформаційної безпеки суб'єктів трудового права.

Проблеми порушення права на захист персональних даних працівників, порушення права інтелектуальної власності та захисту інформаційних даних (результатів праці у вигляді інформації), а також необхідність створення ефективної системи моніторингу діяльності працівників задля оптимізації трудової діяльності підкреслюють актуальність дослідження цього питання.

Метою дослідження є вивчення шляхів модернізації механізмів забезпечення інформаційної безпеки роботодавців та працівників, викликане тенденцією до поєднання трудових відносин з інформаційними технологіями.

Серед основних завдань можна виділити такі: 1) аналіз нормативного врегулювання захисту персональних даних працівників; 2) виявлення тенденцій для запровадження механізмів забезпечення інформаційної безпеки; 3) дослідження процесу моніторингу працівників: його законності та меж допустимості. Як підсумок, необхідно окреслити конкретні механізми захисту права працівників на приватне життя, а також виокремити законні засоби моніторингу діяльності працівників.

Огляд праць з даної проблематики. Інформаційна безпека суб'єктів трудового права являється предметом досліджень багатьох науковців та юристів-практиків. О.Ф. Новікова та Н.А. Азьмук досліджували питання інформаційної безпеки в соціально-трудої сфері, приділили увагу проблемі захисту персональних даних працівників підприємств та суб'єктів цифрових трудових платформ, а також захисту інформаційних даних та права інтелектуальної власності. М.Г. Ісаков та В.Г. Паркулаб займалися вивченням міжнародного досвіду захисту персональних даних працівників, розглядали законність моніторингу діяльності працівників. С.В. Вишневецька приділила увагу вивченню окремих аспектів інформаційної безпеки суб'єктів трудового права з посиланням на практику Європейського суду з прав людини (далі – ЄСПЛ). О.І. Войнаровська дослідила процедуру моніторингу діяльності працівників та порядку законного впровадження такої процедури.

Тема інформаційної безпеки в соціально-трудої сфері є актуальною серед науковців, проте відсутнє єдине консолідоване дослідження недосконалості врегулювання інформаційної безпеки суб'єктів трудового права у національному законодавстві з аналізом конкретних проблем та варіантів їх вирішення.

Основні результати дослідження. Глобальний розвиток інформаційних технологій взаємопов'язаний із модифікацією законодавства країн світу, що значною мірою охоплює і галузь трудового права.

За статистичними даними, станом на 2021 рік, 65,6 % населення світу користується Інтернет-ресурсами. Європейські країни демонструють найбільшу залученість до мережі Інтернет – 87,7 % населення. У свою чергу українці випереджають навіть такі показники користування Інтернетом, їх відсоток складає 93,4 [1].

Запровадження інформаційно-комунікаційних технологій управління трудовими ресурсами сприятиме заміні застарілого вертикального (бюрократичного) режиму управління гнучким цифровим менеджментом. Проте, активне зростання доступу до інформаційних ресурсів вимагає від працівників належного рівня цифрової компетенції та цифрової культури. Незважаючи на те, що відносини «роботодавець - працівник» значно модернізувались, з'явилися нові можливості пошуку роботи, змінилися пріоритети при працевлаштуванні та форми організації трудової діяльності, ці можливості спричинили значне зростання загроз інформаційної небезпеки.

Європейські правові стандарти пріоритезують право на повагу до приватного життя. Реалізація цього права прямо пов'язана з забезпеченням захисту та недоторканості персональних даних. Органи державної влади зобов'язані забезпечити невтручання до приватного життя. Винятком є втручання, що відповідає критеріям законності та необхідності у демократичному суспільстві [2].

Яскравим прикладом налагодженого механізму захисту персональних даних є італійська система захисту. Міністерство праці та соціальної політики Італії використовує систему, яка виконує процедуру реальної автентифікації. Після такої процедури користувачі убезпечені від веб-сайтів невідомого походження, що підлягають автоматичному блокуванню. Для підвищення ефективності організації людських ресурсів, агенції з працевлаштування мають можливості обробляти величезні обсяги інформації, обмінюватись та отримувати доступ до таких даних, а також можуть швидко розповсюджувати інформацію працівникам [3].

Окрім впровадження передових технологій в організацію виробництва та праці, швидкість та якість процесу законотворчості у сфері забезпечення інформаційної безпеки європейських роботодавців та працівників не поступається технологічному прогресу.

Міжнародно-правове регулювання значно випереджає розвиток національного законодавства щодо інформаційної безпеки. Український законодавець вбачає у цьому процесі ілюзорність, оминаючи масштабність технологічного розвитку та можливих «цифрових» проблем.

Відсутність належної уваги з боку національних органів законодавчої влади до питання інформаційної безпеки суб'єктів трудового права створює ланцюжкову реакцію з прогалинами у правничому полі. Незахищеність суб'єктів трудового права в інформаційному полі, відсутність механізмів протидії посяганням на персональні дані, нерегульованість допустимих меж втручання у приватне життя працівників – це перелік, що характеризує низький рівень захищеності від інформаційної небезпеки в Україні.

Учасники трудових правовідносин в Україні потребують оновлення механізмів захисту від інформаційних загроз, пов'язаних з діджиталізацією діяльності, а також модернізації захисту трудових прав працівників.

Єдиний законодавчо регламентований механізм захисту персональних даних працівників продемонстровано у рішенні ЄСПЛ у справі «Суриков проти України». Відповідно до положень Кодексу законів про працю України (далі – КЗпП України) працівники мають право на здорові і безпечні умови праці. Забезпечення безпечних і нешкідливих умов праці покладається на власника або уповноважений ним орган [4].

Забезпечення здорових та безпечних умов праці передбачає і обов'язок захисту персональних даних працівників. Очевидно, що така свобода розсуду, надана національному роботодавцю, не має на меті створення ефективного механізму захисту даних працівників від посягань третіх осіб. Сучасний стан нормативного закріплення гарантії захисту даних працівників не демонструє готовність захистити конфіденційні дані від поширення третім особам, а відтак і третіми особами, зокрема колегами працівника [5].

У проєкті Кодексу законів про працю України дещо ширше надається тлумачення положення про створення безпечних умов праці в аспекті інформаційної безпеки суб'єктів трудового права. Зокрема, пропонується додати до переліку зобов'язань роботодавця, обов'язки щодо забезпечення захисту та конфіденційності персональних даних працівника в порядку, встановленому законодавством, а також у будь-який час на вимогу працівника ознайомлення його з персональними даними, внесення змін до них у разі їх невідповідності фактичним даним [6].

Прийняття нового Кодексу законів про працю України є розтягнутим у часі процесом, проте позитивним зрушенням є той факт, що, розробляючи проєкт Кодексу, законодавець вже враховує необхідність закріплення положень про захист та конфіденційність персональних даних.

У 2020 році Указом Президента України затверджено Стратегію національної безпеки України. На основі положень цієї Стратегії розробляється Стратегія інформаційної безпеки. Варто зазначити, що галузь трудового права загалом не являється предметом врегулювання цих документів. Можна презюмувати, що державні органи опікуються більш глобальними питаннями національної політики та розглядають питання захисту суверенітету, протидії дезінформації, загальнонаціональних загроз та викликів.

Стратегія інформаційної безпеки закріплює питання інституалізації соціальних мереж. Дійсно, незважаючи на те, що приватне життя є основоположним правом людини, діджиталізація все ж таки внесла свої корективи. Збільшення кількості соціальних мереж, їх інтегрованість з іншими сервісами та загальнодоступність ставлять під загрозу право особи на приватність [7].

Така тенденція простежується у трудових правовідносинах. Необхідно усвідомлювати, що кожна особа має бути захищена ще до працевлаштування, перебуваючи у статусі кандидата на посаду. Прийом на роботу супроводжується перевіркою соціальних мереж потенційного працівника як джерела інформації особистого характеру. У певних випадках, відбір працівників за їх особистим контентом може нести дискримінаційний характер [3]. З метою забезпечення захисту прав працівників в аспекті захисту персональних даних, власник або уповноважений ним орган має протидіяти будь-яким проявам суб'єктивізму, заснованого на аналізі акаунтів у соціальних мережах. Допустимими є лише випадки, коли необхідність врахування даних із соціальних мереж дійсно обумовлена специфікою діяльності працівника.

Дедалі більше процес праці переміщується у віртуальний простір. Ця тенденція створила умови для успішного розвитку цифрових трудових платформ [8]. Така система організації праці стає посередником між роботодавцями (замовниками) та працівниками, які мають надати відповідну послугу. Безперечно, що швидкість, мобільність та загальнодоступність є перевагами такої моделі організації праці, проте з її виникненням постала проблема відсутності механізмів захисту прав інтелектуальної власності, забезпечення гарантій оплати виконаної роботи, загроза поширення тіньової зайнятості працівників тощо. Такі ризики зумовлені відсутністю нормативного регулятора у віртуальному просторі. Допоки національний законотворець не врегулює статус цифрових трудових платформ, подібна цифровізація відносин «роботодавець - працівник» не зможе вважатись повноцінною організацією процесу праці.

Корпоративні ресурси являються ще однією системою організації діяльності на підприємствах [8]. Непоодинокими є випадки, коли група працівників має виконувати єдине проєктне завдання з сумісним доступом до даних. Ризик втрати корпоративної інформації, результатів праці, персональних даних працівників має нівелюватись потужним програмним забезпеченням. Власник або уповноважений ним орган має забезпечувати схоронність такої інформації на підприємстві.

Діяльність роботодавців спрямовується на захист комерційної таємниці та забезпечення трудової дисципліни. З цією метою керівники підприємств вдаються до багатьох засобів моніторингу виробничих процесів, проте непоодинокими є випадки порушення права на приватне життя працівників з боку самого роботодавця через застосування неправомірних заходів моніторингу та активністю працівників [9].

Контроль за станом справ на підприємстві, аналіз діяльності працівників, пошук шляхів удосконалення виробництва може досягатись шляхом всебічного моніторингу.

Ще у 2006 році Україною ратифіковано Європейську соціальну хартію (переглянуту), яка закріплює право кожного на гідне ставлення на роботі. Задля забезпечення ефективного реалізації цього права необхідно: 1) поглиблювати поінформованість, поширювати інформацію про сексуальні домагання на робочому місці або у зв'язку з виконанням роботи, сприяти запобіганню таким домаганням і вживати всіх відповідних заходів для захисту працівників від такої поведінки; 2) поглиблювати поінформованість,

поширювати інформацію про систематичні непорядні або явно негативні та образливі дії щодо окремих працівників на робочому місці або у зв'язку з виконанням роботи, сприяти запобіганню таким діям і вживати всіх відповідних заходів для захисту працівників від такої поведінки [10].

У Законі України «Про інформацію» передбачено, що кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [11].

З метою створення належних умов праці, роботодавці повинні контролювати трудову діяльність робітників, але у способи, що не порушують їх основоположних прав і свобод.

Науковці пропонують декілька форм моніторингу: 1) моніторинг телефонних розмов; 2) відеоспостереження 3) GPS-технології [12].

Законодавством України передбачаються гарантії забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. З огляду на це, поінформованість працівників про встановлення механізмів контролю за має бути обов'язковою. Власник або уповноважений ним орган має видати наказ про здійснення запису телефонних розмов, відеоспостереження чи моніторингу місцезнаходження, з яким будуть ознайомлені всі працівники підприємства.

У рішенні ЄСПЛ у справі «Копланд проти Сполученого Королівства» суд зазначає, що у певних ситуаціях моніторинг телефонних розмов, електронної пошти та інтернету може визнаватись «необхідним у демократичному суспільстві» [13].

У національному трудовому законодавстві загалом не врегульовані межі допустимості втручання роботодавця у приватне життя працівників. Зважаючи на те, що оновлення трудового законодавства – це довгий період часу, доцільно було власнику або уповноваженому ним органу приймати корпоративні правила, предметом регулювання яких буде процедура моніторингу працівників, а також регламент користування соціальними мережами з метою забезпечення неухильного дотримання права працівників на приватне життя.

Висновки. Світовий технологічний прогрес суттєво впливає на права та обов'язки суб'єктів трудового права. Пріоритезується право на конфіденційність та недоторканість приватного життя працівників, виникає нагальна потреба в нормативному врегулюванні положень щодо забезпечення інформаційної безпеки, а також необхідність у встановленні меж допустимого контролю з боку роботодавця за діяльністю працівників.

Обов'язок забезпечення невтручання до приватного життя необхідно здійснювати за допомогою єдиного загальнонаціонального нормативного регулятора. Органи державної влади уповноважені на забезпечення невтручання до приватного життя суб'єктів трудового права.

Закріплення прав та обов'язків працівників і роботодавців щодо забезпечення інформаційної безпеки може відбуватись такими шляхами.

1) Закріплення механізмів захисту учасників трудових правовідносин від інформаційних загроз на рівні єдиного загальнообов'язкового нормативно-правового акту;

3) Врегулювання положення щодо створення безпечних умов праці в аспекті інформаційної безпеки суб'єктів трудового права у новому Кодексі законів про працю України;

4) Забезпечення захисту та контролю за законністю процесу працевлаштування з метою протидії проявам суб'єктивізму уповноважених на прийняття нових працівників осіб, заснованого на аналізі акаунтів у соціальних мережах, покласти такий обов'язок на власника підприємства або уповноважений ним орган;

5) Врегулювання статусу цифрових трудових платформ з метою забезпечення захисту прав інтелектуальної власності, гарантій оплати виконаної роботи, недопущення поширенню тіньової зайнятості працівників;

6) Організація встановлення потужного програмного забезпечення на підприємствах з метою недопущення втрати корпоративної інформації, результатів праці та персональних даних працівників;

7) Запровадження корпоративних правил на підприємствах, предметом регулювання яких буде процедура моніторингу працівників, а також регламенту користування соціальними мережами з метою забезпечення дотримання трудової дисципліни на підприємствах з вимогою обов'язкового ознайомлення кожного працівника з порядком впровадження та застосування засобів моніторингу діяльності.

ЛІТЕРАТУРА

1. Internet usage statistics. *Internet World Stat.* 2021. Available at: <https://www.internetworldstats.com/stats.htm>.
2. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. (ратифіковано Законом № 475/97-ВР від 17.07.1997). URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 10.11.2021).
3. М.Г. Ісаков, В.Г. Паркулаб. Особливості трудових відносин у сучасних умовах інформаційних технологій. Науковий вісник публічного та приватного права. 2019. № 5. С. 96-102. DOI: <https://doi.org/10.32844/2618-1258.2019.5-1.17>.
4. Рішення Європейського Суду з прав людини у справі «Суріков проти України» від 26.04.2017 заява № 42788/06. URL: <https://ips.ligazakon.net/document/SOO00966> (дата звернення: 10.11.2021).

5. Кодекс законів про працю України: Кодекс України від 10.12.1971 № 322-VIII. Верховна Рада УРСР. URL: <https://zakon.rada.gov.ua/laws/show/322-08> (дата звернення: 09.11.2021).
6. Проект Трудового кодексу України: проект Кодексу України від 08.11.2019 № 2410. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67331 (дата звернення: 08.11.2021).
7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 №392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 10.11.2021).
8. О.Ф. Новікова, Н.А. Азмук. Інформаційна безпека в соціально-трудої сфері: виклики цифровізації економіки. Економіка та суспільство. 2021. № 30. DOI: <https://doi.org/10.32782/2524-0072/2021-30-30>.
9. М.А. Клочков, Ю.М. Полетаев. Материальная ответственность работодателя перед работником: теоретические и практические аспекты : научно-практическое пособие. Москва : Проспект. 2016. С. 110-115.
10. Європейська соціальна хартія (переглянута) від 03.05.1996 (ратифіковано Законом № 137-V від 14.09.2006). URL: https://zakon.rada.gov.ua/laws/show/994_062#Text (дата звернення: 06.11.2021).
11. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 06.11.2021).
12. О.І. Войнаровська, О.Г. Подольак. Моніторинг працівників. Правовий тиждень. 2013. URL: <http://legalweekly.com.ua/index.php?id=16061&show=news&newsid=123063>.
13. Рішення Європейського Суду з прав людини у справі «Sorland проти Сполученого Королівства» від 03.07.2007 заява № 62617/00. URL: <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-117767&filename=001-117767.pdf&TID=ihgdqbxnfi> (дата звернення: 10.11.2021).

REFERENCES

1. Internet usage statistics. Internet World Stat. 2021. Available at: <https://www.internetworldstats.com/stats.htm>
2. Convention for the Protection of Human Rights and Fundamental Freedoms. (4 November 1950). Ratified by Law № 475/97-VR of 17 July 1997. Retrieved from https://zakon.rada.gov.ua/laws/show/995_004.
3. 10. About the statement of the State sanitary rules of planning and building of settlements/ (1996).
4. M. Isakov, V. Parkulab. (2019). Features of labor relations in modern conditions of information technologies. Scientific Bulletin of Public and Private Law. № 5. 96-120. DOI: <https://doi.org/10.32844/2618-1258.2019.5-1.17>.
5. Judgment of the European Court of Human Rights in the case “Surikov v. Ukraine” (26 April, 2011). Application № 42788/06. Retrieved from <https://ips.ligazakon.net/document/SOO00966>.
6. Labor Code of Ukraine. (1971). Code of Ukraine of December 10, 1981 № 322-VIII. Retrieved from <https://zakon.rada.gov.ua/laws/show/322-08>.
7. Draft Labor Code of Ukraine. (2019). Draft Code of Ukraine of November 8, 2019. № 2410. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67331.
8. On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine". (2020). Decree of the President of Ukraine of September 14, 2020 №392/2020. Retrieved from <https://www.president.gov.ua/documents/3922020-35037>.
9. O. Novikova Olga, N. Azmuk. (2021). Information security in the social and labor sphere: challenges of economy digitalization. Economy and society. № 30. DOI: <https://doi.org/10.32782/2524-0072/2021-30-30>.
10. M.Klochkov, Y. Poletaev. (2016). Liability of the employer to the employee: theoretical and practical aspects: scientific and practical manual. Moscow: Prospectus. 110-115.
11. European Social Charter (revised). (03.05.1996). Ratified by Law № 137-V of September 14, 2006. Retrieved from https://zakon.rada.gov.ua/laws/show/994_062#Text.
12. On information. (1992). Law of Ukraine of October 02, 1992 № 2657-XII. Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
13. O. Voinarovska, O. Podoliak. (2013). Employee monitoring. Legal week. Retrieved from <http://legalweekly.com.ua/index.php?id=16061&show=news&newsid=123063>.