

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ФАКУЛЬТЕТ БІЗНЕСУ ТА СФЕРИ ОБСЛУГОВУВАННЯ

КАФЕДРА ФІНАНСІВ ТА ЦИФРОВОЇ ЕКОНОМІКИ

ГРИБУШИН Богдан Максимович
(студент групи ЕПМ-20)

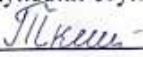
19. - 2. - 1
28. 12. 2023

КВАЛІФІКАЦІЙНА РОБОТА

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТА
В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

(представлена на здобуття ступеня вищої освіти «магістр»
спеціальності 051 «Економіка»
(освітньо-професійна програма «Економіка»)

Допущено до захисту
протокол № 14
від 11 грудня 2023 р.
зав. кафедри фінансів та цифрової
економіки,
д.е.н., проф. Н.Г. Виговська

Науковий керівник
к.е.н., доц. Ткачук В.О.
(науковий ступінь, вчене звання, прізвище та ініціали)

(підпис)

Рецензент
к.е.н., доц. Бурачек І.В.
(науковий ступінь, вчене звання, прізвище та ініціали)

(підпис)

Житомир, 2023 р.

АНОТАЦІЯ

Грибушин Б.М. Захист персональних даних співробітників підприємства в умовах цифрової економіки. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 051 «Економіка». – Державний університет «Житомирська політехніка», Житомир, 2023.

У кваліфікаційній роботі розглядаються персональні дані співробітників підприємств та процедура їх захисту в умовах цифровізації; розглянуто основи захисту персональних даних в європейських правових актах. З'ясовано порядок забезпечення захисту персональних даних співробітників в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради. Запропоновано створення комплексної системи захисту персональних даних в основі програмно-адаптивного захисту підприємства.

Ключові слова: сфера персональних даних, захист персональних даних, принципи захисту персональних даних, цифрова економіка.

ABSTRACT

Hrybushyn B.M. Protection of personal data of employees of the enterprise in the conditions of digital economy. – Manuscript.

Qualifying thesis for obtaining a master's degree in the specialty 051 «Economics». – Zhytomyr Polytechnic State University, Zhytomyr, 2023.

The qualifying thesis examines the personal data of employees of enterprises and the procedure for their protection in the context of digitalisation; the basics of personal data protection in European legal acts are considered. The article clarifies the procedure for ensuring the protection of personal data of employees in the conditions of the Municipal Enterprise «Zhytomyr Tram and Trolleybus Department» of the Zhytomyr City Council. The creation of a comprehensive system of personal data protection based on software-adaptive protection of the enterprise is proposed.

Keywords: personal data sphere, protection of personal data, principles of personal data protection, digital economy.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ.....	9
1.1. Персональні дані співробітників підприємств та їх захист в умовах цифровізації.....	9
1.2. Принципи захисту персональних даних працівників.....	17
1.3. Сучасні основи захисту персональних даних в європейських правових актах.....	26
Висновки до розділу 1.....	39
РОЗДІЛ 2. ОСНОВИ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ.....	41
2.1. Організаційно-економічна характеристика Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.....	41
2.2. Оцінка ефективності управління персоналом підприємства.....	52
2.3. Порядок забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.....	58
Висновки до розділу 2.....	62
РОЗДІЛ 3. УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВА.....	64
3.1. Шляхи удосконалення забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.....	64
3.2. Створення комплексної системи захисту персональних даних в основі програмно-адаптивного захисту підприємства.....	70
Висновки до розділу 3.....	75

ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	81
ДОДАТКИ.....	89

ВСТУП

Актуальність теми. Сучасною політикою «цифровізації України» аргументується необхідність вживання заходів, спрямованих на зміцнення довіри користувачів Інтернет до джерел інформації, включаючи захист персональних даних. Персональні дані користувачів стають головним джерелом конкурентоспроможності підприємства. Збір, опис, зберігання та обробка персональних даних дозволяє отримувати цінну інформацію для використання в ділових процесах, суспільному житті, роботі держави.

Вміння працювати з такими даними та їх аналізувати – це можливість першим отримувати цінні ринкові «інсайти», тобто бути більш конкурентоздатним. Водночас, будучи одним із ключових цифрових трендів, персональні дані актуалізують реальну проблему їх захисту.

Вільний широкий доступ до інформації сприяє створенню можливостей та розвитку особистості, але разом із тим потребує розроблення та впровадження адекватних захисних механізмів, спроможних реально захистити персональні дані особи. Незважаючи на значну увагу з боку суспільства та держави до проблеми забезпечення захисту персональних даних осіб від несанкціонованого втручання та оприлюднення сторонніми особами, сьогодні воно й досі залишається відкритим. Це й зумовлює актуальність проведення дослідження та доцільність пов'язаного із дослідженням механізму захисту персональних даних.

Забезпечення захисту персональних даних громадян посідає зараз одне з провідних місць серед актуальних викликів цифрової трансформації економіки країни. Це підтверджують численні роботи вітчизняних науковців, таких як В.М. Брижко, О.В. Гронь, О.Ю. Наливайко, А.К. Погореленко, І.М. Сопілко, А. Тунік та ін., які пропонують методологічні підходи до класифікації персональних даних, визначають актуальні проблеми захисту персональних даних, розробляють відповідне нормативно-правове поле для використання персональної інформації в бізнес-процесах. Зокрема, підходи до визначення критеріїв класифікації персональних даних розглядає О.Ю. Наливайко, який узагальнює, що основною

підставою для класифікації персональних даних в європейських країнах є рівень вразливості даних, що, в свою чергу, визначає ступінь захисту такої інформації [53, с. 171]. Пропозиції щодо створення національної цілісної системи захисту персональних даних наводить В.М. Брижко. Автор апелює до відсутності ефективного правового механізму щодо адміністративно-організаційного регулювання відносин та відповідальності у сфері захисту персональних даних [54, с. 44].

О.В. Гронь і А.К. Погореленко у своїй праці звертають увагу на необхідності державного контролю за дотриманням правил збору, зберігання та захисту персональної інформації [55, с. 107]. Разом із тим, залишають недостатньо дослідженими питання забезпечення захисту персональних даних співробітників підприємств у цифровій економіці.

Метою кваліфікаційної роботи є розкриття теоретичних і прикладних основ забезпечення захисту персональних даних співробітників підприємства в умовах цифрової економіки, а також розробка рекомендацій щодо його покращення в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.

Для досягнення поставленої мети в роботі визначені для вирішення наступні *завдання*:

- з’ясовано економічний зміст поняття «персональні дані співробітників підприємств» та процедуру їх захисту в умовах цифровізації;
- класифіковано принципи захисту персональних даних працівників;
- розкрито сучасні основи захисту персональних даних в європейських правових актах;
- надано організаційно-економічну характеристику Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради;
- проведено оцінювання ефективності управління персоналом підприємства;
- визначено порядок забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради;

– розглянуто шляхи удосконалення забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради;

– запропоновано створення комплексної системи захисту персональних даних в основі програмно-адаптивного захисту підприємства.

Об’єктом дослідження є господарські процеси в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.

Предметом дослідження у роботі є механізм забезпечення захисту персональних даних співробітників підприємства.

Методи дослідження. У кваліфікаційній роботі використовувались як загальнонаукові, так і спеціальні методи наукового дослідження. Зокрема, при відборі інформації з літературних і довідкових джерел застосовувався метод *абстрагування*, що дозволив зосередитися на найважливіших моментах забезпечення захисту персональних даних співробітників підприємства. Метод *гіпотези* дав можливість сформулювати висновки щодо існування залежності між наявністю сучасних цифрових технологій та безпекою інформаційної діяльності підприємства, в т. ч. в контексті захисту персональних даних співробітників, виявити проблеми захисту персональних даних на підприємстві та запропонувати заходи щодо його посилення в умовах цифрової економіки. Провідну роль при формуванні проміжних і підсумкових результатів відіграли спеціальні методи дослідження, зокрема: історичний, метод спостереження; статистико-економічний метод.

Інформаційною базою дослідження є статті вітчизняних і зарубіжних вчених у фахових виданнях, навчальні посібники, інформаційно-аналітичні бюлетені, матеріали науково-практичних конференцій, електронні ресурси та спеціалізовані портали.

Практичне значення одержаних результатів полягає в розробці науково-методичних і практичних рекомендацій щодо забезпечення захисту персональних даних співробітників в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради.

Особистий внесок студента. Кваліфікаційна робота є самостійно виконаним науковим дослідженням. Усі наукові та прикладні результати, що викладені в роботі та виносяться на захист, одержані особисто автором.

Апробація результатів кваліфікаційної роботи. Основні теоретичні положення та практичні результати дослідження апробовано у доповідях та обговореннях на Всеукраїнській науково-практичній конференції молодих вчених «Глокалізаційні аспекти інноваційного розвитку економіки» до 150-річчя Симона Літмана (м. Одеса, 13 жовтня 2023 р.) та IV Міжнародній науково-практичній конференції «Сучасні виклики сталого розвитку бізнесу» (м. Житомир, 09–10 листопада 2023 р.).

Публікації. За результатами наукових досліджень автором опубліковано 2 наукові праці загальним обсягом 0,32 д.а., з них 2 у матеріалах науково-практичних конференцій, а саме:

1. Ткачук В.О., Грибушин Б.М. Забезпечення відповідності використання блокчейн-технології в обробці персональних даних вимогам GDPR. Глокалізаційні аспекти інноваційного розвитку економіки: збірник матеріалів Всеукраїнської науково-практичної конференції молодих вчених (Одеса, 13 жовтня 2023 р.) [Електронний ресурс]. – Одеса: ОНЕУ, 2023. – С. 72–73.

2. Ткачук В.О., Грибушин Б.М. Обробка персональних даних співробітників підприємства в мережі блокчейн. Сучасні виклики сталого розвитку бізнесу : тези виступів IV Міжнар. наук.-практ. конф. Житомир : Житомирська політехніка, 2023. С. 187–188.

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Обсяг роботи налічує 81 сторінку основного тексту. Робота містить 14 таблиць, 7 рисунків, 65 найменувань використаних джерел, 5 додатків.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

1.1. Персональні дані співробітників підприємств та їх захист в умовах цифровізації

Сучасний глобалізований світ існує в безмежних інформаційних потоках, обсяги яких прагнуть до нескінченності. Вступивши в цифрову еру, еру інформаційних технологій, людство завдяки новітнім телекомунікаційним системам отримало широкий доступ до будь-якої інформації. І користь від цього є очевидною, адже «пошукові системи полегшують доступ до великого обсягу інформації та знань, соціальні мережеві сервіси надають людям можливість спілкуватись по всьому світу, висловлювати думки та мобілізувати підтримку в соціальних, екологічних та політичних цілях, а компанії та споживачі отримують переваги від ефективних і дієвих ринкових технологій, що сприяють зростанню економіки» [22, с. 375].

Разом із тим «широкий доступ» до інформації зовсім не означає «необмежений», оскільки далеко не всі дані можуть бути оприлюднені, зокрема, й ті, що лежать в полі трудового права, – персональні дані працівника. На жаль, запровадження новітніх телекомунікаційних засобів разом із безліччю можливостей із збору, обробки, накопичення великих обсягів інформації та полегшенням й оперативністю її отримання та користування викликало проблему, яка лежить у правовій площині, – певну суперечність, незбалансованість між правом користувача на інформацію і правом володільця інформації на приватність. З огляду на це, а також на технічну складність та непрозорість збирання та обробки великої кількості персональної інформації, з усією очевидністю постає необхідність її належного захисту.

Існують й інші причини для того, щоб вважати захист персональних даних одним з найважливіших завдань не тільки ІТ-спеціалістів, а й працівників: з одного боку, відбувається цифровізація всіх сфер людського буття та активізація професійної

діяльності людини в цифровому просторі; з другого – зростає кількість кібератак та витоків персональних даних у цифровому середовищі, а отже, порушується право на приватність.

Розмірковуючи про нагальність потреби захисту персональних даних працівників, слід зважати й на те, що «зміна умов праці та автоматизація і комп'ютеризація засобів праці, розширення мультимедійного простору спростило доступ до інформації щодо господарської діяльності, договірних зв'язків, трансферу технологій, у т. ч. й у питаннях щодо персоніфікованої інформації про працівників, тобто їхніх персональних даних» [23, с. 207].

На беззаперечній важливості окресленої проблеми наголошує О.М. Рим, яка стверджує, що забезпечення розумного рівня захисту даних особи в контексті зайнятості постало перед новими викликами, які диктує науково-технічний прогрес. Вчена пояснює свою думку і наводить переконливі аргументи: «Велика чисельність працівників оточені різноманітними пристроями чи засобами, які в той чи інший спосіб можуть фіксувати їхні дії чи бездіяльність. Відтак, цифрові технології, що пропонують нові можливості для покращення продуктивності трудового процесу та дистанційної праці, можуть одночасно привести до розмивання меж між робочим та приватним життям, створюючи значні проблеми для конфіденційності працівника. Саме тому новітні технології мають сприяти не лише вільному обміну персональних даних у межах Європейського Союзу (далі – ЄС) та передачі до третіх країн та міжнародних організацій, але також і забезпечувати високий рівень захисту відповідної інформації» [24, с. 342].

Про державне значення цього питання свідчить прийняття Верховною Радою Закону України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI, який став першим кроком до імплементації Україною своїх міжнародних зобов'язань щодо захисту персональних даних. У той же час його ухвалення було лише частиною цього процесу, оскільки закріплені на національному рівні норми сьогодні вже не відповідають міжнародним стандартам.

Тож після ухвалення у 2016 р. Європейським парламентом нового Регламенту щодо захисту персональних даних (GDPR) питання відповідності української системи

захисту персональних даних стандартам ЄС набуло ще більшої актуальності. Це пов'язано з тим, що GDPR має екстериторіальну дію і застосовується для всіх компаній, які обробляють персональні дані резидентів і громадян ЄС, незалежно від місця знаходження такої компанії.

Зрозуміло, що філії/представництва українських організацій повинні відповідати новим вимогам [25, с. 115]. З огляду на це українське законодавство має піддатися відповідним змінам, щоб усунути стримувальні перепони, що існують нині у зв'язку з його застарілістю і заважають розвитку багатьох сфер сучасного суспільства.

Зазначимо, що у Законі України «Про захист персональних даних» практично відсутнє регулювання захисту персональних даних, і трудове законодавство не містить спеціальних норм про захист персональних даних працівника. Науковці вказують на недостатнє регламентування українським законодавцем захисту персональних даних, справедливо стверджуючи: «В той час як Регламент приділяє ґрунтовну увагу саме положенням щодо захисту персональних даних, вітчизняний Закон містить лише дві статті (ст. 5 «Об'єкти захисту» та ст. 24 «Забезпечення захисту персональних»), але ці норми не містять положень щодо захисту даних працівників в належному обсязі» [25, с. 136]. Разом із тим задля справедливості, відмітимо, що у Верховній Раді знаходиться на розгляді проєкт Закону України «Про захист персональних даних» від 25.10.2022 р. № 8153, розроблений з метою приведення нормативного регулювання України в сфері захисту персональних даних у відповідність до нових міжнародних стандартів.

У висновку Комітету з питань цифрової трансформації йдеться, що відсутність нового законодавства, яке б відповідало сучасним міжнародним стандартам у цій сфері та рівню технологічного розвитку, не тільки призводить до незадовільного рівня захисту конституційного права на повагу до приватного життя в Україні, але й може призвести до визнання на міжнародному рівні України як держави, яка не забезпечує належний рівень захисту персональних даних [26]. Тому прийняття вищезгаданого Закону № 8153 є вкрай важливим для України.

У становленні інституту персональних даних та захисту персональних даних важливу роль відіграли міжнародні акти ООН, МОП, Ради Європи (далі – РЄ), ЄС.

Необхідність захисту персональних даних працівника базується на одному з фундаментальних прав людини – захисті від втручання в особисте життя [27, с. 136].

В рамках нашого дослідження розглянемо різні підходи до визначення терміну «персональні дані», який міститься в наукових дослідженнях, міжнародному та українському законодавстві. Уперше визначення персональних даних було надано у Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року № 108, де зазначено, що «персональні дані – це інформація, що стосується конкретної особи або такої особи, яка може бути ідентифікована» [27].

Сьогодні Конвенція РЄ від 1981 р. продовжує виконувати функцію основного документа, що визначає міжнародні принципи прав і свобод людини щодо захисту персональних даних, і є головним світовим правовим стандартом у сфері захисту персональних даних [28, с. 55]. Як зазначають вчені-юристи, на сьогодні це є перший та єдиний міжнародний договір щодо захисту персональних даних, з моменту якого «захист персональних даних виокремився у самостійний вид діяльності» [29].

Відповідно до ст. 2 вищезгаданої Конвенції, персональні дані означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною. Визначення персональних даних про особу містить ст. 11 Закону України «Про інформацію» [30], а також ст. 2 Закону України «Про захист персональних даних» [31]. Зокрема, інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Стаття 2 проєкту Закону України «Про захист персональних даних» від 25 жовтня 2022 р. № 8153 термін «персональні дані» визначає як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано. З цього приводу поділяємо думку О. Бреся, який вважає, що наведене визначення персональних даних у Законі України «Про захист персональних даних», незважаючи на відповідність міжнародній практиці, не є вичерпним і не дає чітких критеріїв того, які саме дані про фізичну особу можна вважати персональними [32, с. 220].

Так само, як і законодавець, узагальнений підхід застосовує Г. Виноградова, яка зазначає, що «персональні дані – це сукупність документованих або публічно оголошених відомостей про фізичну особу» [33, с. 176]. У свою чергу, О. Дяковський розуміє персональні дані як відомості чи сукупність відомостей про живу фізичну особу, яка ідентифікована або може бути конкретно ідентифікована з урахуванням встановленого законом поділу персональних даних» [28, с. 57].

О. Брижко відмічає, що поняття «персональні дані» охоплює об'єктивні та суб'єктивні відомості про особисте, сімейне чи публічне життя фізичної особи, що виражені у формі літер, чисел, графіки, фото, звуку чи відео, символів, якщо вони дозволяють ідентифікувати таку особу. Для визнання відомостей персональними даними обов'язковою є наявність зв'язку між такими відомостями та конкретною особою [34, с. 59].

Таким чином, можна узагальнити, що в існуючих визначеннях поняття «персональні дані» в основу покладений термін «ідентифікація». У загальному значенні ідентифікація (від лат. *Identifico* – «ототожнюю») означає визначення відповідності предмета, біологічного організму, особи (юридичної, фізичної), певним, конкретним, лише їм властивим ознакам.

Ідентифікація особи – визначення за допомогою спеціальних методів тотожності суб'єкта, конкретній особі [35, с. 488]. Зауважимо, що в чинному законодавстві відсутній вичерпний перелік, який вказує, які саме дані про фізичну особу можна вважати персональними, а які до них не відносяться [32]. Нагадаємо, що для забезпечення захисту персональних даних 14 квітня 2016 р. Європейський парламент ратифікував новий Регламент щодо захисту персональних даних. 25 травня 2018 року він набрав чинності та став більш відомий як GDPR (англ. *General Data Protection Regulation*, 2016/679). Цей документ покликаний створити єдиний правовий режим персональних даних та забезпечити їх обробку системою базових принципів.

GDPR визначає «персональні дані» як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»). На перший погляд, формулювання видається простим, проте через високий ступінь узагальненості на практиці часто потребує роз'яснення. У. Шадська для зручності

сприйняття поділяє його на змістовні блоки [36]:

1. «Будь-яка інформація»: персональними даними можуть вважатися будь-які відомості про людину, що відображають її фізичну, фізіологічну, генетичну, економічну, соціальну або культурну ідентичність. Вони діляться на дві категорії: загальні та особливі (чутливі).

2. «Що стосується фізичної особи»: будь-яка інформація повинна мати прямий або непрямий зв'язок із конкретною фізичною особою. Наприклад, зображення людини може дати змогу прямо її ідентифікувати. Проте отримання про неї додаткової інформації через зареєстрований номерний знак автомобіля – це вже буде непряма ідентифікація.

Таким чином, майже усі наведені визначення вказують на однаковий підхід, як на міжнародному, так і національному рівні, до розуміння терміну «персональні дані» [41, с. 191]. Проте у КЗпП України, як основному нормативно-правовому акті у сфері праці, відсутні такі поняття, як «персональні дані працівника», «захист персональних даних працівника» та норми, які гарантують захист персональних даних працівника.

З позицій трудових відносин розглядають персональні дані працівника Г.І. Чанишева та Р.І. Чанишев, які пропонують розуміти такі дані, як інформацію, необхідну роботодавцю у зв'язку з трудовими відносинами, що стосується конкретного працівника та пов'язана з його професійною кваліфікацією, діловими, професійними якостями. Ця інформація стосується також вимог, що можуть бути висунуті до працівника у зв'язку з характером роботи [37, с. 171].

О.В. Оніщенко вказує, що відомості про працівників, відображені у кадрових документах, зокрема про вік, дату та місце народження, місце проживання, ідентифікаційний номер, соціальний статус, пільги, відповідно до закону слід розглядати як персональні дані, що у своїй сукупності складають базу персональних даних або її частину [38, с. 173]. М.В. Сокол та А.В. Тимошук персональними даними працівника вважають відомості про факти, події і обставини життя працівника, що безпосередньо пов'язані з трудовими відносинами, тобто з діловими якостями працівника, що мають безпосереднє відношення до виконуваної ним трудової функції та надаються роботодавцю з метою забезпечення дотримання законів та інших

нормативних правових актів, сприяння працівникові у працевлаштуванні, навчанні, підвищенні кваліфікації і перекваліфікації, забезпеченні охорони праці, контролю за кількістю та якістю виконуваної роботи [39, с. 53].

Кодекс законів про працю України у ст. 24 передбачає, що при укладенні трудового договору громадянин зобов'язаний подати паспорт або інший документ, що посвідчує особу, трудову книжку (у разі наявності) або відомості про трудову діяльність з реєстру застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування, а у випадках, передбачених законодавством, – також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я, відповідний військовообліковий документ та інші документи. Всі ці документи містять інформацію про претендента на посаду, яку відповідно до міжнародних і національних нормативно-правових актів слід вважати персональними даними.

При прийнятті на роботу оригінали документів працівника чи їх копії зберігаються у роботодавця. Крім цього, кадровий облік персоналу передбачає систематизацію інформації про працівників в електронній формі та/або у формі картотек.

Виходячи зі змісту вищезначеної статті КЗпП України, К.М. Мельник небезпідставно стверджує, що під персональними даними працівника слід розуміти будь-яку інформацію, яка стосується конкретної фізичної особи, що працює на підставі трудового договору, та надана роботодавцю або ним зібрана відповідно до законодавства. До персональних даних працівника слід віднести інформацію про вік, дату і місце народження, громадянство, реєстраційний номер облікової картки платника податків, трудову діяльність, стан здоров'я, рівень освіти, володіння українською та іноземними мовами, сімейний стан [40, с. 34]. І цей перелік не є вичерпним. Зрозуміло, що наприклад, перелік конкретних персональних даних працівників промислових підприємств, торгівлі та побуту буде відрізнятися від переліку персональних даних осіб, уповноважених на виконання функції держави або місцевого самоврядування, але роботодавець не повинен вимагати від працівника персональні дані, які не стосуються професійних якостей та кваліфікації.

Важливе, на наш погляд, положення, що стосується збирання інформації,

міститься в Регламенті ЄС 2016/679, де наголошено, що збір інформації щодо працівника повинен обмежуватися даними, які необхідні та доречні з огляду на обсяг трудових прав та обов'язків особи. Окремі питання, які пов'язані із стрімким розвитком цифровізації, виникають у зв'язку з тим, що роботодавці не завжди дотримуються спеціальних правил обробки персональних даних. Наприклад, в країнах ЄС особливе значення надається прозорості та чіткості проведення моніторингу на робочому місці, адже сьогодні поширеною проблемою є законний ступінь контролю за електронною комунікацією працівника [24, с. 345]. Також необхідно звернути увагу на те, що правовим підґрунтям для обробки персональних даних працівника з боку роботодавця є його згода, однак це правило не діє щодо трудових відносин.

Кожен роботодавець змушений обробляти персональні дані всіх своїх працівників. Передусім йдеться про їхні імена, прізвища, номери телефонів, номери банківських рахунків та дані про зарплату. Необхідність їх обробки очевидна, навіть більше – безумовна, оскільки без таких даних не можуть реалізовуватися трудові відносини. Зокрема, роботодавці зобов'язані вести облік днів тимчасової непрацездатності працівників з метою правильного нарахування заробітної плати, так само як і реквізити банківських рахунків потрібні для виплати нарахованої заробітної плати. Без цієї інформації роботодавець не зможе реалізувати свої обов'язки за трудовим договором [24, с. 343].

Таким чином, обробку персональних даних працівника, роботодавець може здійснювати лише у разі фактичної необхідності та за наявності правових підстав. Позитивним є те, що у законопроекті № 8153 від 25.10.2022 р. обробці роботодавцем персональних даних присвячено окремий розділ. Він включає в себе, зокрема, статті, присвячені загальним питанням обробки персональних даних роботодавцем, обробці персональних даних працівників їх представниками, особливим вимогам до обробки роботодавцем персональних даних працівників або кандидатів на працевлаштування та прозорості/обробки персональних даних в цілях трудових правовідносин.

Отже, під персональними даними працівника варто розуміти будь-яку інформацію, що стосується конкретної фізичної особи, яка працює на підставі

трудового договору, і надана особисто такою особою роботодавцеві або зібрана останнім відповідно до законодавства. До персональних даних працівника відносять інформацію про вік, дату і місце народження, громадянство, реєстраційний номер облікової картки платника податків, трудову діяльність, стан здоров'я, рівень освіти, володіння українською та іноземними мовами, сімейний стан. І цей перелік не є вичерпний. Це пов'язано з тим, що необхідний перелік персональних даних працівників може відрізнятися за своїм змістом, виходячи з того, яку вони будуть займати посаду та виконувати трудову функцію.

Наголошено, що, з огляду вирішення проблеми захисту персональних даних працівника в умовах цифровізації, нагально необхідно здійснити систематизацію та кодифікацію національного законодавства у сфері персональних даних відповідно до норм європейського законодавства; розробити єдиний нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, захист персональних даних працівника. Цілком поділяємо думку О. Рим, що наблизитись до забезпечення балансу інтересів роботодавців і працівників під час обробки персональних даних останніх можна, якщо ця обробка відповідатиме таким вимогам: буде адекватною, доречною та обмежуватиметься досягненням необхідної мети; використання, мета та спосіб обробки повинні бути зрозумілі для працівників; працівники повинні мати можливість реалізувати свої права перевіряти, виправляти, припиняти та обмежувати обробку; персональні дані повинні зберігатись не більше, ніж потрібно; персональні дані повинні бути захищені відповідними технічними та організаційними заходами безпеки.

1.2. Принципи захисту персональних даних працівників

Механізм захисту персональних даних працівника ґрунтується на певній системі принципів, завдяки яким такий механізм набуває демократичного характеру та стає соціально орієнтованим. Іншими словами, принципи захисту персональних даних відбивають засадничі соціально-демократичні ідеї, що лежать в основі відповідного

механізму; навіть більше, принципи є одним з його елементів. Відтак, дослідження питання щодо принципів захисту персональних даних надасть змогу визначити ідейно-правову сутність механізму захисту персональних даних працівника. З цього приводу варто погодитись з думкою В.М. Колодія, який зазначає, що принципи права – це ідеологічна категорія, а це означає, що вони, як і право загалом, є формою суспільної свідомості, яка здійснює ідейний, інформаційно-виховний вплив загального характеру, тобто виконує функцію загального закріплення суспільних відносин, що та дає можливість розглядати їх з позиції певних ідей, керівних засад [42, с. 41].

Поняття «принципи» вживається головним чином у значенні ідей, ціннісних орієнтирів, керівних засад, які визначають сутність та відбивають специфіку тієї чи іншої сфери соціальних відносин. За допомогою принципів певні явища, правовідносини, суспільна діяльність набувають сутнісних особливостей відповідної історичної епохи та соціально-правової системи, що прийнята у державі.

Різноманітність правових принципів потребує їх певної систематизації та класифікації за визначеними критеріями. З цього приводу у науковій літературі висувається ряд пропозицій, однак, однією з найбільш розповсюджених наукових концепцій є класифікація принципів права за галузевим критерієм. За даним критерієм принципи права поділяються на загальногалузеві, міжгалузеві та спеціально галузеві. Зважаючи на комплексний характер правовідносин, що виникають у сфері захисту персональних даних, принципи, на яких ґрунтується такі правовідносини також мають міжгалузевий комплексний характер. Зокрема, комплексність досліджуваного виду правовідносин виражається у тому, що вони регламентуються законодавством, що належить до декількох галузей права, основними з яких є інформаційне та трудове право.

Відтак, принципи захисту персональних даних працівника містять засадничі основи обох галузей права. При цьому, слід також вказати на існування загальних принципів, притаманних праву. Традиційно до системи загальних принципів відносяться: верховенство права, законності, пріоритетності життя, здоров'я, особистої безпеки людини та громадянина, особистої недоторканності особи,

демократизму, народовладдя тощо. Що стосується галузевих принципів, то вони різняться залежно від галузі права. Так, І.І. Швидкій до основних принципів правового регулювання трудових відносин працівників відносить [43, с. 14–15]:

- 1) професіоналізм при здійсненні своїх трудових зобов'язань;
- 2) компетентність;
- 3) дисципліна й законність;
- 4) персональна відповідальність за невиконання або неналежне виконання трудових обов'язків;
- 5) розмежування компетенції між працівниками різної кваліфікації;
- 6) оплата праці за трудову діяльність на рівні не нижчому за встановлений рівень мінімальної заробітної плати;
- 7) свобода й добровільність праці;
- 8) договірний характер найманої праці;
- 9) визначеність трудової функції.

Зі свого боку до принципів інформаційного права науковці відносять [44, с. 9–14]:

- 1) свободу одержання та поширення інформації;
- 2) об'єктивність, вірогідність, повноту та точність інформації;
- 3) гармонізацію інтересів особи, суспільства та держави в інформаційній діяльності;
- 4) мінімізацію негативного інформаційного впливу;
- 5) мінімізацію негативних наслідків функціонування інформаційних технологій;
- 6) недопущення несанкціонованого поширення, використання та знищення інформації;
- 7) приналежність інформації до об'єктів цивільних правовідносин, її вільний обіг у визначених законом випадках;
- 8) єдність та різниця інформації та носія інформації;
- 9) об'єктність надання інформації;
- 10) первинність створення інформації;
- 11) обмеження доступу до інформації у визначених випадках;

12) взаємну гармонізацію інформаційного права та всієї системи вітчизняного законодавства.

Таким чином, система принципів трудового та інформаційного права включає загальні принципи, на яких ґрунтується уся галузь права, та спеціальні, на яких засновані окремі інститути та правовідносини, що виникають у межах відповідної галузі.

Деякі з визначених науковцями принципів знайшли своє безпосереднє закріплення в нормативно-правових актах, інші ж слідують зі змісту правових норм. Так, відповідно до Закону України «Про інформацію» основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; вірогідність та повнота інформації; свобода вираження поглядів та переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [45].

Закон України «Про захист персональних даних» [46] не містить окремої статті, яка присвячена принципам правовідносин із захисту персональних даних. Однак, виходячи зі змісту положень норм даного Закону, можна зазначити, що такими принципами є: конфіденційність інформації, що становить персональні дані особи; недопущення збирання, накопичення та використання інформації про особу без її згоди тощо.

Чинний Кодекс законів про працю України (далі – КЗпП України) також не визначає принципи трудових правовідносин. На підставі проведеного вище аналізу, можемо виокремити такі принципи захисту персональних даних працівника:

1. Принцип добровільності надання персональних даних особою під час влаштування на роботу. Зміст даного принципу полягає у тому, що збір інформації про працівника (потенційного працівника) здійснюється роботодавцем або третіми особами виключно на підставі прямої та однозначної згоди особи щодо такого збору. При цьому, згода працівника (потенційного працівника) на збір інформації про нього у разі, якщо він самостійно подає документи, які відповідно до частини 4 статті 6 Закону України «Про захист персональних даних» є первинними джерелами

відомостей про фізичну особу (видані на її ім'я документи, підписані нею документи, відомості, які особа надає про себе), згода такого працівника презюмується лише у відношенні конкретно обраного роботодавця (до якого подаються документи з метою працевлаштування) або для конкретної мети (працевлаштування). У інших випадках обов'язковою є письмова згода суб'єкта персональних даних.

2. Принцип вірогідності та повноти інформації, що складає персональні дані працівника. Даний принцип у науковій літературі визначається не лише, як спеціальний принцип інформаційних правовідносин, а й однією з ключових вимог щодо інформації та захисту інформації взагалі. При цьому вірогідність інформації є досить істотним принципом інформаційних відносин та основоположною вимогою щодо інформації, у зв'язку з чим потребує свого законодавчого визначення у Законі України «Про інформацію», зокрема, у такому формулюванні як відповідність, адекватність та ідентичність отриманих даних фактичним умовам або є властивістю інформації, яка визначає ступінь об'єктивного, точного зображення подій, фактів, що мали місце [47, с. 57].

У контексті обробки персональних даних про працівника дотримання даного принципу обумовлено особливою важливістю мети, з якою здійснюється збір та обробка персональних даних. За загальним правилом відповідальність за вірогідність персональних даних несе особа, яка подає такі дані. Разом із тим обов'язком роботодавця є перевірка вірогідності та повноти поданої інформації, яка складає персональні дані працівника. Крім того, важливо згадати про те, що за вірогідність та повноту тих даних, які формуються роботодавцем у ході виконання працівником трудової функції (відомості про заробітну плату, здійсненні відрахування до фонду загальнообов'язкового державного соціального страхування тощо) відповідальність перед третіми особами (органами державної фіскальної служби, органами Пенсійного фонду тощо) та працівником несе роботодавець.

3. Принцип адекватності, достатності та ненадмірності збору та обробки персональних даних працівника. Даний принцип відповідає принципу Європейського союзу (далі – ЄС) щодо пропорційності захисту публічного та особистого інтересу особи та означає, що будь-які вимоги роботодавця щодо необхідності представлення

працівником (потенційним працівником) інформації про себе мають бути обґрунтованими конкретною необхідністю, яка відповідає меті збору та обробки персональних даних. У якості порушення даного принципу деякі науковці наводять практичну ситуацію – запровадження роботодавцями процедури ідентифікації персоналу з використанням відбитків пальців. Відцифровані відбитки пальців повинні у такому випадку зберігатися в окремому реєстрі володільця. Метою обробки було забезпечення реалізації обов’язків роботодавця, а саме підтримання трудової дисципліни та створення належних умов праці, забезпечення пропускового режиму на підприємстві.

При цьому, як зазначають науковці, на практиці з цього приводу надходить чимала кількість скарг. Зокрема, заявники скаржаться на примусовий характер впровадження таких систем, які супроводжуються погрозами з боку роботодавців звільнити тих працівників, хто не погоджується надати відбитки пальців [48, с. 46]. У цьому зв’язку слід зазначити, що згідно із визначенням терміну «біометричні дані», що міститься в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [49] відцифровані відбитки пальців рук є біометричними даними.

Відтак, достатність та ненадмірність таких заходів значною мірою обумовлена видом діяльності підприємства, установи або організації та визначається з урахуванням співвідношення можливих негативних наслідків для роботодавця, якщо працівник відмовиться від надання таких даних про себе, та для працівника, якщо роботодавець не забезпечить їх належне зберігання та схоронність.

4. Принцип відповідальності роботодавця за стан збереження та забезпечення захисту персональних даних працівника – означає, що за стан збереженості персональних даних працівника, які зібрані та зберігаються у роботодавця або за його замовленням третіми особами, несе відповідальність роботодавець. Так само, останній несе відповідальність за несанкціоноване використання даних працівника, рівень безпеки зберігання даних в інформаційних системах тощо.

О.В. Олійник вказує також на принцип комплексного підходу до організації забезпечення інформаційної безпеки, який передбачає створення органічно

взаємозв'язаної сукупності сил, засобів та спеціальних методів, спрямованих на забезпечення безпеки інформації, що підлягає захисту та сфери її обігу [50, с. 172]. Цей принцип, на нашу думку, є невіддільним елементом принципу відповідальності роботодавця за стан збереження та забезпечення захисту персональних даних працівника.

Для забезпечення схоронності та недопущення несанкціонованого використання персональних даних працівника роботодавець має забезпечити надійність інформаційно-телекомунікаційних систем, у яких зберігаються такі данні, а також недоступність інформації для сторонніх осіб, яка зберігається на паперових носіях чи інших джерелах інформації.

5. Принцип безперервності забезпечення захисту персональних даних працівника. Принцип безперервності забезпечення інформаційної безпеки, на думку М.В. Бем, І.М. Городиського та інших, полягає у повсякденному (безперервному) застосуванні як загальних, так та спеціальних засобів та методів забезпечення інформаційної безпеки на всіх її етапах життєвого циклу [48, с. 173]. У відношенні до захисту персональних даних працівника цей принцип також означає, що роботодавець має визначити відповідальну особу за зберігання персональних даних працівників, встановлення належної системи безпеки тощо.

6. Принцип використання персональних даних працівника роботодавцем виключно з метою забезпечення виконання працівником трудової функції та виконання роботодавцем своїх повноважень. Як вже згадувалось раніше, добровільність збирання та обробки персональних даних працівника, які подані особою самостійно у процесі працевлаштування та сформовані роботодавцем у ході виконання працівником трудової функції, презюмується лише у випадку, якщо відповідне збирання та обробка здійснюються із заздалегідь визначеною метою – забезпечення трудової дисципліни, належного виконання працівником трудової функції та реалізації роботодавцем своїх повноважень у відносинах з державною фіскальною службою, іншими органами. У зв'язку з цим у науковій літературі наголошується, що якщо особа надала згоду на обробку персональних даних, які по своїй суті непотрібні для досягнення поставленої мети обробки, така обробка

розглядатиметься як непропорційна та становитиме порушення законодавства про захист персональних даних [48, с. 46–47].

7. Принцип відкритості та прозорості використання роботодавцем персональних даних працівника. Даний принцип означає, що обробка персональних даних працівника здійснюється відкрито для самого працівника, тобто, працівник має право у будь-який час звернутися до роботодавця для отримання актуальної інформації про себе, яка зберігається у роботодавця. Крім того, працівник має право знати для якої мети обробляються його персональні дані, які треті особи мають до них доступ тощо, для чого роботодавець має повідомляти по це працівника. Суб'єкт даних повинен мати право доступу до персональних даних, які збирають щодо нього, та реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її.

Принцип прозорості вимагає, щоб будь-яка інформація, призначена для громадськості або суб'єкта даних, була стислою та зрозумілою, з використанням чітких та простих формулювань, а також, за необхідності, із застосуванням засобів візуалізації. Таку інформацію можна надавати в електронному форматі, наприклад, через веб-сайт, коли її адресовано громадськості. Це, зокрема, є доцільним у ситуаціях, коли збільшення кількості агентів та технологічна складність практичної діяльності перешкоджають обізнаності та розумінню суб'єкта даних того, чи збирають її або його персональні дані, хто їх збирає та для якої цілі, як, наприклад, у випадку онлайн-реклами [51].

8. Принцип чіткості визначення мети збору та використання персональних даних працівника. За загальним правилом збір та обробка персональних даних працівника здійснюється з метою забезпечення виконання працівником його трудової функції належним чином, а також реалізації роботодавцем своїх повноважень. Разом з тим, у випадку, якщо обробка персональних даних здійснюється також із іншою метою, остання має бути чітко сформульована для того, щоб згода на таку обробку була надана працівником в однозначній формі.

9. Принцип виключності випадків обмеження прав працівника при обробці його персональних даних. Випадки обмеження прав суб'єкта персональних даних,

зокрема, надання персональних даних працівника на запит третіх осіб, обробка персональних даних для інших цілей без згоди працівника, визначені у ст. 25 Закону України «Про захист персональних даних». У цій статті зазначається, що обмеження дії ст. 6–8 цього Закону може здійснюватися у випадках, які передбачені законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав та свобод суб'єктів персональних даних чи інших осіб [46].

Узагальнюючи випадки обмеження прав суб'єкта персональних даних, М.В. Бем, І.М. Городиський та інші виокремлюють такі умови відповідних обмежень [48, с. 99]:

- 1) передбачене законом;
- 2) необхідне/пропорційне;

3) переслідує одну з легітимних цілей – національної безпеки, економічного добробуту або захисту прав та свобод суб'єктів персональних даних чи інших осіб.

Крім того, дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється:

- 1) фізичною особою виключно для особистих чи побутових потреб;

2) виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів [46].

Така обробка може здійснюватися виключно за умови знеособлення персональних даних. Використання персональних даних працівниками суб'єктів відносин, пов'язаних із персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків, що виключає розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків [52, с. 100].

Отже, припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав та свобод, встановлених нормативно-правовим актом чи договором спираються на комплекс основоположних ідей та засад, які в правовій науці називаються принципами. Розглянуті принципи захисту персональних даних

працівника складають фундаментальні засади, на яких функціонує механізм захисту персональних даних.

1.3. Сучасні основи захисту персональних даних в європейських правових актах

Враховуючи активність у використанні технологій та мереж і, одночасно, загрози несанкціонованої автоматизованої обробки персональних даних, європейські країни з кінця 1970 років почали приймати спеціалізовані закони та приєднуватися до Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.81 р. [12; 13, с. 66–72]. Головною передумовою цього була зростаюча активність поширення автоматизованих баз даних, розвиток телекомунікацій та потреба у забезпеченні приватного життя людини згідно принципів Європейської Конвенції «Про захист прав людини та основоположних свобод» (Рим, 04.XI.1950 р.) [13, с. 35–45].

Через декілька років принципи Конвенції Ради Європи № 108, з точки зору економічних інтересів, були деталізовані у Директиві 95/46/ЄС Європейського парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» від 24.10.95 р. [13, с. 273–293], а також у Директиві 97/66/ЄС Європейського парламенту та Ради «Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі» від 15.12.97 р. [13, с. 337–344]. Ці міжнародні акти вважаються першими міжнародно-правовими стандартами, що визначають умови гармонізації національних законодавств у сфері захисту персональних даних як для європейських, так й інших країн світу. Вони сприяли трансформації європейського розуміння поняття «приватасу» («приватність» – право на недоторканість особистого та сімейного життя) у бік застосування заходів захисту права на інформаційний суверенітет особи, зокрема, права людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами.

Сьогодні існує більш ніж 100 міжнародно-правових актів – конвенцій,

протоколів, директив, рекомендацій Ради Європи та Європейського Союзу, які прямо або побічно відносяться до правового регулювання захисту персональних даних. Разом із тим проблема неправомірних і несанкціонованих дій у сфері персональних даних фізичних осіб залишається актуальною і однозначно не вирішеною, як в юридичному, так і практичному сенсі (рис. 1.1):

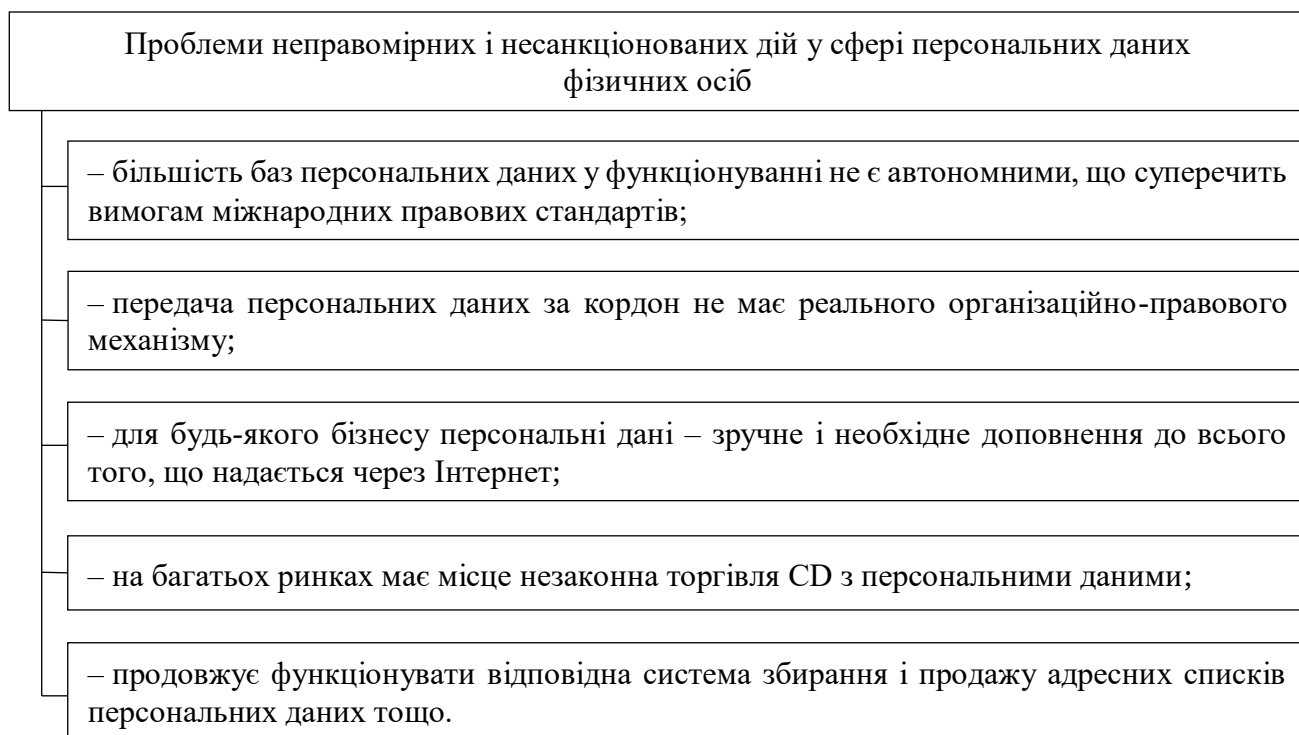


Рис. 1.1. Проблеми неправомірних і несанкціонованих дій у сфері персональних даних фізичних осіб

Загалом, інформацію про особисте чи сімейне життя, зміст розмов, майновий стан, медичні відомості, теле- чи відео- особисте меню, вибір книг, газет чи журналів, зміст файлів на комп'ютерах та на автовідповідачах – все це та багато іншого за бажанням можна поєднати, проаналізувати та інтерпретувати (навіть створити негативний «викривлений портрет» особи) так, що людина, модель її поведінки виглядатиме «прозорою», в усіх своїх якостях та проявах.

У останні роки Європейська Комісія намагається створити та запровадити нову міжнародну систему захисту персональних даних на базі не лише правил про те, як здійснювати діяльність (директив), але й завдяки встановленню правил прямої дії (регламенту), які визначають безпосередній порядок регулювання діяльності. У травні місяці 2016 року Європейський Парламент і Рада затвердили постанову про

нові правила і порядок захисту персональних даних («Пакет захисту даних»), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні, що включає наступні документи:

- Регламент (ЄС) 2016/679 від 27.04.16 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних (Регламент «GDPR»)) [14];

- Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.16 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД» [15];

- Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» [16].

Як вже зазначалося у [8], Європейський Парламент і Рада прийняли рішення про скасування Директиви 95/46/ЄС Європейського Парламенту і Ради від 24.10.95 р. та введення в дію Регламенту (ЄС) 2016/679 від 27.04.16 року. В офіційному прес-релізі ЄС це пояснюється таким чином: «Європейська комісія висунула свою реформу ЄС про захист даних для того, щоб зробити Європу придатною для життя в цифрову епоху. Більше 90 % європейців говорять, що вони хочуть ті ж права захисту даних як в країнах ЄС – і незалежно від того, де обробляються їх дані» [14].

Мета і принципи Регламенту «GDPR» залишаються співзвучними з положеннями Директиви 95/46/ЄС, дія якої передбачена до 2018 р. Разом із тим економічна інтеграція і розвиток ринку ЄС в умовах активного застосування інформаційних технологій призвели до значного збільшення трансграничних потоків персональних даних, зокрема завдяки можливостям Інтернету. Нові технології і глобалізація принесли з собою нові проблеми для захисту персональних даних. Масштаби їх збору і використання значно зросли. Технології змінюють як економіку,

так і соціальне життя. Одночасно, відмінності, що існують в підходах до застосування Директиви 95/46/ЄС до обробки і захисту персональних даних в державах-членах ЄС, перешкоджають вільному переміщенню персональних даних на всій європейській території.

Ефективний захист персональних даних на європейській території вимагає зміцнення і встановлення в деталях прав суб'єктів даних і обов'язків тих, хто обробляє і визначає обробку персональних даних, конкретність повноважень для моніторингу виконання правил із захисту персональних даних, а також еквівалентних санкцій за їх порушення в державах-членах ЄС. Це передбачає необхідність правової визначеності і прозорості для всіх малих і середніх підприємств, точності обов'язків і ефективної співпраці між уповноваженими органами держав-членів ЄС. Для забезпечення захисту фізичних осіб і усунення перешкод на шляху потоків персональних даних в рамках ЄС, національні системи обробки та захисту персональних даних повинні бути еквівалентними у всіх державах-членах ЄС. Тому Європейська Комісія пропонує здійснити реформу системи захисту даних для того, щоб зробити Європу придатною для життя в цифрову епоху.

Основне поняття у сфері захисту персональних даних – це «персональні дані», визначення якого з часом поступово змінювалося. Перше визначення було надано у Конвенції Ради Європи № 108 від 1981 р.: «персональні дані означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (суб'єкт даних)» [12]. У 1995 р. Директивою 95/46/ЄС було надано таке визначення: «персональні дані – це будь-яка інформація про особу – ідентифіковану або таку, що може бути ідентифікована; такою, що може бути ідентифікована, вважається будь-яка особа чия особистість може визначатися прямо чи не прямо, зокрема, через ідентифікаційний номер або один чи декілька специфічних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності» [17].

У 2011 р., згідно прийнятого Європейською Комісією рішення [18], «персональні дані – будь-яка інформація, що відноситься до особистого, професійного або суспільного життя людини – ім'я (особисті реквізити), фотографії, адреси

електронної пошти, банківські реквізити, повідомлення на сайтах соціальних мереж, медична інформація, IP-адреса комп'ютера та інше, що завгодно». За визначенням, яке сформульовано у Регламенті «GDPR» (2016 р.), – «персональні дані означають будь-яку інформацію, що стосується ідентифікованої фізичної особи або фізичної особи, що ідентифікується («суб'єкта даних»); фізична особа, що ідентифікується – це особа, яка може бути ототожнена прямо або опосередковано, зокрема, з ім'ям, ідентифікаційним номером, даними про місцеположення, онлайн-ідентифікатором, з одним чи декількома специфічними чинниками для встановлення фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи» [14].

По відношенню до встановленого в Директиві 95/46/ЄС Європейського Парламенту і Ради від 1995 р. визначенню персональних даних, у Регламенті «GDPR» воно має аналогічний, але не тотожний з нею зміст. У ньому більш конкретизовано поняття персональних даних та розширений обсяг обов'язків і повноважень відповідних суб'єктів. Генетичні відомості визначені як персональні дані, що відносяться до успадкованих або набутих генетичних характеристик фізичної особи, які є результатом аналізу біологічного зразка, зокрема аналізу хромосом, дезоксирибонуклеїнової (ДНК) або рібонуклеїнової (РНК) кислоти. До відомостей, які стосуються минулого, поточного або майбутнього стану фізичного або психічного здоров'я фізичної особи, додано інформацію щодо надання медичних послуг. Запропоновано визначення «біометричні дані», яке означає особисті дані, одержані в результаті конкретної технічної обробки, пов'язаної з фізичними, фізіологічними або поведінковими характеристиками фізичної особи, що дозволяє підтвердити унікальну ідентифікацію цієї фізичної особи, такі як зображення особи або її дактилоскопічні дані.

Як наголошується у Регламенті «GDPR», захист фізичних осіб у зв'язку з обробкою персональних даних є фундаментальним правом. При цьому, це право не є абсолютним. Воно повинне розглядатися у зв'язку з його функцією в суспільстві і бути збалансованим з іншими основними правами, відповідно до принципу пропорційності, який має бути визначений у базовому законі країни.

Основні принципи обробки персональних даних, які означені у документах «Пакета захисту даних», визначають дотримання наступного (рис. 1.2):

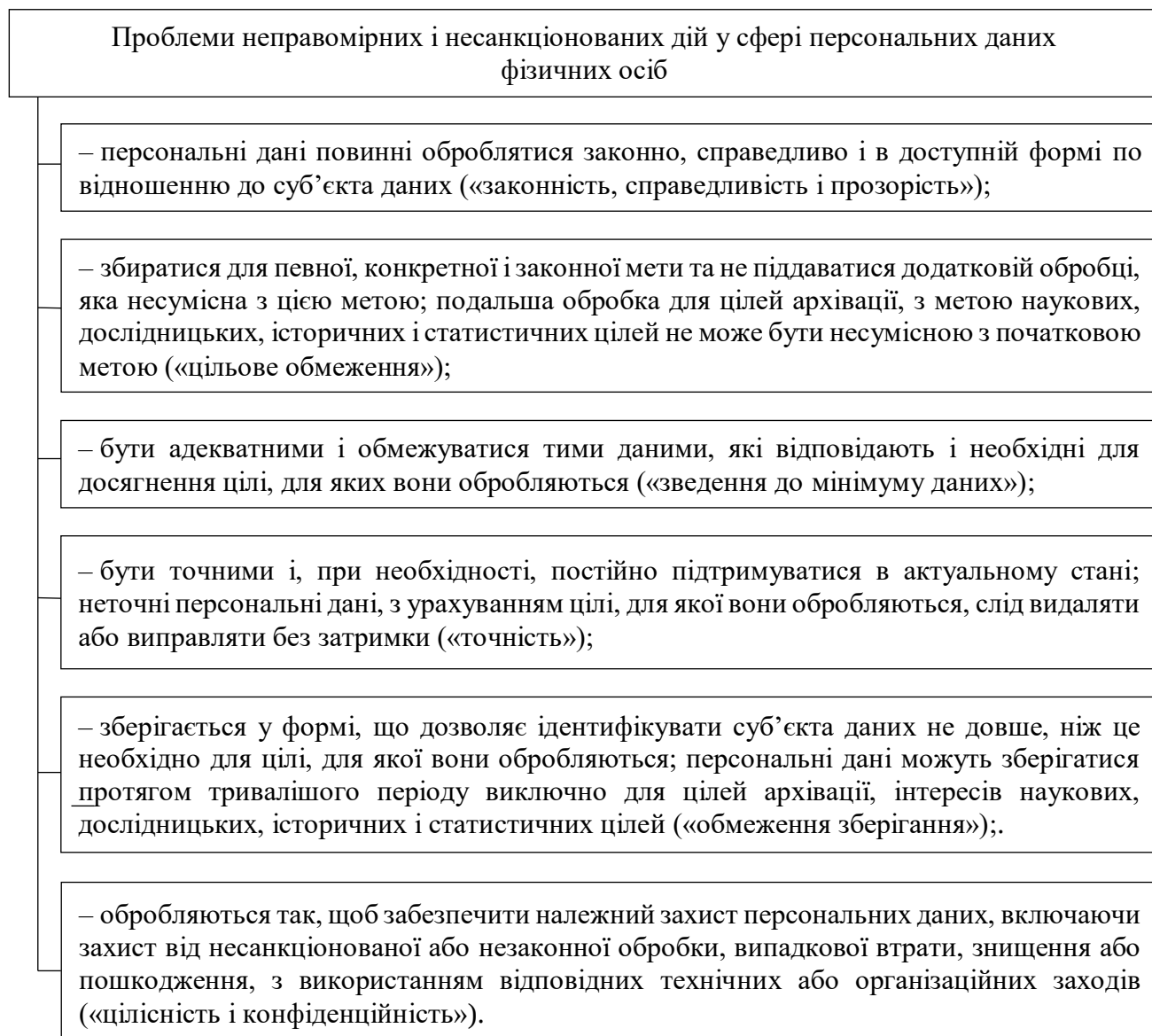


Рис. 1.2. Основні принципи обробки персональних даних

Нові правила застосовуються до обробки даних фізичних осіб у компаніях, підприємствах тощо, які розміщуються не тільки на європейській території, але і здійснюють свою діяльність за межами ЄС і пов'язані з обробкою персональних даних в рамках ЄС. Правила не поширюються на обробку даних про юридичних осіб, а також на дані, які відносяться до анонімної інформації і померлих осіб.

Правила Регламенту «GDPR» не застосовуються до обробки персональних даних фізичною особою в ході чисто особистої або побутової діяльності і, таким чином, без зв'язку з професійною або комерційною діяльністю. Особиста або побутова

діяльність може включати, зокрема, листування, використання особистої адреси (е-пошта), здійснення онлайн-діяльності у мережах та ін., у відзначеному контексті діяльності. Суб'єкт даних повинен мати можливість передавати свої персональні дані з однієї системи електронної обробки в іншу, без втручання інших осіб.

Регулювання згідно положень Регламенту «GDPR» не застосовується до обробки персональних даних для забезпечення національної безпеки і діяльності правоохоронних органів (для цілей попередження, розслідування), а також до обробки персональних даних державами-членами ЄС по відношенню до загальної зовнішньої політики і політики безпеки ЄС.

Персональні дані, які обробляються державними органами в цілях запобігання, розслідування, виявлення або судового переслідування злочинів або виконання покарань, зокрема по запобіганню загрозам суспільної безпеки і вільного переміщення таких даних, регулюються іншим правовим актом ЄС, а саме Директивою (ЄС) 2016/680 Європейського парламенту і Ради (див. далі).

Кожна держава-член ЄС зобов'язана мати незалежний наглядовий орган для розслідування скарг і застосування адміністративних санкцій відносно правопорушень, а також співробітничати з незалежними наглядовими органами інших держав, забезпечуючи взаємну допомогу, організацію сумісних операцій, виявлення і судове переслідування порушень і виконання покарань.

Регламент «GDPR» вводить поняття «контролер» і «процесор», які забезпечують засоби обробки персональних даних. «Контролер» означає фізичну або юридичну особу, державний орган, установу або інший орган, який, поодиночці або спільно з іншими, визначає цілі і засоби обробки персональних даних, згідно законодавства. «Процесор» означає фізичну або юридичну особу, державний орган, установу або інший орган, який обробляє персональні дані за дорученням контролера. Також, в компаніях, підприємствах тощо мають бути призначені спеціалісти по захисту даних.

Регламент «GDPR» передбачає наступні санкції, які можуть бути накладені, зокрема: штраф в розмірі від 10,0 млн євро (або до 2 % від річного обігу за попередній фінансовий рік) до 20,0 млн євро (або до 4 % від річного обігу попереднього фінансового року). Безпосереднє застосування Регламенту «GDPR» передбачено з

25 травня 2018 року для всіх держав-членів ЄС, які до вказаного терміну повинні привести свої національні законодавства в повну відповідність з положеннями нових правил.

Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.16 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД» (Директива «Поліція і органи юстиції») містить 107 пункту преамбули та 64 статті. Метою цієї Директиви є створення сильної, узгодженої і вищого рівня основи для ефективної судової і поліцейської співпраці по кримінальних справах в ЄС по відношенню до процесів обробки і захисту персональних даних компетентними органами і обміну даними між компетентними органами держав-членів для запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів та виконання кримінальних покарань, зокрема запобігання загрозам суспільної безпеки.

Компетентними органами можуть бути не тільки державні органи, такі як судові органи, поліція або інші правоохоронні органи, але і будь-який інший орган або юридична особа, якій державою-членом довірено право здійснювати державну владу і суспільні повноваження для цілей цієї Директиви. Якщо такий орган або організація обробляє персональні дані для цілей, відмінних від цілей цієї Директиви, застосовується Регламент «GDPR». Дозволено надавати персональні дані іншим компетентним органам тільки в конкретних випадках і відповідно до законодавства держави-члена.

Будь-яка обробка персональних даних повинна здійснюватися законно, бути справедливою і прозорою для суб'єктів даних, і виконуватися тільки згідно конкретно встановленої мети. Це саме по собі не перешкоджає правоохоронним органам у проведенні заходів, таких як таємні розслідування або відеоспостереження. Така діяльність може здійснюватися в цілях запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, зокрема по охороні проти і запобігання загрозам суспільної безпеки, тією

мірою, яка встановлена законом і є необхідною, і відповідною мірою в демократичному суспільстві, з урахуванням законних інтересів фізичної особи, зацікавленої.

Захист фізичних осіб застосовується до обробки персональних даних за допомогою автоматизованих засобів, а також для ручної обробки. Файли або набори файлів, а також їх титульні сторінки, які не структуровані відповідно до певних критеріїв, під дію цієї Директиви не підпадають. Директивою визначається, що рівень захисту прав і свобод фізичних осіб відносно обробки персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, зокрема гарантування запобігання загрозам суспільної безпеки, повинен бути еквівалентним у всіх державах-членах.

Сьогодні для вищевказаних цілей застосовується Рамкове рішення Ради ЄС 2008/977/ПВД «Про захист персональних даних у зв'язку з їх обробкою в рамках поліцейської і судової співпраці по кримінальних справах» [19], чинність якої скасовується у 2018 р., згідно з цією Директивою. Закон держави-члена, яка здійснює обробку персональних даних в рамках цієї Директиви, повинен визначати, які особисті дані підлягають обробці, мету обробки і процедури для збереження цілісності і конфіденційності персональних даних, а також процедури їх знищення, забезпечуючи тим самим достатні гарантії проти ризику зловживань і свавілля. При реалізації Директиви в національному законодавстві, держави-члени повинні вказати, які правила, що викладені в Регламенті «GDPR», застосовуються.

Державам-членам, відносно обробки персональних даних, надана можливість забезпечити вищий рівень гарантій захисту, ніж той, який встановлений Директивою «Поліція і органи юстиції». Можна звернути увагу на те, що ще у 1981 р. у ст. 11 Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» було визначено: «Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб'єктам даних більший ступінь захисту, ніж передбачено цією Конвенцією» [12].

Директива «Поліція і органи юстиції» не застосовується до обробки персональних даних в ході діяльності установ або підрозділів, що займаються питаннями національної безпеки, яка підпадають під дію розділу V Договору про Європейський Союз. Обробка персональних даних повинна бути спрямована на зміцнення співпраці держав-членів в боротьбі з тероризмом та іншими серйозними злочинами у всіх країнах ЄС.

Директива не перешкоджає дотриманню принципу доступу до офіційних документів. Відповідно до Регламенту «GDPR» персональні дані, які зазначені у офіційних документах державних або приватних органів для виконання задач, що проводиться на користь суспільства, можуть бути розкриті відповідно до законодавства ЄС або національного законодавства. Директива для органів поліції і юстиції спрямована на гармонізацію законів в державах-членах відносно обробки і обміну персональних даних між поліцією і судовими органами. З метою врахування різних правових традицій держав-членів, вона надає свободу дій в певних областях, зокрема, вказівки державам-членам на обов'язковість виконання конкретних операцій і процедур в національних правилах по кримінальних справах відносно обробки персональних даних судовими органами не передбачено.

Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» (Директива PNR) містить 39 пунктів преамбули та 99 статей. Метою Директиви PNR є забезпечення безпеки і захисту життя людей, а також створення правової основи для захисту персональних даних авіапасажирів міжнародних рейсів. Її положення спрямовані на запобігання, виявлення, розслідування і судове переслідування терористичних злочинів та серйозних злочинів шляхом регулювання передачі даних PNR від авіакомпаній державам-членам ЄС, а також обробку даних PNR компетентними органами в державах-членах ЄС.

Зібрані дані PNR можуть бути оброблені тільки для профілактики, виявлення, розслідування і судового переслідування терористичних і серйозних злочинів. Вони включають: ім'я пасажирів, дату поїздки, маршрут проходження, відомості про

квитки, контактні дані з турагентом, через якого політ був замовлений, використовувані засоби платежу, номер місця, відомості про багаж. Директива PNR передбачає необхідність створення і застосування критеріїв оцінки терористичних і серйозних злочинів, які повинні зводити до мінімуму помилковість ідентифікаційних систем. Авіаперевізники вже давно збирають і обробляють дані PNR в комерційних цілях.

Директива PNR не накладає на них зобов'язань збору і збереження додаткових даних. Нові правила визначають стандарт ЄС для обробки і використання даних PNR та включають положення, що відносяться до:

- мети, з якою дані PNR будуть оброблені в контексті правоохоронної діяльності (використання в розслідуваннях і судових переслідуваннях конкретних осіб);

- зберігання даних PNR (протягом 4,5 років), із суворою процедурою доступу до повної інформації (перелік даних, які збираються авіаперевізниками, представлений в Додатку 1 до Директиви PNR);

- обміну даними PNR між державами-членами ЄС та між державами-членами ЄС і третіми країнами. Обмін даними здійснюється за допомогою мереж обміну (електронних засобів), за умов забезпечення їх сумісності для форматів даних PNR і відповідних протоколів. Забезпечення створення однакових умов сумісності, застосовних до передачі (електронної передачі) даних від авіаперевізників, покладено на Комісію ЄС. Ці повноваження мають здійснюватися відповідно до Регламенту (ЄС) № 182/2011 Європейського парламенту і Ради «Про правила і загальні принципи механізму контролю державами-членами ЄС та здійснення Комісією ЄС виконавчих повноважень» [20];

- посилення гарантій захисту приватного життя та персональних даних працівників, зокрема шляхом підвищення ролі національних наглядових органів і обов'язкового призначення співробітника по захисту даних PNR у відповідних організаціях;

- визначення в кожній державі-члені ЄС компетентного органу для профілактики, виявлення, розслідування або судового переслідування терористичних і серйозних злочинів для забезпечення виконання положень Директиви PNR.

Національний контролюючий орган (Національний орган нагляду) кожної держави-члена відповідає за консультування і моніторинг застосування на своїй території прийнятих національних нормативних положень, згідно Директиви PNR;

– призначення в кожному органі реєстрації авіапасажирів (ОРА) співробітника по захисту даних, відповідального за контроль обробки даних PNR і реалізацію правових гарантій. ОРА зобов'язаний вести облік наступних операцій обробки: збір, консультації, розкриття інформації та її стирання. Протоколи консультацій і розкриття інформації повинні містити, зокрема, мету, дату і час проведення таких операцій і вказувати, наскільки це можливо, відомості про особу людини, яка консультувалася.

Записи мають бути використані виключно для цілей перевірки, самоконтролю, забезпечення цілісності і безпеки даних або аудиту. ОРА повинен надавати записи по запиту Національного наглядового органу;

– встановлення правил відносно санкцій, зокрема фінансових, до авіаперевізників, які не передають дані.

Пропозиції Європейської Комісії про нові правила і порядок захисту персональних даних в контексті «Пакету захисту даних» викликали багато дискусій, суперечок і внесення значної кількості поправок. Ось деякі з них:

– вимоги мати в кожній компанії, підприємстві тощо штатного співробітника по захисту даних є новим для багатьох країн ЄС і піддається критиці у зв'язку з потребами додаткових фінансових витрат;

– реалізація нових правил ЄС по обробці і захисту персональних даних потребує всеосяжних змін ділової практики для всіх компаній (особливо неєвропейських) і додаткових адміністративними витрат;

– регламент розроблений з акцентом на соціальні мережі і провайдерів, але не достатньою мірою визначає вимоги до обробки даних співробітниками по захисту даних в компаніях (організаціях);

– передача даних не розглядається як один з ключових аспектів для захисту даних в контексті важливості і необхідності визначення вимог для функціонування соціальних мереж і провайдерів;

– слід чекати конфліктів в тлумаченні положень Регламенту ЄС 2016/679 і практики регулювання відносин з іншими неєвропейськими державами, що мають свої закони, правила і практику.

Отже, персональні дані посідають особливе місце в інформаційних відносинах. Проблема їх захисту та поширення все життя супроводжує людину та пронизує будь-які сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і держави.

Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях всіх міжнародних стандартів, передбачає обов'язкове дотримання конкретних умов застосування персональних даних для будь-яких суб'єктів інформаційних відносин, при яких персональні дані повинні бути доступними для суб'єкта даних, точними і оновлюватися, отримані законним способом, оброблятися з конкретною метою та за згодою на це суб'єкта даних і в кількості мінімально необхідній для визначеної мети, використовуватися тільки згідно визначеної мети, захищеними від несанкціонованого доступу та незаконної обробки.

Суб'єкт персональних даних має право на те, щоб не приймалося рішення, яке ґрунтується виключно на автоматизованій обробці його даних. Таким чином, будь-яка обробка персональних даних повинна здійснюватися законно, бути справедливою і прозорою для суб'єктів даних, та виконуватися тільки згідно конкретно визначеної мети.

Законодавство про захист персональних даних має значний масив багатогранних та різнопланових документів, освоїти який не просто. На сьогоднішній день у цій області населення має слабе уявлення про свої права і їх застосуванні на практиці, фахівців дуже мало і нові вимоги можуть погіршити ситуацію. Тому є необхідність у введенні в систему освіти за напрямом «інформаційне право» окремої спеціалізації по юридичним та техніко-технологічним аспектам захисту персональних даних в цифрову епоху.

Висновки до розділу 1

Під персональними даними працівника варто розуміти будь-яку інформацію, що стосується конкретної фізичної особи, яка працює на підставі трудового договору, і надана особисто такою особою роботодавцеві або зібрана останнім відповідно до законодавства. До персональних даних працівника відносять інформацію про вік, дату і місце народження, громадянство, реєстраційний номер облікової картки платника податків, трудову діяльність, стан здоров'я, рівень освіти, володіння українською та іноземними мовами, сімейний стан. І цей перелік не є вичерпний. Це пов'язано з тим, що необхідний перелік персональних даних працівників може відрізнятися за своїм змістом, виходячи з того, яку вони будуть займати посаду та виконувати трудову функцію.

Наголошено, що, з огляду вирішення проблеми захисту персональних даних працівника в умовах цифровізації, нагально необхідно здійснити систематизацію та кодифікацію національного законодавства у сфері персональних даних відповідно до норм європейського законодавства; розробити єдиний нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, захист персональних даних працівника. Цілком поділяємо думку О. Рим, що наблизитись до забезпечення балансу інтересів роботодавців і працівників під час обробки персональних даних останніх можна, якщо ця обробка відповідатиме таким вимогам: буде адекватною, доречною та обмежуватиметься досягненням необхідної мети; використання, мета та спосіб обробки повинні бути зрозумілі для працівників; працівники повинні мати можливість реалізувати свої права перевіряти, виправляти, припиняти та обмежувати обробку; персональні дані повинні зберігатись не більше, ніж потрібно; персональні дані повинні бути захищені відповідними технічними та організаційними заходами безпеки.

Припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав та свобод, встановлених нормативно-правовим актом чи договором спираються на комплекс основоположних ідей та засад, які в правовій науці називаються принципами. Розглянуті принципи захисту персональних даних

працівника складають фундаментальні засади, на яких функціонує механізм захисту персональних даних.

Персональні дані посідають особливе місце в інформаційних відносинах. Проблема їх захисту та поширення все життя супроводжує людину та пронизує будь-які сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і держави.

Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях всіх міжнародних стандартів, передбачає обов'язкове дотримання конкретних умов застосування персональних даних для будь-яких суб'єктів інформаційних відносин, при яких персональні дані повинні бути доступними для суб'єкта даних, точними і оновлюватися, отримані законним способом, оброблятися з конкретною метою та за згодою на це суб'єкта даних і в кількості мінімально необхідній для визначеної мети, використовуватися тільки згідно визначеної мети, захищеними від несанкціонованого доступу та незаконної обробки.

РОЗДІЛ 2

ОСНОВИ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ КОМУНАЛЬНОГО ПІДПРИЄМСТВА «ЖИТОМИРСЬКЕ ТРАМВАЙНО- ТРОЛЕЙБУСНЕ УПРАВЛІННЯ» ЖИТОМИРСЬКОЇ МІСЬКОЇ РАДИ

2.1. Організаційно-економічна характеристика Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради

Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради засноване на власності територіальної громади м. Житомир. Засновником підприємства є територіальна громада м. Житомир в особі Житомирської міської ради. Загальні відомості про досліджуване підприємство наведено в табл. 2.1:

Таблиця 2.1

Загальна інформація про підприємство

Ознака		Інформація про об'єкт	
Найменування (повне, скорочене)		Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради	
		КП «ЖТТУ» ЖМР	
Код за ЄДРПОУ		03328310	
Дата видачі свідоцтва про державну реєстрацію		23.01.1992 р.	
Код території за КОАТУУ		1810100000	
Територія (область)		Житомирська	
Місцезнаходження (поштова адреса)		Вул. Вітрука, 11, м. Житомир, Житомирська обл., Україна, 10025	
Міжміський код	0412	Телефон	(0412) 33-30-20; 068-843-17-58
E-mail	tty_nvc@ukr.net	Факс	(0412) 33-30-20
Основні види діяльності:	Код за КВЕД	Найменування виду діяльності	
1	49.31	Пасажирський наземний транспорт міського та приміського сполучення	
2	43.99	Інші спеціалізовані будівельні роботи, н.в.і.у.	
3	85.32	Професійно-технічна освіта	
4	49.39	Інший пасажирський наземний транспорт, н.в.і.у.	
5.	52.29	Інша допоміжна діяльність у сфері транспорту	

У своїй діяльності підприємство керується Конституцією України, законами України, іншими нормативно-правовими актами, рішеннями Житомирської міської

ради, розпорядженнями міського голови, рішеннями виконавчого комітету Житомирської міської ради та Статутом підприємства.

У відповідності до основної діяльності, Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради здійснює міські перевезення тролейбусами, трамваями та автобусами із застосуванням автоматизованої системи оплати проїзду [63]. Підприємство має дозвіл на перевезення пасажирів і небезпечних вантажів автомобільним транспортом № 062326 від 13.06.2012 р.

Підприємство також надає юридичним і фізичним особам якісні послуги на договірній основі, зокрема [64]:

- 1) виготовлення, ремонт та реставрування деталей, вузлів, агрегатів;
- 2) ремонт електродвигунів постійного та змінного струму;
- 3) надання автопослуг самоскидом, автокраном, автовишкою, трактором, евакуатором;
- 4) проведення ремонту, технічного обслуговування та випуску автотранспортних засобів;
- 5) паркування транспортних засобів;
- 6) мийка великогабаритних транспортних засобів;
- 7) розміщення реклами;
- 8) надання комерційних послуг з перевезення окремих груп пасажирів трамваями та тролейбусами для проведення святкових заходів та екскурсій;
- 9) послуги високовольтної електротехнічної лабораторії з проведенням вимірювань, випробовувань в електроустановках, відшуку місць пошкодження силових кабелів, випробовування електрозахисних засобів;
- 10) монтажні та ремонтні роботи в електроустановках;
- 11) послуги громадського харчування;
- 12) супровід негабаритних вантажів по місту.

Цікаво, що серед основних факторів ризику діяльності на самому підприємстві виокремлюють:

- відключення електроенергії;

- різку зміну цін на електроносії;
- різку зміну погодних умов.

Організаційна структура підприємства є лінійно-функціональною. Вона представлена в Додатку А.

Маємо відзначити, що у звітному році підприємство було збитковим, про що свідчить формування чистого збитку у розмірі 94829 тис. грн. При чому за цим показником спостерігається тенденція до погіршення фінансово-економічного стану підприємства (табл. 2.2).

Таблиця 2.2

Основні фінансово-економічні показники діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради за період 2020–2022 роки, тис. грн

Показники	Роки			Відхилення 2022 р. до 2020 р.	
	2020	2021	2022	+/-	%
1. Чистий дохід (виручка), тис. грн	58534	81256	88627	30093	51,41
2. Валовий:					
– прибуток, тис. грн;	0	0	0	0	х
– збиток, тис. грн	150967	176549	154071	3104	2,06
3. Чистий:					
– прибуток, тис. грн;	0	0	0	0	х
– збиток, тис. грн	38970	26095	94829	55859	у 2,43 р.б.
4. Середньооблікова чисельність штатних працівників, чол.	863	871	725	-138	-15,99
5. Середньорічна вартість активів, тис. грн, у т. ч.:					
– необоротних;	211856	342545	354466	142610	67,31
– оборотних	20910	25215	31379	10469	50,07
6. Середньорічна вартість основних засобів, тис. грн	175889	300075	333711	157822	89,73
7. Фондовіддача, грн / грн	0,33	0,27	0,27	-0,06	-18,18
8. Коефіцієнт оборотності оборотних активів, об. в рік	2,80	3,22	2,82	0,02	х
9. Продуктивність праці, тис. грн / чол.	67,83	93,29	122,24	54,41	80,22
10. Рентабельність господарської діяльності, %	0,00	0,00	0,00	0,00	х

За даними табл. 2.2 можемо відзначити, що чистий дохід Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради збільшився з 58534 тис. грн у 2020 р. до 88627 тис. грн у 2022 р., тобто зріс на 51,41 %. Разом із тим на підприємстві не вдалося сформувати чистий

прибуток. Так, у 2022 р. було отримано збиток у розмірі 94829 тис. грн, що на 55859 тис. грн, або у 2,43 рази більше ніж у базовому році.

Середньорічна вартість необоротних активів підприємства за період 2020–2022 роки зросла на 67,31 % і у звітному році склала 354466 тис. грн. За цей же проміжок часу середньорічна вартість оборотних активів збільшилася на 10469 тис. грн, або на 50,07 %.

Коефіцієнт фондівіддачі у 2022 р. склав 0,27, що свідчить про те, що на 1 грн основних виробничих фондів виробляється 0,25 грн готової продукції. За період 2020–2022 роки цей коефіцієнт зменшився на 0,06 одиниць.

Зважаючи на збитковий характер діяльності підприємства, його діяльність є нерентабельною.

Сукупні витрати підприємства за період 2020–2022 роки збільшилися в 1,4 рази. Загалом для відстеження динаміки фінансових показників діяльності підприємства можна скористатися даними табл. 2.3.

Таблиця 2.3

**Динаміка фінансових результатів діяльності Комунального підприємства
«Житомирське трамвайно-тролейбусне управління» Житомирської міської
ради за період 2020–2022 роки, тис. грн**

Показники	Роки			Відхилення 2022 р. до 2020 р.	
	2020	2021	2022	+/-	%
1	2	3	4	5	6
Сукупний дохід (витрати)	(38970)	(26095)	(94829)	-55859	у 1,4 р.б.
Чистий дохід	58534	81256	88627	30093	51,41
Собівартість реалізованої продукції (товарів, робіт, послуг)	209501	257805	242698	33197	15,85
Валовий:					
– прибуток;	0	0	0	0	х
– збиток	150967	176549	154071	3104	2,06
Інші операційні доходи	158851	189468	175823	16972	10,68
Адміністративні витрати	6805	6825	6974	169	2,48
Витрати на збут	0	0	0	0	х
Інші операційні витрати	33783	18099	97642	63859	189,03
Фінансовий результат від операційної діяльності:					
– прибуток;	0	0	0	0	х
– збиток	32704	12005	82864	50160	153,38
Доход від участі в капіталі	0	0	0	0	х

Продовження табл. 2.3

1	2	3	4	5	6
Інші фінансові доходи	109	94	522	413	378,90
Інші доходи	2039	2466	1409	-630	-30,90
Інші фінансові доходи	109	94	522	413	378,90
Витрати від участі в капіталі	0	0	0	0	х
Інші витрати	1410	1962	191	-1219	-86,45
Прибуток (збиток) від впливу інфляції на монетарні статті	0	0	0	0	х
Фінансовий результат до оподаткування:					
– прибуток;	0	0	0	0	х
– збиток	38970	26095	94829	55859	143,34
Витрати (дохід) з податку на прибуток	0	0	0	0	х
Прибуток (збиток) від припиненої діяльності після оподаткування	0	0	0	0	х
Чистий:					
– прибуток;	0	0	0	0	х
– збиток	38970	26095	94829	55859	у 2,43 р.б.

За даними табл. 2.3 можемо відзначити суттєве збільшення собівартості реалізованої продукції (товарів, робіт, послуг). Так, у 2022 р. собівартість реалізованої продукції склала 242698 тис. грн., що на 33197 тис. грн, або на 15,85 %, більше ніж у 2020 р. Також варто відзначити суттєве збільшення інших операційних доходів Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради з 158851 тис. грн у 2020 р. до 175823 тис. грн у 2022 р., тобто на 16972 тис. грн, або на 10,68 %.

В загальному ефективність діяльності підприємства характеризують показники чистого прибутку та рентабельності, що представлено в табл. 2.4.

Таблиця 2.4

Оцінка рентабельності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради за період 2020–2022 роки

Показники	Роки			Відхилення 2022 р. до 2020 р.	
	2020	2021	2022	+/-	%
Чистий прибуток (збиток), тис. грн	(38970)	(26095)	(94829)	55859	у 2,43 р.б.
Власний капітал, тис. грн	72500	61762	307156	234656	у 4,24 р.б.
Рентабельність продукції, %	27,94	31,52	36,52	8,58	х
Рентабельність операційної діяльності, %	-55,87	-14,77	-93,50	-37,63	х
Рентабельність сукупного капіталу, %	-53,75	-42,25	-30,87	22,88	х
Рентабельність власного капіталу, %	-53,75	-42,25	-30,87	22,88	х
Період окупності власного капіталу	-4,40	-2,37	-3,24	1,16	х

За даними табл. 2.4 відзначимо, що у зв'язку із загальною збитковістю підприємства у період 2020–2022 роки більшість ключових коефіцієнтів рентабельності підприємства хоч і мали позитивну динаміку, однак все ж таки мали від'ємне значення. А показник рентабельність операційної діяльності підприємства взагалі погіршився на 37,63 %.

Витрати є грошовими активами, які підприємство витрачає на свою діяльність. Вони можуть бути класифіковані за різними ознаками, такими як: призначення, строк використання, вид економічної діяльності тощо. Найбільш поширені класифікації витрат – за призначенням, які включають: витрати на зарплату; закупівлю сировини та матеріалів; витрати на рекламу та маркетинг; адміністративні витрати тощо.

При класифікації витрат і доходів підприємства важливо враховувати вимоги законодавства, а також особливості конкретного виду економічної діяльності підприємства. Це дозволяє бути більш точним та об'єктивним у фінансовому обліку та забезпечити ефективне управління діяльністю підприємства.

Витрати підприємства представляють собою грошові потоки, пов'язані з наданням послуг, в тому числі з оплатою праці, витратами на закупівлю сировини та матеріалів, витратами на енергетику, транспорт та інфраструктуру, оплатою податків і зборів, іншими витратами підприємства.

Аналіз структури операційних витрат підприємства демонструє переважання у їх складі саме витрат на оплату праці (табл. 2.5):

Таблиця 2.5

**Аналіз структури операційних витрат Комунального підприємства
«Житомирське трамвайно-тролейбусне управління»
Житомирської міської ради у 2020–2022 роках**

Показники	Роки						Відхилення 2022 р. до 2020 р.		
	2020		2021		2022		+/-	%	п.с.
	Тис. грн	%	Тис. грн	%	Тис. грн	%			
1	2	3	4	5	6	7	8	9	10
Матеріальні затрати	56891	22,75	64512	22,82	71160	20,49	14269	25,08	-2,26
Витрати на оплату праці	113331	45,32	131154	46,39	114499	32,97	1168	1,03	-12,35

Продовження табл. 2.5

1	2	3	4	5	6	7	8	9	10
Відрахування на соціальні заходи	28031	11,21	32060	11,34	28195	8,12	164	0,59	-3,09
Амортизація	19598	7,84	38691	13,68	40695	11,72	21097	107,65	3,88
Інші операційні витрати	32238	12,89	16312	5,77	92765	26,71	60527	у 1,87 р.б.	13,82
Разом	250089	100,00	282729	100,00	347314	100,00	97225	38,88	0,00

За даними табл. 2.5 відзначимо, що за період 2020–2022 роки загальний розмір операційних витрат Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради збільшився на 97225 тис. грн, або на 38,88 %. Цікаво, що у їх складі найбільшу питому вагу в звітному році займали витрати на оплату праці (32,97 %), а найменшу – відрахування на соціальні заходи (8,12 %). Зокрема, витрати на оплату праці збільшилися на 1168 тис. грн, або на 1,03 %, тоді як відрахування на соціальні заходи – на 164 тис. грн, або на 0,59 %. Разом із тим варто наголосити, що найбільше зростання відбулося за статтею інших операційних витрат (на 13,82 пунктів), а найбільше скорочення – за статтею витрат на оплату праці (на 12,35 пунктів).

Витрати від звичайної діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради характеризуються суттєвим збільшенням собівартості реалізованої продукції (табл. 2.6).

Таблиця 2.6

Аналіз структури і динаміки витрат від звичайної діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради у 2020–2022 роках

Показники	Роки						Відхилення 2022 р. до 2020 р.		
	2020		2021		2022		+/-	%	п.с.
	Тис. грн	%	Тис. грн	%	Тис. грн	%			
1	2	3	4	5	6	7	8	9	10
Собівартість реалізованої продукції	209501	81,04	257805	86,11	242698	67,19	33197	15,85	-13,85
Адміністративні витрати	6805	2,63	6825	2,28	6974	1,93	169	2,48	-0,70
Інші операційні витрати	33783	13,07	18099	6,05	97642	27,03	63859	у 1,89 р.б.	13,96
Фінансові витрати	7004	2,71	14688	4,91	13705	3,79	6701	95,67	1,08

Продовження табл. 2.6

1	2	3	4	5	6	7	8	9	10
Втрати від участі в капіталі	0	0,00	0	0,00	0	0,00	0	x	0,00
Інші витрати	1410	0,55	1962	0,66	191	0,05	-1219	-86,45	-0,49
Разом витрат від звичайної діяльності	258503	100,00	299379	100,00	361210	100,00	102707	39,73	0,00

За даними табл. 2.6 варто відзначити, що сумарні витрати від звичайної діяльності підприємства за період 2020–2022 роки збільшилися на 102707 тис. грн, або на 39,73 %. В структурі цих витрат найбільшу питому вагу займала собівартість реалізованої продукції, частка якої скоротилася з 81,04 % у 2020 р. до 67,19 % у 2022 р., тобто на 13,85 пункти. По суті, це було найбільш відчутне зменшення серед усіх елементів витрат від звичайної діяльності. В той же час найбільше зростання відбулося за елементом інших операційних витрат. Можемо також відзначити відсутність серед елементів сумарних витрат від звичайної діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради втрати від участі в капіталі.

Для оцінювання ефективності управління витратами та дієвого їх контролю пропонується система показників, яку наведено у табл. 2.7. На їх основі було відзначено збільшився вартості загальних операційних витрат на 1 грн операційних доходів, що є негативним сигналом для підприємства.

Таблиця 2.7

Оцінювання ефективності витрат Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради у 2020–2022 роках

Показники	Роки			Відхилення 2022 р. до 2020 р.	
	2020	2021	2022	+/-	%
1	2	3	4	5	6
1. Загальні операційні витрати на 1 грн операційних доходів	1,15	1,04	1,31	0,16	13,91
1.1. Коефіцієнт питомої собівартості реалізованої продукції	0,96	0,95	0,92	-0,04	x
1.2. Коефіцієнт питомих адміністративних витрат	0,03	0,03	0,03	0,00	x

Продовження табл. 2.7

1	2	3	4	5	6
1.3. Коефіцієнт питомих інших операційних витрат	0,16	0,08	0,45	0,29	x
2. Витрати на 1 грн. доходів від іншої звичайної діяльності	0,69	0,80	0,14	-0,55	-79,71
3. Собівартість реалізованої продукції на 1 грн. чистого доходу	3,58	3,17	2,74	-0,84	-23,46

За даними табл. 2.7 маємо відзначити, що у звітному періоді на 1 грн операційних доходів, яку отримало підприємство, припало 1,31 грн. операційних витрат. За аналізований період цей показник збільшився на 0,16 пунктів, що є негативним сигналом для підприємства. Коефіцієнт питомої собівартості реалізованої продукції Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради в період 2020–2022 роки зменшився на 0,04 пункти, що свідчить про незначне зменшення питомої ваги собівартості реалізованої продукції в складі загальних операційних витрат. Тут також спостерігається стабільно низька частка адміністративних витрат і суттєве збільшення (на 0,29 пункти) частки інших операційних витрат. Окремо хотілося б відзначити, що у 2022 У складі операційних витрат Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради найбільшу питому вагу в звітному році займали витрати на оплату праці, а найменшу – відрахування на соціальні заходи

Фінансовий стан є однією з найважливіших характеристик діяльності підприємства, що характеризується забезпеченістю його відповідним обсягом фінансових ресурсів, необхідних для здійснення ефективної господарської діяльності та своєчасних грошових розрахунків за своїми зобов'язаннями. Фінансова діяльність має бути направлена на забезпечення систематичного надходження та ефективного використання фінансових ресурсів, дотримання розрахункової та кредитної дисципліни, досягнення раціонального співвідношення власних та залучених коштів, фінансової стійкості з метою ефективного функціонування підприємства, що забезпечує перевезення пасажирів.

Фінансовий стан Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради визначається сукупністю показників, серед яких доцільно звернути увагу на показники фінансової стійкості та

показники ліквідності та платоспроможності. Зокрема, оцінювання стану фінансової стійкості підприємства проведемо за даними табл. 2.8.

Таблиця 2.8

**Оцінка фінансової стійкості Комунального підприємства «Житомирське
трамвайно-тролейбусне управління» Житомирської міської ради
за період 2020–2023 роки**

Показники	Нормативне значення	Роки			Відхилення 2022 р. до 2020 р.	
		2020	2021	2022	+/-	%
1. Коефіцієнт фінансової залежності	1,67–2,5	4,71	6,38	1,23	–3,48	x
2. Коефіцієнт маневреності власного капіталу	>0,1	–0,52	–0,54	0,05	0,57	x
3. Коефіцієнт співвідношення залученого і власного капіталу	<1	3,71	5,38	0,23	–3,48	x
4. Коефіцієнт фінансової стійкості	>0,75	0,82	0,85	0,94	0,12	x
5. Коефіцієнт фінансової стабільності	1	0,27	0,19	4,36	4,09	x

За даними табл. 2.8 варто відзначити, що у 2022 р. коефіцієнт фінансової залежності склав 1,23, що дещо менше за нормативне значення. Занадто низька залежність може говорити про неповне використання можливостей підприємством. Для підвищення значення необхідно, як очевидно, залучати додаткові позикові кошти кредитних організацій, банків, інших підприємств і т.д. Це дозволить активізувати виробничу і збутову діяльність, що призведе до збільшення фінансового результату роботи підприємства або дозволить досягти інших цілей. За період 2020–2022 роки цей показник зменшився на 3,48 пункти.

Коефіцієнт маневреності робочого капіталу у звітному році склав 0,05 і був нижче за нормативне значення, що свідчить про недостатність власних фінансових ресурсів підприємства для фінансування необоротних активів і частини оборотних. Коефіцієнт співвідношення залученого і власного капіталу має від’ємну динаміку, що свідчить про послаблення залежності підприємства від зовнішніх інвесторів і кредиторів, тобто про певне зростання фінансової стійкості.

Коефіцієнт фінансової стійкості у звітному році становив 0,94, що вище мінімального значення нормативу і говорить про достатньо стійке фінансове

положення підприємства. Крім того, за період 2020–2022 роки воно навіть покращилося. Коефіцієнт фінансової стабільності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради за період 2020–2022 роки збільшився на 4,09 пункти і склав у звітному році 4,09, що майже в 4 рази перевищує нормативне значення. Таке суттєве збільшення показника можна пояснити пропорційним зростанням суми власного капіталу підприємства.

Таким чином, варто відзначити, що Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради не в повній мірі використовує власні можливості. При цьому у останні роки підприємство послабило залежність від зовнішніх інвесторів і кредиторів, тобто є достатньо фінансово стійким. Також з позитивного можна відзначити 4-хкратне перевищення власного капіталу над позиковими коштами.

Отже, підприємство здійснює міські перевезення тролейбусами, трамваями та автобусами із застосуванням автоматизованої системи оплати проїзду. В останні роки підприємство було збитковим, про що свідчить формування чистого збитку у кожному з періодів досліджуваного діапазону. При чому за цим показником спостерігається тенденція до погіршення фінансово-економічного стану підприємства. Більшість ключових коефіцієнтів рентабельності підприємства хоч і мали позитивну динаміку, однак все ж таки мали від'ємне значення. А показник рентабельність операційної діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради взагалі погіршився на 37,63 %.

Витрати підприємства представляють собою грошові потоки, пов'язані з наданням послуг, в тому числі з оплатою праці, витратами на закупівлю сировини та матеріалів, витратами на енергетику, транспорт та інфраструктуру, оплатою податків і зборів, іншими витратами підприємства. Аналіз структури операційних витрат підприємства демонструє переважання у їх складі саме витрат на оплату праці працівників, які, крім того, мають намічену тенденцію до збільшення.

Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради не в повній мірі використовує власні можливості. При

цьому у останні роки підприємство послабило залежність від зовнішніх інвесторів і кредиторів, тобто є достатньо фінансово стійким. Також з позитивного можна відзначити 4-кратне перевищення власного капіталу над позиковими коштами.

2.2. Оцінка ефективності управління персоналом підприємства

Ефективність функціонування підприємства в сучасних ринкових умовах, забезпечення його сталого і конкурентоспроможного розвитку залежить, насамперед, від персоналу, здатності співробітників у найоптимальніший спосіб вирішувати поставлені перед ними завдання.

Від формування персоналу підприємства, його кількісної і якісної збалансованості та рівня використання значною мірою залежить ефективність використання всіх інших складових виробничих ресурсів, забезпечення високих результатів діяльності підприємств, їх динамічний науково-технічний і соціальний розвиток.

Однією з передумов успішного економічного розвитку як на мікро-, так і на макро- рівнях є врахування інтересів працівників у будь-яких діях, спрямованих на підвищення ефективності функціонування підприємства. Без такого врахування не можна досягти підвищення ефективності в широкому розумінні. Раціональне використання персоналу є основою збільшення обсягу виконання робіт, надання послуг та підвищення матеріального добробуту працівників підприємства.

За умов ринкової економіки підприємство самостійно вирішує, що і як планувати, визначає потребу в кадрах за фахом, професіями, рівнем кваліфікації; розробляє плани зі збільшення продуктивності праці; розраховує рівень оплати праці та інших виплат з метою забезпечення максимально можливого прибутку від реалізації виробничо-господарської діяльності. Тому оцінювання ефективності управління персоналом є одним з найважливіших напрямів економічної роботи на підприємстві, метою якого є виявлення резервів підвищення ефективності виробництва за рахунок збільшення його обсягу при кращому використанні

працівників, що безпосередньо залежить від умов праці і розмірів заробітної плати.

До ключових показників з праці, які доцільно включати у аналіз стану персоналу, належать:

- продуктивність праці;
- трудомісткість виробництва продукції;
- середньооблікова чисельність штатних працівників;
- загальний фонд робочого часу середнього робітника, середня тривалість робочого дня (зміни), кількість відпрацьованих днів (змін), годин одним працівником;
- фонд оплати праці;
- середня заробітна плата працівників (середньомісячна, середньорічна по підприємству).

Структурна характеристика персоналу Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради визначається складом і кількісним співвідношенням окремих категорій і груп працівників підприємства. Якісний склад персоналу характеризується професійною віковою структурою та стажем роботи. Структуру персоналу за стажем можна розглядати як в плані загального стажу, так і стажу роботи на даному підприємстві.

Структура персоналу за освітнім рівнем передбачає виділення працівників за вищою, середньою спеціальною та повною загальною середньою освітою. На формування різних видів структур персоналу як на макро-, так і мікро- рівнях у найближчі роки будуть впливати ряд факторів на загальні тенденції, а саме:

- інтенсивний перерозподіл працівників зі сфери промислового виробництва в інформаційну сферу та сферу послуг;
- заміна вивільненого персоналу на персонал з вищим загальним і професійним рівнем;
- зростання частки розумової праці, що збільшить попит на кваліфіковану робочу силу (програмістів, операторів, наладчиків).

Персонал організації знаходиться в постійному русі внаслідок найму одних працівників і звільнення інших. Процес оновлення колективу за рахунок вибуття одних і найму інших називається змінністю персоналу.

Щоб правильно організувати працю на підприємстві, Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради укладає трудові договори з працівниками в порядку, передбаченому законодавством України, під розписку ознайомлює працівників з наказом про їх прийняття на підприємство та відправляє відповідне повідомлення в Державну фіскальну службу.

Підприємство не включає до трудових договорів умови, що погіршують становище працівників порівняно з чинним законодавством, спільно з профспілковою стороною розробляє правила внутрішнього трудового розпорядку, вносить до них зміни і доповнення, затверджує їх на загальних зборах трудового колективу, розробляє і затверджує посадові інструкції, з якими ознайомлює своїх працівників. Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради надає працівникам роботу відповідно до їх професій, займаний посаді та кваліфікації, не вимагає від працівників виконання роботи, не обумовленої трудовим договором (контрактом) та посадовою інструкцією.

Підприємство здійснює звільнення працівників з підстав, зазначених у п. 1. ст. 40 КЗпП України лише у випадках, якщо неможливо перевести працівника, за його згодою, на іншу роботу, та за попередньою згодою профспілкового органу первинної профспілкової організації, членом якої є працівник (крім випадку ліквідації підприємства), та надає профспілковій стороні обґрунтоване письмове подання про розірвання трудового договору з працівником.

У ринкових умовах господарювання надзвичайно важливим для кожного підприємства стає визначення оптимальної чисельності працівників. Метою визначення чисельності працівників є необхідність оцінювання їхнього рівня для прийняття рішень, спрямованих на раціоналізацію трудової складової в діяльності підприємства.

Чисельність працівників на підприємстві передбачає виконання відповідних етапів аналітичної роботи. Забезпечення підприємства персоналом розпочинається з вивчення відповідності фактичної чисельності плановій потребі загалом та за окремими категоріями і групами (табл. 2.9). Відхилення фактичної чисельності від планової прийнято називати абсолютним.

Таблиця 2.9

**Динаміка чисельності і структури персоналу підприємства
у період 2020–2022 роки, осіб**

№ з/п	Показники	2020 р.	2021 р.	2022 р.	Відхилення 2022 р. до 2020 р.	
					+/-	%
1.	Середньооблікова чисельність штатних працівників, у т. ч.:	863	871	725	-138	-15,99
2.	Персонал основного виду діяльності, з них:	736	742	643	-93	-12,64
2.1	– керівники;	29	32	22	-7	-24,14
2.2	– спеціалісти;	65	63	47	-18	-27,69
2.3	– службовці;	37	31	26	-11	-29,73
2.4	– робітники	682	691	601	-81	-11,88
3.	Непромисловий персонал	127	129	82	-45	-35,43

За даними табл. 2.9 можна відзначити, що за період 2020–2022 роки середньооблікова чисельність штатних працівників підприємства зменшилася на 138 осіб, або на 15,99 %. У складі персоналу Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради переважає чисельність персоналу основного виду діяльності. Так, у звітному році їх чисельність склала 643 особи, або 88,69 % від середньооблікової чисельності штатних працівників. Серед працівників основного виду діяльності, звичайно, найбільшу частку мали робітники, чисельність яких зменшилася з 682 осіб у 2020 р. до 601 особи у 2022 р., тобто на 11,88 %.

За гендерною ознакою в структурі персоналу підприємства зберігається відносна рівновага з деяким переважанням чисельності жінок, про що свідчать дані табл. 2.10.

Таблиця 2.10

**Динаміка чисельності і структура персоналу підприємства за статтю
у 2020–2022 роках, осіб**

Показники	2020 р.		2021 р.		2022 р.		Відхилення 2022 р. до 2020 р.		
	Осіб	Питома вага, %	Осіб	Питома вага, %	Осіб	Питома вага, %	+/-	%	п.с.
Середньооблікова чисельність штатних працівників	863	100,00	871	100,00	725	100,00	-138	-15,99	0,00
з них:									
– жінки;	473	54,81	462	53,04	370	51,03	-103	-21,78	-3,77
– чоловіки	390	45,19	409	46,96	355	48,97	-35	-8,97	3,77

За даними табл. 2.10 відзначимо, що у звітному році чисельність жінок у складі персоналу підприємства склала 51,03 %. За досліджуваний період вона зменшилася на 103 особи, або 21,78 %.

У віковому складі персоналу Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради переважає частка працівників працездатного віку (36–59 років), чисельність яких у 2022 р. склала 458 осіб (табл. 2.11).

Таблиця 2.11

**Вікова структура персоналу Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради
у 2020–2022 роках, осіб**

Показники	2020 р.		2021 р.		2022 р.		Відхилення 2022 р. до 2020 р.	
	Осіб	Питома вага, %	Осіб	Питома вага, %	Осіб	Питома вага, %	+/-	%
Середньооблікова чисельність штатних працівників	863	100	871	100	725	100	-138	-15,99
з них: до 35 років;	226	26,2	247	28,4	202	27,8	-25	-10,86
36–59 років;	545	63,1	531	61	458	63,2	-86	-15,86
старші 60 років	92	10,7	93	10,6	65	9	-26	-28,78

За даними табл. 1.14 відзначимо, що у віковому складі працівників підприємства переважає чисельність осіб у максимально працездатному віці. Також досить великою є частка молодих людей віком до 35 років. У 2022 р. частка таких працівників склала 27,8 %.

Наявність молодих працівників є хорошим показником для досліджуваного підприємства, оскільки свідчить про спробу стабілізувати штат працівників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради, балансує між багатолітнім досвідом роботи дорослих працівників і креативним мисленням та свіжим поглядом на поточні проблеми діяльності молоді.

У складі персоналу за рівнем освіти переважають працівники з середньою спеціальною освітою, частка яких у всіх досліджуваних роках коливалася від 72,54 до 75,45 % (табл. 2.12).

Таблиця 2.12

**Склад та структура персоналу підприємства за освітою
у 2020–2022 роках**

Показники	2020 р.		2021 р.		2022 р.		Відхилення 2022 р. до 2020 р.	
	Осіб	Питома вага, %	Осіб	Питома вага, %	Осіб	Питома вага, %	+/-	%
Середньооблікова чисельність штатних працівників	863	100,00	871	100,00	725	100,00	-138	-15,99
з них: з вищою освітою;	136	15,76	127	14,58	102	14,07	-34	-25,00
з середньою спеціальною освітою;	626	72,54	636	73,02	547	75,45	-79	-12,62
з загальною середньою освітою	101	11,70	108	12,40	76	10,48	-25	-24,75

За даними табл. 2.12 відзначимо, що у відповідності до специфіки діяльності підприємства в його складі переважає частка працівників з середньою спеціальною освітою. У 2022 р. вона склала 75,45 %. Також відзначимо значну частку працівників з вищою освітою. Ці працівники зайняті переважно в економічних підрозділах підприємства.

Отже, аналіз рівня ефективності управління персоналом в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради показав чітку відповідність персоналу за параметрами віку, статті, рівня освіти тощо специфічному виду діяльності підприємства, а саме забезпеченню курсування пасажирського наземного транспорту міського та приміського сполучення. Працівники мають переважно спеціальну технічну освіту. За гендерною ознакою помітне незначне перевищення частки зайнятих у штаті жінок.

2.3. Порядок забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради

Щоб відповідно до закону забезпечити захист персональних даних працівників, найперше, що було зроблено на підприємстві, – це затверджено наказом список осіб, які мають право доступу до персональних даних співробітників. У наказі визначено, які саме особи із цього списку для яких цілей можуть використовувати персональні дані працівників. Тобто в ньому чітко зазначено, хто і навіщо це робить. Кожний співробітник має доступ лише до тих персональних даних, які необхідні йому у зв'язку з виконанням посадових (службових) обов'язків.

На підприємстві розроблено форму під назвою «Зобов'язання про нерозголошення персональних даних». Згідно з ч. 3 ст. 10 Закону України «Про захист персональних даних № 2297 від 01.06.10 р. [46], цю форму в обов'язковому порядку підписують всі співробітники, які мають доступ до персональних даних працівників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради (співробітники бухгалтерії, відділу кадрів, члени комісії із соціального страхування тощо). Строк дії такого зобов'язання не припиняється навіть після припинення роботи з персональними даними (це може бути як звільнення, так і переведення до іншого структурного підрозділу підприємства, де не доведеться працювати з персональними даними інших співробітників).

Цю форму дають працівнику на підпис під час прийняття на роботу (або переведення з іншого відділу, де немає доступу до персональних даних). Датою отримання доступу до персональних даних вважається дата підписання співробітником зобов'язання, а датою позбавлення такого права вважається дата його звільнення (переведення на іншу посаду, де не буде доступу до персональних даних) – п. 3.8–3.9 Типового порядку обробки персональних даних. От як виглядає таке зобов'язання в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради (рис. 2.1):

Директору Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради Лазарєву С.Ю. інспектора з кадрів Петренка Петра Петровича
Зобов'язання
Я, інспектор з кадрів Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради Петренко Петро Петрович, зобов'язуюся не розголошувати персональні дані співробітників, які стали мені відомі у зв'язку з виконанням мною посадових обов'язків.
25.11.22 р. П.П. Петренко

Рис. 2.1. Зразок зобов'язання про нерозголошення персональних даних співробітників

Згідно з п. 3.5 Типового порядку обробки персональних даних, на підприємстві ведуть облік працівників, які мають доступ до персональних даних. Для цих цілей використовується журнал обліку таких працівників. Законодавчо не встановлено форму цього журналу, тому в умовах підприємства його ведуть в довільній формі, як показано на зразку (табл. 2.13).

Таблиця 2.13

Зразок журналу обліку співробітників, які мають доступ до персональних даних

№ з/п	П.І.Б. співробітника	Посада	Дата надання права роботи з персональними даними, № наказу	Дата звільнення / переведення на іншу посаду, № наказу
1	2	3	4	5
1.	Петренко Петро Петрович	Інспектор з кадрів	25.11.22 р., наказ № 21-Л (про прийняття на роботу)	03.11.23 р., наказ № 231-Л (про звільнення)
2.				
...				

На наступному етапі адміністрація повідомляє працівників про володільця його персональних даних, склад і зміст зібраних даних, їх права, а також про мету збору персональних даних. На підприємстві всіх співробітників про це повідомляють не в усній формі, а під підпис. Тоді в разі перевірки завжди буде можливість підтвердити

той факт, що співробітник був у обов'язковому порядку повідомлений про свої права у сфері захисту персональних даних у повному обсязі.

На Комунальному підприємстві «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради розроблене Повідомлення для всіх працівників про обробку їх персональних даних, зразок якого представлений на рис. 2.2. Таким чином у відділі кадрів підприємства зберігається належним чином затверджений оригінал Повідомлення про порядок обробки персональних даних, з яким кожний співробітник ознайомлений під підпис. Для цих цілей на підприємстві ведуть журнал ознайомлення з повідомленням, який зберігається в особовій справі кожного співробітника.

Також зі змістом такого Повідомлення ознайомлюють усіх новоприйнятих співробітників. Для цього використовують журнал, або роблять позначку в наказі про прийняття на роботу (наприклад, «З Повідомленням про порядок обробки персональних даних ознайомлений. Підпис»).

Нарешті, на Комунальному підприємстві «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради розроблено Положення про порядок обробки і захисту персональних даних. У цьому документі відображено все, про що було зазначено вище. За основу, звичайно, взято Типовий порядок обробки персональних даних.

Чинним законодавством передбачено як адміністративну, так і кримінальну відповідальність за порушення вимог про захист персональних даних. Адміністративна відповідальність застосовується на підставі ст. 18839 Кодексу України про адміністративні правопорушення (далі – КУпАП), зокрема за такі порушення:

– недотримання встановленого законодавством порядку захисту персональних даних, що призвело до незаконного доступу до таких даних або порушення прав суб'єкта персональних даних. Передбачено штраф у розмірі від 300 до 1000 неоподаткованого мінімуму доходів громадян (НМДГ) (від 5,1 до 17,0 тис. грн), що застосовується до посадових осіб підприємств, а також до фізичних осіб-суб'єктів підприємницької діяльності;

Повідомлення про обробку персональних даних працівників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради

Відповідно до вимог Закону від 01.06.10 р. № 2297-VI «Про захист персональних даних» повідомляємо, що в цілях реалізації трудових правовідносин Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради проводить обробку персональних даних працівників за правилами чинного законодавства. На підприємстві виконується обробка таких персональних даних співробітників:

1. Паспортні дані, індивідуальний податковий номер (ПН).
2. Дані про здобутий освітній ступінь.
3. Дані про трудову діяльність.
4. Дані про військовий облік (за наявності).
5. Дані про стан здоров'я (відповідно до ст. 24 КЗпП України).
6. Дані про сімейний стан, а також про зареєстрованих осіб за адресою проживання.
7. Адреса реєстрації, а також адреса фактичного проживання, номер телефону.
8. Відомості про співробітника, які підтверджують його право на отримання пільг і компенсацій (інвалідність, статус матері-одиначки тощо).

Зазначені персональні дані передаються в установленому законодавством порядку до органів фіскальної служби, Пенсійного фонду, служби зайнятості, а також до інших органів державної влади і місцевого самоврядування відповідно до законодавства. Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради вживає заходи із захисту персональних даних співробітників від несанкціонованої обробки. У зв'язку із цим обробка персональних даних здійснюється виключно співробітниками, які підписали Зобов'язання про нерозголошення персональних даних, що стали їм відомі в результаті виконання своїх трудових обов'язків.

Згідно зі ст. 8 Закону від 01.06.10 р. № 2297-VI «Про захист персональних даних» кожен співробітник Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради має право:

- знати місцезнаходження і спосіб збору своїх персональних даних, мету їх обробки, а також знати, хто є власником його персональних даних;
- отримати гарантії захисту своїх персональних даних від несанкціонованої обробки і незаконного знищення;
- отримувати інформацію про третіх осіб, яким повідомляються його персональні дані;
- отримувати доступ до своїх персональних даних;
- у разі незаконної обробки або зазначення недостовірних персональних даних вимагати їх знищення або зміни.

Директор Комунального підприємства
«Житомирське трамвайно-тролейбусне управління»
Житомирської міської ради
25.11.2022 р.

Лазарєв С.Ю.

Рис. 2.2. Зразок Повідомлення про обробку персональних даних працівників підприємства

– при повторному подібному порушенні, допущеному протягом року, – штраф може становити від 1 000 до 2 000 НМДГ (від 17, 0 до 34,0 тис. грн).

Протоколи про адміністративні порушення, передбачені цією статтею КУпАП, мають право складати уповноважені особи секретаріату Уповноваженого (ст. 255 КУпАП). А рішення про застосування штрафу приймає суд (ст. 221 КУпАП). Кримінальна відповідальність у цій сфері передбачена ст. 182 Кримінального кодексу – за незаконний збір, зберігання, використання, знищення, розповсюдження конфіденційної інформації. Тобто інформації про фізичну особу (ч. 2 ст. 21 Закону від 02.10.92 р. № 2657-ХІІ «Про інформацію») [65].

Отже, на підприємстві розроблено Положення про роботу з персональними даними працівників, чітко визначено коло осіб, які мають доступ до цих даних, належним чином оформлено усі необхідні документи (зобов'язання про нерозголошення персональних даних співробітників, журнал обліку співробітників, які мають доступ до персональних даних, типовий порядок обробки персональних даних, повідомлення про обробку персональних даних працівників підприємства). Адже порушення у сфері захисту персональних даних працівників чреваті досить серйозними санкціями для адміністрації підприємства.

Висновки до розділу 2

Підприємство здійснює міські перевезення тролейбусами, трамваями та автобусами із застосуванням автоматизованої системи оплати проїзду. В останні роки підприємство було збитковим, про що свідчить формування чистого збитку у кожному з періодів досліджуваного діапазону. При чому за цим показником спостерігається тенденція до погіршення фінансово-економічного стану підприємства. Більшість ключових коефіцієнтів рентабельності підприємства хоч і мали позитивну динаміку, однак все ж таки мали від'ємне значення. А показник рентабельність операційної діяльності Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради взагалі погіршився на 37,63 %.

Витрати підприємства представляють собою грошові потоки, пов'язані з наданням послуг, в тому числі з оплатою праці, витратами на закупівлю сировини та матеріалів, витратами на енергетику, транспорт та інфраструктуру, оплатою податків і зборів, іншими витратами підприємства. Аналіз структури операційних витрат підприємства демонструє переважання у їх складі саме витрат на оплату праці працівників, які, крім того, мають намічену тенденцію до збільшення.

Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради не в повній мірі використовує власні можливості. При цьому у останні роки підприємство послабило залежність від зовнішніх інвесторів і кредиторів, тобто є достатньо фінансово стійким. Також з позитивного можна відзначити 4-кратне перевищення власного капіталу над позиковими коштами.

Аналіз рівня ефективності управління персоналом в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради показав чітку відповідність персоналу за параметрами віку, статті, рівня освіти тощо специфічному виду діяльності підприємства, а саме забезпеченню курсування пасажирського наземного транспорту міського та приміського сполучення. Працівники мають переважно спеціальну технічну освіту. За гендерною ознакою помітне незначне перевищення частки зайнятих у штаті жінок.

На підприємстві розроблено Положення про роботу з персональними даними працівників, чітко визначено коло осіб, які мають доступ до цих даних, належним чином оформлено усі необхідні документи (зобов'язання про нерозголошення персональних даних співробітників, журнал обліку співробітників, які мають доступ до персональних даних, типовий порядок обробки персональних даних, повідомлення про обробку персональних даних працівників підприємства). Адже порушення у сфері захисту персональних даних працівників чреваті досить серйозними санкціями для адміністрації підприємства.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВА

3.1. Шляхи удосконалення забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради

Актуальною вважається загроза, яка може бути реалізована та передбачає небезпеку. Для оцінювання реалізації загрози застосовуються два показники: рівень початкової захищеності та частота (імовірність) реалізації даної загрози.

При створенні переліку актуальних загроз безпеки кожного ступеня початкової захищеності ставиться у відповідність чисельний коефіцієнт (Y_1), а саме:

- 0 – для високого ступеня початкової захищеності;
- 5 – для середнього ступеня початкової захищеності;
- 10 – для низького ступеня початкової захищеності.

Під імовірністю реалізації загрози мається на увазі обчислювальний експертним шляхом показник, що характеризує, наскільки імовірною є реалізація конкретної загрози. При обчисленні переліка актуальних загроз безпеки кожної градації імовірності виникнення загрози ставиться у відповідність чисельний коефіцієнт (Y_2), а саме:

- 0 – для малоймовірної загрози;
- 2 – для низької імовірності загрози;
- 5 – для середньої імовірності загрози;
- 10 – для високої імовірності загрози.

З урахуванням викладеного, коефіцієнт реалізації загрози Y буде обчислюватись співвідношенням за формулою 3.1:

$$Y = (Y_1 + Y_2) / 20. \quad (3.1)$$

Модель загроз забезпечення захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління»

Житомирської міської ради розглянуто в табл. 3.1.

Таблиця 3.1

**Модель загроз забезпечення захисту персональних даних
співробітників підприємства**

№ з/п	Загроза	Y ₂	Y	Можливість реалізації	Небезпека	Актуальність
1.	Загроза витоку акустичної інформації	0	0,25	низька	низька	неактуальна
2.	Загрози витоку візуальної інформації	0	0,35	середня	низька	неактуальна
3.	Загрози, направлені на перехоплення паролів, модифікацію базової системи вводу/виводу, перехоплення керування завантаженням	5	0,5	середня	середня	актуальна
4.	Загрози виявлення паролів	5	0,5	середня	середня	актуальна
5.	Загроза впровадження шкідливого програмних продуктів	5	0,5	середня	середня	актуальна
6.	Загрози сканування, направлені на виявлення типу ОС, мережеских адрес, робочих місць, відкритих портів та служб, відкритих з'єднань	10	0,75	висока	висока	актуальна
7.	Загрози впровадження помилкового об'єкту мережі	2	0,35	середня	низька	неактуальна
8.	Загрози віддаленого запуску застосунків	2	0,35	середня	низька	неактуальна
9.	Загрози нав'язування хибного маршруту шляхом несанкціонованої зміни маршрутно-адресних даних	2	0,35	середня	низька	неактуальна

Таким чином, серед виявлених проблем на базі підприємств особливий інтерес викликає комплексна загроза витоку інформації про працівників підприємства. Витоком інформації вважають безконтрольний вихід конфіденційної (приватної) інформації за межі підприємства або кола осіб, яким вона була довірена.

Витік інформації з Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради можна пояснити збігом низки факторів. Ці фактори охоплюють різні аспекти, починаючи від зовнішньої співпраці та потенційного промислового шпигунства і закінчуючи внутрішніми прогалинами в управлінні даними та протоколами безпеки.

Одним із важливих чинників витоку інформації є спільна робота з іншими компаніями. Обмін конфіденційними даними під час партнерства та співпраці може ненавмисно призвести до того, що важлива інформація стане доступною стороннім особам. Промислове шпигунство, як навмисне, так і ненавмисне, стає відчутнішим,

коли обмін інформацією між організаціями відбувається без належного захисту.

Іншим ключовим аспектом, що сприяє порушенню, є недотримання особистих вимог при поводженні з носіями даних. Така недбалість може полягати в неправильному поводженні з фізичними носіями інформації або неналежному захисті цифрових сховищ, що створює вразливості, які можуть бути використані зловмисниками.

Технічна інфраструктура відіграє ключову роль в інформаційній безпеці, і виникнення помилок і збоїв у роботі серверного обладнання є важливим фактором. Недоліки в проектуванні та впровадженні систем безпеки ще більше посилюють ці вразливості, уможливорюючи несанкціонований доступ до конфіденційної інформації.

Недотримання встановлених правил експлуатації систем захисту даних також відіграє значну роль у витоку інформації. Це може включати ігнорування або обхід стандартних операційних процедур і протоколів, які призначені для захисту конфіденційних даних.

Крім того, неадекватні технічні заходи безпеки сприяють порушенню інформаційної безпеки. Недостатнє екранування, відсутність пристроїв для зменшення шуму, відсутність віконних чіпів та скомпрометовані пломби – все це разом створює середовище, вразливе до несанкціонованого доступу та витоку даних.

Узагальнено основні причини витоку інформації в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради подані на рис. 3.1.

В цілому було відзначено три напрями витоку інформації про працівників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради, а саме:

- розголошення, тобто несанкціоноване доведення персональної інформації до осіб, які не мають права доступу до неї тими, хто цим правом володіє;
- несанкціонований доступ до інформації;
- отримання конфіденційної інформації розвідками, яке може здійснюватися за допомогою технічних засобів (технічна розвідка) або за допомогою агентурних методів (агентурна розвідка).



Рис. 3.1. Основні причини витоку інформації за межі підприємства

Будь-яке перенесення даних здійснюється через систему зв'язку. У випадку несанкціонованого переміщення інформації вона перетворюється у канал витоку. З метою встановлення високого рівня захищеності персональних даних під час розробки та впровадження систем обробки інформації підприємствам доцільно використовувати методи забезпечення її надійного захисту. Їх умовно поділяють на правові, програмно-технічні та організаційно-економічні (рис. 3.2).

До організаційних методів захисту інформації потрібно також віднести розмежування доступу до інформації. Наразі доступ має кожний системний адміністратор. У зв'язку з даним фактом, виникає ризик отримання несанкціонований доступ (НСД) до інформації з обмеженим доступом (ІзОД) шляхом отримання доступу до робочого місця одного з системних адміністраторів. Для запобігання даної загрози потрібно дозволити лише одній людині у відділі мати доступ до інформації та максимально захистити її робочу станцію.

Усі методи забезпечення захисту персональних даних на рівні підприємства будуть більш ефективними, якщо їх інтегрувати до алгоритму дій. На основі вищезазначеного можна виокремити такі рекомендації щодо ефективного захисту особистої інформації для суб'єктів персональних даних (споживачів):

1. Не користуватися громадським WiFi – хакери можуть створити мережу-двійника з аналогічною назвою і перехопити персональні дані користувача.

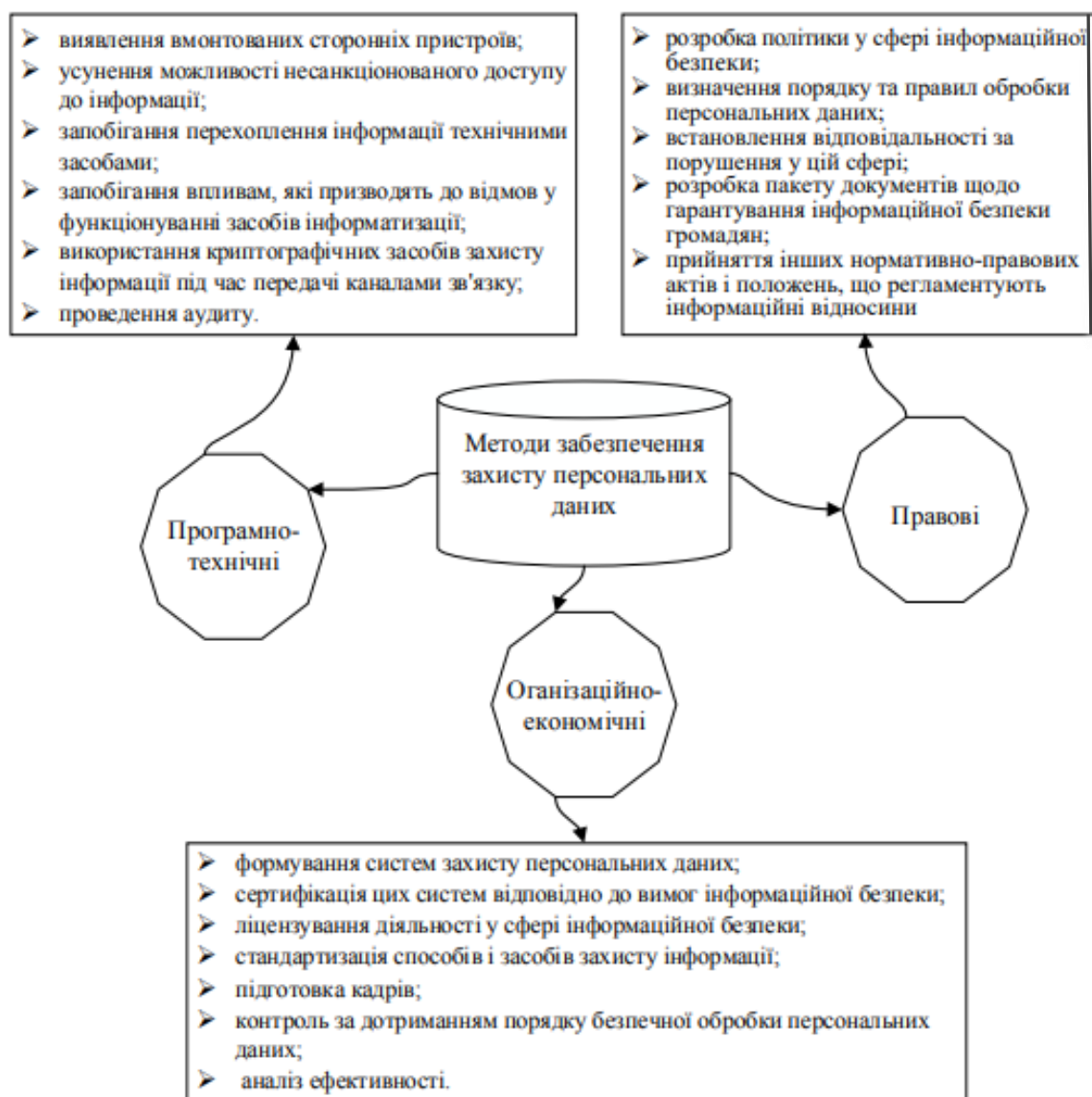


*Рис. 3.2. Методи забезпечення захисту персональних даних працівників в умовах
Комунального підприємства «Житомирське трамвайно-тролейбусне управління»
Житомирської міської ради*

2. Встановлювати для своїх акаунтів надійні паролі, використовувати мобільні додатки-генератори складних паролів. Час від часу варто змінювати паролі і не використовувати однакові комбінації для різних акаунтів.

3. Шифрувати повідомлення – цієї рекомендації легко дотримуватись, оскільки більшість месенджерів використовують шифрування.

4. Уникати використання функції «увійти за допомогою Facebook/Google». У багатьох випадках в сторінку, на якій відбувається вхід, інтегровані сторонні бібліотеки JavaScript, які здатні перехоплювати дані, що надійшли від

Facebook/Google, вилучати інформацію про користувача і передавати її третій стороні.

5. Перевіряти адресний рядок сайтів. Якщо він починається із протоколу «https», то обмін даних є захищеним. Це означає безпечний обмін даними, оскільки інформація, що передається між вашим пристроєм і веб-сайтом, шифрується. Будьте обережні при взаємодії з веб-сайтами, які не використовують цей захищений протокол, особливо при передачі конфіденційної інформації.

6. Створення комплексної системи захисту інформації в основі програмно-адаптивного захисту комунального підприємства, що має ґрунтуватися на адаптивних механізмах захисту, включати програмні рішення, розроблені для розвитку та адаптації до нових загроз. Регулярно оновлювати та проводити аудит інфраструктури безпеки для забезпечення її ефективності проти нових кіберзагроз.

Якщо витік персональних даних таки трапився, не слід бути пасивним, необхідно подавати скарги, вимагати вилучення даних у тих, хто заволодів ними незаконно, залучати правоохоронні органи тощо.

Отже, більшість витоку персональних даних відбувається через людський чинник – навмисні чи ненавмисні дії працівників підприємств. З метою мінімізації загроз масових витоків персональних даних про споживачів, необхідно здійснити такі заходи: удосконалити законодавчий фундамент, підвищити ефективність контролюючої системи та рівень правової грамотності населення.

Сьогодні потребують урегулювання питання щодо обов'язковості застосування заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог українського законодавства. Держава має сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту. У цій сфері доцільно проводити і соціальну рекламу. У разі успішного поєднання цих трьох факторів стає можливим надійний захист персональних даних громадян, зменшення кількості і складності крадіжок та шахрайств у системі роботи пасажирського наземного транспорту. Рекомендовано заходи, серед яких – створення складних паролів для акаунтів, перевірка адресного рядку сайтів, уникнення використання громадського Wi-Fi тощо.

3.2. Створення комплексної системи захисту персональних даних в основі програмно-адаптивного захисту підприємства

Аудит захисту персональних даних співробітників Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради показав, що на підприємстві циркулює інформація, що має високу ступінь важливості. Для створення комплексної системи захисту інформації необхідно передбачити засоби для нейтралізації цих загроз. Ці засоби мають ґрунтуватись на та не суперечити законам України, федеральним законам, нормативно правовим актам, постановленням та розпорядженням Уряду України. Механізми захисту, які використовуються для побудування захищених систем, повинні бути взаємопов'язані за місцем, часом та характером дії. Комплексність передбачає також використання різноманітних методів та засобів захисту інформації: організаційних, технічних, програмних, криптографічних, правових. Система захисту повинна мати декілька рівнів, що перекривають один одного.

Інженерно-технічні засоби захисту мають бути направлені на запобігання доступу порушників до приміщення офісу, до інформаційної середовища та розмежування повноважень користувачів.

Програмно-апаратна система захисту повинна забезпечувати конфіденційність, цілісність та доступність інформації, що опрацьовується.

Організаційні методи захисту інформації включають до себе міри, події та дії, які повинні виконувати повноважні особи у процесі роботи з інформацією для забезпечення заданого рівня безпеки. Елементи організаційного захисту повинні включати до себе не тільки документи, пов'язані з роботою з конфіденційною інформацією, а й документи, що забезпечують організацію захищеного документообігу з учасниками системи електронного документообігу.

Для забезпечення надійного захисту даних від загрози впливу шкідливого програмного забезпечення на всіх робочих станціях і сервері підприємства повинні бути встановлені антивірусні пакети з безперервним автоматичним обов'язковим оновленням антивірусних баз з локального дзеркала, розміщеного на сервері.

Призначення антивірусного програмного забезпечення Zillya для Windows – забезпечення надійної високоякісної захисту робочих місць і персонального комп'ютера від вірусів і інших шкідливих програм. Антивірус української компанії «Лабораторія Zillya!», перша версія якого з'явилася у квітні 2009 року. Надає користувачеві захист від вірусів, троянських програм, шпигунських програм, руткітів, рекламних програм, а також невідомих загроз за допомогою проактивного захисту. Антивірус сертифіковано ДССЗЗІ, рівень захисту Г-2. Має високу ймовірність успішного запуску процесу сканування на зараженому ПК – навіть з зовнішнього носія без установки в систему. Переваги антивірусного програмного забезпечення Zillya для Windows:

- ефективний засіб постійного моніторингу здоров'я комп'ютера; перехоплення «на льоту» всіх звернень до файлів на дисках;
- захист конфіденційної інформації – краще в галузі виявлення троянських програм і клавіатурних шпигунів;
- недосяжна для конкурентів якість виявлення і нейтралізація складних вірусів, таких як MaosBoost, Sector;
- мінімальне навантаження на ресурси ПК і непомітна дія при роботі користувача з іншими додатками;
- захист від вірусів, що використовують rootkit-технології;
- визначення вірусів в архівах будь-якого ступеня вкладеності та в упакованих об'єктах;
- унікальна технологія несигнатурного пошуку та інтелектуальний евристичний аналізатор – захист від невідомих загроз;
- захист від масових розсилок вихідної електронної кореспонденції поштовими хробаками.

Антивірус Bitdefender для Windows Servers – це додаток для захисту файлових серверів під керуванням ОС Windows Server від усіх типів шкідливих програм. Рішення розроблено з урахуванням підвищених вимог до серверів для роботи в умовах високих навантажень.

Додаток контролює всі вхідні і вихідні потоки даних на комп'ютері-електронну

пошту, інтернет-трафік і мережеві взаємодії. Глибока інтеграція всіх компонентів програми дозволяє уникнути системних конфліктів і забезпечує високу швидкість роботи програми.

Інсталювання програми на робочі станції, налаштування параметрів її роботи, своєчасне оновлення баз сигнатур та програмних модулів, а також оперативне реагування в критичних ситуаціях – всі ці завдання адміністратор мережі може вирішувати віддалено та централізовано, використовуючи консоль керування Bitdefender.

Евристичний аналізатор, що входить до складу антивірусу Bitdefender, забезпечує захист від нових шкідливих програм ще до того, як їх опис додається в бази сигнатур. Додаток аналізує всі процеси, запущені у системі, своєчасно попереджаючи користувача про небезпеку; в разі необхідності імітує запуск підозрілих програм в ізолюваному віртуальному середовищі; дозволяє відновити дані, пошкоджені шкідливим ПЗ.

Нове антивірусне ядро дозволяє регулярно оновлювати його окремі модулі без перевстановлення програми. Завдяки цьому користувачі завжди мають у своєму розпорядженні найсучасніші методи захисту від нових шкідливих програм.

Однією з важливих задач при експлуатації інформаційних систем є забезпечення цілості даних, тому необхідно мати механізм для швидкого відновлення втрачених даних. Це може бути забезпечено шляхом побудови розвиненої системи резервного копіювання, що періодично створює копії інформації з метою її подальшого відновлення в разі часткового або повного руйнування. До системи резервного копіювання доцільно пред'явити наступні вимоги:

- використання технології «клієнт-сервер» при реалізації системи мережевого резервного копіювання;
- забезпечення автоматизації робіт резервного копіювання;
- використання адекватного носія резервної копії;
- виконання верифікації та стиснення інформації;
- швидке відновлення серверів мережі після аварії;
- резервне копіювання баз даних прикладних систем в оперативному режимі;

- підтримка гетерогенного середовища;
- розвинені засоби управління і моніторингу.

Даним вимогам задовольняє програмне забезпечення Acronis Backup & Recovery 10 Advanced Server.

Acronis Backup & Recovery 10 Advanced Server – продукт, розроблений для підприємства будь-якого розміру, росте разом з компанією, легко масштабується від локальних конфігурацій до роботи у великих територіально розподілених мережах на тисячі машин. Він надає організаціям розширені можливості резервного копіювання та відновлення системи: дедуплікацію даних, підвищену безпеку, панель моніторингу операцій. Основні переваги Acronis Backup & Recovery 10 Advanced Server:

- швидке і надійне відновлення;
- процеси резервного копіювання та відновлення усіх робочих станцій та серверів керуються з єдиної централізованої панелі моніторингу, що відображає інформацію про всі виконувані або заплановані завдання;
- дедублікація на рівні файлів та блоків виключає повторне резервне копіювання одних і тих же даних, що істотно скорочує витрати на передачу та зберігання резервних копій;
- групове опрацювання завдань за допомогою політик резервного копіювання та відновлення дозволяє автоматизувати однотипні дії, такі як відновлення багатьох машин в мережі, і не витрачати час на індивідуальний запуск кожного завдання.

Задля запобігання витоку інформації шляхом перехоплення мережевого трафіку слід використовувати технологію IP in IP. IP in IP – це протокол IP-тунелювання, який інкапсулює один IP-пакет в інший IP-пакет. Інкапсуляція одного IP пакета в інший IP пакет, це додавання зовнішнього заголовка з SourceIP – точкою входу в тунель, і Destination – точкою виходу з тунелю. При цьому внутрішній пакет не був змінений (крім поля TTL, який зменшився). Поля «Do not Fragment» і «The Type of Service» повинні бути скопійовані в зовнішній пакет. Якщо розмір пакета більше ніж Path MTU, пакет фрагментується в інкапсуляторі, оскільки зовнішній заголовок має бути включеним. Декапсулятор повинен буде зібрати пакет. Налаштований тунель допомагає зменшити кількість діючих політик IPsec. Оскільки у тунелі відбувається

інкапсуляція трафіку то можливо будувати будь-які маршрути, прописуючи лише дві адреси у політиках IPsec. Для підвищення рівню безпеки потрібно використовувати шифрування IPsec (рис. 3.3).

The image shows a configuration window for IPsec. It has two main sections: 'Auth. Algorithms' and 'Encr. Algorithms'. In the 'Auth. Algorithms' section, 'md5' is unchecked, 'sha1' is checked, 'null' is unchecked, 'sha256' is unchecked, and 'sha512' is unchecked. In the 'Encr. Algorithms' section, 'null' is unchecked, 'des' is unchecked, '3des' is unchecked, 'aes-128 cbc' is checked, 'aes-192 cbc' is checked, 'aes-256 cbc' is checked, 'blowfish' is unchecked, 'twofish' is unchecked, 'camellia-128' is unchecked, 'camellia-192' is unchecked, 'camellia-256' is unchecked, 'aes-128 ctr' is unchecked, 'aes-192 ctr' is unchecked, 'aes-256 ctr' is unchecked, 'aes-128 gcm' is unchecked, 'aes-192 gcm' is unchecked, and 'aes-256 gcm' is unchecked. At the bottom, there is a 'Lifetime' field set to '00:30:00' and a 'PFS Group' dropdown menu set to 'modp1024'.

Рис. 3.3. Шифрування трафіку в IPsec

Шифрування дозволяє приховати інформацію, що передається за тунелем, що не дозволяє зловмиснику прочитати дану інформацію навіть за умови її отримання.

Отже, Комунальному підприємству «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради важливо створити комплексну системи інформаційної безпеки. Визнаючи високі ставки, пов'язані з обігом конфіденційної інформації, необхідно впроваджувати заходи, які нейтралізують потенційні загрози, дотримуючись при цьому законодавчої бази України, федеральних законів та відповідних нормативно-правових актів.

Інженерно-технічні заходи безпеки, зосереджені на запобіганні доступу та розмежуванні повноважень користувачів, є важливим компонентом загальної системи безпеки. Водночас, програмно-апаратна система безпеки повинна гарантувати конфіденційність, цілісність і доступність оброблюваної інформації.

Організаційні методи, включаючи безпечний документообіг та дотримання

визначених протоколів безпеки, доповнюють технічні аспекти, забезпечуючи цілісний підхід до захисту інформації. Крім того, встановлення та використання надійного антивірусного програмного забезпечення, прикладом якого є Zillya Antivirus та Bitdefender Antivirus, є першочерговим компонентом захисту робочих станцій та серверів від шкідливих загроз.

Використання передових систем резервного копіювання, таких як Acronis Backup & Recovery 10 Advanced Server, має вирішальне значення для забезпечення цілісності даних і швидкого відновлення в разі втрати даних або збою в роботі системи. Ці системи забезпечують автоматизацію, дедуплікацію та централізоване керування, необхідні для підтримки безперервності роботи.

Для запобігання витоку інформації через перехоплення мережевого трафіку, впровадження технології IP в IP в поєднанні з шифруванням IPsec стає складним рішенням. Ця технологія не лише інкапсулює дані для безпечної передачі, але й забезпечує конфіденційність шляхом шифрування переданої інформації, перешкоджаючи потенційним зловмисникам.

Комплексна система інформаційної безпеки, запропонована в цьому документі, відображає цілісну і активну стратегію. Прийнявши ці рекомендації, підприємство може зміцнити свій захист від нових кіберзагроз, тим самим захистивши персональні дані співробітників і підтримуючи цілісність своїх операцій відповідно до правових стандартів.

Висновки до розділу 3

Більшість витоків персональних даних, як навмисних, так і ненавмисних, пов'язані з людським фактором, насамперед з діями працівників підприємств. Для мінімізації загрози масштабних витоків персональних даних, що стосуються споживачів, необхідний комплексний підхід. Удосконалення законодавчої бази, підвищення ефективності системи контролю та підвищення правової грамотності населення є першочерговими кроками. Крім того, обов'язкове впровадження заходів з інформаційної безпеки та кіберзахисту відповідно до українського законодавства

має стати пріоритетом. Держава повинна активно залучати наукові установи, навчальні заклади, організації, громадські об'єднання та громадян до розробки та впровадження заходів з кібербезпеки, доповнюючи це соціальною рекламою.

Аудит практики захисту персональних даних Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради підкреслює життєву важливість створення комплексної системи інформаційної безпеки. Ця система повинна відповідати нормативно-правовій базі та правилам і включати організаційні, технічні, програмні, криптографічні та правові засоби захисту. Важливим є багаторівневий захист, що включає інженерні та технічні заходи, спрямовані на запобігання доступу та розмежування повноважень користувачів.

Водночас, програмно-апаратна система безпеки повинна забезпечувати конфіденційність, цілісність і доступність оброблюваної інформації. Організаційні методи, включаючи безпечний документообіг і дотримання протоколів безпеки, доповнюють технічні аспекти, формуючи цілісний підхід до захисту інформації. Встановлення надійного антивірусного програмного забезпечення, наприклад, Zillya Antivirus та Bitdefender Antivirus, має вирішальне значення для захисту робочих станцій та серверів від зловмисних загроз.

Просунуті системи резервного копіювання, такі як Acronis Backup & Recovery 10 Advanced Server, відіграють ключову роль у забезпеченні цілісності даних і сприяють швидкому відновленню в разі втрати даних або збоїв у роботі системи. Ці системи з функціями автоматизації, дедуплікації та централізованого керування необхідні для підтримки безперервності роботи. Для запобігання витоку інформації через перехоплення мережевого трафіку, впровадження технології IPsec в IPsec в поєднанні з шифруванням IPsec є витонченим рішенням. Ця технологія інкапсулює дані для безпечної передачі і забезпечує конфіденційність, зменшуючи потенційні загрози.

Таким чином, запропонована комплексна система інформаційної безпеки в поєднанні з рекомендованими заходами забезпечує цілісну та проактивну стратегію. Впровадження цих рекомендацій посилить захист підприємства від нових кіберзагроз, захистить персональні дані та підтримає його операційну цілісність в межах правових стандартів.

ВИСНОВКИ

Під персональними даними працівника варто розуміти будь-яку інформацію, що стосується конкретної фізичної особи, яка працює на підставі трудового договору, і надана особисто такою особою роботодавцеві або зібрана останнім відповідно до законодавства. До персональних даних працівника відносять інформацію про вік, дату і місце народження, громадянство, реєстраційний номер облікової картки платника податків, трудову діяльність, стан здоров'я, рівень освіти, володіння українською та іноземними мовами, сімейний стан. І цей перелік не є вичерпний. Це пов'язано з тим, що необхідний перелік персональних даних працівників може відрізнятися за своїм змістом, виходячи з того, яку вони будуть займати посаду та виконувати трудову функцію.

Наголошено, що, з огляду вирішення проблеми захисту персональних даних працівника в умовах цифровізації, нагально необхідно здійснити систематизацію та кодифікацію національного законодавства у сфері персональних даних відповідно до норм європейського законодавства; розробити єдиний нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, захист персональних даних працівника. Цілком поділяємо думку О. Рим, що наблизитись до забезпечення балансу інтересів роботодавців і працівників під час обробки персональних даних останніх можна, якщо ця обробка відповідатиме таким вимогам: буде адекватною, доречною та обмежуватиметься досягненням необхідної мети; використання, мета та спосіб обробки повинні бути зрозумілі для працівників; працівники повинні мати можливість реалізувати свої права перевіряти, виправляти, припиняти та обмежувати обробку; персональні дані повинні зберігатись не більше, ніж потрібно; персональні дані повинні бути захищені відповідними технічними та організаційними заходами безпеки.

Припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав та свобод, встановлених нормативно-правовим актом чи договором спираються на комплекс основоположних ідей та засад, які в правовій науці називаються принципами. Розглянуті принципи захисту персональних даних

працівника складають фундаментальні засади, на яких функціонує механізм захисту персональних даних.

Персональні дані посідають особливе місце в інформаційних відносинах. Проблема їх захисту та поширення все життя супроводжує людину та пронизує будь-які сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і держави.

Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях всіх міжнародних стандартів, передбачає обов'язкове дотримання конкретних умов застосування персональних даних для будь-яких суб'єктів інформаційних відносин, при яких персональні дані повинні бути доступними для суб'єкта даних, точними і оновлюватися, отримані законним способом, оброблятися з конкретною метою та за згодою на це суб'єкта даних і в кількості мінімально необхідній для визначеної мети, використовуватися тільки згідно визначеної мети, захищеними від несанкціонованого доступу та незаконної обробки.

Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради як об'єкт дослідження здійснює міські перевезення пасажирів тролейбусами, трамваями та автобусами із застосуванням автоматизованої системи оплати проїзду. В останні роки підприємство було збитковим, про що свідчить формування чистого збитку у кожному з періодів досліджуваного діапазону. При чому за цим показником спостерігається тенденція до погіршення фінансово-економічного стану підприємства. Більшість ключових коефіцієнтів рентабельності підприємства хоч і мали позитивну динаміку, однак все ж таки мали від'ємне значення. А показник рентабельність операційної діяльності підприємства взагалі погіршився на 37,63 %.

Витрати підприємства представляють собою грошові потоки, пов'язані з наданням послуг, в тому числі з оплатою праці, витратами на закупівлю сировини та матеріалів, витратами на енергетику, транспорт та інфраструктуру, оплатою податків і зборів, іншими витратами підприємства. Аналіз структури операційних витрат

підприємства демонструє переважання у їх складі саме витрат на оплату праці працівників, які, крім того, мають намічену тенденцію до збільшення.

Комунальне підприємство «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради не в повній мірі використовує власні можливості. При цьому у останні роки підприємство послабило залежність від зовнішніх інвесторів і кредиторів, тобто є достатньо фінансово стійким. Також з позитивного можна відзначити 4-кратне перевищення власного капіталу над позиковими коштами.

Аналіз рівня ефективності управління персоналом в умовах Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради показав чітку відповідність персоналу за параметрами віку, статті, рівня освіти тощо специфічному виду діяльності підприємства, а саме забезпеченню курсування пасажирського наземного транспорту міського та приміського сполучення. Працівники мають переважно спеціальну технічну освіту. За гендерною ознакою помітне незначне перевищення частки зайнятих у штаті жінок.

На підприємстві розроблено Положення про роботу з персональними даними працівників, чітко визначено коло осіб, які мають доступ до цих даних, належним чином оформлено усі необхідні документи (зобов'язання про нерозголошення персональних даних співробітників, журнал обліку співробітників, які мають доступ до персональних даних, типовий порядок обробки персональних даних, повідомлення про обробку персональних даних працівників підприємства). Адже порушення у сфері захисту персональних даних працівників чреваті досить серйозними санкціями для адміністрації підприємства.

Більшість витоків персональних даних, як навмисних, так і ненавмисних, пов'язані з людським фактором, насамперед з діями працівників підприємств. Для мінімізації загрози масштабних витоків персональних даних, що стосуються споживачів, необхідний комплексний підхід. Удосконалення законодавчої бази, підвищення ефективності системи контролю та підвищення правової грамотності населення є першочерговими кроками. Крім того, обов'язкове впровадження заходів з інформаційної безпеки та кіберзахисту відповідно до українського законодавства має стати пріоритетом. Держава повинна активно залучати наукові установи,

навчальні заклади, організації, громадські об'єднання та громадян до розробки та впровадження заходів з кібербезпеки, доповнюючи це соціальною рекламою у цій сфері.

Аудит практики захисту персональних даних Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради підкреслює життєву важливість створення комплексної системи інформаційної безпеки. Ця система повинна відповідати нормативно-правовій базі та правилам і включати організаційні, технічні, програмні, криптографічні та правові засоби захисту. Важливим є багаторівневий захист, що включає інженерні та технічні заходи, спрямовані на запобігання доступу та розмежування повноважень користувачів.

Водночас, програмно-апаратна система безпеки повинна забезпечувати конфіденційність, цілісність і доступність оброблюваної інформації. Організаційні методи, включаючи безпечний документообіг і дотримання протоколів безпеки, доповнюють технічні аспекти, формуючи цілісний підхід до захисту інформації. Встановлення надійного антивірусного програмного забезпечення, наприклад, Zillya Antivirus та Bitdefender Antivirus, має вирішальне значення для захисту робочих станцій та серверів від зловмисних загроз.

Просунуті системи резервного копіювання, такі як Acronis Backup & Recovery 10 Advanced Server, відіграють ключову роль у забезпеченні цілісності даних і сприяють швидкому відновленню в разі втрати даних або збоїв у роботі системи. Ці системи з функціями автоматизації, дедуплікації та централізованого керування необхідні для підтримки безперервності роботи. Для запобігання витоку інформації через перехоплення мережевого трафіку, впровадження технології IPsec в IPsec в поєднанні з шифруванням IPsec є витонченим рішенням. Ця технологія інкапсулює дані для безпечної передачі і забезпечує конфіденційність, зменшуючи потенційні загрози.

Таким чином, запропонована комплексна система інформаційної безпеки в поєднанні з рекомендованими заходами забезпечує цілісну та проактивну стратегію. Впровадження цих рекомендацій посилить захист підприємства від нових кіберзагроз, захистить персональні дані та підтримає операційну цілісність в межах правових стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авраменко А.В. Принципи захисту персональних даних працівників. Актуальні проблеми держави і права : зб. наук. праць. Вип. 82 / редкол.: В.В. Завальнюк (голов. ред.) та ін. Одеса : Видавничий дім «Гельветика», 2019. С. 3–9.
2. Борисова Л.В., Тулупов В.В. Захист прав суб'єктів персональних даних. Форум права. 2013. № 1. С. 96–100.
3. Гуцу С.Ф. Захист персональних даних працівників на підприємствах, установах та організаціях. Гуманітарний часопис. 2012. № 4. С. 123–129.
4. Брижко В., Базанов Ю. [та ін.]. Е-майбутнє та інформаційне право ; за ред. д.е.н., проф. М. Швеця. [2-е вид., доп.]. К. : ТОВ «ПанТот», 2006. 234 с.
5. Брижко В., Радянська А., Швець М. Порівняльне-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. К. : Тріумф, 2006. 256 с.
6. Брижко В., Базанов Ю. [та ін.]. Електронний банкінг у контексті захисту персональних даних : за ред. чл.-кореспондента АПрН України М. Швеця. К. : ТОВ «ПанТот», 2008. 141 с.
7. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві : зб. матеріалів виступів на наук.-практ. конференції «Проблеми захисту прав людини в інформаційному суспільстві» (м. Київ, 1 липня 2016 р.). К. : Вид-во «Політехніка», 2016. С. 6–8.
8. Баранов О., Брижко В. Захист персональних даних в сфері Інтернет речей. Інформація і право. 2015. № 2(17). С. 75–81.
9. Сопілко І.М. Механізм захисту персональних даних: проблеми та перспективи. Юридичний вісник. 2013. № 2(27). С. 66–70.
10. Мельник К.С. Інституційно-правовий захист персональних даних в Європейському Союзі. Національний юридичний журнал: теорія і практика. 2014. № 3. С. 275–280.
11. Гнатюк С.Л. Актуальні питання захисту персональних даних у віртуальному

середовищі (на прикладі технологій та сервісів «хмарного» обчислення) [Електронний ресурс]: аналітична записка. – Режим доступу: <http://www.niss.gov.ua/articles/1090>. – Дата звернення: 11.12.2023.

12. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Електронний ресурс]: Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Strasbourg, 28.1.1981. – Режим доступу: <http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm>. – Дата звернення: 11.12.2023.

13. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних : посібн. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ «ПанТот», 2006. – 509 с.

14. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Електронний ресурс]: Reglamente (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. – Дата звернення: 11.12.2023.

15. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA [Електронний ресурс]: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу: <https://eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680&prev=search>. – Дата звернення: 11.12.2023.

16. On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [Електронний ресурс]: Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу: <https://consilium.europa.eu/en/press/press->

releases/2016/04/21-council-adopts-eu-pnr-directive/&prev=search. – Дата звернення: 11.12.2023.

17. On the Protection of Individuals with regard to the of Personal Data and on the free movement of such Data [Електронний ресурс]: Directiva 95/46/EC of the European Parliament and of the Council. – Режим доступу: <https://www.evropa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html>. – Дата звернення: 11.12.2023.

18. On the application of patients' rights in cross-border healthcare [Електронний ресурс]: Directive 2011/24/EU of the European Parliament and of the Council, of 9 March 2011. – Режим доступу: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L.2011.088.01.0045.01.ENG&toc=OJ:L:2011:088:TOC>. – Дата звернення: 11.12.2023.

19. On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [Електронний ресурс]: Council scope decision 2008/977/JHA, of 27 November 2008. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.350.01.0060.01.ENG&toc=OJ:L:2008:350:TOC. – Дата звернення: 11.12.2023.

20. On laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [Електронний ресурс]: Regulation (EU) No 182/2011 of the European Parliament and of the Council, of 16 February 2011. – Режим доступу: http://eurlex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2011.055.01.0001.01.ENG&toc=OJ:L:2011:055:TOC. – Дата звернення: 11.12.2023.

21. On combating terrorism: Council Framework Decision, of 13 June 2002 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2002.164.01.0003.01.ENG&toc=OJ:L:2002:164:TOC. – Дата звернення: 11.12.2023.

22. Посібник з європейського права у сфері захисту персональних даних. К. : К.І.С., 2020. 432 с.

23. Серода О. Актуальні питання правового механізму захисту персональних даних працівника в умовах європейської інтеграції. Юридичний науковий

електронний журнал. 2023. № 1. С. 207–211.

24. Рим О.М. Трудове право Європейського Союзу: моногр. Львів : ГАЛИЧ-ПРЕС, 2020. 596 с.

25. Основи ІТ права: навч. посібн. / Т.В. Бачинський, Р.І. Радейко та ін.; за заг. ред. Т.В. Бачинського. 3-тє вид., допов. та переробл. К. : Юрінком Інтер, 2021. 244 с.

26. Висновок Комітету з питань цифрової трансформації [Електронний ресурс]. – Режим доступу: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/1550956>. – Дата звернення 11.12.2023.

27. Про захист осіб у зв'язку з автоматичною обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 року № 108. Офіційний вісник України. 2011. № 1. С. 701.

28. Дяковський О.С. Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. Інформація і право. № 3 (22). 2017. С. 51–56.

29. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В.М. Брижко, А.І. Радянська, М.Я. Швець. К. : Тріумф, 2006. С. 22.

30. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/card/2657-12>. – Дата звернення 11.12.2023.

31. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>. – Дата звернення 11.12.2023.

32. Брель О. Персональні дані як об'єкт інформаційних правовідносин за участю суб'єктів господарювання. Право України. 2011. № 4. С. 220–224.

33. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні : навч. посібн. К. : Юстиніан, 2006. 117 с.

34. Брижко В.М. Модальність правової визначеності у сфері захисту та безпеки приватності персональних даних. Інформація і право. № 4 (39). 2021. С. 52–69.

35. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2009. 1726 с.

36. Шадська У. Захист персональних даних за правилами GDPR [Електронний ресурс]. – Режим доступу: [http:// espl.com.ua/news/zakhyst-personal-nykhdanykh-zapravylamy-gdpr](http://espl.com.ua/news/zakhyst-personal-nykhdanykh-zapravylamy-gdpr). – Дата звернення 11.12.2023.

37. Чанишева Г.І., Чанишев Р.І. Право на інформацію за трудовим законодавством України: монографія. Одеса : Фенікс, 2012. 196 с.

38. Оніщенко О.В. Персональні дані працівників: деякі особливості використання. Вісник Академії адвокатури. 2012. № 3(25). С. 173–175.

39. Сокол М.В., Тимошук АВ. Поняття персональних даних працівника та їх відмежування від іншої інформації. Право та державне управління. 2020. № 2. С. 48–54.

40. Мельник К.Ю. Захист персональних даних працівника: проблеми термінології. Актуальні проблеми приватного та публічного права : матер. V Міжнар. наук.-практ. конф., присв. 94-річчю з дня народження чл.-кор. НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора О.І. Процевського (31 березня 2023 р.). Харків, 2023. 624 с.

41. Середа О.Г., Красюк Т.В. Персональні дані працівника та їх захист в умовах цифровізації. Електронне наукове видання «Аналітично-порівняльне правознавство». – 2023. – № 3. С. 188–193. – Режим доступу: <http://journal-app.uzhnu.edu.ua/article/view/284674/278766>. – Дата звернення: 13.12.2023.

42. Колодій В.М. Принципи права: генеза, поняття, класифікація та реалізація. Альманах права. 2012. Вип. 3. С. 42–46.

43. Швидкій І.І. Особливості правового регулювання праці працівників ДАІ як суб'єктів трудових правовідносин : автореф. дис. канд. юр. наук : спец. 12.00.05 «Трудове право; право соціального забезпечення. Луганськ, 2009. 21 с.

44. Баранов О. Система принципів інформаційного права. Правова інформатика. 2006. № 2 (10). С. 5–15.

45. Про інформацію : Закон України від 02 жовтня 1992 р. № 2657-XII. Відомості

Верховної Ради України. 1992. № 48. Ст. 650.

46. Про захист персональних даних: Закон України від 01 червня 2010 р. №2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

47. Політанський В.С. Принципи інформаційно-правових відносин. Часопис Київського університету права. 2013. № 1. С. 55–60.

48. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посібн. К. : К.І.С., 2015. 220 с.

49. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус [Електронний ресурс] : Закон України від 20 листопада 2012 р. № 5492-VI. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/5492-17>. – Дата звернення: 13.12.2023.

50. Олійник О.В. Принципи забезпечення інформаційної безпеки України. Науковий вісник Ужгородського університету. Серія «Право». 2012. Вип. 18. С. 170–173.

51. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних та про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [Електронний ресурс]: Регламент Європейського парламенту та Ради від 27 квітня 2016 р. № 2016/679. – Режим доступу: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>. – Дата звернення: 13.12.2023.

52. Борисова Л.В., Тулупов В.В. Захист прав суб'єктів персональних даних. Форум права. 2013. № 1. С. 96–100.

53. Наливайко О.Ю. Методологічні аспекти класифікації персональних даних. Держава і право. 2014. Вип. 64. С. 167–172.

54. Брижко В.М. Захист персональних даних: реалії та практика сучасності. Інформація і право. 2013. №3(9). С. 31–48.

55. Гронь О.В., Погореленко А.К. Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського національного університету. 2018. Вип. 19, ч. 1. С. 102–108.

56. Кушинова Н.Г. Запровадження та розвиток сучасних персонал-технологій в управлінні персоналом / Н.Г. Кушинова // Вісник Запорізького національного університету. – 2018. – №4 (40). – С. 134–141.

57. Лясківський І. ССРА, GDPR, Закон України «Про захист персональних даних». Вони однакові? [Електронний ресурс]. – Режим доступу: <https://legalitgroup.com/ccpa-gdpr-zakon-ukrayini-pro-zahist-personalnih-danih-voniodnakovi/>. – Дата звернення: 15.12.2023.

58. Тунік А. Захист персональних даних: аналіз вітчизняного законодавства. Право України. 2011. №8. С. 97–100.

59. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн [Електронний ресурс]. Юридична газета. – Режим доступу: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html>. – Дата звернення: 15.12.2023.

60. Цифрова адженда України – 2020 [Електронний ресурс]: проєкт. – К.: HiTECH Office, 2016. – 90 с. – Режим доступу: https://issuu.com/mineconomdev/docs/digital_agenda_ukraine-v2__1_/83. – Дата звернення: 15.12.2023.

61. Ткачук В.О., Грибушин Б.М. Забезпечення відповідності використання блокчейн-технології в обробці персональних даних вимогам GDPR. Глокалізаційні аспекти інноваційного розвитку економіки: збірник матеріалів Всеукраїнської науково-практичної конференції молодих вчених (Одеса, 13 жовтня 2023 р.) [Електронний ресурс]. – Одеса: ОНЕУ, 2023. – С. 72–73.

62. Ткачук В.О., Грибушин Б.М. Обробка персональних даних співробітників підприємства в мережі блокчейн. Сучасні виклики сталого розвитку бізнесу : тези виступів IV Міжнар. наук.-практ. конф. Житомир : Житомирська політехніка, 2023. С. 187–188.

63. Офіційна веб-сторінка Житомирського ТТУ [Електронний ресурс]. – Режим доступу: <https://ttu.zt.ua>. – Дата звернення: 20.12.2023.

64. Послуги Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради [Електронний ресурс]. – Режим доступу: <https://ttu.zt.ua/poslugi.html>. – Дата звернення: 20.12.2023.

65. Персональні дані співробітників: що важливо знати кадровику [Електронний ресурс]. – Режим доступу: <https://uteka.ua/ua/publication/commerce-12-dokumentooborot-2-personalnye-dannye-sotrudnikov-chto-vazhno-znat-kadroviku>. – Дата звернення: 21.12.2023.

ДОДАТКИ

ДОДАТОК А

Додаток А

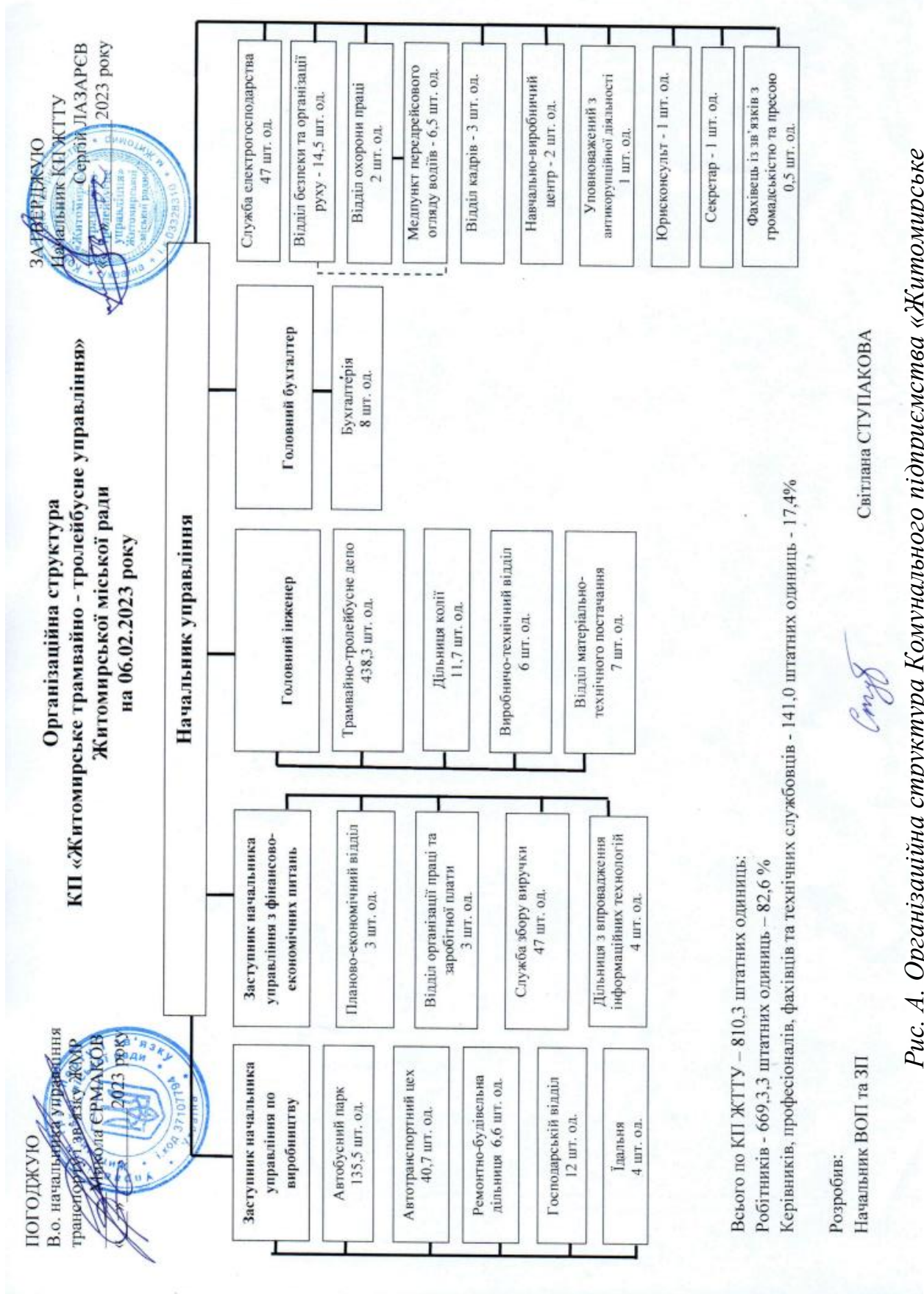


Рис. А. Організаційна структура Комунального підприємства «Житомирське трамвайно-тролейбусне управління» Житомирської міської ради станом на 06.02.2023 р.

Підприємство **Комунальне підприємство " Житомирське трамвайно-тролейбусне управління"**
Житомирської міської ради

Територія **ЖИТОМИРСЬКА**

Організаційно-правова форма господарювання **Комунальне підприємство**

Вид економічної діяльності **Пасажирський наземний транспорт міського та приміського сполучення**

Середня кількість працівників ² **871**

Адреса, телефон **вулиця Вітрука, буд. 11, м. ЖИТОМИР, ЖИТОМИРСЬКА обл., 10025**

Одиниця виміру: тис. грн. без десяткового знака (окрім розділу IV Звіту про фінансові результати (Звіту про сукупний дохід) (форма №2), грошові показники якого наводяться в гривнях з копійками)

Складено (зробити позначку "v" у відповідній клітинці):
за національними положеннями (стандартами) бухгалтерського обліку
за міжнародними стандартами фінансової звітності

Дата (рік, місяць, число) **2022/12/31**

за ЄДРРНО **03328310**

Коди
UA18040190010057814
150
49.31

Катод **1**

КОПФГ

КВЕД

V

Баланс (Звіт про фінансовий стан)
на 31 грудня 2021 р.

Форма №1 Код за ДКУД **1801001**

А К Т И В	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Необоротні активи			
Нематеріальні активи	1000	8	9
первісна вартість	1001	562	566
накопичена амортизація	1002	554	557
Незавершені капітальні інвестиції	1005	67 016	17 907
Основні засоби	1010	248 967	351 182
первісна вартість	1011	347 349	483 177
знос	1012	98 382	131 995
Інвестиційна нерухомість	1015	-	-
первісна вартість інвестиційної нерухомості	1016	-	-
знос інвестиційної нерухомості	1017	-	-
Довгострокові біологічні активи	1020	-	-
первісна вартість довгострокових біологічних активів	1021	-	-
накопичена амортизація довгострокових біологічних активів	1022	-	-
Довгострокові фінансові інвестиції:			
які обліковуються за методом участі в капіталі інших підприємств	1030	-	-
інші фінансові інвестиції	1035	-	-
Довгострокова дебіторська заборгованість	1040	-	-
Відстрочені податкові активи	1045	-	-
Гудвіл	1050	-	-
Відстрочені аквізиційні витрати	1060	-	-
Залишок коштів у централізованих страхових резервних фондах	1065	-	-
Інші необоротні активи	1090	-	-
Усього за розділом I	1095	315 991	369 098
II. Оборотні активи			
Запаси	1100	13 507	14 693
виробничі запаси	1101	13 467	14 608
незавершене виробництво	1102	-	-
готова продукція	1103	-	-
товари	1104	40	85
Поточні біологічні активи	1110	-	-
Депозити перестрахування	1115	-	-
Векселі одержані	1120	-	-
Дебіторська заборгованість за продукцію, товари, роботи, послуги	1125	1 681	1 060
Дебіторська заборгованість за розрахунками:			
за виданими авансами	1130	3 613	4 080
з бюджетом	1135	289	289
у тому числі з податку на прибуток	1136	289	289
Дебіторська заборгованість за розрахунками з нарахований доходів	1140	-	-
Дебіторська заборгованість за розрахунками із внутрішніх розрахунків	1145	-	-
Інша поточна дебіторська заборгованість	1155	718	863
Поточні фінансові інвестиції	1160	-	-
Гроші та їх еквіваленти	1165	5 463	3 669
готівка	1166	136	119
рахунки в банках	1167	5 292	3 516
Витрати майбутніх періодів	1170	233	264
Частка перестраховика у страхових резервах	1180	-	-
у тому числі в:			
резервах довгострокових зобов'язань	1181	-	-
резервах збитків або резервах належних виплат	1182	-	-

резервах незароблених премій	1183	-	-
інших страхових резервах	1184	-	-
Інші оборотні активи	1190	5	3
Усього за розділом II	1195	25 509	24 921
III. Необоротні активи, утримувані для продажу, та групи вибуття	1200	-	-
Баланс	1300	341 500	394 019

Пасив	Код рядка	На початок звітної періоду	На кінець звітної періоду
1	2	3	4
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400	322 737	322 737
Внески до незареєстрованого статутного капіталу	1401	-	-
Капітал у дооцінках	1405	-	-
Додатковий капітал	1410	17 181	17 656
емісійний дохід	1411	-	-
накопичені курсові різниці	1412	-	-
Резервний капітал	1415	-	-
Нерозподілений прибуток (непокритий збиток)	1420	(246 528)	(272 623)
Неоплачений капітал	1425	(20 890)	(6 008)
Вилучений капітал	1430	(-)	(-)
Інші резерви	1435	-	-
Усього за розділом I	1495	72 500	61 762
II. Довгострокові зобов'язання і забезпечення			
Відстрочені податкові зобов'язання	1500	-	-
Пенсійні зобов'язання	1505	-	-
Довгострокові кредити банків	1510	205 939	260 795
Інші довгострокові зобов'язання	1515	-	-
Довгострокові забезпечення	1520	-	-
довгострокові забезпечення витрат персоналу	1521	-	-
Цільове фінансування	1525	-	13 030
благодійна допомога	1526	-	-
Страхові резерви	1530	-	-
у тому числі:	1531	-	-
резерв довгострокових зобов'язань			
резерв збитків або резерв належних виплат	1532	-	-
резерв незароблених премій	1533	-	-
інші страхові резерви	1534	-	-
Інвестиційні контракти	1535	-	-
Призовий фонд	1540	-	-
Резерв на виплату джек-поту	1545	-	-
Усього за розділом II	1595	205 939	273 825
III. Поточні зобов'язання і забезпечення			
Короткострокові кредити банків	1600	-	-
Векселі видані	1605	-	-
Поточна кредиторська заборгованість за:			
довгостроковими зобов'язаннями	1610	-	28 977
товари, роботи, послуги	1615	47 251	12 910
розрахунками з бюджетом	1620	1 460	1 699
у тому числі з податку на прибуток	1621	-	-
розрахунками зі страхування	1625	1 348	971
розрахунками з оплати праці	1630	5 292	5 064
Поточна кредиторська заборгованість за одержаними авансами	1635	78	127
Поточна кредиторська заборгованість за розрахунками з учасниками	1640	-	-
Поточна кредиторська заборгованість із внутрішніх розрахунків	1645	153	99
Поточна кредиторська заборгованість за страховою діяльністю	1650	-	-
Поточні забезпечення	1660	1 169	1 992
Доходи майбутніх періодів	1665	3 199	2 632
Відстрочені комісійні доходи від перестраховиків	1670	-	-
Інші поточні зобов'язання	1690	3 111	3 961
Усього за розділом III	1695	63 061	58 432
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття	1700	-	-
V. Чиста вартість активів недержавного пенсійного фонду	1800	-	-
Баланс	1900	341 500	394 019

Керівник

Головний бухгалтер

ЕП ЛАЗАРСВ
СЕРГІЙ
ЮРІЙОВИЧ
ЕП ЛУТАЙ
Валентина
Михайлівна

Лазарсв Сергій Юрійович

Лутай Валентина Михайлівна

¹ Кодифікатор адміністративно-територіальних одиниць та територій територіальних громад.

² Визначається в порядку, встановленому центральним органом виконавчої влади, що реалізує державну політику у сфері статистики.

Підприємство	Комунальне підприємство " Житомирське трамвайно-тролейбусне управління" Житомирської міської ради	Дата (рік, місяць, число)	2023	01	01
Територія	ЖИТОМИРСЬКА	за ЄДРПОУ	03228210	ДОКУМЕНТ ПРИЙНЯТО 112 000 101 5001005/814	
Організаційно-правова форма господарювання	Комунальна власність	за КОПФГ	150		
Вид економічної діяльності	Пасажирський наземний транспорт міського та приміського сполучення	за КВЕД	49.31		
Середня кількість працівників	2 725				
Адреса, телефон	вулиця Вітрука, буд. 11, м. ЖИТОМИР, ЖИТОМИРСЬКА обл., 10025	334921			
Одиниця виміру: тис. грн. без десяткового знака (окрім розділу IV Звіту про фінансові результати (Звіту про сукупний дохід) (форма №2), грошові показники якого наводяться в гривнях з копійками)					
Складено (зробити позначку "v" у відповідній клітинці):					
за національними положеннями (стандартами) бухгалтерського обліку					
за міжнародними стандартами фінансової звітності					

Баланс (Звіт про фінансовий стан)
на 31 грудня 2022 р.

Форма №1 Код за ДКУД 1801001

А К Т И В	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Необоротні активи			
Нематеріальні активи	1000	9	12
первісна вартість	1001	566	570
накопичена амортизація	1002	557	558
Незавершені капітальні інвестиції	1005	17 907	23 583
Основні засоби	1010	351 182	316 239
первісна вартість	1011	483 177	488 273
знос	1012	131 995	172 034
Інвестиційна нерухомість	1015	-	-
первісна вартість інвестиційної нерухомості	1016	-	-
знос інвестиційної нерухомості	1017	-	-
Довгострокові біологічні активи	1020	-	-
первісна вартість довгострокових біологічних активів	1021	-	-
накопичена амортизація довгострокових біологічних активів	1022	-	-
Довгострокові фінансові інвестиції:			
які обліковуються за методом участі в капіталі інших підприємств	1030	-	-
інші фінансові інвестиції	1035	-	-
Довгострокова дебіторська заборгованість	1040	-	-
Відстрочені податкові активи	1045	-	-
Гудвіл	1050	-	-
Відстрочені аквізиційні витрати	1060	-	-
Залишок коштів у централізованих страхових резервних фондах	1065	-	-
Інші необоротні активи	1090	-	-
Усього за розділом I	1095	369 098	339 834
II. Оборотні активи			
Запаси	1100	14 693	14 988
виробничі запаси	1101	14 608	14 902
незавершене виробництво	1102	-	-
готова продукція	1103	-	38
товари	1104	85	47
Поточні біологічні активи	1110	-	-
Депозити перестрахування	1115	-	-
Векселі одержані	1120	-	-
Дебіторська заборгованість за продукцію, товари, роботи, послуги	1125	1 060	1 883
Дебіторська заборгованість за розрахунками:			
за виданими авансами	1130	4 080	9 990
з бюджетом	1135	289	289
у тому числі з податку на прибуток	1136	289	289
Дебіторська заборгованість за розрахунками з нарахованих доходів	1140	-	-
Дебіторська заборгованість за розрахунками із внутрішніх розрахунків	1145	-	-
Інша поточна дебіторська заборгованість	1155	863	660
Поточні фінансові інвестиції	1160	-	-
Гроші та їх еквіваленти	1165	3 669	9 653
готівка	1166	119	77
рахунки в банках	1167	3 516	9 330
Витрати майбутніх періодів	1170	264	371
Частка перестраховика у страхових резервах	1180	-	-
у тому числі в:			
резервах довгострокових зобов'язань	1181	-	-
резервах збитків або резервах належних виплат	1182	-	-

резервах незароблених премій	1183	-	-
інших страхових резервах	1184	-	-
Інші оборотні активи	1190	3	3
Усього за розділом II	1195	24 921	37 837
III. Необоротні активи, утримувані для продажу, та групи вибуття	1200	-	-
Баланс	1300	394 019	377 671

Пасив	Код рядка	На початок звітної періоду	На кінець звітної періоду
1	2	3	4
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400	322 737	757 737
Внески до незареєстрованого статутного капіталу	1401	-	-
Капітал у дооцінках	1405	-	-
Додатковий капітал	1410	17 656	17 597
емісійний дохід	1411	-	-
накопичені курсові різниці	1412	-	-
Резервний капітал	1415	-	-
Нерозподілений прибуток (непокритий збиток)	1420	(272 623)	(367 452)
Неоплачений капітал	1425	(6 008)	(100 726)
Вилучений капітал	1430	(-)	(-)
Інші резерви	1435	-	-
Усього за розділом I	1495	61 762	307 156
II. Довгострокові зобов’язання і забезпечення			
Відстрочені податкові зобов'язання	1500	-	-
Пенсійні зобов’язання	1505	-	-
Довгострокові кредити банків	1510	260 795	36 501
Інші довгострокові зобов’язання	1515	-	-
Довгострокові забезпечення	1520	-	-
довгострокові забезпечення витрат персоналу	1521	-	-
Цільове фінансування	1525	13 030	13 030
благодійна допомога	1526	-	-
Страхові резерви	1530	-	-
у тому числі:	1531	-	-
резерв довгострокових зобов’язань			
резерв збитків або резерв належних виплат	1532	-	-
резерв незароблених премій	1533	-	-
інші страхові резерви	1534	-	-
Інвестиційні контракти	1535	-	-
Призовий фонд	1540	-	-
Резерв на виплату джек-поту	1545	-	-
Усього за розділом II	1595	273 825	49 531
III. Поточні зобов’язання і забезпечення			
Короткострокові кредити банків	1600	-	-
Векселі видані	1605	-	-
Поточна кредиторська заборгованість за:			
довгостроковими зобов'язаннями	1610	28 977	-
товари, роботи, послуги	1615	12 910	11 910
розрахунками з бюджетом	1620	1 699	307
у тому числі з податку на прибуток	1621	-	-
розрахунками зі страхування	1625	971	28
розрахунками з оплати праці	1630	5 064	2 560
Поточна кредиторська заборгованість за одержаними авансами	1635	127	107
Поточна кредиторська заборгованість за розрахунками з учасниками	1640	-	-
Поточна кредиторська заборгованість із внутрішніх розрахунків	1645	99	70
Поточна кредиторська заборгованість за страховою діяльністю	1650	-	-
Поточні забезпечення	1660	1 992	2 930
Доходи майбутніх періодів	1665	2 632	2 350
Відстрочені комісійні доходи від перестраховиків	1670	-	-
Інші поточні зобов'язання	1690	3 961	722
Усього за розділом III	1695	58 432	20 984
IV. Зобов’язання, пов’язані з необоротними активами, утримуваними для продажу, та групами вибуття	1700	-	-
V. Чиста вартість активів недержавного пенсійного фонду	1800	-	-
Баланс	1900	394 019	377 671

Керівник

ЕП ЛАЗАРЄВ

СЕРГІЙ

ЮРІЙОВИЧ

ЕП Лутай

Валентина

Михайлівна

Лазарєв Сергій Юрійович

Лутай Валентина Михайлівна

Головний бухгалтер

ЕП ЛАЗАРЄВ

СЕРГІЙ

ЮРІЙОВИЧ

ЕП Лутай

Валентина

Михайлівна

Лазарєв Сергій Юрійович

Лутай Валентина Михайлівна

1. Кодифікатор адміністративно-територіальних одиниць та територій територіальних громад.

2. Визначається в порядку, встановленому центральним органом виконавчої влади, що реалізує державну політику у сфері статистики.

Підприємство

Комунальне підприємство " Житомирське трамвайно-тролейбусне управління" Житомирської міської ради

(найменування)

Звіт про фінансові результати (Звіт про сукупний дохід)

за

Рік 2021

р.

Дата (рік, місяць, число)

за ЄДРПОУ

КОДИ

2022

01

01

03328310

ДОКУМЕНТ ПРИЙНЯТО

Форма № 2 Код за ДКУД

1801003

I. ФІНАНСОВІ РЕЗУЛЬТАТИ

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	81 256	58 534
Чисті зароблені страхові премії	2010	-	-
премії підписані, валова сума	2011	-	-
премії, передані у перестраховування	2012	-	-
зміна резерву незароблених премій, валова сума	2013	-	-
зміна частки перестраховиків у резерві незароблених премій	2014	-	-
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(257 805)	(209 501)
Чисті понесені збитки за страховими виплатами	2070	-	-
Валовий:			
прибуток	2090	-	-
збиток	2095	(176 549)	(150 967)
Дохід (витрати) від зміни у резервах довгострокових зобов'язань	2105	-	-
Дохід (витрати) від зміни інших страхових резервів	2110	-	-
зміна інших страхових резервів, валова сума	2111	-	-
зміна частки перестраховиків в інших страхових резервах	2112	-	-
Інші операційні доходи	2120	189 468	158 851
у тому числі:	2121	-	-
дохід від зміни вартості активів, які оцінюються за справедливою вартістю			
дохід від первісного визнання біологічних активів і сільськогосподарської продукції	2122	-	-
дохід від використання коштів, вивільнених від оподаткування	2123	-	-
Адміністративні витрати	2130	(6 825)	(6 805)
Витрати на збут	2150	(-)	(-)
Інші операційні витрати	2180	(18 099)	(33 783)
у тому числі:	2181	-	-
витрати від зміни вартості активів, які оцінюються за справедливою вартістю			
витрати від первісного визнання біологічних активів і сільськогосподарської продукції	2182	-	-
Фінансовий результат від операційної діяльності:			
прибуток	2190	-	-
збиток	2195	(12 005)	(32 704)
Дохід від участі в капіталі	2200	-	-
Інші фінансові доходи	2220	94	109
Інші доходи	2240	2 466	2 039
у тому числі:	2241	-	164
дохід від благодійної допомоги			
Фінансові витрати	2250	(14 688)	(7 004)
Втрати від участі в капіталі	2255	(-)	(-)
Інші витрати	2270	(1 962)	(1 410)
Прибуток (збиток) від впливу інфляції на монетарні статті	2275	-	-

Фінансовий результат до оподаткування:			
прибуток	2290	-	-
збиток	2295	(26 095)	(38 970)
Витрати (дохід) з податку на прибуток	2300	-	-
Прибуток (збиток) від припиненої діяльності після оподаткування	2305	-	-
Чистий фінансовий результат:			
прибуток	2350	-	-
збиток	2355	(26 095)	(38 970)

II. СУКУПНИЙ ДОХІД

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Дооцінка (уцінка) необоротних активів	2400	-	-
Дооцінка (уцінка) фінансових інструментів	2405	-	-
Накопичені курсові різниці	2410	-	-
Частка іншого сукупного доходу асоційованих та спільних підприємств	2415	-	-
Інший сукупний дохід	2445	-	-
Інший сукупний дохід до оподаткування	2450	-	-
Податок на прибуток, пов'язаний з іншим сукупним доходом	2455	-	-
Інший сукупний дохід після оподаткування	2460	-	-
Сукупний дохід (сума рядків 2350, 2355 та 2460)	2465	(26 095)	(38 970)

III. ЕЛЕМЕНТИ ОПЕРАЦІЙНИХ ВИТРАТ

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Матеріальні затрати	2500	64 512	56 891
Витрати на оплату праці	2505	131 154	113 331
Відрахування на соціальні заходи	2510	32 060	28 031
Амортизація	2515	38 691	19 598
Інші операційні витрати	2520	16 312	32 238
Разом	2550	282 729	250 089

IV. РОЗРАХУНОК ПОКАЗНИКІВ ПРИБУТКОВОСТІ АКЦІЙ

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Середньорічна кількість простих акцій	2600	-	-
Скоригована середньорічна кількість простих акцій	2605	-	-
Чистий прибуток (збиток) на одну просту акцію	2610	-	-
Скоригований чистий прибуток (збиток) на одну просту акцію	2615	-	-
Дивіденди на одну просту акцію	2650	-	-

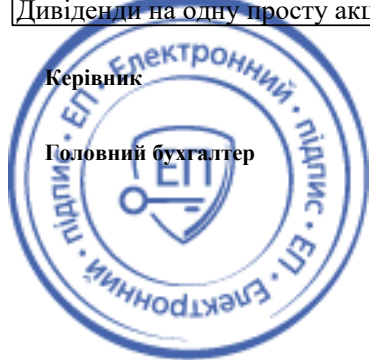
Керівник

Головний бухгалтер

СЕРГІЙ
ЮРІЙОВИЧ
ЕП ЛУТАЙ
Валентина
Михайлівна

Лазарев Сергій Юрійович

Лутай Валентина Михайлівна



Підприємство **Комунальне підприємство " Житомирське трамвайно-тролейбусне управління" Житомирської міської ради**

(найменування)

Звіт про фінансові результати (Звіт про сукупний дохід)

за

Рік 2022

р.

Дата (рік, місяць, число)

за ЄДРПОУ

КОДИ

2023

01

01

03328310

ДОКУМЕНТ ПРИЙНЯТО

Форма № 2 Код за ДКУД 1801003

I. ФІНАНСОВІ РЕЗУЛЬТАТИ

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	88 627	81 256
Чисті зароблені страхові премії	2010	-	-
премії підписані, валова сума	2011	-	-
премії, передані у перестрахування	2012	-	-
зміна резерву незароблених премій, валова сума	2013	-	-
зміна частки перестраховиків у резерві незароблених премій	2014	-	-
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(242 698)	(257 805)
Чисті понесені збитки за страховими виплатами	2070	-	-
Валовий:			
прибуток	2090	-	-
збиток	2095	(154 071)	(176 549)
Дохід (витрати) від зміни у резервах довгострокових зобов'язань	2105	-	-
Дохід (витрати) від зміни інших страхових резервів	2110	-	-
зміна інших страхових резервів, валова сума	2111	-	-
зміна частки перестраховиків в інших страхових резервах	2112	-	-
Інші операційні доходи	2120	175 823	189 468
у тому числі:	2121	-	-
дохід від зміни вартості активів, які оцінюються за справедливою вартістю			
дохід від первісного визнання біологічних активів і сільськогосподарської продукції	2122	-	-
дохід від використання коштів, вивільнених від оподаткування	2123	-	-
Адміністративні витрати	2130	(6 974)	(6 825)
Витрати на збут	2150	(-)	(-)
Інші операційні витрати	2180	(97 642)	(18 099)
у тому числі:	2181	-	-
витрати від зміни вартості активів, які оцінюються за справедливою вартістю			
витрати від первісного визнання біологічних активів і сільськогосподарської продукції	2182	-	-
Фінансовий результат від операційної діяльності:			
прибуток	2190	-	-
збиток	2195	(82 864)	(12 005)
Дохід від участі в капіталі	2200	-	-
Інші фінансові доходи	2220	522	94
Інші доходи	2240	1 409	2 466
у тому числі:	2241	-	-
дохід від благодійної допомоги			
Фінансові витрати	2250	(13 705)	(14 688)
Втрати від участі в капіталі	2255	(-)	(-)
Інші витрати	2270	(191)	(1 962)
Прибуток (збиток) від впливу інфляції на монетарні статті	2275	-	-

Фінансовий результат до оподаткування:			
прибуток	2290	-	-
збиток	2295	(94 829)	(26 095)
Витрати (дохід) з податку на прибуток	2300	-	-
Прибуток (збиток) від припиненої діяльності після оподаткування	2305	-	-
Чистий фінансовий результат:			
прибуток	2350	-	-
збиток	2355	(94 829)	(26 095)

II. СУКУПНИЙ ДОХІД

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Дооцінка (уцінка) необоротних активів	2400	-	-
Дооцінка (уцінка) фінансових інструментів	2405	-	-
Накопичені курсові різниці	2410	-	-
Частка іншого сукупного доходу асоційованих та спільних підприємств	2415	-	-
Інший сукупний дохід	2445	-	-
Інший сукупний дохід до оподаткування	2450	-	-
Податок на прибуток, пов'язаний з іншим сукупним доходом	2455	-	-
Інший сукупний дохід після оподаткування	2460	-	-
Сукупний дохід (сума рядків 2350, 2355 та 2460)	2465	(94 829)	(26 095)

III. ЕЛЕМЕНТИ ОПЕРАЦІЙНИХ ВИТРАТ

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Матеріальні затрати	2500	71 160	64 512
Витрати на оплату праці	2505	114 499	131 154
Відрахування на соціальні заходи	2510	28 195	32 060
Амортизація	2515	40 695	38 691
Інші операційні витрати	2520	92 765	16 312
Разом	2550	347 314	282 729

IV. РОЗРАХУНОК ПОКАЗНИКІВ ПРИБУТКОВОСТІ АКЦІЙ

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Середньорічна кількість простих акцій	2600	-	-
Скоригована середньорічна кількість простих акцій	2605	-	-
Чистий прибуток (збиток) на одну просту акцію	2610	-	-
Скоригований чистий прибуток (збиток) на одну просту акцію	2615	-	-
Дивіденди на одну просту акцію	2650	-	-

Керівник

ЕП ЛАЗАРЄВ
СЕРГІЙ
ЮРІЙОВИЧ
ЕП ЛУТАЙ
Валентина
Михайлівна

Лазарев Сергій Юрійович

Головний бухгалтер

Лутай Валентина Михайлівна

