МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Навчально-науковий інститут публічного управління
Кафедра менеджменту, публічного управління та персоналу

БЕРЕЗА Надія Вікторівна

Удосконалення діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю. / Improving the activity of the state authority body in matters of ensuring compliance with labor legislation.

спеціальність: 281 - Публічне управління та адміністрування
освітньо-професійна програма - Публічне управління та адміністрування

Кваліфікаційна робота

Виконала студентка групи
ДСПУАзм-21
Н. В. Береза
_____

Науковий керівник:
д.е.н., професор, Г. Л.
Монастирський
_____

Кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **М. М. Шкільняк**

ТЕРНОПІЛЬ - 2024

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Різноманітність характеру і змісту праці знаходить своє відображення у різноманітності видів праці. Найчастіше виділяють чотири групи ознак, які відрізняють той чи інший вид трудової діяльності: зміст і характер праці; предмет і продукт праці; засоби і способи праці; умови праці. Ефективний менеджмент передбачає чітку регламентацію для встановлення меж, рамок діяльності державних органів, установ, організацій і підприємств. Результатом цього є регламент, який являє собою сукупність правил, положень, що визначають порядок роботи будь-якої організаційної системи, а також проведення офіційних заходів, нарад, засідань і ін., місце управління на кожному рівні ієрархії, місце в системі суспільного виробництва тощо. Розроблені і прийняті регламенти підвищують організованість, надійність, якість і культуру менеджменту. У практиці регулювання трудових відносин та організації праці надзвичайно важлива регламентація трудової діяльності працівників, чітко формалізований опис посадових обов'язків співробітників і засоби забезпечення цих обов'язків. Головним інструментом при вирішенні даних завдань є Посадова інструкція, що є локальним організаційним документом, в якому визначено завдання, функції, основні права, обов'язки і відповідальність працівника при здійсненні ним трудової діяльності відповідно до посади, займаної відповідно до трудового договору.

Ступінь висвітлення в літературі. Різносторонність та багатогранність процесу регламентування праці персоналу організацій знайшла своє відображення у працях багатьох науковців. Питання, що стосуються науково-методичних форм організації праці та регламентації трудової діяльності працівників докладно відображені в працях вітчизняних фахівців (В. В. Травіна, В.А. Дятлова, Г.Г. Мелікьяна, Р.П. Колосової).

Однак, дослідження системи регламентування праці персоналу організацій на даний час залишається актуальним.

Метою дослідження є розробка практичних рекомендацій щодо вдосконалення діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю.

Відповідно до визначеної мети були поставлені наступні **завдання:**

– дослідити теоретико – правові та методичні засади регламентування діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю;

– проаналізувати механізм регламентування діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю;

– здійснити оцінку інформаційно-комунікаційного забезпечення регламентування діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю;

– розробити напрями щодо удосконалення системи діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю.

Об’єктом дослідження є діяльність Південно-Західного міжрегіонального управління Державної служби з питань праці .

Предметом дослідження є механізм регламентування діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю.

Методи дослідження. Науково-методичною основою дослідження виступають чинні законодавчі, нормативно-правові акти та науково-методичні положення з визначених питань. При вирішенні поставлених у дипломній роботі завдань застосовано такі методи: метод SVOT-аналізу, системного аналізу, метод вибіркового спостереження, метод порівняння, метод експертних оцінок.

Практичне значення одержаних результатів полягає у тому, що обґрунтовані наукові положення і рекомендації є основою для вирішення науково-практичних проблем забезпечення діяльності органу державної влади в питаннях забезпечення дотримання законодавства про працю.

РОЗДІЛ 1
ТЕОРЕТИКО – ПРАВОВІ ТА МЕТОДИЧНІ ЗАСАДИ РЕГЛАМЕНТУВАННЯ ПРАЦІ ПЕРСОНАЛУ ОРГАНІЗАЦІЇ

1.1.Сутність і значення регламентування праці персоналу організації

У сучасній європейській економіці, що характеризується потоками інформації, послуг, фінансових ресурсів, а також працівників, спостерігаються динамічні інтеграційні тенденції. Це пов'язано з тим, що зростає взаємозалежність між окремими державами, які, з одного боку, посилаються на різноманітність, а отже, певну індивідуальність, а з іншого - прагнуть до сильної уніфікації норм і загальних стандартів, головним чином у законодавчій сфері.

Ця тенденція за своїм значенням виходить за межі європейської спільноти. Поняття міжнародної інтеграції пов'язане з міжнародною взаємозалежністю, яка є вираженням інтернаціоналізації економічних процесів і соціальних відносин.

У контексті «етіології» імплементації положень Співтовариства про захист викривачів варто зазначити, що ці мотиви сягають своїм корінням рішень, притаманних англосаксонській системі. В Європі, яка історично обплутана все ще помітними впливами, зумовленими умовним поділом на «Захід» і «Схід», викривання асоціювалося і досі асоціюється з негативними асоціаціями, тобто асоціюється з донощицтвом. Різна зрілість правових режимів, що регулюють викривання відповідно до положень Директиви, запроваджених у різних країнах ЄС (порівняння цих правових рішень наведено у Додатку), також підкреслює цей дихотомічний поділ Європи. Тому не випадково, що саме держави-члени так званого «Західного блоку» в першу чергу імплементували національне правове регулювання. Варто також зазначити, що законодавець ЄС не запроваджував правила щодо викривачів у вигляді регламенту, який би мав пряму дію в окремих країнах ЄС. Культурні,

соціальні тощо відмінності окремих держав-членів, ставлення до викривання, в тому числі історичні, та усталені стереотипи, пов'язані з наслідками викривання (страх перед репресіями), є причинами того, що в рамках так званої спільної компетенції законодавець ЄС запровадив положення про викривання у вигляді директиви, надавши певну законодавчу свободу окремим державам-членам.

З точки зору соціально-економічних аспектів, зростаючої глобалізації, переплетення капіталів і ресурсів, а також захисту суспільних інтересів, про які йдеться в цілях директиви, у законодавця ЄС немає достатніх підстав вважати, що окремі законодавчі системи держав-членів будуть однаково відповідати цілям директиви. Адже на практиці може виявитися, наприклад, що репресивні дії проти викривача будуть по-різному каратися законами окремих держав-членів ЄС. Це може призвести до недосягнення цілей Директиви на практиці, оскільки повідомлення у зв'язку з роботою відбувається, як правило (рекомендована регламентом форма), на так званому рівні компанії. Це, в свою чергу, ставить питання про те, чи буде система захисту викривачів ефективною, якщо особи, які приймають рішення (наприклад, підприємці), захочуть зважити ризики - серйозність порушення, його вплив та наслідки переслідування. Санкції, відповідно до положень Директиви, мають бути ефективними, пропорційними та стримуючими, але таке загальне формулювання підлягає індивідуальному тлумаченню. Ця полеміка важлива для підвищення обізнаності адресатів Директиви, оскільки вона стосується безпосередньо їх - тобто викривача та юридичної особи/організації (роботодавця - залежно від правовідносин між викривачем та юридичною особою[2]). Дійсно, мета на рівні установ полягає в тому, щоб трактувати положення Директиви в протилежному сенсі, ніж це випливає з її назви. Зрештою, йдеться про запобігання правовим порушенням шляхом впровадження системи викриттів та адекватного, відповідного до законодавства визначення предмета повідомлень, а не про захист викривача, виражений у спеціальному законі , як це робиться в Директиві . Зворотне сприйняття призвело б до аналізу оцінки рангу повідомлення в кожному конкретному випадку на основі своєрідної дилеми: чи

варто запобігати (розслідування та подальші дії), чи можлива відплата, наприклад, розставання з викривачем.

Таким чином, з огляду на соціально-економічну мету положень Директиви, тобто захист суспільних інтересів і права ЄС, їх можна вважати превентивними, а не інтервенціоністськими за своїм характером, оскільки лише в цьому випадку вони повністю відповідатимуть ідеї права Співтовариства. Крім того, це зобов'язання в першу чергу стосується юридичних осіб і лише в другу чергу - державної системи. Якби це було не так, законодавець ЄС не визначив би в загальних рисах (каталог порушень, що міститься в тексті директиви) і детально (каталог і посилання на інші положення, що містяться в додатку до директиви) інтереси, що підлягають захисту. З цієї причини Директиву також умовно поділяють на виключні та спільні повноваження відповідно до законодавства Європейського Союзу.

Беручи до уваги зазначені компетенції, оцінка впливу дотримання положень законодавства за правом ЄС буде описана в цьому розділі без положень, які в кінцевому підсумку будуть діяти в Україні (для ілюстрації законодавчого процесу та намірів розробників законопроекту будуть зроблені лише посилання на проект закону про захист викривачів). У поточному законодавчому процесі матеріальна та персональна сфера дії Директиви не зазнала змін, тоді як наступні проекти закону про захист викривачів суттєво відрізняються в інших аспектах - як щодо положень Директиви, так і між собою. З метою аналізу соціально-економічного контексту запобігання порушенням закону в даному питанні було зроблено припущення, що джерело встановлення положень ЄС та їх мета є більш важливими, ніж автономний спосіб, в який законодавець буде регулювати ці рішення. Характер впливу Співтовариства, а водночас і глобальний вплив, як зазначалося раніше, забезпечує точку відліку для намірів положень, їх тлумачення та застосування.

Стаття 249 Договору про заснування Європейського Співтовариства зазначає, що «Директива є обов'язковою щодо результату, який має бути досягнутий, для кожної держави-члена, якій вона адресована, але залишає

національним органам влади вибір форми і методів». На практиці це означає, що акт формулює цілі, які адресати - будь-якими засобами, формами і методами - зобов'язані досягти.

Такий підхід наштовхує на думку, що відповідальність за запобігання порушенням повністю покладається на юридичну особу, а не на державну систему (остання лише визначає форми, засоби та методи, залишаючи юридичним особам певний вибір). Державна система виконує лише контрольно-наглядову функцію і є своєрідним втручанням у забезпечення дотримання застосування права Європейського Союзу. Саме тому, серед іншого, Директива передбачає можливість нотифікації через зовнішній канал, який «експлуатується» «державним апаратом».

Неможливо також не помітити, що положення Директиви de lege lata стосуються питання «виробничих відносин» та «груп інтересів». Дійсно, є чіткі посилання на спробу усунути або, принаймні, зменшити існуючу асиметрію між роботодавцями та працівниками. Оскільки саме юридична особа несе відповідальність за запобігання порушенням закону та захист викривачів, це означає, що ми маємо справу із запобіганням своєрідній схильності організації (як групи інтересів, яка може мати так званий високий ступінь ризику) переслідувати власний інтерес (переважно економічний) не завжди у відповідності до закону. З точки зору трудових відносин (як найбільш постійної форми зайнятості, а отже, такої, що підлягає захисту), організовані інтереси праці та капіталу виникають природним чином[3]. Крім того, представники працівників (профспілки) також повинні мати свою автономну вагу в контексті захисту положень Директиви. Прикладом може слугувати проект регулювання законодавства про захист викривачів у Україні, згідно з яким процедура викриття підлягає консультаціям з профспілковими організаціями. Більше того, в кінцевому підсумку може статися так, що процедура вимагатиме узгодження з профспілковими організаціями, що надасть профспілкам більше повноважень у цій сфері (еволюція цього рішення простежується в наступних проектах закону про захист викривачів).

Окремим питанням, до якого не залишився байдужим законодавець ЄС, є підвищення обізнаності про викривання (що підпадає під соціальний вплив Директиви). У ст. 47 Директиви зазначено, що "Для ефективного виявлення та запобігання порушенням права Союзу важливо, щоб відповідна інформація надходила до тих, хто знаходиться найближче до джерела проблеми, хто має найкращі можливості для її розслідування та повноваження, якщо це можливо, для її виправлення. Тому, як правило, викривачів слід заохочувати до використання внутрішніх каналів повідомлення в першу чергу , а також до повідомлення своєму роботодавцю, якщо вони можуть скористатися такими каналами і можуть обґрунтовано очікувати, що повідомлення, зроблене таким чином, буде успішним. Особливо це стосується випадків, коли особи, які повідомляють про порушення, вважають, що порушення може бути ефективно усунуто в межах організації та не існує ризику помсти. Таким чином, юридичні особи в приватному та державному секторах повинні встановити відповідні внутрішні процедури для отримання та подальшого розгляду повідомлень. Таке заохочення також поширюється на випадки, коли такі канали були створені, навіть якщо такого зобов'язання не було передбачено законодавством ЄС або національним законодавством. Цей принцип має сприяти просуванню належної комунікації та корпоративної соціальної відповідальності в організаціях, де ті, хто подає звіти, розглядаються як такі, що роблять значний внесок у самовідновлення та досконалість організації».

Зростаюча глобалізація та технологічний розвиток роблять сучасне суспільство суспільством ризику. Концепція суспільства ризику була створена німецьким соціологом У. Беком [6] у 1986 році. Беком у 2021 році. Посилаючись на концепцію Бека та її систематизацію, здійснену П. Станкевича, можна виділити наступні типи ризиків/ризиків у діахронічному вимірі: доіндустріальні ризики - зовнішні по відношенню до суспільства загрози, непередбачувані, не прораховані; ризики індустріальної епохи - результат людських дій і вибору, найбільш схожі на класичне розуміння ризику, що означає ймовірність втрати певної величини; великі ризики пізнього модерну -

діалектичний синтез доіндустріальних ризиків та ризиків індустріальної доби, які неможливо передбачити, з наділндивідуальним характером ризиків, де ризики є продуктом технологічного розвитку.

У часи зростаючої глобалізації та впливу повсюдних ризиків виникла потреба у розробці нормативно-правових актів, які б сприяли мінімізації ризиків порушень «знизу-вгору», тобто на рівні компаній. Таке припущення є методологічно правильним, оскільки бізнес-ризики є більш вимірюваними та оцінюваними, ніж непередбачувані ризики неконтрольованого характеру. Нарешті, важливим є також методологічне припущення (положення Директиви запозичують широко прийняту модель комплаєнс-менеджменту), що мінімізація ризику порушення на рівні компанії може зменшити виникнення глобальних ризиків (наприклад, у сфері екології).

У пункті (48) Директиви зазначено, що « Для юридичних осіб приватного сектору зобов'язання щодо створення внутрішніх каналів повідомлення має бути пропорційним їхньому розміру та рівню ризику, який їхня діяльність становить для суспільних інтересів». Поняття «ризик» з'являється в тексті Директиви кілька разів, у різних контекстах її застосування, що підтверджує правомірність тлумачення положень з точки зору необхідності їх оцінки, мінімізації, пом'якшення тощо.

Слід також підкреслити, що модель надання праці еволюціонувала протягом багатьох років з розвитком цивілізації, а це означає, що законодавець ЄС, створюючи понятійний словник Директиви, передбачав, що в суспільстві ризику саме «контекст, пов'язаний з роботою», має більше значення, ніж договірні правовідносини у формі трудових відносин. З цієї причини захист викривача суб'єктивно розширюється.

Еволюція моделі забезпечення роботою в суспільстві ризику (відтворена в таблиці нижче) наближає положення і цілі Директиви до прогресивних змін в економічних і виробничих відносинах. Вона також зачіпає поняття «робота в мережевому суспільстві - цей контекст вже розглядається в наступних директивах Європейського Союзу, які готуються до прийняття.

Директива (ЄС) 2019/1937 Європейського Парламенту та Ради від 23 жовтня 2019 року про захист викривачів була прийнята з метою забезпечення послідовності дотримання законодавства ЄС у контексті захисту викривачів.

З іншого боку, його назва викликає певні проблеми з інтерпретацією, адже чи справді йдеться про захист викривачів? Цей захист видається вторинним, оскільки апріорі не можна припустити, що викривач взагалі потребуватиме такого захисту. Насправді, первинним є профілактичний ефект положень Директиви, який переважає як юридичні наслідки порушень, так і потенційно негативні наслідки для самого викривача.

Як зазначено в тексті Директиви, метою положень про захист викривачів «є покращення правозастосування законодавства та політики Союзу в конкретних сферах шляхом встановлення загальних мінімальних стандартів, що забезпечують високий рівень захисту викривачів ». Таким чином, профілактична мета має пріоритет над інструментами та засобами захисту викривачів, які мають сервісний характер.

Таким чином, якщо з точки зору існування права ЄС оцінити ранг вищезгаданої Директиви, то можна впевнено стверджувати, що вона підтримує дотримання, а отже, і запобігання, всіх взаємопов'язаних положень права Співтовариства.

Таким чином, можна припустити, що в умовах множинності директив і регламентів та делегування частини законодавчої компетенції в рамках так званої спільної компетенції, законодавець ЄС, ухвалюючи Директиву, мав на меті запровадити інструмент контролю та запобігання порушенням положень права ЄС, але вже на рівні установ (організацій/юридичних осіб). Дійсно, у джерелі заснування законодавець вбачає ризики загрози суспільним інтересам, якщо організація не дотримується законодавства, на яке поширюється дія Директиви.

Зазначені нижче сфери права ЄС, які пов'язані з системою викривання, були обрані з урахуванням критерію релевантності, відповідно до методологічних припущень, зроблених при відборі галузей, на які впливають

положення Директиви та які досліджуються в рамках цього проекту. Цей критерій враховує наступні припущення: чим більша ймовірність повідомлення про порушення, тим більша кількість осіб, які працюють (перебувають у робочому контексті) в організаціях, що здійснюють свою діяльність у сфері, на яку поширюється законодавство ЄС, тим більша ймовірність порушень; чим більшим є ризик порушення закону, тим ефективнішим має бути запобігання порушенням; статистично найбільша кількість населення користується транспортними послугами, будівництвом, є групою споживачів (у т.ч. продуктів продуктів харчування), «занурене» в необхідність захисту довкілля, а також користується виробничими благами - в ролі працівника, отримувача послуг, покупця тощо; статистично найбільше населення користується послугами транспорту, будівництва, є групою споживачів (у т.ч. продуктів харчування).

1.2.Методичні підходи до формування системи регламентування праці персоналу організації

Ця сфера не виокремлена в положеннях Директиви як така, що підлягає повідомленню про порушення. Надмірне тлумачення або, прямо кажучи, неправильне тлумачення, що з'являється навіть у публічному просторі, яке пов'язує Директиву з системою трудового права, може бути наслідком певного спрощеного мислення. Дійсно, положення Директиви вводять поняття «контекст, пов'язаний з роботою», яке випливає з того факту (підтвердженого численними дослідженнями), що особа, яка перебуває у правовідносинах (наприклад, у трудових відносинах), перебуває у найбільш тісному зв'язку з організацією (тут: роботодавцем), а отже, має найбільше знань про можливі порушення закону, і тому найчастіше є викривачем. У контексті системи трудового права актуальним стає лише захист від переслідування. Можливо, законодавець ЄС справедливо виходив з того, що каталог суб'єктів та об'єктів не повинен перетинатися. Адже це різні речі - «про що» можна повідомляти,

«хто» може повідомити про порушення, «хто» захищений і «хто і за що» може понести потенційне покарання. На противагу цьому, механізм узгодженості соціальної політики та політики зайнятості ЄС є відправною точкою для положень Директиви, оскільки саме в статистичній площині відбувається повідомлення про порушення та їх з'ясування на рівні правовідносин, пов'язаних з наданням роботи. Уже в перших реченнях тексту Директиви (її витягів) читаємо, що «особи, які працюють на державну або приватну організацію або контактують з нею у зв'язку зі своєю професійною діяльністю, часто першими дізнаються про загрози або шкоду суспільним інтересам, що виникають у цьому контексті».

Європейський Союз вже давно прагне сприяти соціальному прогресу та покращенню умов життя і праці всіх громадян. Цей принцип закріплений у преамбулі Договору про функціонування Європейського Союзу (далі - ДФЄС). Як зазначено в ДФЄС, зокрема в статті 153, ЄС доповнює політичні ініціативи окремих держав-членів ЄС, встановлюючи мінімальні вимоги, яких повинні дотримуватися всі держави-члени.

Європейська політика у сфері зайнятості, соціальних питань та рівних можливостей спрямована на покращення умов життя та праці людей шляхом сприяння створенню більшої кількості якісних робочих місць, розвитку навичок та рівності, а також забезпечення соціального захисту та соціальної інтеграції. Для досягнення цих цілей ЄС розробляє та просуває політику, спрямовану на забезпечення рівних можливостей та рівного доступу до ринку праці, підвищення зайнятості та мобільності робочої сили, покращення якості робочих місць та умов праці, надання інформації та консультацій працівникам, боротьбу з бідністю та соціальною ізоляцією, сприяння рівним можливостям та боротьбу з дискримінацією, а також модернізацію систем соціального забезпечення.

Як бачимо, поняття «рівний доступ до робочих місць», «рівність», «антидискримінація» або «соціальна інтеграція» є стовпами безпеки зайнятості в глобальному сенсі. Тому ми бачимо посилання на цілі, що містяться в

Директиві, які в суб'єктивному контексті охоплюють також претендентів на роботу, які мають право повідомляти про порушення закону, і колишніх працівників. Дійсно, добре відомо, що динаміка зайнятості, коливання на ринку праці та прогресуюча мобільність працівників означають, що саме ця група повинна бути гарантом дотримання законодавства Співтовариства на організаційному (тут: робочому) рівні, зважаючи на різноманітність їхнього досвіду роботи та місць роботи. Тому ця група є особливо захищеною від переслідувань - як зазначено в положеннях Директиви та на основі національних положень, прийнятих на її основі.

Контекст економічних мотивів Директиви досить часто з'являється в публічному дискурсі. У дискусіях про нове законодавство ЄС, спрямоване на посилення захисту про нове законодавство ЄС щодо посилення захисту викривачів зазначила Віра Юрова, Комісар ЄС з питань юстиції, прав споживачів та гендерної рівності: "Нове законодавство про захист викривачів буде революційним. У глобалізованому світі, де спокуса максимізувати прибуток навіть за рахунок порушення закону є реальною, ми повинні підтримувати людей, які готові йти на ризик і розкривати серйозні порушення законодавства ЄС. Цього вимагає доброчесність європейців".

Як ми читаємо в резюме законодавства ЄС, «шахрайство і корупція становлять серйозну загрозу безпеці та фінансовим інтересам Європейського Союзу. Захист цих інтересів є пріоритетом для інституцій ЄС, як з точки зору забезпечення найкращого використання коштів платників податків, так і в боротьбі з організованою злочинністю та тероризмом, для яких корупція створює сприятливий ґрунт».

Ми також бачимо, що посилання на запобігання шахрайству та переслідування за нього ґрунтується на міцній правовій базі. Дійсно, такою основою для боротьби з шахрайством та будь-якою іншою незаконною діяльністю, що зачіпає фінансові інтереси ЄС, є стаття 325 Договору про заснування Європейського Союзу, яка зобов'язує ЄС та його держави-члени захищати бюджет Європейського Союзу.

Інституції ЄС мають на меті: впорядкувати та модернізувати законодавство, що стосується корупції; моніторинг прогресу в боротьбі з корупцією в державах-членах в рамках Європейського семестру; підтримка реалізації національних антикорупційних заходів шляхом надання фінансування, технічної допомоги та обміну досвідом.

Важливість захисту від шахрайства та корупції підкреслюється статтею 83(1) ДФЄС, яка визнає корупцію «єврозлочином» і класифікує її як особливо тяжкий злочин, що має транскордонний вимір. На основі цього положення Європейський парламент і Рада Європейського Союзу прийняли Директиву (ЄС) 2017/1371 про боротьбу з шахрайством на шкоду фінансовим інтересам ЄС засобами кримінального права (цитується в тексті аналізованої директиви, що підкреслює, як зазначено вище, її всеохоплюючий характер).

Згідно зі статтею 169 ДФЄС , «споживча політика передбачає захист здоров'я, безпеки та інтересів майже півмільярда потенційних споживачів, які відіграють важливу економічну та політичну роль у суспільстві»[9].

Європейський Союз працює над гармонізацією законодавства щодо захисту споживачів та їхніх прав з 1970-х років.

Метою регулювання є гарантування високого рівня захисту прав споживачів через єдиний ринок, у тому числі в таких швидкозростаючих сферах, як електронна комерція, енергопостачання та фінансові послуги. Споживча політика вважається однією з основних складових єдиного внутрішнього ринку Європейського Союзу. Тому її сфера застосування та принципи визначені в Маастрихтському договорі, який підкреслює, що «Співтовариство сприяє досягненню високого рівня захисту прав споживачів за допомогою заходів, які воно застосовує (...) в контексті створення внутрішнього ринку, конкретних дій, які підтримують і доповнюють політику, що проводиться державами-членами з метою захисту здоров'я, безпеки та економічних інтересів споживачів, а також для забезпечення їх належного інформування».

Спроба обмежити контрактні переваги та захистити конкуренцію також очевидна в цих нормативних актах. У зв'язку з вільним переміщенням споживчих товарів, а також засобів виробництва, що є наслідком прагнення до зростання глобальних економічних гравців і, відповідно, відносної монополізації, на спільному ринку необхідні адекватні правила конкуренції. Їх основним завданням має бути захист від недобросовісної конкуренції на єдиному внутрішньому ринку Європейського Союзу.

Свідченням прогресуючої потреби у ще більш широкому захисті прав споживачів, особливо в епоху динамічного розвитку електронної комерції, є прийняття Директиви (ЄС) 2019/2161 Європейського Парламенту та Ради від 27 листопада 2019 року про внесення змін до Директиви Ради 93/13/ЄЕС та Директив Європейського Парламенту та Ради 98/6/ЄС, 2005/29/ЄС і 2011/83/ЄС щодо кращого застосування та модернізації правил захисту прав споживачів ЄС.

РОЗДІЛ 2
ОЦІНКА СИСТЕМИ РЕГЛАМЕНТУВАННЯ ПРАЦІ ПЕРСОНАЛУ ТА МЕХАНІЗМУ ЇЇ ЗАБЕЗПЕЧЕННЯ В ДІЯЛЬНОСТІ ДОСЛІДЖУВАНОГО ОРГАНУ ДЕРЖАВНОЇ ВЛАДИ

2.1.Аналіз організаційного забезпечення регламентування праці персоналу в досліджуваній державній установі

Відповідно до частини 1 статті 22 Трудового кодексу, вступаючи в трудові відносини, працівник зобов'язується виконувати роботу, визначену роботодавцем, під його керівництвом, у визначеному роботодавцем місці та у визначений роботодавцем час, а роботодавець зобов'язується виконувати роботу за винагороду, визначену роботодавцем. Визначення трудових відносин, що регулюються Кодексом, однозначно передбачає наявність у роботодавця певних управлінських повноважень, які як іманентна ознака цих відносин є суттєвим критерієм їх ідентифікації, що відрізняє трудові відносини від інших правовідносин, пов'язаних з працевлаштуванням. На думку М. Герсдорфа, «(...) трудові відносини фактично характеризуються роботою під керівництвом, що є неодмінним елементом будь-якої зайнятості працівника». Оскільки трудове законодавство зобов'язує роботодавця під загрозою покарання забезпечити належну організацію праці[3], підготувати виробничий процес таким чином, щоб гарантувати безпечні та гігієнічні умови праці для працівників, невід'ємним наслідком цього, на мою думку, є надання йому певних управлінських повноважень, які дозволять йому належним чином організувати робоче середовище та хід роботи, що задовольняють вимогам закону, а також керувати цим ходом роботи на постійній основі таким чином, щоб створити належні умови для належного співробітництва сторін трудових правовідносин у процесі їх виконання. На думку Т. Зелінського, «організація виробничого процесу вимагає підпорядкування працівника роботодавцю, що є суттєвою ознакою трудових правовідносин». Роботодавець як суб'єкт, відповідальний за

організацію та перебіг трудового процесу, повинен мати гарантовані законом управлінські повноваження щодо конкретизації - за допомогою обов'язкових до виконання розпоряджень - обов'язків працівника, які за своєю природою досить загально викладені в договорі та нормативних актах. На думку Х. Левандовського, це випливає з того, що на момент встановлення трудових відносин неможливо детально визначити обов'язки працівника. Тому суб'єкт працевлаштування повинен мати право конкретизувати цей обов'язок, і саме для цього слугують управлінські повноваження, гарантовані йому трудовим законодавством.

Іншою важливою причиною, чому законодавець наділив роботодавця управлінськими повноваженнями щодо конкретизації обов'язків працівника, визначення підпорядкованості працівника в трудовому процесі, є ризик, який несе роботодавець у зв'язку з працевлаштуванням працівників та здійсненням трудового процесу. Саме роботодавець за власний рахунок забезпечує працівників необхідними для цього процесу засобами (інструментами, сировиною, матеріалами) і саме роботодавець має право користуватися «плодами» їхньої праці. На думку З. Кубота, «роботодавець, який несе ризик роботи, що надається працівником, не може бути позбавлений повноважень визначати поведінку працівника в процесі праці». У подібному ключі висловлюється і Т. Зелінський, на думку якого «про повний відхід від принципу підпорядкування у трудових відносинах не може йти мова хоча б тому, що роботодавець, який несе наслідки невинності або непридатності працівника до роботи певного виду (так званий особистий ризик), не може бути позбавлений впливу на поведінку працівників, за яких він несе відповідальність».

В умовах ринкової економіки суб'єкт господарювання, несучи ризик своєї діяльності, прагне забезпечити максимально ефективний та результативний трудовий процес. Для того, щоб залишатися конкурентоспроможним на економічному ринку, він повинен мати повноваження, які гарантують йому безпосередній вплив на організацію трудового процесу (що дозволяє йому - шляхом видання обов'язкових до виконання наказів - конкретизувати обов'язки

найнятих ним працівників), включаючи відповідний підбір, розстановку і використання робочої сили. Управлінські повноваження дозволяють роботодавцю ефективно використовувати наявний у його розпорядженні трудовий потенціал, зменшуючи ризик його відсутності або непридатності. Важливу роль цих повноважень роботодавця в контексті ризику, який несе суб'єкт господарювання, підкреслював Л. Писарчик, вказуючи, що за допомогою цих повноважень «роботодавець може впливати на об'єкт виконання працівника, оновлюючи або конкретизуючи обов'язки працівника, пристосовуючи їх таким чином до мінливих умов виконання і потреб підприємства, завдяки чому робота може виконуватися в періоди існуючого попиту і зберігає свою корисність».

Отже, управлінські повноваження роботодавця слід ототожнювати з компетенцією роботодавця впливати на поведінку працівника під час надання роботи (у процесі праці) та відповідними обов'язками працівника перед суб'єктом господарювання в предметі виконуваної роботи. На думку Г. Левандовського, ці повноваження поширюються на все, що стосується надання роботи, яку на підставі договору та доповнюючих його положень працівник передає в розпорядження роботодавця. Повноваження директивного характеру, що стосуються «самого об'єкта зобов'язання, тобто виду роботи, місця і часу її виконання, вважаються основним ядром управлінських повноважень. На думку Г. Левандовського, «їх зміст полягає у безпосередньому формуванні трудового процесу шляхом видання розпоряджень. Це конкретизує обов'язки працівника, які за своєю природою викладені в досить загальному вигляді в договорі та нормативних актах". Окрім конкретизації виду роботи (покладання на працівника завдань, які він повинен виконувати), способу, часу та місця її виконання, управлінські повноваження роботодавця також стосуються сфери порядку та організації трудового процесу.

Однак управлінські повноваження, які гарантуються роботодавцю в рамках трудових відносин, не є абсолютними, і законодавець конкретизує межі їх застосування. У доктрині трудового права загальновизнано, що положення,

яке міститься в ч. 1 ст. 100 КЗпП, слід вважати основоположним з точки зору визначення цих меж. Відповідно до цього положення, працівник зобов'язаний, серед іншого, виконувати розпорядження свого керівника, що стосуються роботи, якщо вони не суперечать положенням закону або трудового договору. З цього положення можна зробити справедливий висновок, що найважливішими межами управлінських повноважень роботодавця в трудовому процесі є положення чинного законодавства та трудового договору або іншого акта, що створює трудові відносини. На думку Г. Левандовського, головним чинником, що визначає зазначені тут межі, є трудовий договір, який повинен бути поставлений тут на перше місце перед положеннями закону. Особисто я не зовсім поділяю цю точку зору. З точки зору меж управлінських повноважень роботодавця в трудовому процесі, я б на перше місце поставив положення чинного законодавства, а вже потім трудовий договір. Саме такий порядок передбачений частиною 1 статті 100 КЗпП, яка цитувалася вище, а також статтею 18 КЗпП. - положення трудового договору не можуть бути менш сприятливими для працівника, ніж положення трудового законодавства. Це означає, що сторони не можуть розширити ці межі у змісті трудового договору, а лише мають можливість обмежити обсяг управлінських повноважень. Однак вони завжди повинні дотримуватися чинних правових норм і, зокрема, трудовий договір не може повністю виключати аспекти підпорядкування, які визначають ідентичність трудових відносин (управлінські повноваження), згідно з якими робота виконується під керівництвом роботодавця (ч. 1 ст. 22 Трудового кодексу).

Крім того, серед обмежень управлінських повноважень роботодавця є також положення про відповідність соціально-економічній меті та принципам суспільного співіснування. Вони випливають зі статті 8 Трудового кодексу, згідно з якою ніхто не може користуватися своїм правом всупереч соціальному та економічному призначенню цього права або принципам суспільного співіснування. Така дія чи бездіяльність правовласника не вважається реалізацією права і не користується захистом. Іноді в літературі на цю тему

також можна зустріти погляди, які, посилаючись на історичне тлумачення, вважають за доцільне включати звичай в межі управлінських повноважень роботодавця.

Характеристику меж управлінських повноважень роботодавця у трудовому процесі необхідно розпочати з норм права. Саме вони вводять у правовий порядок конструкцію добровільно-підпорядкованих трудових відносин, згідно з якою працівник зобов'язується виконувати роботу певного виду для роботодавця та під його керівництвом, у місці та у час, визначені роботодавцем (ч. 1 ст. 22 КЗпП), і саме вони визначають допустимий обсяг управлінських повноважень суб'єкта працевлаштування. Вже з процитованого тут положення видно, що працівник не передає в розпорядження роботодавця всю свою здатність до праці в цілому, а лише зобов'язується виконувати певний вид роботи. Роботодавець може лише у виняткових випадках вимагати від нього виконання іншої роботи, лише на підставі та в межах положень трудового законодавства. В принципі, законодавець допускає таку можливість у трьох випадках, а саме в ситуації: доручення працівникові іншої роботи, ніж та, що визначена трудовим договором, у зв'язку з обґрунтованою потребою роботодавця, на строк не більше 3 місяців протягом календарного року (ч. 4 ст. 42 КЗпП); доручення іншої підходящої роботи, ніж та, що визначена трудовим договором, на строк не більше 3 місяців протягом календарного року.); доручити іншу підходящу роботу на час простою (ч. 3 ст. 81 Трудового кодексу); залучити працівника до роботи понад встановлену для нього норму робочого часу у разі необхідності проведення рятувальних робіт для захисту життя чи здоров'я людей, майна або довкілля чи для усунення аварії (п. 1 ч. 1 ст. 151 Трудового кодексу). У всіх зазначених тут випадках працівник зобов'язаний виконувати іншу роботу іншого характеру, що також опосередковано випливає з обов'язку працівника - на підставі абз. 4 ч. 2 ст. 100 Трудового кодексу. - обов'язку дбати про благополуччя на робочому місці.

Правильність твердження про те, що положення чинного законодавства є найважливішим обмеженням управлінських повноважень роботодавця в

трудовому процесі, підтверджується expressis verbis статтею 100 § 1 Трудового кодексу, згідно з якою працівник зобов'язаний виконувати розпорядження свого керівника, які стосуються роботи, якщо вони не суперечать положенням законодавства. Термін «положення закону», що використовується тут, слід тлумачити дуже широко. Він стосується не лише положень кримінального права або закону про правопорушення, як колись вважалося, але й будь-яких норм статутного характеру, які захищають певне благо або надають певне право, зокрема, якщо це стосується благ або прав, гарантованих працівникові. На думку Г. Левандовського, «цю роль виконує будь-яке положення, що передбачає обов'язок поводитися певним чином (наказ або заборона), незалежно від того, чи адресатом такого положення є безпосередньо працівник, чи положення адресоване роботодавцю, а працівник є лише його "виконавцем"». На думку М. Свєнціцького, при використанні терміну «правові норми» в контексті меж управлінських повноважень роботодавця слід мати на увазі всі правові норми, порушення яких наражає особу, яка виконує наказ, на кримінальну, адміністративну або фінансову відповідальність, а також інші обов'язкові положення, навіть якщо їх порушення не призводить до таких наслідків . Перш за все, тут необхідно згадати положення про захист життя і здоров'я працівників, зокрема, ч. 2 ст. 207 Трудового кодексу, згідно з якою роботодавець зобов'язаний охороняти здоров'я і життя працівників шляхом забезпечення безпечних і гігієнічних умов праці, а також ст. 210 Трудового кодексу, яка надає працівникам право відмовитися від виконання роботи або залишити робоче місце у разі безпосередньої загрози здоров'ю чи життю працівників або інших осіб. На думку В. Пьотровського, працівник зобов'язаний відмовитися від виконання наказу, який суперечить закону, особливо якщо він стосується стандартів безпеки та охорони здоров'я, захисту навколишнього середовища, або якщо його виконання може загрожувати життю чи здоров'ю людини.

Крім того, межі управлінських повноважень роботодавця в трудовому процесі встановлюються, зокрема, положеннями законодавства, що регулюють

робочий час, положеннями про рівне ставлення до працівників у сфері зайнятості та недискримінацію працівників, положеннями про повагу до гідності та інших особистих благ працівника, положеннями, що зобов'язують роботодавця запобігати мобінгу на робочому місці або положеннями про захист персональних даних працівників. Застосування вищезазначених обмежень підтверджується Верховним Судом, який у своєму рішенні від 8 грудня 2005 року постановив, що «видання роботодавцем законних трудових інструкцій, як правило, не є порушенням гідності (особистих прав) працівника, нерівним ставленням або дискримінацією чи мобінгом».

Серед вищезазначених обмежень управлінських повноважень роботодавця найбільший інтерес викликають положення про захист гідності працівника та інших особистих благ. На думку З. Гураля, рішення роботодавця, прийняте на підставі ч. 4 ст. 42 Трудового кодексу, доручити висококваліфікованому працівникові, який раніше працював на посаді, що повністю враховує його кваліфікацію, виконувати просту фізичну роботу, слід вважати порушенням гідності працівника . У рішенні від 21 лютого 2008р. Верховний Суд зазначив, що «доручення на підставі ч. 4 ст. 42 КЗпП звільненому голові правління товариства роботи, що не вимагає високої кваліфікації, яка виконується у виробничому цеху серед робітників ручної праці, може становити порушення роботодавцем обов'язку поважати гідність працівника, якщо воно мало ознаки умисної, свідомої і недобросовісної дії, спрямованої на приниження і дискредитацію працівника. Таке порушення може бути підставою для розірвання трудового договору з працівником без попередження на підставі п.11 ст. 55 Трудового кодексу». На думку З. Гураля, з точки зору порушення гідності працівника слід також розглядати часте залучення працівника до понаднормової роботи з не надто прихованою метою обмеження вільного часу працівника, необхідного для підвищення його професійної кваліфікації. У свою чергу, М. Гладох вказує, що положення про захист гідності працівників та інших особистих прав зобов'язують роботодавця утримуватися від надання їм вказівок в образливій формі або оцінки їхньої

роботи в принизливій форм . Згідно з рішенням Верховного Суду від 11 лютого 1999 року, психологічний стрес, викликаний незгодою працівника з керівником, може - залежно від джерел і перебігу конфлікту - бути кваліфікований як зовнішній кофактор інсульту, коли керівник неналежним чином використовує свою компетенцію давати підлеглим вказівки, пов'язані з роботою.

У тематичній літературі та судових рішеннях низку суперечностей і сумнівів у контексті меж управлінських повноважень роботодавця в трудовому процесі викликають положення, що регулюють мобінг у трудових правовідносинах. На думку Г. Шевчик, залучення працівника до низькооплачуваної понаднормової роботи всупереч його волі може бути проявом моббінгу. На думку автора, проявами мобінгу є також ситуації, коли роботодавець переслідує працівника дорученнями, які важко виконати. У рішенні від 5 грудня 2006р. Верховний Суд зазначив, що «застосування роботодавцем мобінгу може полягати у вчиненні дій навіть у межах наданих йому законом повноважень (шляхом видання наказів) і може стосуватися всіх працівників».

Іноді законодавець прямо звужує межі управлінських повноважень роботодавця щодо певних категорій працівників. По-перше, це може бути продиктовано необхідністю підвищеного захисту життя і здоров'я працівників у конкретній ситуації. Наприклад, це стосується вагітних жінок. Роботодавець не може вимагати від них виконання особливо важких і шкідливих для здоров'я робіт (ст. 176 Трудового кодексу) , а також залучати їх до надурочних робіт або робіт у нічний час, забороняється направляти їх за межі постійного місця роботи і застосовувати до них систему переривчастого робочого часу (ч. 1 ст. 178 Трудового кодексу). У рішенні від 19 березня 2002р. Верховний Суд зазначив, що вагітність є важливою обставиною з точки зору формування трудових відносин. Вона не тільки обмежує свободу роботодавця розірвати трудовий договір, але й змінює сферу підпорядкування працівника. Це породжує нові обов'язки з боку роботодавця і збільшує права працівника. Що

стосується вагітних жінок, то ступінь підпорядкування вказівкам роботодавця значно зменшується, оскільки скорочуються обов'язки працівника, про необхідність виконання яких роботодавець може розпорядитися шляхом видання обов'язкового до виконання розпорядження. По-друге, звуження меж управлінських повноважень роботодавця щодо певних груп працівників також може бути продиктоване специфікою їхньої роботи, яка вимагає автономії у способах виконання ними своїх обов'язків. Це стосується, зокрема, суддів, юрисконсультів або лікарів, щодо яких - через специфіку їхньої роботи - положення, що регулюють їхній правовий статус, виключають підпорядкування щодо способу виконання ними своєї роботи, передбачаючи їхню «матеріальну» автономію з точки зору рішень, які вони приймають.

Крім того, загальновизнано, що критерії, які визначають межі управлінських повноважень роботодавця у трудових відносинах, встановлюються не лише положеннями закону, але й нормами автономного трудового права, зокрема, положеннями колективного договору або трудового розпорядку, що визначають організацію і порядок роботи на конкретному робочому місці, а також організацію робочого часу (системи і графіки робочого часу, обов'язкові для даного роботодавця). На думку З. Сальви, невідповідність наказу роботодавця цим нормам звільняє працівника від обов'язку підпорядкування.

Роботодавець, який при здійсненні управлінських повноважень, покладених на нього трудовими відносинами щодо працівників, порушує межі, встановлені законом, наражає себе, зокрема, на відповідальність за відшкодування шкоди, відповідальність за проступок, а в разі прямої загрози загибелі або тяжкого ушкодження здоров'я працівника - на кримінальну відповідальність. Крім того, якщо роботодавець, приймаючи управлінські рішення, допускає серйозне порушення своїх основних зобов'язань перед працівником, зокрема, зобов'язання забезпечити безпечні та гігієнічні умови праці (статті 13 і 207 КЗпП), працівник може розірвати трудовий договір без попередження відповідно до статті 55 КЗпП.

З точки зору правових наслідків перевищення роботодавцем встановлених законом меж своїх управлінських повноважень, найбільше суперечок і сумнівів у літературі на цю тему і в судових рішеннях викликає питання допустимості відмови працівника від виконання розпоряджень, відданих з порушенням закону. На цьому тлі в доктрині трудового права можна виділити кілька різних позицій. У міжвоєнний період був представлений радикальний погляд, неприйнятний сьогодні, згідно з яким на працівника покладався абсолютний обов'язок виконувати всі розпорядження роботодавця, без можливості оцінки їх відповідності чинним правовим нормам і без урахування їх правових наслідків. Згідно з іншою позицією, працівник зобов'язаний лише відмовитися виконувати вказівки, які суперечать кримінальному законодавству (абсолютна відсутність обов'язкової сили). З іншого боку, якщо вказівки роботодавця порушують інші положення закону, працівник зобов'язаний їх виконувати після отримання попереднього підтвердження їх змісту від свого керівника. У такому випадку саме керівник несе відповідальність за всі наслідки дій, вчинених працівником на виконання незаконного наказу (протиправність дії підлеглого працівника скасовується). На думку М. Рафач-Кшижановської, в такому випадку ми маємо справу з презумпцією правильності наказу роботодавця .

Інші представники доктрини трудового права дотримуються іншої точки зору, вважаючи, що працівник повинен відмовитися від виконання не тільки розпоряджень, виконання яких становитиме каране діяння, але й розпоряджень, які явно суперечать іншим нормам права, а також розпоряджень, які є суспільно шкідливими. З. Сальва був менш категоричним у цьому питанні, вказуючи, що в ситуації, коли накази суперечать наказам і заборонам, що випливають з інших нормативних актів, крім кримінального права, працівник може лише - але не зобов'язаний - відмовитися від їх виконання (їх відносної обов'язковості). У контексті того, що працівник не зобов'язаний виконувати вказівку роботодавця, Х. Левандовскі йде ще далі, надаючи працівникові право відмовитися від виконання вказівки керівника також у ситуації, коли вона не порушує жодних

положень закону, але в оцінці працівника - на основі його кваліфікації та професійної підготовки - вказівка є дефектною і працівник переконаний у реальності загрози заподіяння шкоди. Я не зовсім поділяю цю точку зору. Вважаю, що в ситуації, коли наказ відповідає вимогам, викладеним у ч. 1 ст. 100 Трудового кодексу, зокрема, коли він не порушує положень чинного законодавства, працівник не може відмовитися від його виконання, навіть якщо він оцінює його критично, ставлячи під сумнів його легітимність. На думку Я. Скочинського, «за невиконання наказу, який належить до сфери підпорядкування роботодавця, працівник несе відповідальність, навіть якщо наказ є об'єктивно дефектним». Саме роботодавець несе ризик трудового процесу, і саме він повинен оцінювати доцільність наданої вказівки. Передача цієї оцінки працівникам може призвести до дезорганізації роботи та негативних наслідків для роботодавця, зокрема, фінансового характеру.

Наведені міркування однозначно підтверджують тезу про те, що право роботодавця здійснювати управлінські повноваження щодо працівників не є абсолютним і що роботодавець повинен дотримуватися певних меж цього права. Однак ці межі не були чітко врегульовані в законі, про що свідчить, наприклад, низка сумнівів і суперечностей, які вже давно виникли в літературі з цього питання і в судовій практиці. На думку Г. Левандовського, «питання про межі управлінських повноважень у трудових відносинах має важливе теоретичне і практичне значення. У ньому міститься одна з основних проблем сучасного трудового права, що полягає в гармонізації його захисної та організаційної функцій. Це пов'язано з тим, що йдеться, з одного боку, про забезпечення раціональної організації колективної праці, яка є основою належного функціонування підприємств та установ, а з іншого - про захист прав та інтересів працівників».

Вважаю, що de lege ferenda слід докласти зусиль для більш чіткого визначення меж управлінських повноважень роботодавця, зокрема є потреба в тому, щоб законодавець чітко врегулював правові наслідки їх перевищення.

Зокрема, це стосується права працівників відмовитися від виконання розпоряджень роботодавця, виданих з порушенням аналізованих тут меж.

2.2.Механізм регламентування трудових процесів виконавчої роботи персоналу досліджуваної державної установи

Вимоги до діяльності громадських організацій пов'язані із запровадженням у цих інституціях методів управління, запозичених із практики суб'єктів господарювання. Проявом цієї тенденції є обов'язковість впровадження управлінського контролю та пов'язаних з ним процедур управління ризиками з метою забезпечення законного та своєчасного виконання завдань громадських організацій, а також ефективного витрачання бюджетних коштів.

Одним із ключових напрямів цієї діяльності є кадровий ризик, який охоплює низку потенційних (виражених у вигляді певної ймовірності) подій, що виникають внаслідок кадрових рішень, які є значущими для діяльності даного типу установи. Проблемою тут стає вибір відповідних організаційних рішень, а також принципів і методів вимірювання цієї категорії ризику.

З огляду на це, метою статті є привернення уваги до змісту, процесуальних та інструментальних засад вимірювання кадрових ризиків у публічних організаціях. У статті пропонується авторський інструмент для розробки карти складових кадрового ризику, адаптований до специфіки цього типу організацій.

Державні організації, зокрема, центральні та місцеві органи влади, державна освіта та вищі навчальні заклади, служби охорони здоров'я, забезпечення державної безпеки, правового та інституційного порядку, виконують дуже важливі та об'ємні функції в сучасному суспільстві. Вони випливають з державної політики та потреб місцевих громад, відповідно до принципів субсидіарності держави та розвитку громадянського суспільства. Таким чином, двадцяте і двадцять перше століття стали свідками значного

розвитку цього типу організацій. П.Ф. Друкер зазначає, що після Другої світової війни сектор державних послуг розширювався набагато швидше, ніж приватний сектор.

З іншого боку, спостереження за функціонуванням публічних організацій призводить до виявлення багатьох недоліків у сфері управління. Нераціональне використання значних фінансових ресурсів, дії в рамках короткого часового горизонту та уникнення глибших змін є основними прикладами таких недоліків.

Тому зараз багатьом громадським організаціям пропонується впроваджувати ринкові принципи роботи та методи управління, запозичені з практики економічних організацій. Ці постулати відображені, серед іншого, в концепції нового публічного менеджменту, а також публічного співуправління. Вони вказують на необхідність застосування в публічному секторі правил належної економії та ефективності функціонування, зосередження уваги на ставленні до заявника як до отримувача публічних послуг належної якості та надійності виконання, а також запровадження принципів конкуренції в організацію цього сектору.

Одним із напрямів управлінського контролю є також управління ризиками, реалізація якого спрямована на підтримку керівництва суб'єкта у виконанні поставлених цілей і покладених на нього суспільних завдань через формування навичок і ставлення, що зумовлюють ефективне прийняття рішень в умовах нових можливостей і загроз. Діяльність у цій сфері менеджменту спрямована на виявлення, вимірювання, контроль і управління ризиками з метою їх максимального зменшення та страхування (а також захисту) від їхніх наслідків. Цей ризик є результатом невизначеності, пов'язаної з процесами прийняття рішень щодо майбутніх періодів, і, залежно від прийнятих поглядів, його можна розглядати як можливість втрат та/або можливість скористатися сприятливими умовами діяльності. Впровадження управління ризиками може забезпечити низку переваг для громадських організацій, серед яких:

- сприяння досягненню цілей організації шляхом виявлення потенційних можливостей і невдач запланованої діяльності;

- надання попереджувальних сигналів про загрози, що насуваються, щоб можна було відносно швидко до них підготуватися;

- скоротити час і витрати, пов'язані з подоланням ризиків, які вже матеріалізувалися;

- підвищити довіру до громадських організацій з боку зовнішніх партнерів, у тому числі комерційних структур, які працюють у рамках державно-приватного партнерства;

- сприяння налагодженню контактів з фінансовими установами, які цінують заходи з управління ризиками, що вживаються контрагентами;

- захист іміджу громадських організацій шляхом швидкого виявлення ризиків та впровадження превентивних заходів і засобів контролю для їх мінімізації.

У літературі виділяють різні види (типи) ризиків, класифіковані за певними критеріями. Одним з них є кадровий ризик, який набуває особливого значення в публічних організаціях через важливу роль людського фактору в їх функціонуванні та розвитку. Він є результатом залучення керівництва до кадрової діяльності в умовах високої невизначеності, а також недосконалості процесів управління людськими ресурсами в організації. Він виражається як функція ймовірності настання негативної події в результаті прийнятих кадрових рішень і масштабу негативних наслідків цієї події для належного функціонування організації.

Кадровий ризик та його наслідки є дуже важливими для громадських організацій. Він передбачає, серед іншого, забезпечення високого рівня управління та залучення працівників в умовах домінування державної або місцевої власності, захист широкого спектру секретної інформації та гарантування належного рівня надання публічних послуг. Тут також важливо забезпечити відповідність здійснюваної діяльності законодавству та

підтримувати високий рівень етики і прозорості діяльності, спрямованої на ефективність бюджетних витрат.

Досягненню цих переваг сприяє належне впровадження та функціонування процесу управління кадровими ризиками, першим кроком якого має бути ідентифікація цієї категорії ризиків в організації. Далі слідує оцінка кадрового ризику та визначення його пріоритетності, що вимагає вимірювання за допомогою спеціальних методів і методик з використанням адекватних вимірювальних інструментів.

Наразі громадські організації перебувають на ранніх стадіях впровадження систем управлінського контролю та управління ризиками. Результати нашого власного дослідження, проведеного методом опитування документів у 151 обраній державній установі, свідчать про те, що майже в половині з них (46%) управлінський контроль функціонує в обмеженому обсязі, а найбільш серйозною перешкодою для його повноцінного впровадження є недоліки у сфері управління ризиками. Тому пропозиції щодо організаційних, методологічних та інструментальних рішень з управління ризиками, включаючи управління кадровими ризиками, є особливо важливими для цих організацій.

Вимірювання кадрових ризиків є важливим процесом, який сприяє покращенню управління державними організаціями. Але, водночас, це складний виклик через низький рівень охоплення та кількісної оцінки багатьох сфер, що входять до сфери управління людськими ресурсами.

В літературі та на практиці розроблено багато методів та інструментів для вимірювання кадрових ризиків. Ця стаття представляє одну з таких пропозицій - реєстр ризиків. Детальне обговорення використання цього методу в громадських організаціях показує його численні переваги та потенціал для різних висновків у сфері ідентифікації та пом'якшення кадрових ризиків.

РОЗДІЛ 3
ВДОСКОНАЛЕННЯ СИСТЕМИ РЕГЛАМЕНТУВАННЯ ПРАЦІ ПЕРСОНАЛУ ДОСЛІДЖУВАНОЇ ДЕРЖАВНОЇ УСТАНОВИ

До спалаху пандемії COVID-19 багато переваг вбачалися насамперед у використанні віддаленої роботи. Очікувалося, що використання комп'ютерних технологій зменшить витрати на робочу силу, надасть можливість бізнесу зростати, а працівникам - більшу свободу та автономію, а також досвід роботи.

Сьогодні все частіше визнається, що віддалена робота повинна супроводжуватися певними змінами, пов'язаними з регулюванням і застосуванням відповідного управління інформаційною безпекою. Інформаційна безпека важлива як для суб'єктів приватного сектору, так і для суб'єктів державного сектору. В результаті все більш широкого використання Інтернету в робочому житті, інформація піддається все більшому масштабу і різноманітності загроз. Тому необхідно впроваджувати відповідні заходи безпеки для захисту інформації від навмисної або ненавмисної модифікації, знищення, перехоплення або розкриття.

Описуючи системну модель управління інформаційною безпекою, засновану на стандарті ISO 27001:2017, ми зазначаємо, що вона може бути хорошим орієнтиром для організацій у побудові, впровадженні та вдосконаленні системи управління інформаційною безпекою. Вона може бути важливим інструментом, що дозволяє організаціям ефективно управляти ризиками інформаційної безпеки, в тому числі в контексті віддаленої роботи.

У розмовній мові поняття безпеки асоціюється з досягненням стану спокою, стану відсутності загрози. З розвитком ІКТ постала проблема забезпечення безпеки ІКТ-систем і середовищ, в яких вони використовуються, щоб оброблювану в них інформацію і послуги, які вони надають, можна було вважати захищеними. При цьому під безпекою розуміється безперешкодне функціонування цих систем під час виконання покладених на них завдань, що здійснюються на користь установи. Згідно з Kosiński, інформаційна безпека

розуміється як впевненість у захисті доступу до зібраної інформації та впевненість у захисті інформації, що передається.

Інформацію «слід розуміти як передачу повідомлень будь-якої природи і структури носія, що збагачує наші знання». Інформація також є товаром, і часто має стратегічне значення (для держави, компанії, конкретної особи).

Інформація є одним з найцінніших ресурсів організації. З точки зору бізнесу, саме інформація має певну цінність для організації. Тому, щоб забезпечити її безпеку, вона повинна бути захищена, що може бути важливим для забезпечення прибутковості, підтримання ліквідності та дотримання правових норм, а також для збереження репутації організації.

Забезпечення інформаційної безпеки - це певний тип практики, що передбачає впровадження політик і процедур для захисту інформації та запобігання втраті або крадіжці даних.

Вернер і Щепанюк визначають інформаційну безпеку організації як стан, в якому:

- Елементи, що складають систему безпеки, характеризуються здатністю захищати від поточних і майбутніх порушень (загроз) функціонування або втрати конкретних цінностей; тобто система є стійкою до всіх типів загроз, тобто внутрішніх, зовнішніх, випадкових, навмисних.

- Інформаційна безпека досягається і підтримується на прийнятних рівнях конфіденційності, цілісності та доступності.

- Забезпечується автентичність та підзвітність суб'єктів, пов'язаних з авторизацією користувачів, які використовують певну інформацію та послуги.

- Як працівники організації, так і отримувачі інформації та послуг (громадяни, підприємці, працівники, що працюють в інших організаціях) усвідомлюють загрози інформаційній безпеці та є вразливими до них.

- Суб'єкти загроз (в тому числі внутрішні зловмисники) мають мало можливостей використовувати системи ІКТ для створення загроз, використовуючи слабкості, вразливості та прогалини в безпеці.

Важливо пам'ятати, що інформаційна безпека - це не лише бізнес-вимога, яка покращує організацію завдяки перевагам застосування розроблених політик обробки інформації, але й юридичне зобов'язання. Недотримання вимог законодавства може призвести до серйозних наслідків у вигляді адміністративних фінансових санкцій або навіть припинення діяльності.

До найважливіших законодавчих вимог щодо захисту певної категорії інформації належать:

- захист персональних даних (клієнтів, підрядників, працівників, колег);

- захист секретів компанії (технологій, стратегій, ноу-хау);

- захист фінансової та податкової інформації (фінанси, рахунки, рахунки-фактури, заробітна плата);

- захист інформації з обмеженим доступом (державна таємниця);

- професійна таємниця (медична, юридична, банківська).

Інформаційна безпека - дуже широке поняття. Це пов'язано з тим, що воно охоплює захист інформації незалежно від її форми, наприклад, цифрової інформації, паперових документів, усних повідомлень. Однак, незалежно від форми, інформаційна безпека повинна відповідати так званим атрибутам безпеки.

У літературі визначено три основні атрибути інформаційної безпеки та інформаційних систем:

- Конфіденційність, тобто забезпечення застосування затверджених обмежень на розголошення та доступ до інформації, включаючи заходи щодо захисту приватного життя та особистої інформації. Втрата конфіденційності, тобто несанкціоноване розголошення інформації.

- Цілісність, що означає захист від неналежної модифікації або знищення інформації, включаючи забезпечення неспростування та автентичності інформації. Втрата цілісності означає несанкціоновану модифікацію або знищення інформації.

- Доступність, що означає забезпечення своєчасного та надійного доступу до інформації та її використання. Втрата доступності означає порушення

доступу до інформації або можливості використання інформації чи інформаційної системи.

Вернер і Щепанюк розширюють ці три базові атрибути (конфіденційність, цілісність, доступність) додатковими атрибутами, такими як підзвітність, надійність, автентичність. Як зазначають Вернер і Щепанюк, перші три з наведених атрибутів - конфіденційність, цілісність, доступність - застосовуються до інформації в будь-якій формі. На відміну від них, підзвітність, надійність та автентичність стосуються захисту інформації в системах ІКТ, тобто цифрової інформації.

Інформаційна безпека має вирішальне значення для сучасних організацій, які все більше покладаються на цифрові технології. Вона передбачає забезпечення конфіденційності, цілісності та доступності даних, захист від несанкціонованого доступу, модифікації та втрати інформації. Для компаній інформація є цінним ресурсом, що безпосередньо впливає на їхню прибутковість, ліквідність та репутацію. Атрибути інформаційної безпеки - конфіденційність, цілісність і доступність - є ключовими для ефективного управління ризиками та підтримки операційної стабільності організації. З можливістю віддаленої роботи впровадження ефективних стратегій інформаційної безпеки стає необхідним для захисту даних від сучасних загроз.

Дистанційна робота в українському законодавстві має досить коротку історію. Її перші організовані прояви датуються 2007 роком, коли до Трудового кодексу було додано главу про дистанційну роботу. Однак, незважаючи на існування такої можливості, зростання інтересу до дистанційної моделі виконання обов'язків відбулося значно пізніше, а його пік припадає лише на 2020-2022 роки, коли законодавець вперше використав поняття дистанційної роботи. Раптове зростання інтересу до такої форми зайнятості було пов'язане з необхідністю адаптації умов праці до глобальної епідеміологічної ситуації, а також з технологічним зростанням і широким впровадженням сучасних технологій в робочі системи.

Поняття дистанційної роботи з'явилося в українському трудовому законодавстві в березні 2020 року. Протягом багатьох років її називали так званою віддаленою роботою, основною формою якої була так звана телеробота.

Епідемія COVID-19 призвела до поширення дистанційної роботи, яка станом на 2020 рік все ще існувала у трьох правових формах:

- надомна робота;

- дистанційна робота в рамках положень так званого «антикризового щита»;

- дистанційна робота поза межами вищезазначених режимів.

З 7 квітня 2023 року положення про дистанційну роботу були внесені до Кодексу законів про працю. Вони передбачають, що дистанційна робота може виконуватися повністю або частково в місці, вказаному працівником і погодженому з роботодавцем у кожному конкретному випадку, в тому числі за домашньою адресою працівника, зокрема з використанням засобів прямого зв'язку на відстані.

Впровадження дистанційної роботи є викликом для роботодавців з точки зору управління інформаційною безпекою. Це пов'язано з тим, що вони зобов'язані впроваджувати окремі процедури інформаційної безпеки, в тому числі для інформації, яка не є персональними даними.

У літературі можна знайти опис можливостей та загроз дистанційної роботи, що розглядаються як з точки зору працівника, так і з точки зору роботодавця. Автори цієї публікації зосередилися виключно на інцидентах, пов'язаних з відсутністю інформаційної безпеки при дистанційній роботі, що розглядаються з боку роботодавця. До таких ризиків належать:

- Фішингові атаки на працівників, які працюють віддалено. Працівники можуть отримувати фальшиві електронні листи, які виглядають як офіційні повідомлення з робочого місця, з проханням підтвердити конфіденційні дані або увійти на фальшиві веб-сайти. Як наслідок, дані для входу в системи компанії можуть бути викрадені, що призводить до витоку інформації.

- Застаріле програмне забезпечення та відсутність безпеки. Якщо віддалені працівники не оновлюють своє програмне забезпечення або не використовують належні засоби захисту, це відкриває двері для атак шкідливих програм або інших видів кібератак, які можуть поставити під загрозу системи компанії.

- Несанкціоноване використання мереж Wi-Fi. Якщо співробітники використовують публічні мережі Wi-Fi або інші незахищені інтернет-з'єднання під час віддаленої роботи, це наражає компанію на ризик перехоплення даних третіми особами.

- Втрата мобільних пристроїв з конфіденційними даними. Якщо працівник, який працює віддалено, втрачає пристрій, що містить конфіденційні дані компанії, відсутність належних заходів безпеки, таких як шифрування даних, може призвести до витоку інформації.

- Недостатня обізнаність працівників про політику безпеки. Якщо працівники не знають або не дотримуються політики інформаційної безпеки компанії, наприклад, діляться конфіденційними даними з неавторизованими особами або використовують приватні акаунти для передачі даних компанії, вони наражають компанію на ризик.

- Атаки на віддалені системи. Шкідливе програмне забезпечення впроваджується в систему віддаленого співробітника, в результаті чого доступ до даних блокується, а в обмін на розблокування системи вимагається викуп.

Ці інциденти наочно демонструють, як недотримання політики інформаційної безпеки при віддаленій роботі може призвести до різноманітних проблем і наразити компанію на серйозний ризик втрати даних або кібератак. Впровадження відповідних процедур і політик безпеки, а також підвищення обізнаності співробітників є ключем до забезпечення інформаційної безпеки у віддаленому робочому середовищі.

Тому впровадження системи управління інформаційною безпекою є стратегічним рішенням для організації. На створення та впровадження системи управління інформаційною безпекою впливають потреби та цілі організації,

вимоги до безпеки, процеси, що діють в організації, а також розмір та структура організації. У цьому контексті впровадження віддаленої роботи в організації, безумовно, впливає на потреби безпеки та вимоги до процесів організації, оскільки змінюється структура інформаційних потоків. Інформація більше не обробляється тільки в приміщенні роботодавця або в місцях, організованих роботодавцем. При дистанційній роботі цінна для роботодавця інформація може також оброблятися вдома у працівника або в іншому узгодженому віддаленому робочому місці. Таким чином, запровадження дистанційної роботи створює виклик для роботодавців з точки зору управління інформаційною безпекою.

Система управління інформаційною безпекою (СУІБ) - це не що інше, як операційна стратегія для забезпечення належного захисту інформації. Ця стратегія покликана забезпечити постійне вдосконалення операцій і процедур з метою оптимізації ризиків, пов'язаних з порушенням конфіденційності. Іншими словами, система інформаційної безпеки повинна захищати від загроз таким чином, щоб забезпечити безпеку організації:

- безперервність бізнес-операцій;
- мінімізацію втрат;
- максимізацію прибутку на інвестиції та бізнес-діяльність.

СУІБ, що відповідає стандарту ISO/IEC 27001, визнана рішенням, яке забезпечує конфіденційність, цілісність і доступність інформації, захист якої зараз є природною вимогою нашого часу.

ISO 27001 (або ISO/IEC 27001) - це міжнародний стандарт для стандартизації систем управління інформаційною безпекою (СУІБ). Стандарт визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. Крім того, він містить настанови щодо оцінки та управління ризиками інформаційної безпеки (Resilia, 2022).

Відповідно до ISO/IEC 27000, система управління інформаційною безпекою (СУІБ) - це «набір політик, процедур, керівних принципів і заходів,

що використовуються організацією для захисту своїх інформаційних активів» (PN-EN ISO/IEC 27000:2020-07).

За словами авторів, ISO 27001 підтримує організації у дотриманні правил інформаційної безпеки та законодавства щодо віддаленої роботи кількома способами:

- Рамковий стандарт відповідності - ISO 27001 забезпечує основу для створення системи управління інформаційною безпекою. Впровадження цього стандарту дозволяє організації встановити послідовні та відповідні процедури та політики інформаційної безпеки.

- Врахування законодавчих вимог - при впровадженні ISO 27001 організаціям необхідно враховувати чинне законодавство з інформаційної безпеки, яке включає в себе аспекти, пов'язані з віддаленою роботою. Стандарт допомагає включити ці вимоги в систему управління інформаційною безпекою.

- Виявлення та управління ризиками невідповідності - ISO 27001 покладає на організацію обов'язок виявляти та управляти ризиками, пов'язаними з недотриманням законів та нормативно-правових актів. Це включає ризики інформаційної безпеки, пов'язані з віддаленою роботою.

- Постійне вдосконалення системи - впровадження ISO 27001 вимагає постійного вдосконалення системи управління інформаційною безпекою. Організаціям необхідно стежити за змінами законів і нормативних актів, що стосуються віддаленої роботи, і оновлювати свої процедури, щоб залишатися на рівні законодавчих вимог.

- Підвищення довіри з боку регуляторних органів - сертифікація за стандартом ISO 27001 може підвищити довіру регуляторних та наглядових органів, демонструючи, що організація вживає належних заходів для захисту інформації, в тому числі в контексті віддаленої роботи.

Враховуючи ці аспекти, ISO 27001 не тільки забезпечує основу для управління інформаційною безпекою при віддаленій роботі, але також дозволяє організаціям дотримуватися чинних нормативних актів і законодавства, пов'язаних із захистом даних в цьому специфічному контексті.

ISO 27001 визначає стандартні вимоги та настанови щодо управління інформаційною безпекою в організаціях. Стандарт містить Додаток А, який є, мабуть, найвідомішим додатком серед усіх стандартів ISO. Насправді, цей додаток є важливим інструментом для управління ризиками інформаційної безпеки (Stinet, 2023). Він містить 114 пунктів і пов'язані з ними цілі контролю, які можна впровадити для захисту інформації організації. Ці цілі контролю вважаються загальними цілями у сфері інформаційної безпеки.

Варто зазначити, що Додаток А не є обов'язковим, але використовується як керівництво для розробки власних стандартів контролю та процедур безпеки, які відповідають вимогам вашої організації та її контексту. Впровадження конкретних стандартів контролю залежить від оцінки ризиків та потреб організації.

Організації, які не мають впровадженої системи управління інформаційною безпекою ISO 27001, мають можливість використовувати Додаток А як посібник при розробці або вдосконаленні своєї поточної системи інформаційної безпеки. Додаток А до ISO 27001 можна розглядати як так званий контрольний список з набором контрольних точок для підтримки організацій в управлінні інформаційною безпекою.

Додаток А можна використовувати двома способами:

- при розробці стратегії безпеки компанії - шляхом вибору тих контрольних точок, які можуть бути застосовані до конкретної організації.

- при оцінці готовності організації до процесу управління інформаційною безпекою - як оцінка вже впровадженої стратегії безпеки та як основа для вдосконалення наявної системи.

З огляду на відгуки зовнішніх аудиторів ISO 27001, підхід до інформаційної безпеки при дистанційній роботі до і після впровадження ISO 27001 може суттєво змінитися.

До того, як організація впровадила ISO 27001, в контексті інформаційної безпеки віддаленої роботи часто можна спостерігати наступні аспекти:

- Відсутність узгоджених стандартів. До впровадження ISO 27001 компанії можуть працювати без чітких стандартів інформаційної безпеки для віддаленої роботи. Часто в організації не вистачає послідовних процедур і політик для забезпечення цієї безпеки.

- Реактивний підхід. Без ISO 27001 підхід до інформаційної безпеки для віддаленої роботи може бути реактивним, а не проактивним. Компанії можуть реагувати на інциденти, а не запобігати їм.

- Недостатня обізнаність про ризики. До впровадження стандарту обізнаність працівників про ризики інформаційної безпеки при віддаленій роботі часто навіть незначна, що може призвести до більшої вразливості до атак. Після впровадження ISO 27001 помітні позитивні моменти:

- Визначені стандарти та процедури. Після впровадження ISO 27001 компанія має узгоджені стандарти, процедури та інструкції з інформаційної безпеки при віддаленій роботі, що забезпечує структурований підхід до управління ризиками.

- Проактивний підхід. ISO 27001 сприяє проактивному підходу до інформаційної безпеки. Організації стають більш здатними передбачати потенційні ризики та вживати превентивних заходів.

- Підвищення обізнаності. Впровадження ISO 27001 призводить до підвищення обізнаності співробітників про ризики та процедури інформаційної безпеки при віддаленій роботі завдяки навчанню та освіті.

- Моніторинг та вдосконалення. ISO 27001 вимагає моніторингу та вдосконалення систем інформаційної безпеки. Після впровадження організації проводять регулярні перевірки та оновлення, щоб адаптуватися до мінливих загроз.

В результаті, впровадження ISO 27001 в дистанційній роботі призводить до більш структурованого, проактивного та усвідомленого підходу до інформаційної безпеки, що, в свою чергу, знижує ризики та підвищує ефективність діяльності з інформаційної безпеки.

Впровадження форми віддаленої роботи, спричинене пандемією COVID-19, врятувало багато компаній від банкрутства, а їхніх працівників - від безробіття. Таким чином, це запустило процес аналізу вигод і втрат, спричинених можливістю впровадження такої форми роботи в постпандемічний період. До спалаху пандемії COVID-19 у використанні дистанційної форми роботи вбачалося багато переваг. Очікувалося, що використання комп'ютерних технологій зменшить витрати на працевлаштування, надасть можливість бізнесу розвиватися, а працівникам - більшу свободу та автономію, а також досвід роботи. Сьогодні все частіше визнається, що віддалена робота повинна супроводжуватися певними змінами, пов'язаними з регулюванням і застосуванням належного управління інформаційною безпекою.

Впровадження ISO 27001 стає ключовим орієнтиром для організацій, забезпечуючи структурну основу для ефективного управління інформаційною безпекою в контексті віддаленої роботи. Стандарт дозволяє визначити процедури, політики та контрольні точки, необхідні для захисту даних, як в корпоративних мережах, так і у віддалених робочих середовищах.

Переваги впровадження рішення, описаного в статті, не обмежуються мінімізацією ризиків. Впровадження ISO 27001 або використання так званого контрольного списку - це також крок до створення структурної основи для ефективного управління інформаційною безпекою не тільки в мережах компанії, але і в умовах віддаленої роботи. Таке рішення не тільки захищає цілісність, конфіденційність і доступність інформації, але й сприяє підвищенню операційної ефективності організації, підтримці прибутковості та дотриманню правових норм. Таким чином, впровадження рішення, описаного в статті, є необхідним кроком на шляху до забезпечення безпеки та оптимізації діяльності організації в нових реаліях віддаленої роботи.

ВИСНОВКИ

Висвітлення питання викривання та захисту так званих «викривачів» з урахуванням правового, економічного та соціального контексту є першим на сьогодні настільки широким висвітленням цієї теми. Це пов'язано з авторським баченням цілісного аналізу обставин та мотивів, що вплинули на прийняття Директиви (ЄС) 2019/1937 Європейського Парламенту та Ради від 23 жовтня 2019 року про захист викривачів.

Тема захисту викривачів викликає багато емоцій. З одного боку, нею займаються науковці та лідери громадської думки, ретельно досліджуючи мотиви, мету та вплив нових положень права Співтовариства; з іншого боку, вона є предметом широкої громадської та навіть медійної дискусії. Кількість інтерпретацій, що випливають з аналізу положень Директиви, іноді суперечливих, а також законодавча невизначеність (на дату цієї публікації в Україні не було прийнято жодного закону, який би регулював захист викривачів) призводять до плутанини. Таким чином, правове регулювання не встигає за потребами та реальністю - діяльністю юридичних осіб, що працюють у державному та приватному секторах, які очікують на національні рішення, крім тих, які ефективно досягнуть цілей Директиви. Значна частка компаній працює в капітальних, організаційних і трудових відносинах глобального характеру і тому очікує, що національні правила будуть достатньо універсальними, щоб чітко захищати інтереси всіх сторін, на яких поширюється право Європейського Союзу. Автори вважають, що адресати положень Директиви (особи, які здійснюють законодавчу роботу на національному рівні, потенційні викривачі та юридичні особи) повинні бути поінформовані про її наміри, беручи до уваги зобов'язання тлумачити національне законодавство відповідно до права Співтовариства.

Тому посилання в різних розділах роботи на останній проект Закону про захист викривачів мають лише договірний та порівняльний характер. Це пов'язано з тим, що невідомо, якою буде остаточна форма чинного

законодавства в Україні. З огляду на ці знаки питання, автори вирішили доповнити теоретичну частину публікації звітом про дослідження, проведене в групі підприємців, що представляють сектори, на які особливо впливають положення Директиви. Вони також вирішили, що голос практиків - вивчення їхніх знань та очікувань у контексті запропонованих положень на основі Директиви - є важливим і може сприяти проведенню більш ретельного та авторитетного законодавчого, наукового та практичного аналізу.

Ми мали намір підготувати практичний документ, який може слугувати посібником із законодавства ЄС (з посиланням на ширший контекст права Співтовариства та права прав людини), належної практики (шляхом формулювання питання з точки зору комплаєнсу, управління комплаєнсом та корпоративного управління) та відносин із соціальними партнерами (профспілками). У додатку до дослідження також підготовлено резюме законодавчих рішень, прийнятих в окремих країнах ЄС. Він може бути особливо корисним для тих реципієнтів законодавства, які працюють у сфері транснаціональних відносин.