Шифр: «Save Data21»

НАУКОВА РОБОТА

на тему: «Забезпечення захисту персональних даних співробітників підприємств у цифровій економіці з використанням технології блокчейн»

ЗМІСТ

ВСТУП

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. Зокрема, велику увагу світової спільноти привернув перебіг онлайн-кампанії фірми «Cambridge Analytica», якій, на думку багатьох експертів, завдячує своєю перемогою тоді ще кандидат у президенти США Д. Трамп. Було встановлено, що фірма вдалася до несанкціонованого доступу до персональних даних 50 млн. користувачів соцмережі «Facebook» для визначення політичних симпатій американців та впливу на них через релевантну рекламу та публікації [23].

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 [14, 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 [3, 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 [6, с. 107]. Разом із тим, залишають недостатньо дослідженими питання забезпечення захисту персональних даних співробітників підприємств у цифровій економіці із застосуванням сучасних децентралізованих високонавантажуваних баз даних (наприклад, блокчейн).

Актуальність зазначеної наукової проблеми зумовила вибір теми, постановку мети і завдань дослідження, логіку та структуру представленої роботи. Так, *метою* написання наукової роботи є розкриття теоретичних і практичних аспектів захисту персональних даних співробітників підприємств в умовах цифрової економіки з використанням технології блокчейн.

Для досягнення мети в науковій роботі поставлено та вирішено такі *завдання:*

– з’ясувати економічний зміст персональних даних співробітників та їх складові;

– визначено основи забезпечення захисту персональних даних співробітників;

– розкрито міжнародну практику захисту персональних даних на підприємствах;

– наведено способи моніторингу персональних даних співробітників;

– розкрито особливості обробки персональних даних співробітників з

використанням технології блокчейн;

– наведено способи забезпечення відповідності використання блокчейн-технології в обробці персональних даних вимогам GDPR.

Об'єктом дослідження у науковій роботі є персональні дані співробітників підприємств.

Предметом дослідження виступає механізм забезпечення захисту персональних даних співробітників підприємств у цифровій економіці з використанням технології блокчейн.

У науковій роботі використовувались загальнонаукові та спеціальні *методи дослідження*. Зокрема, у першому розділі застосовувався метод *абстрагування*, що дозволив зосередитися на найважливіших особливостях персональних даних співробітників та забезпеченні їх захисту на підприємствах. Використання методу *гіпотези* дало можливість сформувати висновки про відповідність рівня захисту персональних даних співробітників вимогам положень вітчизняних та міжнародних законодавчих актів. У другому розділі наукової роботи вирішальну роль при формуванні проміжних і підсумкових результатів відіграли спеціальні методи дослідження. Так, за допомогою історичного методу вдалося проілюструвати розвиток офіційних сервісів, що дозволяють перевірити достовірність документів особи, методу спостереження – розкрити особливості забезпечення захисту персональних даних співробітників підприємств.

Наукова новизна одержаних результатів полягає в поглибленні теоретичних і методичних аспектів забезпечення захисту персональних даних співробітників підприємств у цифровій економіці з використанням технології блокчейн. Найбільш суттєві наукові результати, що характеризують новизну проведеного дослідження та розкривають основний зміст наукової роботи, полягають у такому:

набули подальшого розвитку:

– методика моніторингу персональних даних співробітників, що авторами представляється як сукупність застосовуваних для аналізу даних про співробітників (або пошукачів вакансій) окремих відкритих інформаційних систем (офіційних сервісів) та сервісів комплексної перевірки фізичних осіб, що дозволяють

встановити дійсність особистих документів осіб, які проходять перевірку, підтвердити чи спростувати факт їх викрадення чи втрати та ін.;

– обґрунтовано перелік проблемних моментів надання згоди фізичною особою на обробку її персональних даних, а також самої процедури обробки персональних даних, що дало можливість виснувати про однакову значимість для забезпечення захищеності персональних даних зусиль як самих працівників, так і роботодавців.

Практичне значення одержаних результатів полягає в розробці науково-методичних і практичних рекомендацій щодо забезпечення захисту персональних даних співробітників підприємств в умовах цифрової економіки з використанням технології блокчейн. Висновки та рекомендації проведеного дослідження мають практичне значення, про що свідчить упровадження наукових результатів ДП «Крупозавод Озерянка» ТОВ «ІПС» (*Save Data21*) (довідка про впровадження від 20.01.21 р.).

Апробація результатів наукової роботи. Основні положення та найважливіші результати проведеного дослідження доповідалися на міжнародних науково-практичних конференціях «Сучасні виклики сталого розвитку бізнесу» (*Save Data21*, 5–6 листопада 2020 р.) і «Актуальні проблеми управління соціально-економічними системами» (м. Луцьк, 11 грудня 2020 р.).

За результатами наукових досліджень авторами опубліковано 2 наукові праці загальним обсягом 0,24 д.а., з них 2 у матеріалах конференцій, а саме:

1. *Save Data21*. Захист персональних даних в цифровій економіці / *Save Data21* // Сучасні виклики сталого розвитку бізнесу: тези виступів Міжнар. наук. конф. (5–6 листопада 2020 р.). – *Save Data21*, 2020. – С. 84.

2. *Save Data21*. Бази для обробки персональних даних співробітників підприємств та їх характеристика / *Save Data21* // Актуальні проблеми управління соціально-економічними системами: матеріали VI Міжнар. наук.-практ. інтернет-конф. (11 грудня 2020 р.). – Луцьк: ІВВ Луцького НТУ, 2020. – С. 117–118.

Наукова робота складається зі вступу, двох розділів, висновків, списку використаних джерел і додатків. Написана на 30 сторінках основного змісту. Містить 6 рисунків, 30 найменувань використаних джерел, 5 додатки.

РОЗДІЛ 1
ОСНОВИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВ

1.1. Економічний зміст персональних даних співробітників та їх складові

Роботодавці збирають і обробляють персональні дані своїх працівників щодня та з різними цілями. Дані можуть стосуватися виплат працівникам заробітної плати, відпускних, обліку лікарняних, виплат у зв'язку з вагітністю та пологами, оцінки результатів роботи та ін. Частину такої інформації на підприємстві зобов'язані збирати та обробляти відповідно до трудового законодавства, інша частина даних обробляється для внутрішніх цілей.

Необхідно враховувати всі вимоги Загального положення про захист даних (General Data Protection Regulation, GDPR) [25] та особливості національного законодавства, які потребують постійного моніторингу, оскільки держави-члени можуть встановлювати свої власні правила та обмеження. Окремі закони країн і колективні договори підприємств можуть передбачити більш конкретні правила для забезпечення захисту прав і свобод щодо обробки персональних даних працівників.

Згідно з підходом General Data Protection Regulation (далі – GDPR), персональні дані представляють собою будь-яку інформацію, що відноситься до ідентифікованої фізичної особи (суб'єкт даних), по якій прямо або опосередковано можна її визначити [10, с. 51]. До такої інформації можна віднести [15]: ім'я; дані про місцезнаходження; онлайн ідентифікатор (обліковий запис); один або декілька факторів, характерних для фізичної, генетичної, розумової, економічної, культурної та соціальної ідентичності цієї фізичної особи.

Визначення широке і достатньо чітко дає зрозуміти, що навіть IP-адреси користувачів також можуть бути персональними даними. Важливо відмітити, що існують деякі типи даних, що відносяться до категорії особливих або конфіденційних персональних даних. Це інформація, що містить: расове або етнічне походження, політичні погляди, релігійні або філософські переконання та членство

в профспілках. Окрім того, до цієї групи відносяться генетичні та біометричні дані, що можуть бути використані для ідентифікації фізичної особи, дані про стан здоров'я, відомості, що стосуються сексуального життя або орієнтації.

Вичерпний перелік суб'єктів відносин, пов'язаних із персональними даними, визначається ст. 4 Закону України «Про захист персональних даних» [17]. У відповідності до цього закону до суб'єктів відносин, пов'язаних із персональними даними, відносять:

– суб'єкта персональних даних (фізична особа, персональні дані якої оброблюються);

– володільця та розпорядника бази персональних даних – ними можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону;

– третю особу – будь-яка інша особа, якій володілець або розпорядник бази персональних даних здійснює передачу цих даних;

– уповноважений державний орган з питань захисту персональних даних;

– інші державні органи та органи місцевого самоврядування, які здійснюють захист персональних даних.

Загалом існує шість законних баз для обробки персональних даних співробітників, і щоб обробка таких даних на певному підприємстві відповідала вимогам GDPR, служба персоналу має базувати свою діяльність з обробки персональних даних на одній із цих баз. З цього переліку баз роботодавці зазвичай покладаються на перші чотири (рис. 1.1):

Рис. 1.1. Законні бази (підстави) для обробки персональних даних співробітників

Говорячи про згоду, дану за відносинами працівника та роботодавця, дуже важко в результаті отримати її в належному вигляді. Якщо працівник хоче

відмовити роботодавцю в такій згоді, завжди існує ймовірність того, що він враховує можливі наслідки своїх дій. І дана згода по суті дозволяє працівнику уникнути неприємних ситуацій або поганих відносин з роботодавцем. Якщо на підприємстві як база для обробки персональних даних використовується саме згода, то у працівника має бути вільний вибір щодо надання або ненадання такої згоди, а також право відкликати її без наслідків для своєї посади. Спеціалісти служби персоналу підприємства повинні добре знати національне законодавство та володіти інформацією про те, чи існують певні ситуації або типи обробки даних, коли немає можливості обробити дані працівників навіть за наявності згоди.

Якщо мова йде про виконання співробітниками умов договору, то тут вже існують певні персональні дані, які потрібно обробити, щоб кожній із сторін виконати свої зобов'язання за договором. Наприклад, для виплати зарплати потрібно обробити реквізити рахунків працівників та іншу особисту інформацію. Крім того існує спеціальна категорія персональних даних, які потребують додаткового захисту, оскільки обробка таких типів даних може спричиняти серйозні та неприйнятні ризики для основних прав і свобод людини. Ця категорія даних включає питання, що стосуються расового чи етнічного походження працівників, релігійних переконань, біометричних даних, даних про стан здоров'я та ін.

Іншою законною підставою, на яку покладається багато підприємств при обробці персональних даних працівників (крім державних органів), є законний інтерес. Законні інтереси включають обробку даних, необхідну для цілей законних інтересів роботодавця або законних інтересів третьої сторони. Виняток становлять ті випадки, коли ці інтереси перекриваються основними правами та свободами суб'єкта даних, що вимагають захисту персональних даних, особливо якщо особа є дитиною чи неповнолітньою. І нарешті, дотримання законодавчих зобов'язань вимагає від підприємств обробляти персональні дані працівників для виконання своїх юридичних зобов'язань. Наприклад, податкове законодавство може вимагати розкриття інформації про заробітну плату місцевій владі.

Коли спеціалісти служби персоналу обирають відповідну законну базу (підставу, основу) для обробки персональних даних своїх працівників, вони

зобов’язані надати співробітникам інформацію про те [27]:

– для яких конкретних цілей будуть використовуватися персональні дані;

– якою є законна основа для обробки таких даних;

– як відбувається дотримання прав працівників під час обробки їх персональних даних;

– хто на підприємстві може надати більше інформації про обробку персональних даних;

– хто є кінцевими одержувачами цих даних;

– як довго будуть зберігати персональні дані співробітників у розпорядженні особи чи служби, яка здійснює їх обробку.

Виходячи з цього, для того, щоб працівники підприємства були краще поінформовані щодо процедури обробки персональних даних, служба персоналу може розкрити методику обробки персональних даних співробітників у відповідному довіднику підприємства. Самих працівників потрібно оперативно повідомляти про будь-які зміни в обробці їх персональних даних у таких деталях, щоб кожен з них міг зрозуміти наслідки обробки.

Зберігати особисті дані працівників слід не довше, ніж це дійсно необхідно, особливо якщо особа більше не працює на підприємстві. Однак можуть бути законні причина зберігати особисті дані колишніх працівників досить тривалий час, наприклад, у відповідності до національного трудового законодавства, законодавства про охорону здоров’я чи податкового законодавства.

Отже, у різних цілях роботодавці проводять збір і обробку персональних даних своїх співробітників. Під такими даними загалом розуміють будь-яку інформацію, що відноситься до ідентифікованої фізичної особи, по якій прямо або опосередковано можна її визначити. З-поміж усіх можливих законних баз для обробки персональних даних співробітників роботодавці в основному покладаються на згоду, договір, законний інтерес і необхідність дотримання законодавчих зобов’язань. Втім не залежно від обраної бази служба персоналу підприємства має обов’язково поінформувати співробітників про те, якою є законна основа для обробки таких даних, хто є кінцевими одержувачами цих даних, як довго будуть

зберігати персональні дані співробітників у розпорядженні особи чи служби, яка здійснює їх обробку та ін. Найкраще це реалізувати у вигляді розробленої службою персоналу методики обробки персональних даних співробітників у відповідному довіднику підприємства.

1.2. Забезпечення захисту персональних даних співробітників

Загалом захист – це заходи, що здійснюються системою для контролю доступу, захисту даних (конфіденційність, цілісність, доступність), опис процесів і процедур, захисту від атак, технічної підтримки, тренування та підготовка персоналу [22, с. 83]. Захист персональних даних є сукупністю правових, організаційних і технічних заходів, спрямованих на недопущення неправомірних дій з персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми персональними даними. Крім того, у Вікіпедії захист персональних даних представляється як комплекс заходів технічного, організаційного та організаційно-технічного характеру, спрямованих на захист відомостей, що відносяться до певної або визначеної на підставі такої інформації фізичної особи (суб'єкта персональних даних) [9].

Забезпечення захисту персональних даних у базах персональних даних покладається на володільця персональних даних. Згідно із Законом України «Про захист персональних даних» №2297-VI від 01.06.2010 р., володілець персональних даних представляє собою фізичну або юридичну особу, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки. Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, зокрема від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них.

Такий захист важливий із погляду на значну кількість персональних даних, що обробляються володільцями персональних даних за допомогою управляючих

елементів веб-ресурсів у мережі Інтернет. Найчастіше персональні дані із використанням веб-ресурсів обробляються у межах таких процесів, як:

– заповнення відвідувачами веб-ресурсів анкет;

– реєстрація та отримання логіна та пароля;

– реєстрація з використанням облікового запису соціальної мережі;

– надання електронної адреси відвідувача для зворотного зв'язку.

Вважаємо за доцільне окремо відзначити такі процеси, як:

1) подання для розгляду кандидатури особи на вакантне робоче місце резюме чи CV через онлайн-сервіси як самого підприємства, так і спеціалізованих сайтів (work.ua, rabora.ua тощо). В резюме дуже часто людина розкриває про себе практично всю персональну інформацію, до якої при цьому легко отримати доступ;

2) соціальне онлайн-опитування респондентів – навіть анонімне опитування працівників за певним порядком розставлених питань дозволяє безпомилково ідентифікувати людину.

При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних персональних даних, які одночасно є відомостями про особу, яка ідентифікована, до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися у процесі ідентифікації особи: відомостей про оплату послуг з використанням платіжних карт, логіни та паролі, записи у соціальній мережі, номери телефонів, електронні адреси тощо.

Основою для використання персональних даних співробітників є надана ними згода на обробку цих даних. Надання суб'єктом персональних даних письмової згоди на збір, обробку та використання даних на перший погляд видається логічним кроком у взаємовідносинах між працівниками та адміністрацією підприємства. Проте реальний стан справ щодо використання таких згод яскраво засвідчує їх недосконаліть. Зокрема, серед проблем у практиці застосування згоди на обробку персональних даних співробітників (і звичайно клієнтів) підприємств необхідно відзначити такі [18]:

1) безальтернативність згоди – люди зазвичай не мають змоги змінити текст «згоди на обробку персональних даних», наприклад, обмеживши можливість

передачі інформації третім особам або визначивши час, після якого персональні дані мають бути видалені;

2) непропорційність обсягу персональних даних та повноважень на їхню обробку – підприємствам, які збирають та ведуть бази персональних даних, зручно просити у своїх співробітників і клієнтів надати згоду одразу за всіма можливими положеннями, щоб у разі будь-яких змін у бізнес-процесах робота з базами даних залишалася формально санкціонованою;

3) надмірність та неможливість відслідкувати надані згоди – замовляючи товари чи послуги (клієнт), або виконуючи свої посадові обов'язки, що передбачають роботу особливого характеру (працівник), особа вимушена регулярно підписувати бланки згоди на обробку своїх персональних даних. У результаті цього практично кожен клієнт (або працівник) опиняється в ситуації, коли ним підписано багато згод на обробку персональних даних, часто з надмірним обсягом повноважень щодо їхньої обробки та використання, проте немає жодної можливості встановити всіх суб'єктів, яким така згода була надана;

4) паперова бюрократія – багато підприємств добросовісно витрачають час і ресурси на розробку бланків, оформлення та зберігання заяв про надання згоди на обробку персональних даних і намагаються вести власні бази персональних даних згідно з вимогами чинного законодавства. Разом із тим, беручи до уваги зазначене вище такі витрати підприємств не видаються виправданими та не посилюють захист персональних даних;

5) незахищеність персональних даних – вимога щодо необхідності підписання згоди на обробку персональних даних на практиці не захищає від недобросовісного їх поширення. Наприклад, у відкритому доступі досі розміщені так звані «телефонні довідники», в яких можна знайти повне ім'я особи, її адресу, номер телефону, дату народження на ін.

Також важливо відзначити ряд проблем, які виникають безпосередньо під час обробки персональних даних співробітників. Насамперед, тут варто відзначити відсутність чіткого розуміння складових персональних даних і видів інформації про особу, які відносяться законодавством до персональних даних –законодавством

України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону України «Про захист персональних даних» до різноманітних ситуацій, в т. ч. при обробці персональних даних в інформаційних базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в економічній, соціальній та інших сферах суспільного життя [19, с. 67]. Крім того, сьогодні відсутнє належне нормативно-правове регулювання порядку проведення та механізмів проведення перевірок приміщень, де обробляються персональні дані – сьогодні представники уповноваженого органу мають право безперешкодно потрапляти до будь-якого приміщення, де обробляються персональні дані (тобто практично до кожного офісу та в кожну квартиру), що є рівнозначним праву на проведення обшуку, яке до сьогодні мали лише правоохоронні органи [17].

Іншим проблемним моментом, що потребує надійної системи захисту персональних даних в процесі їх обробки, є розміщення цих даних в мережі Інтернет. Оскільки персональні дані є або можуть бути об'єктом використання в автоматизованій системі обробки, люди, користуючись Інтернет, залишають там велику кількість своїх даних. І, що головне, використання даних нічим не обмежене і не врегульоване, тобто фактично такі дані залишаються не захищеними. Такі бази даних постійно вдосконалюються, уніфікуються і щораз більше стосуються приватного життя людини [24].

Щоб захистити свої персональні дані від протиправних посягань, особа може використовувати будь-які не заборонені законом засоби. Зокрема, у випадку незаконної обробки персональних даних та втручання в особисте життя особи, суб'єкт персональних даних вправі звернутися до володільця та/або розпорядника персональних даних з вмотивованою вимогою:

– заборонити таку обробку;

– внести зміни до своїх персональних даних (у випадку їх недостовірності);

– вимагати їх видалення (знищення).

Разом із тим для підвищення захищеності персональних даних співробітників

мають застосовувати заходи і самі роботодавці. Так, багато дослідників охорони персональних даних висловлюють думку, про те, що персональні дані мають бути поділені на персональні дані загального характеру та вразливі персональні дані. Поділ персональних даних на дані загального характеру (прізвище, ім'я, по батькові, дата та місце народження, громадянство, місце проживання) та вразливі персональні дані (про стан здоров'я – історія хвороби, діагнози тощо; етнічна належність; ставлення до релігії; ідентифікаційні коди чи номери; підпис; відбитки пальців, записи голосу, фотографії; про розмір доходів, про вклади та рахунки в банках, нерухомість, податковий статус; кредитна історія; дані про судимість та інші форми притягнення особи до кримінальної, адміністративної чи дисциплінарної відповідальності; результати професійного тестування тощо) передбачено європейськими стандартами. Взагалі європейськими нормативними актами забороняється збирання, зберігання, використання та поширення без згоди суб'єкта саме вразливих персональних даних, а не взагалі всіх персональних даних, як це зроблено у вітчизняному законодавстві [20, с. 97].

Отже, необхідність обробки персональних даних співробітників на підприємствах актуалізує потребує забезпечення їх надійного захисту. Захист персональних даних представляє собою сукупність заходів, спрямованих на недопущення неправомірних дій з персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми даними. Щоб захистити свої персональні дані від протиправних посягань, особа може використовувати будь-які не заборонені законом засоби, серед яких можна виокремити вимогу припинити обробку даних, змінити або видалити дані тощо.

1.3. Міжнародна практика захисту персональних даних на підприємствах

Підхід Європейського Союзу до забезпечення захисту персональних даних базується на розвитку «цифрових знань» і «цифрової грамотності», які мають

підвищити рівень безпеки обороту персональних даних в цифровому середовищі. Також «цифрові знання» покликані поглибити розуміння користувачами інтернет-ресурсів непублічних персональних даних і можливих наслідків їх просочування у відкритий доступ [30].

За межами Європейського Союзу (далі – ЄС) дотримуватися загального регламенту захисту даних (EU GDPR) повинні будуть насамперед (рис. 1.2):

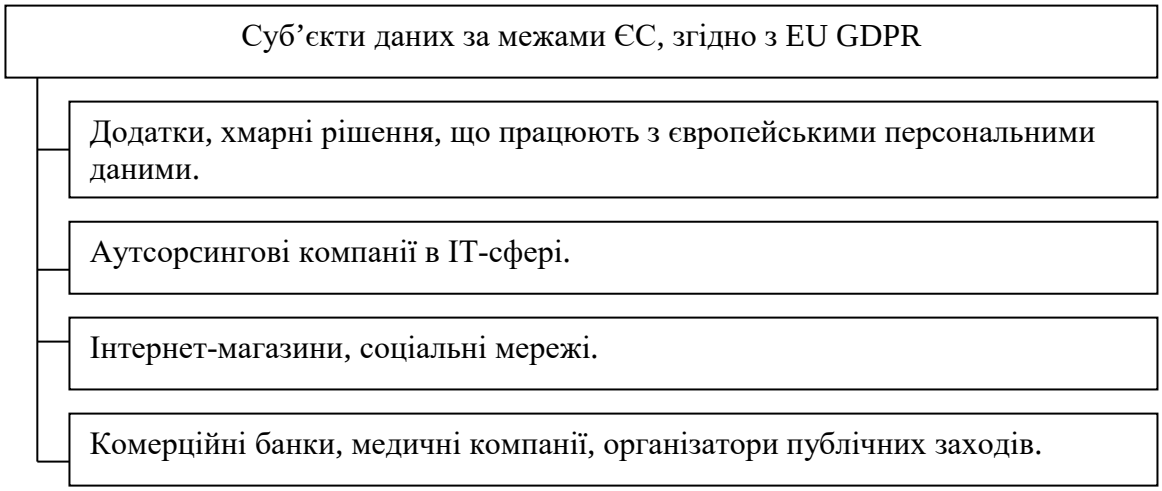

Рис. 1.2. Суб'єкти даних за межами ЄС

В разі недотримання вимог GDPR підприємства (організації, установи) ризикують втратити європейських клієнтів, ринки збуту та бути оштрафованими за порушення норм до 20 млн. євро або на 2–4% від свого річного обороту. При визначенні необхідності дотримуватися вимог GDPR підприємства можуть керуватися наступними вказівками (Додаток А):

Якщо підприємство попадає під дію нового європейського регламенту про захист даних, або планує поставку товарів чи послуг в країни ЄС, то рекомендується провести комплексне оцінювання методів і засобів обробки персональних даних, що використовуються на підприємстві, та привести їх у відповідність до нових правил GDPR. Також потрібно переглянути політику конфіденційності та положення рамкових угод з користувачами щодо обробки їх персональних даних.

Для відповідності вимогам GDPR необхідно розробити внутрішню політику захисту даних, навчити персонал, провести перевірку діяльності з обробки даних, налагодити процес документування процесів обробки, впровадити заходи з організації системи конфіденційності, а також призначити співробітника,

відповідального за обробку персональних даних.

Хоча нові вимоги до обробки персональних даних достатньо серйозні та жорсткі, в них є і позитивні сторони для вітчизняних підприємств, зокрема:

– простіше дотримуватися єдиного набору правил захисту і обробки даних, ніж враховувати національні нюанси обробки персональних даних кожної окремої європейської країни, як це доводилося робити до введення GDPR;

– реформа направлена на стимулювання економічного росту шляхом скорочення витрат та бюрократії для підприємств, що працюють в ЄС;

– дотримання одного правила замість 28 (кількість країн-членів ЄС) допоможе малим і середнім підприємствам вийти на нові ринки;

– в деяких випадках зобов'язання можуть змінюватися в залежності від розміру бізнесу, природи даних, що оброблюються, та інших факторів.

Підприємствам необхідно заздалегідь продумати механізми реагування на запити європейських регуляторів і суб'єктів персональних даних, що можливі в рамках GDPR, наприклад, про уточнення даних, їх видалення, припинення обробки чи передачі іншому підприємству в рамках права на переміщення даних.

Сучасний європейський підхід до обробки персональних даних може бути викладений у вигляді наступних принципів:

1) законність, справедливість та прозорість – персональні дані повинні оброблятися законно, справедливо та прозоро. Будь-яку інформацію про мету, методи та обсяги обробки персональних даних слід викладати максимально доступно та просто;

2) обмеження застосування – персональні дані необхідно збирати та використовувати виключно з метою, що була заявлена підприємством (або онлайн-сервісом);

3) мінімізація даних – забороняється збирати особисті дані в більшому обсязі, ніж той, що потрібен для досягнення мети обробки;

4) точність – особисті дані, які являються неточними, повинні бути видалені або виправлені (за вимогою користувача);

5) обмеження зберігання – персональні дані мають зберігатися у формі, яка

дозволяє ідентифікувати суб’єкти даних на строк не більше, ніж це необхідно для досягнення мети обробки;

6) цілісність та конфіденційність – при обробці даних співробітників і клієнтів підприємство зобов’язане забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення та пошкодження.

Щодо технічних засобів, необхідних для реалізації дотримання норм GDPR, потрібно визнати, що жодне окреме рішення не може забезпечити відповідність підприємства положенням про захист даних. Вимоги надто широкі і покривають усі аспекти – від управління до зобов’язань за контрактом. Проте, на думку В. Нужного, допомогти підприємству досягти відповідності зобов’язанням із убезпечення даних може набір рішень Gemalto’s SafeNet (Додаток Б).

Ядром системи для захисту даних тут виступає програмно-апаратний комплекс Keysecure, призначений для створення, зберігання та управління життєвим циклом криптографічних ключів для шифрування даних. Навколо Keysecure, в залежності від типу даних, що мають захищатися, архітектури системи зберігання даних та сервісів, що беруть участь в обробці, можуть бути застосовані наступні програмні продукти Gemalto:

1) ProtectV – для шифрування дисків віртуальних машин VMWare, AWS, Azure;

2) ProtectDB – для шифрування баз даних Oracle, MS SQL, IBM DB2, Teradata;

3) ProtectFile – для вибіркового шифрування папок та файлів на робочих станціях користувачів та файлових серверах Windows або Linux.

Що стосується питання захисту персональних даних в інших країнах, традиційно, найбільш розвиненою юрисдикцією вважається США. Однією з причин необхідності розвитку такого законодавства є значна кількість порушень у сфері персональних даних. У зв’язку з цим у 2020 р. у штаті Каліфорнія був прийнятий новий закон про захист персональних даних, що базувався на положеннях California Consumer Privacy Act 2018 (далі – CCPA). Насамперед, його важливість полягає в тому, що в Каліфорнії знаходяться такі компанії як Facebook, Google, Apple, що працюють з персональними даними користувачів по всьому світу [21].

Метою закону є захист персональних даних, які обробляють юридичні особи

приватного права та є розпорядниками такої інформації. Саме тому цим законом користувачам надається право дізнатися відомості про те, як компанія розпоряджається їхніми даними, а також можливість вимагати видалення інформації про себе та зупинення її розповсюдження. За невиконання вимог закону передбачені значні штрафи у кілька тисяч доларів, навіть якщо компанія порушує законодавство через необережність. Таким чином, завдяки впровадженню цього закону Каліфорнія підвищила дисциплінованість та відповідальність юридичних осіб під час роботи з персональними даними фізичних осіб.

Щодо CCPA варто відзначити, що цей акт встановлює більш широку предметну юрисдикцію, вказуючи, що дія акту поширюється на правові відносини щодо збору, обробки та продажу персональної інформації осіб, включаючи розкриття такої інформації з метою досягнення бізнес-цілей [13]. Дія CCPA поширюється на компанії, які ведуть свою бізнес-діяльність у штаті Каліфорнія, тобто ведуть діяльність з метою отримання фінансового, матеріального або грошового прибутку. Окрім того, відповідно до Податкового кодексу штату, компанії, які розташовані поза межами штату, також, за певних умов, можуть бути визнані такими, що ведуть у ньому свою бізнес-діяльність у межах штату. Однак, якщо компанія збирає та продає персональні дані поза межами штату, то CCPA не має над нею влади.

Отже, міжнародна практика захисту персональних даних співробітників на підприємствах спирається насамперед на положення норм GDPR і CCPA. Якщо підприємство попадає під дію європейського регламенту про захист даних, або планує поставку товарів чи послуг в країни ЄС, то воно має провести комплексне оцінювання методів і засобів обробки персональних даних і привести їх у відповідність до правил GDPR. Для цього необхідно розробити внутрішню політику захисту даних, навчити персонал, провести перевірку діяльності з обробки даних, налагодити процес документування процесів обробки, впровадити заходи з організації системи конфіденційності та ін. CCPA встановлює більш широку предметну юрисдикцію, вказуючи, що дія акту поширюється на правові відносини щодо збору, обробки та продажу персональної інформації осіб, включаючи розкриття такої інформації з метою досягнення бізнес-цілей.

РОЗДІЛ 2
МОНІТОРИНГ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ТА СПОСОБИ ПІДВИЩЕННЯ РІВНЯ ЇХ ЗАХИСТУ НА ПІДПРИЄМСТВАХ

2.1. Способи моніторингу персональних даних співробітників

В контексті моніторингу персональних даних співробітників службою персоналу, насамперед, варто відзначити, що існують сервіси комплексної перевірки фізичних осіб, наприклад, YouControl, Clarify Project або OpenDataBot. Вони акумулюють інформацію з кількох офіційних реєстрів за ключовими даними особи. Так, якщо в таких сервісах ввести повне ім’я людини, то можна отримати інформацію про адресу її реєстрації. Там будуть вказані вулиця, будинок, номер квартири, а також поштовий індекс. Утім це стосується тільки людей, які є фізичними особами-підприємцями, засновниками або керівниками підприємства. Якщо людина є фізичною особою-підприємцем, то на цій же сторінці можна побачити вид її діяльності.

Сервіси дають інформацію про наявність податкового боргу, його розмір, причини утворення і стягувача. Якщо людина, яку шукають, є національним публічним діячем (політиком, керівником державного підприємства та ін.), то ця інформація внесена в окремому підпункті досьє сервісів. Там зазначається, чи пов’язана людина родинними або бізнес-зв’язками з публічними діячами. Якщо людина є у розшуку або потрапила під дію закону про люстрацію, це теж буде зазначено в досьє на сайтах-агрегаторах.

Маючи реєстраційний номер облікової картки платника податків (далі – РНОКПП), можна дізнатися, яким автомобілем володіє людина. Агрегатори надають. За наявності РНОКПП можна дізнатися інформацію про нерухомість особи. Нерухомість можна знайти і в Державному реєстрі прав на нерухоме майно. Там можна шукати за адресою, якщо відоме розташування житла, але невідомим залишається його власник. Щоправда, інформаційна довідка з цього реєстру не є безкоштовною, а авторизуватися в системі можна лише через єдиний цифровий

підпис (далі – ЄЦП).

У реєстрі «Судова влада» та на сайтах-агрегаторах є інформація про те, де, з ким і за що людина судилася. Вказуються тип справи, назва суду, статус учасника справи – позивач чи відповідач. Крім деталей справи, там зазначаються час і місце її розгляду, якщо справа ще триває.

Якщо людина є власником бізнесу або очолює якусь організацію, відомості про цей бізнес теж легко знайти на сайтах-агрегаторах. Там можна дізнатися адресу підприємства, відомості про його власника та бенефіціара, чим займається організація, з ким вона пов'язана, та чи були порушення в роботі.

Послуги таких сервісів є платними, хоч і доступними для кожного. Але кожна фізична особа має можливість цілком безкоштовно перевірити відкриті дані про себе за допомогою офіційних реєстрів, що діють в Україні. Зокрема, Державна міграційна служба України (далі – ДМС України) має сервіс для проведення перевірки за базою недійсних документів. **Сервіс «Перевірка недійсних документів»** доступний за посиланням: *https://nd.dmsu.gov.ua/*. Він дозволяє перевірити дійсність: паспорта громадянина України, закордонного паспорту, тимчасового посвідчення громадянина України, посвідки на тимчасове або постійне проживання та ін. Наприклад, для перевірки дійсності паспорту громадянина України у формі картки достатньо (рис. 2.1):

1) обрати цей тип документа серед наявного переліку;

2) ввести серію та номер документа (для паспорта звичайного зразку) або комбінацію з 9 цифр (для паспорту у формі картки);

3) пройти reCAPTCHA, що призначена для блокування ботів.

Як бачимо, в результаті уведення довільної комбінації з 9 цифр (у ID-картці саме стільки) система по суті підтвердила дійсність паспорту громадянина (на скріншотах частина цифр нами навмисно прихована).

Знаючи номер дійсного паспорту (ID-картки), можна перевірити його на предмет викрадення або втрати власником. Для цього ідеально підходить **сервіс «Розшук»** Міністерства внутрішніх справ України (далі – МВС України), що доступний за посиланням: *https://wanted.mvs.gov.ua/passport/*.

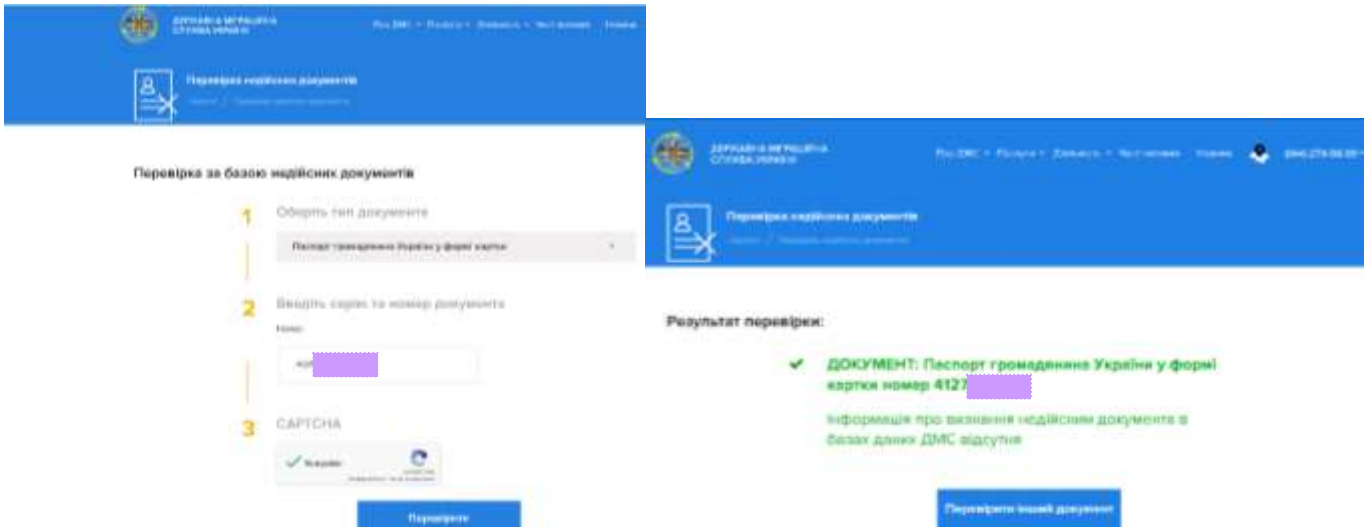

Рис. 2.1. Робота з сервісом «Перевірка недійсних документів» ДМС України

Достатньо лише ввести серію і номер паспорту (або лише номер для ID-картки) – і сервіс виведе дані про перебування / не перебування цього документу серед викрадених / втрачених (рис. 2.2):

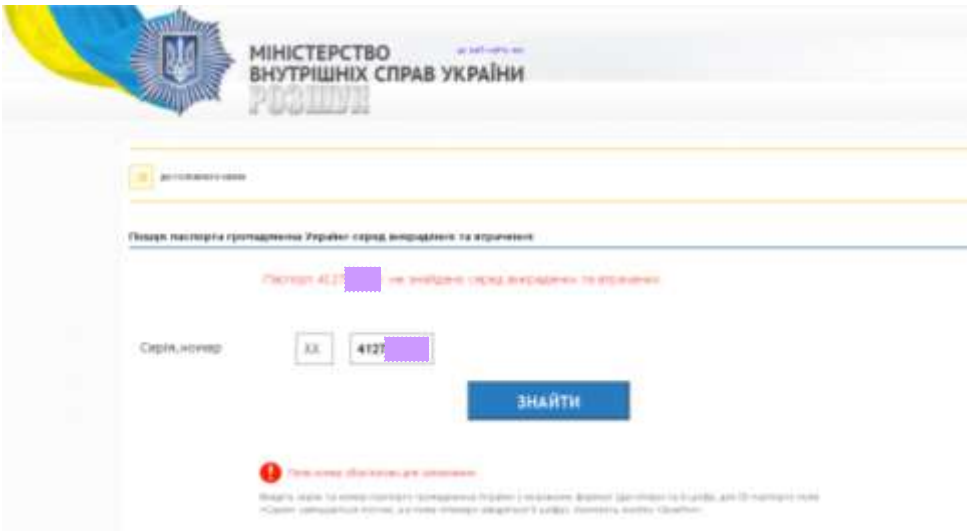

Рис. 2.2. Робота з сервісом «Розшук» МВС України

Якщо людина представляє собою особу, уповноважену на виконання функцій держави або місцевого самоврядування і в обов'язковому порядку веде персональну декларацію, то інформацію про неї можна отримати в Єдиному державному реєстрі декларацій (сервіс доступний за посиланням: *https://public.nazk.gov.ua/*) (рис. 2.3).

Швидко ознайомившись із роботою сервісу, можна виснувати, що виключно за повним ім'ям людини можна без труднощів з'ясувати наступну інформацію: місце роботи; назву займаної посади; перелік об'єктів нерухомості, які є у розпорядженні людини; інформацію про членів сім'ї суб'єкта декларування; джерела доходу та ін.

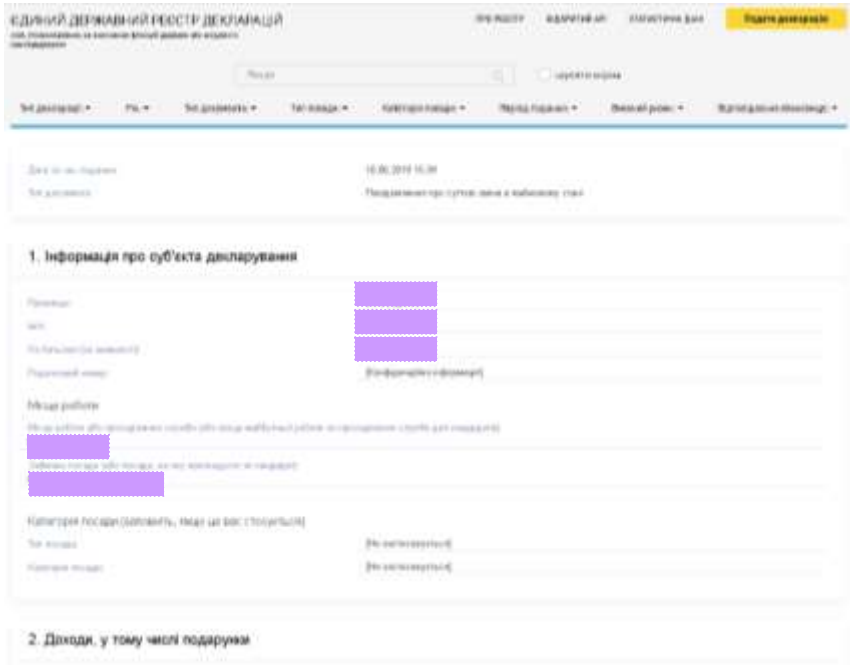

Рис. 2.3. Робота з Єдиним державним реєстром декларацій

Отже, моніторинг персональних даних співробітників можливий шляхом застосування для аналізу даних про співробітників (або пошукачів вакансій) окремих відкритих інформаційних систем (офіційних сервісів), що дозволяють встановити дійсність особистих документів осіб, які проходять перевірку, підтвердити чи спростувати факт їх викрадення чи втрати тощо, та сервісів комплексної перевірки фізичних осіб.

2.2. Обробка персональних даних співробітників з використанням технології блокчейн

У світі, де персональні дані оброблялися централізовано, був розроблений GDPR. Активний розвиток в останні роки саме децентралізованих систем обробки персональної інформації ставить перед експертами все нові запитання та виклики. У зв’язку з цим 8 листопада 2018 року Commission Nationale Informatique Libertes (CNIL/DPA) надала роз’яснення щодо особливостей обробки персональних даних співробітників з використанням технології блокчейн. Блокчейн – це своєрідна база даних, у якій дані зберігаються і розподілені між великою кількістю вузлів

(комп'ютерів) та записи про які доступні всім користувачам мережі [2, с. 205; 28]. Схематично функціонування блокчейну можна відобразити таким чином (рис. 2.4):

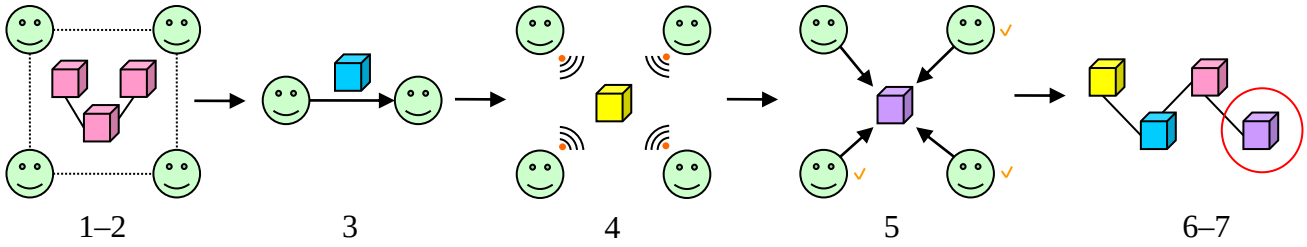

Рис. 2.4. Функціонування блокчейну в контексті роботи з персональними даними

Примітка: 1 – блокчейн існує у вигляді регістру в формі ланцюга з блоків інформації; 2 – кожен вузол (комп'ютер) має власну копію регістру; 3 – кожна нова транзакція представлена у вигляді блоку інформації; 4 – блок інформації доступний кожному вузлу в мережі; 5 – істинність кожного нового блоку інформації має бути підтверджена більшістю вузлів мережі; 6 – лише після підтвердження істинності блоку він додається до ланцюга регістра; 7 – після додавання нового блоку інформації до ланцюга регістра він не може бути видалений чи змінений.

З огляду на те, що провідні компанії світу активно впроваджують блокчейн у власний бізнес, можна зазначити, що використання даної технології є доцільним та перспективним. Головним недоліком у цьому є лише достатньо висока вартість розробки власної високонавантаженої бази даних [4, с. 35].

З блокчейн програмні додатки більше не мають потреби в розгортанні на централізованому сервері: їх можна запускати в тимчасовій мережі, яка не контролюється якоюсь однією стороною. Ці додатки на основі блокчейн можуть використовуватися для координації дій великої чисельності людей, які можуть організувати свою діяльність без допомоги третьої сторони. Технологія блокчейн – це засіб, за допомогою якого люди можуть координувати спільні дії, безпосередньо взаємодіяти один з одним і керувати собою більш безпечним і децентралізованим способом [12, с. 140].

Загалом виділяють публічний та приватний види блокчейну [8, с. 211]. Публічний блокчейн повністю децентралізований. У такому блокчейні відсутні особи, які володіють контролем над ним. Будь-яка особа може бачити транзакції та надсилати власні транзакції на підтвердження. Приватний блокчейн, зі свого боку, базується на тих самих принципах, однак його адміністрування здійснюється конкретними особами або корпоративно. Для підключення до такого блокчейну необхідний дозвіл адміністратора.

Блокчейн може містити персональні дані двох типів:

1. Ідентифікуючі дані учасників мережі, зокрема їхній публічний та приватний ключ. Публічний ключ представляє собою алфавітно-цифрову послідовність символів, згенерована для конкретного облікового запису (аканту). Він ідентифікує кожний обліковий запис у блокчейні та доступний всім учасникам мережі. Відповідно до роз'яснень CNIL, публічний ключ є персональними даними особи, однак необхідність його використання зумовлена самою архітектурою блокчейну, тому мінімізувати такі дані чи встановити обмежений строк для їх зберігання неможливо.

Приватний ключ – це вже секретна алфавітно-цифрова послідовність символів, згенерована для конкретного облікового запису. Такий ключ використовується учасником блокчейну для управління своїм обліковим записом. Приватний ключ не відомий іншим учасникам мережі та використовується кожним учасником самостійно від власного імені, тому положення GDPR на такі дані за загальним правилом не поширюватимуться.

2. Інші персональні дані – транзакції, які надсилаються учасниками на підтвердження в мережу блокчейн, можуть містити персональні дані третіх осіб. На такі персональні дані поширюватиметься дія положень GDPR.

Для визначення ролей учасників блокчейну у контексті GDPR необхідно розрізняти два основних суб'єкти:

1) учасник блокчейну, який надсилає транзакції на підтвердження в мережу (participant);

2) учасник блокчейну, який підтверджує в мережі транзакції, надіслані іншим учасником (miner).

Відповідно до роз'яснень CNIL учасник блокчейну (participant), який надсилає на підтвердження транзакції, що містять персональні дані, буде виступати контролером у розумінні GDPR за умов, що такий учасник є юридичною або фізичною особою та здійснює обробку персональних даних в межах професійної чи підприємницької діяльності.

На думку CNIL, учасник блокчейну (miner), який лише підтверджує транзакції,

що містять персональні дані, надіслані іншим учасником, самостійно не визначає цілей та мети обробки персональних даних, а тому повинен виступати обробником у розумінні GDPR. У такому випадку на практиці виникатимуть труднощі з дотриманням положень ст. 28 GDPR, що передбачає обов'язок контролера укласти письмовий договір з кожним обробником персональних даних. Зважаючи на велику чисельність учасників та здебільшого анонімний характер блокчейну [5, с. 53], стає зрозумілим, що укладання договору між контролером та обробниками – учасниками блокчейну є неможливим.

Технологія блокчейн зі спеціальними протоколами, що допускають різну ступінь анонімності та конфіденційності, може забезпечити захист персональних даних, допускаючи при цьому використання цих даних в додатках з штучним інтелектом. Наприклад, користувач може використовувати блокчейн з особистою інформацією про здоров'я і розкривати певні елементи цієї інформації виключно для певних цілей [11, с. 276].

З точки зору практичного застосування у практиці діяльності сучасного підприємства у сфері захисту персональних даних, блокчейн має ряд переваг, а саме:

1) немає необхідності підтверджувати повторно, наприклад у нотаріуса, для кожної операції дійсність документів, які є верифікованими і зберігаються в учасників мережі;

2) блокчейн допомагає звірити дійсність документів у різних учасників мережі без необхідності здійснення паперового документообороту. Це суттєво економить час за операцію, оскільки не потрібно витрачати час і засоби на підготовку і доставку документів адресату, очікувати на факт перевірки документів сторонами;

3) персональну інформацію в такій розподіленій мережі неможливо загубити, а будь який її учасник може контролювати розміщенні там дані, надаючи доступ виключно за запитом.

Отже, захисту персональних даних співробітників на етапі їх обробки може сприяти використання підприємствами технології блокчейн, що представляє собою засіб, за допомогою якого люди можуть координувати спільні дії, безпосередньо взаємодіяти один з одним і керувати собою більш безпечним і децентралізованим

способом. Ця технологія допускає різну ступінь конфіденційності даних і може забезпечити їх надійний захист, допускаючи при цьому використання цих даних в додатках з штучним інтелектом.

2.3. Забезпечення відповідності використання блокчейн-технології в обробці персональних даних вимогам GDPR

Забезпечення відповідності блокчейн-технології вимогам GDPR в процесі обробки персональних даних, насамперед, потребує обґрунтування рішення про використання блокчейн для обробки персональних даних. Якщо використання блокчейну не є критичним для досягнення цілей обробки, DPA рекомендує обирати інші технічні рішення. Якщо ж все-таки стоїть завдання використовувати блокчейн в операціях з обробки персональних даних, тоді надважливим є забезпечення реалізації прав суб'єктів даних, оскільки саме цей критерій є одним з основних при оцінюванні відповідності вимогам GDPR.

Всі права суб'єкта персональних даних, передбачені GDPR, можна умовно поділити на дві групи:

– права, які повністю сумісні з вимогами GDPR та принципами блокчейну (право бути поінформованим, право на доступ до персональних даних, право на обмеження опрацювання, право на мобільність даних тощо). Загалом реалізація цих прав відповідає технічним можливостям блокчейну;

– права, реалізація яких за допомогою блокчейну викликає труднощі на практиці (право на виправлення (редагування), право на стирання (видалення), право на заперечення (уточнення даних).

У разі збереження персональних даних в мережі блокчейн технічно неможливо реалізувати запит суб'єкта персональних даних на виправлення чи зміну таких даних, тому DPA наполегливо рекомендує не зберігати персональні дані у формі відкритого тексту. Виходом із даної ситуації може бути збереження персональних даних у формі відкритого тексту поза межами блокчейну зі збереженням в самій

мережі лише доказів існування таких даних.

DPA рекомендує використовувати у блокчейн-проектах наступні технічні рішення:

1) commit – використовується у разі застосування криптографічного методу зі схемою зобов'язань (commitment scheme). Commit є своєрідним «закритим ящиком» з прихованим вмістом. Зазначений «закритий ящик» передається між сторонами, однак він не розкриває інформації, що міститься в ньому, до моменту, доки не буде відправлено ключ доступу («reveal»). У разі видалення ключа доступу (наприклад, на запит суб'єкта даних), зникає технічна можливість перевірити, яка інформація була передана. У такому випадку, сам commit більше не буде викликати ризику для безпеки персональних даних;

2) хеш – алфавітно-цифрова послідовність символів, що генерується як результат обробки даних хеш-функцією з ключем доступу. Фактично хеш-функція присвоює набору вхідних даних (наприклад, відомостям про прізвище, ім'я та по батькові особи, адресу та ін.) унікальну комбінацію літер і цифр. При цьому зміна хоча б одного символу у вхідних даних кардинально змінює вихідний хеш. Хеш-функція є лінійною (односторонньою), тому за вихідним хешем неможливо відновити вхідні дні. Видалення ключа доступу (наприклад, на запит суб'єкта даних) матиме наслідком неможливість встановлення вхідної інформації. У такому випадку, хеш більше не буде викликати ризику для безпеки персональних даних.

Зазначені технічні способи не дозволяють повною мірою реалізувати права суб'єкта даних на видалення чи зміну персональних даних, однак вони забезпечують досягнення аналогічних за своєю суттю правових наслідків, оскільки за умови видалення ключів доступу, контролер фактично втрачає доступ до персональних даних. Зазначений факт безумовно буде враховуватись контролюючими органами при вирішенні питання щодо відповідності вимогам GDPR. Якщо жоден із зазначених способів шифрування не може бути реалізовано, DPA передбачає можливість розміщення персональних даних у формі відкритого тексту, однак виключно за умов, коли це виправдано метою обробки даних та коли оцінка впливу на захист даних підтвердила прийнятність ризиків.

Варто відзначити, що всі вимоги GDPR із забезпечення безпеки персональних даних співробітників підприємств стосуються і проектів, де застосовується блокчейн. Водночас DPA рекомендує вживати і додаткові заходи, серед яких варто відзначити такі: передбачити технічні та організаційні процедури для обмеження впливу потенційного збою алгоритму (зокрема, вразливості криптографічного механізму) на безпеку транзакцій; забезпечувати безпеку секретних ключів (зокрема, зберігати їх на захищених носіях тощо).

В будь-якому разі обробка персональних даних з використанням технології блокчейн підпадає під правове регулювання GDPR. Учасник мережі блокчейн (participant), який надсилає на підтвердження транзакції, що містять персональні дані, виступатиме контролером, в той час як учасник, який підтверджує таку транзакцію (miner), в більшості випадків виступатиме обробником.

Для забезпечення узгодженості діяльності, що передбачає застосування технології блокчейн, з вимогами GDPR підприємства мають дотримуватися ряду базових засад, що наведені в Додатку В.

Отже, якщо перед підприємством стоїть завдання використовувати блокчейн в операціях з обробки персональних даних співробітників, тоді надважливим є забезпечення реалізації прав суб’єктів даних, оскільки саме цей критерій є одним з основних при оцінюванні відповідності вимогам GDPR. Для забезпечення узгодженості діяльності, що передбачає застосування технології блокчейн, з вимогами GDPR необхідно здійснювати обробку даних з використанням технології блокчейн виключно за наявності об’єктивної необхідності в цьому, зберігати персональні дані у формі відкритого тексту поза межами блокчейну зі збереженням в мережі блокчейн лише доказів існування таких даних або їх зашифрованого варіанту, забезпечити належні технічні та організаційні заходи безпеки.

ВИСНОВКИ

У науковій роботі поглиблено теоретичні та методичні аспекти забезпечення захисту персональних даних співробітників підприємств у цифровій економіці. Результати проведеного дослідження дали змогу зробити ряд висновків:

1. У різних цілях роботодавці проводять збір і обробку персональних даних своїх співробітників. Під такими даними загалом розуміють будь-яку інформацію, по якій прямо або опосередковано можна визначити фізичну особу.

2. Необхідність обробки персональних даних співробітників на підприємствах актуалізує потребує забезпечення їх надійного захисту. Захист персональних даних представляє собою сукупність заходів, спрямованих на недопущення неправомірних дій з персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми даними.

3. Міжнародна практика захисту персональних даних спирається на положення норм GDPR і CCPA. Згідно з нормами GDPR слід розробити внутрішню політику захисту даних, провести перевірку діяльності з обробки даних, налагодити процес документування процесів обробки та ін. CCPA поширюється на правові відносини щодо збору, обробки та продажу персональної інформації осіб.

4. Моніторинг персональних даних співробітників можливий шляхом застосування для аналізу даних про співробітників окремих відкритих інформаційних систем і сервісів комплексної перевірки фізичних осіб.

5. Захисту персональних даних співробітників на етапі їх обробки може сприяти використання підприємствами технології блокчейн, що представляє собою засіб, за допомогою якого люди можуть координувати спільні дії, безпосередньо взаємодіяти один з одним і керувати собою більш безпечним способом.

6. Для узгодженості діяльності, що передбачає застосування блокчейн, з вимогами GDPR необхідно здійснювати обробку даних з використанням технології блокчейн виключно за об'єктивної необхідності, зберігати персональні дані у формі відкритого тексту поза межами блокчейну зі збереженням в мережі блокчейн лише доказів існування таких даних, забезпечити належні заходи безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Беем М.В. Захист персональних даних: правове регулювання та практичні аспекти: наук.-практ. посібн. / М.В. Беем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. – К.: К.І.С., 2015. – 220 с.

2. Бречко О.В. Інституційні та організаційно-економічні детермінанти використання блокчейн-технологій у фінансовому секторі / О.В. Бречко, В.Є. Воробець // Інноваційна економіка. – 2020. – №3–4 [83]. – С. 204–211.

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

4. Воржакова Ю.П. Ефективне управління персоналом з використанням технології блокчейн – міф чи реальність? / Ю.П. Воржакова, К.Г. Мельник // Сучасні підходи до управління підприємством: електор. зб. наук. праць, 2019. – С. 27–37.

5. Воробець В. Переваги використання блокчейн-технології в умовах цифровізації фінансових інструментів / В. Воробець // Світ фінансів. – 2020. – №2 (63). – С. 49–61.

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

7. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних інформаційних систем / С.С. Єсімов // Науковий вісник Львівського державного університету внутрішніх справ. – 2013. – Вип. 3. – С. 198–208.

8. Жогов В.С. Технологія блокчейн як сучасний засіб підвищення ефективності забезпечення реалізації та захисту об’єктів авторських і суміжних прав, виражених у цифровій формі / В.С. Жогов // Юридичний науковий електронний журнал. – 2020. – №2. – С. 209–214.

9. Защита персональных данных [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Защита_персональных_данных. – Дата звернення: 09.01.2021.

10. Коваль В.О. Захист персональних даних в Інтернет / В.О. Коваль,

Л.В. Константинова // Інформаційна безпека та комп'ютерні технології: II Міжнар. наук.-практ. конф. (20–22 квітня 2017 р.). – Кропивницький: ЦНТУ, 2017. – С. 51–52.

11. Кратасюк К.О. Захист особистих даних з технологією блокчейн / К.О. Кратасюк, В.А. Світличний // Актуальні питання протидії кіберзлочинності та торгівлі людьми: зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.). – Харків: ХНУВС, 2018. – С. 274–277.

12. 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.

13. Лясківський І. CCPA, GDPR, Закон України «Про захист персональних даних». Вони однакові? [Електронний ресурс] / І. Лясківський. – Режим доступу: https://legalitgroup.com/ccpa-gdpr-zakon-ukrayini-pro-zahist-personalnih-danih-voni-odnakovi/. – Дата звернення: 09.01.2021.

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

15. Нужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018 року [Електронний ресурс]. – Режим доступу: https://channel4it.com/publications/Nov-vimogi-S-do-zahistu-personalnih-danih-z-travnya-2018-roku-30154.html. – Дата звернення: 24.12.2020.

16. Пархоменко В.Л. Задача побудови раціональної системи передачі даних / В.Л. Пархоменко, В.Г. Сайко, В.І. Кравченко // Сучасний захист інформації. – 2017. – №1. – С. 15–20.

17. Про захист персональних даних [Електронний ресурс]: Закон України №2297-VI від 01.06.2010 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text. – Дата звернення: 24.12.2020.

18. Проблеми захисту персональних даних [Електронний ресурс]. – Режим доступу: http://kmp.ua/uk/analytics/infoletters/personal-data-protection-issues-according-to-laws-of-ukraine/. – Дата звернення: 08.01.2021.

19. Сопілко І.М. Механізм захисту персональних даних: проблеми та

перспективи / І.М. Сопілко // Юридичний вісник. – 2013. – №2(27). – С. 66–70.

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

21. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн [Електронний ресурс] / В. Фісун // 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: 09.01.2021.

22. Цифрова адженда України – 2020 [Електронний ресурс]: проект. – К.: HiTECH Office, 2016. – 90 с. – Режим доступу: https://issuu.com/mineconomdev/docs/digital_agenda_ukraine-v2__1_/83. – Дата звернення: 25.12.2020.

23. Чуприна М. Блокчейн і GDPR. Чи бути реєстрам на блокчейн? [Електронний ресурс] / М. Чуприна // Юридична газета. – Режим доступу: https://yur-gazeta.com/publications/practice/inshe/blokcheyn-i-gdpr-chi-buti-reestram-na-blokcheyn.html. – Дата звернення: 18.01.2021.

24. Щербатюк М. Особливості захисту персональних даних в Інтернеті [Електронний ресурс]. – Режим доступу: https://inau.ua/document/osoblyvosti-zahystu-personalnyh-danyh-v-interneti. – Дата звернення: 13.01.2021.

25. GDPR / General Data Protection Regulation [Електронний ресурс]. – Режим доступу: https://dataprivacymanager.net/glossary/gdpr-general-data-protection-regulation/. – Дата звернення: 25.12.2020.

26. GDPR та блокчейн: поєднати не поєднане [Електронний ресурс]. – Режим доступу: https://legalitgroup.com/gdpr-ta-blokchejn-poyednati-nepoyednane/. – Дата звернення: 16.01.2021.

27. Processing personal data of employees [Електронний ресурс]. – Режим доступу: https://dataprivacymanager.net/processing-personal-data-of-employees/. – Дата звернення: 25.12.2020.

28. Ray S. How Blockchains Will Enable Privacy [Електронний ресурс] / S. Ray // Towards Data Science. – Режим доступу: https://towardsdatascience.com/how-blockchains-will-enable-privacy-1522a846bf65. – Дата звернення: 18.01.2021.

29. *Save_Data21*. Бази для обробки персональних даних співробітників підприємств та їх характеристика / *Save_Data21* // Актуальні проблеми управління соціально-економічними системами: матеріали VI Міжнар. наук.-практ. інтернет-конф. (11 грудня 2020 року, м. Луцьк). – Луцьк: ІВВ Луцького НТУ, 2020. – С. 117–118.

30. *Save_Data21*. Захист персональних даних в цифровій економіці / *Save_Data21* // Сучасні виклики сталого розвитку бізнесу: тези виступів Міжнар. наук. конф. (5–6 листопада 2020 р.). – *Save Data21*, 2020. – С. 84.

ДОДАТКИ

Додаток А

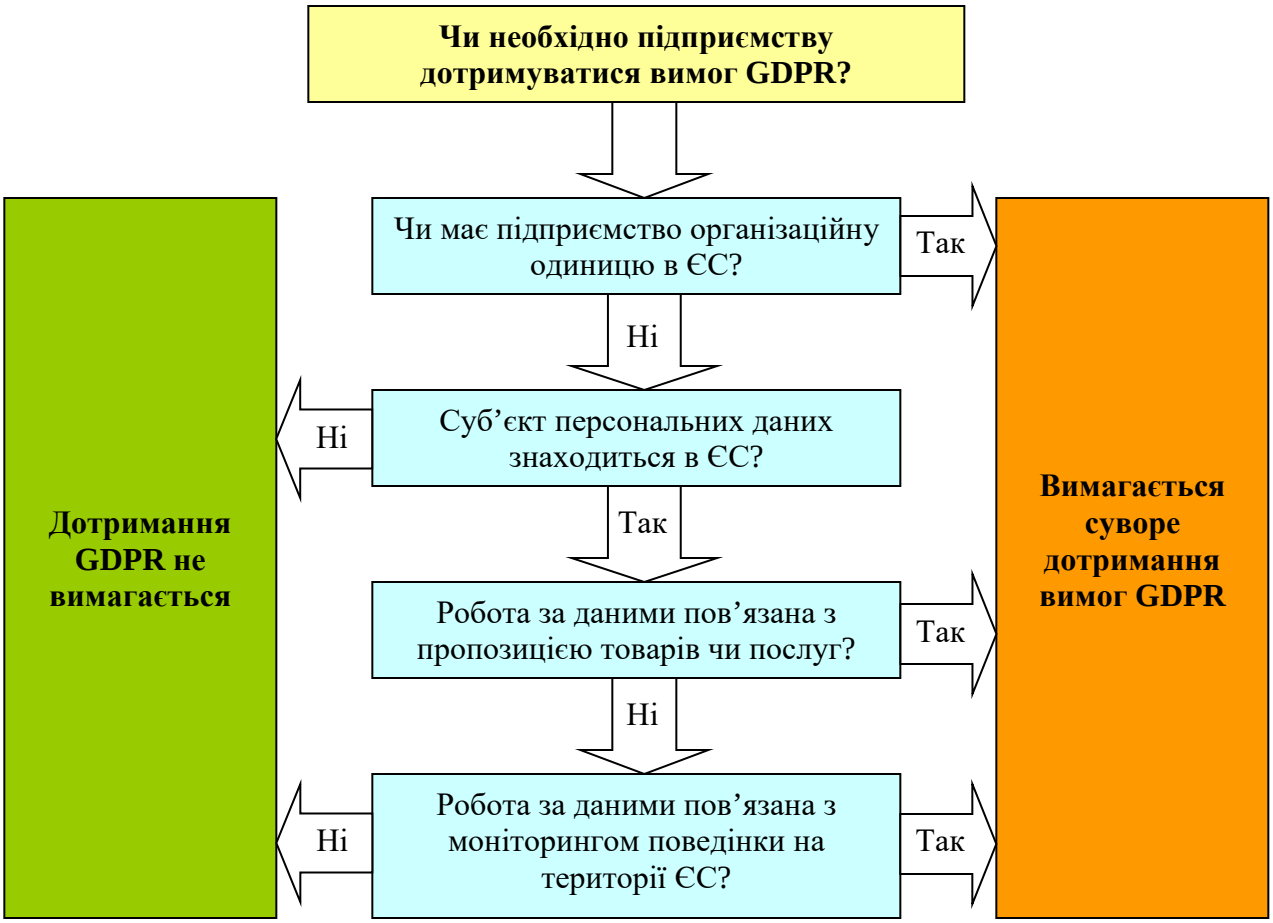

Рис. А. Рекомендації щодо необхідності дотримання вимог GDPR

Додаток Б

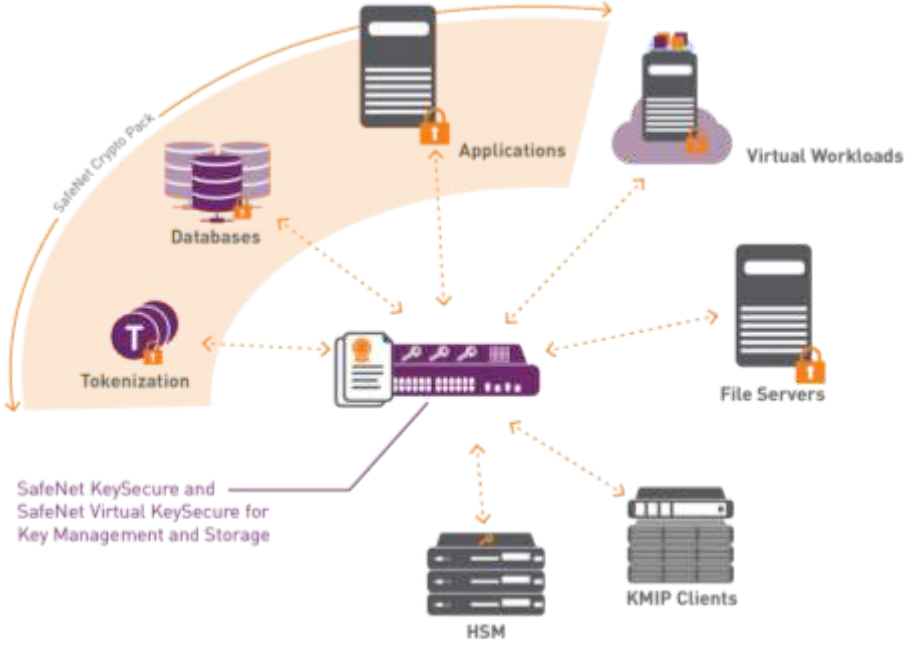

Рис. Б. Інформаційна панель Gemalto 2FA

Додаток В

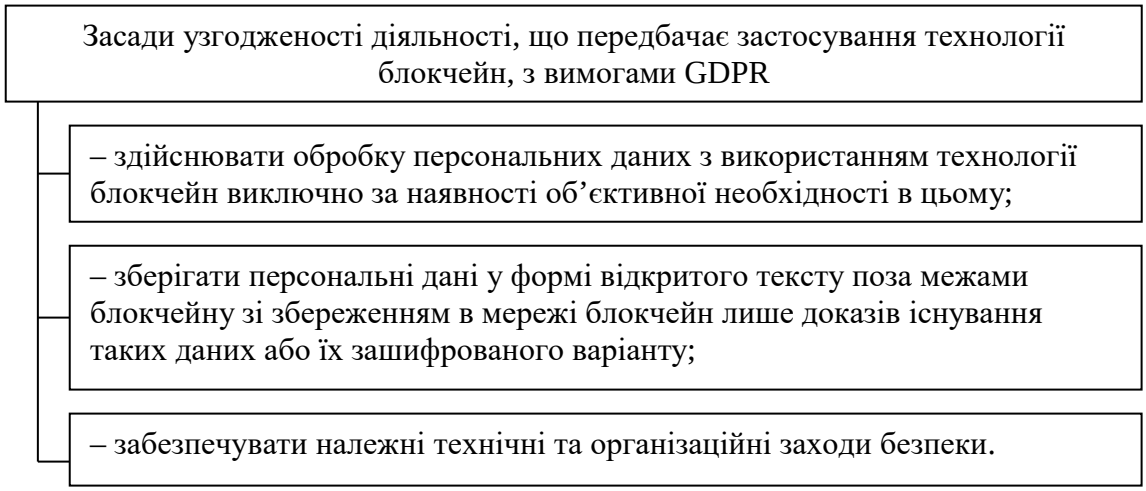

Рис. В. Базові засади для забезпечення відповідності блокчейн-проектів вимогам GDPR

Додаток Д

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет (Факультет бізнесу, Кафедра економіки)
Державна аудиторська служба України
Рада підприємців при Кабінеті Міністрів України (м. Київ)
Інститут економіки природокористування та сталого розвитку НАН України (м. Київ)
Волинський обласний осередок ВГО «Спілка економістів України»
Університет «КРОК» (м. Київ)
Київський національний університет будівництва і архітектури (м. Київ)
Міжнародний економіко–гуманітарний університет ім. академ. С.Дем'янчука (м. Рівне)
Державний університет «Житомирська політехніка» (м. Житомир)
Географічний факультет Київського національного університету ім. Т. Шевченка (м.Київ)
ГО «Європейський аналітичний Центр» (м. Київ)
Всеукраїнський науково–практичний журнал «Фінансовий контроль» (м. Київ)
Український журнал «Економіст» (м. Київ)
Полесский государственный университет (м. Пінськ, Білорусь)
Люблінський технічний університет (м. Люблін, Польща)
Економіко–гуманітарний університет у Варшаві (м. Варшава, Польща)
Технічний університет – Варна (м. Варна, Болгарія)
Сільськогосподарська академія університету імені Вітовта Великого (м. Каунас, Литва)
Університет «Союз – Нікола Тесла» (м. Белград, Сербія)
Чжецзянський технологічний університет (м. Ханчжоу, Китай)
Університет Хучжоу (м. Хучжоу, Китай)

Збірник матеріалів

VI МІЖНАРОДНОЇ НАУКОВО–ПРАКТИЧНОЇ ІНТЕРНЕТ–КОНФЕРЕНЦІЇ

«АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИМИ СИСТЕМАМИ»

11 грудня 2020 року

м. Луцьк

Продовження дод. Д

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет (Факультет бізнесу, Кафедра економіки)
Державна аудиторська служба України
Рада підприємців при Кабінеті Міністрів України (м. Київ)
Інститут економіки природокористування та сталого розвитку НАН України (м. Київ)
Волинський обласний осередок ВГО «Спілка економістів України»
Університет «КРОК» (м. Київ)
Київський національний університет будівництва і архітектури (м. Київ)
Міжнародний економіко-гуманітарний університет ім. академ. С.Дем'янчука (м. Рівне)
Державний університет «Житомирська політехніка» (м. Житомир)
Географічний факультет Київського національного університету ім. Т. Шевченка (м.Київ)
ГО «Європейський аналітичний Центр» (м. Київ)
Всеукраїнський науково-практичний журнал «Фінансовий контроль» (м. Київ)
Український журнал «Економіст» (м. Київ)
Полесский государственный университет (м. Пінськ, Білорусь)
Люблінський технічний університет (м. Люблін, Польща)
Економіко-гуманітарний університет у Варшаві (м. Варшава, Польща)
Технічний університет – Варна (м. Варна, Болгарія)
Сільськогосподарська академія університету імені Вітовта Великого (м. Каунас, Литва)
Університет «Союз – Нікола Тесла» (м. Белград, Сербія)
Чжецзянський технологічний університет (м. Ханчжоу, Китай)
Університет Хучжоу (м. Хучжоу, Китай)

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИМИ СИСТЕМАМИ

Матеріали VI Міжнародної науково-практичної інтернет-конференції «Актуальні проблеми управління соціально-економічними системами». Луцький НТУ

11 грудня 2020 року

Луцьк – 2020

Продовження дод. Д

УДК 338.24 : 330.342 (063)
А 43
ББК 65.050 : 65.013

Рецензенти:
Голян В.А. – д.е.н., професор, ГО «Європейський аналітичний центр»;
Барський Ю.М. – д.е.н., професор, Волинський національний університет ім. Лесі Українки.

Рекомендовано Вченою радою Луцького національного технічного університету (протокол № 6 від 24 грудня 2020 р.)

А 43 **Актуальні проблеми управління соціально-економічними системами: матеріали VI Міжнар. наук.-практ. інтернет-конф., Луцьк, 11 груд. 2020 р., Луцьк: ІВВ Луцького НТУ, 2020. 387 с.**

Збірник містить матеріали учасників VI Міжнародної науково-практичної інтернет-конференції «Актуальні проблеми управління соціально-економічними системами», що охоплюють проблеми управління національним господарством, галузями та господарськими комплексами; управління державними фінансами, регіонального менеджменту та міжнародного співробітництва в контексті подальшої євроінтеграції України; менеджменту та економіки підприємства; управління персоналом, трудового потенціалу, лідерства; ринку праці, зайнятості населення, соціального партнерства; управління логістичними процесами на різних рівнях господарювання, а також фінансового та обліково-аналітичного забезпечення управлінських процесів.

Для науковців, аспірантів, студентів, практиків, які досліджують проблеми управління соціально-економічними системами різних рівнів.

VI Міжнародна науково-практична інтернет-конференція «Актуальні проблеми управління соціально-економічними системами». Луцький НТУ, 11 грудня 2020 року

Save Data21

БАЗИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ ПІДПРИЄМСТВ ТА ЇХ ХАРАКТЕРИСТИКА

Роботодавці збирають і обробляють персональні дані своїх працівників щодня та з різними цілями. Дані можуть стосуватися виплат працівникам заробітної плати, відпускних, обліку лікарняних, виплат у зв'язку з вагітністю та пологами, оцінки результатів роботи та ін. Частину такої інформації на підприємстві зобов'язані збирати та обробляти відповідно до трудового законодавства, інша частина даних обробляється для внутрішніх цілей.

Необхідно враховувати всі вимоги Загального положення про захист даних (General Data Protection Regulation, GDPR) [2] та особливості національного законодавства, які потребують постійного моніторингу, оскільки держави-члени можуть встановлювати свої власні правила та обмеження. Окремі закони країн і колективні договори підприємств можуть передбачити більш конкретні правила для забезпечення захисту прав і свобод щодо обробки персональних даних працівників.

Загалом існує шість законних баз для обробки персональних даних співробітників, і щоб обробка таких даних на певному підприємстві відповідала вимогам GDPR, служба персоналу має базувати свою діяльність з обробки персональних даних на одній із цих баз. З цього переліку баз роботодавці зазвичай покладаються на перші чотири (рис. 1):

Рис. 1. Законні бази (підстави) для обробки персональних даних співробітників

Говорячи про згоду, дану за відносинами працівника та роботодавця, дуже важко в результаті отримати її в належному вигляді (коли вона насправді є вільною, конкретною, однозначною та ін.). Якщо працівник хоче відмовити роботодавцю в такій згоді, завжди існує ймовірність того, що він враховує можливі наслідки своїх дій. І дана згода по суті дозволяє працівнику уникнути неприємних ситуацій або поганих відносин з роботодавцем. Якщо на підприємстві як база для обробки персональних даних використовується саме згода, то у працівника має бути вільний вибір щодо надання або ненадання такої згоду, а також право відкликати її без наслідків для своєї посади.

Спеціалісти служби персоналу підприємства повинні добре знати національне законодавство та володіти інформацією про те, чи існують певні ситуації або типи обробки даних, коли немає можливості обробити дані працівників навіть за наявності згоди.

Якщо мова йде про виконання співробітниками умов договору, то тут вже існують певні персональні дані, які потрібно обробити, щоб кожній із сторін виконати свої зобов'язання за договором. Наприклад, для виплати заробітної плати потрібно обробити реквізити рахунків працівників та іншу особисту інформації. Крім того існує спеціальна категорія персональних даних, які потребують додаткового захисту, оскільки обробка таких типів даних може спричиняти серйозні та неприйнятні ризики для основних прав і свобод людини. Ця категорія

даних включає питання, що стосуються расового чи етнічного походження працівників, політичних поглядів, релігійних або філософських переконань, членства в профспілках, генетичних даних, біометричних даних з метою однозначної ідентифікації фізичної особи, даних про стан здоров'я та ін.

Іншою законною підставою, на яку покладається багато підприємств при обробці персональних даних працівників (крім державних органів), є законний інтерес. Законні інтереси включають обробку даних, необхідну для цілей законних інтересів роботодавця або законних інтересів третьої сторони. Виняток становлять ті випадки, коли ці інтереси перекриваються основними правами та свободами суб'єкта даних, що вимагають захисту персональних даних, особливо якщо особа є дитиною чи неповнолітньою.

І нарешті, дотримання законодавчих зобов'язань вимагає від підприємств обробляти персональні дані працівників для виконання своїх юридичних зобов'язань. Наприклад, податкове законодавство може вимагати розкриття інформації про заробітну плату місцевій владі.

Коли спеціалісти служби персоналу обирають відповідну законну базу (підставу, основу) для обробки персональних даних своїх працівників, вони зобов'язані надати співробітникам інформацію про те [1]:

– яким чином (для яких конкретних цілей) будуть використовуватися персональні дані співробітників;

– якою є законна основа для обробки таких даних;

– як відбувається дотримання прав працівників під час обробки їх персональних даних;

– хто на підприємстві може надати більше інформації про обробку персональних даних;

– хто є кінцевими одержувачами цих даних;

– як довго будуть зберігати персональні дані співробітників у розпорядженні особи чи служби, яка здійснює їх обробку.

Виходячи з цього, для того, щоб працівники підприємства були краще поінформовані щодо процедури обробки персональних даних, служба персоналу може розкрити методику обробки персональних даних співробітників у відповідному довіднику підприємства або у легкодоступному внутрішньому документі. Самих працівників потрібно оперативно повідомляти про будь-які зміни в обробці їх персональних даних у таких деталях, щоб кожен з них міг зрозуміти наслідки обробки.

Зберігати особисті дані працівників слід не довше, ніж це дійсно необхідно, особливо якщо особа більше не працює на підприємстві. Однак можуть бути законні причина зберігати особисті дані колишніх працівників досить тривалий час, наприклад, у відповідності до національного трудового законодавства, законодавства про охорону здоров'я чи податкового законодавства.

Отже, управління кадровими процесами на підприємствах передбачає збір та обробку персональних даних співробітників. Такі дані часто необхідні службі персоналу безпосередньо для виконання взятих на себе зобов'язань за договорами. Обробка персональних даних працівників здійснюється виключно на законних підставах (базах), серед яких найчастіше фігурують згоди, договори, законні інтереси та беззаперечне дотримання законодавчих зобов'язань.

1. Processing personal data of employees [Електронний ресурс]. – Режим доступу: https://dataprivacymanager.net/processing-personal-data-of-employees/. – Дата звернення: 13.12.2020.

2. GDPR / General Data Protection Regulation [Електронний ресурс]. – Режим доступу: https://dataprivacymanager.net/glossary/gdpr-general-data-protection-regulation/. – Дата звернення: 13.12.2020.

Продовження дод. Д

НАУКОВЕ ВИДАННЯ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИМИ СИСТЕМАМИ

Матеріали IV Міжнародної науково-практичної інтернет-конференції «Актуальні проблеми управління соціально-економічними системами». Луцький НТУ

11 грудня 2020 року

Відповідальний за випуск:
д.е.н., професор Шубалий О.М.

Відповідальний секретар:
Хомік В.В.

Матеріали подано в авторській редакції

Підписано до друку 18.12.2020 р.
Формат 60x84/16
Ум. друк. арк. _____ Обл.-вид. арк. _____
Тираж 300 прим. Зам. №

Інформацйно-видавничий відділ
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
Друк – РВВ Луцького НТУ

Додаток Е

ТЕЗИ

МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

«СУЧАСНІ ВИКЛИКИ СТАЛОГО РОЗВИТКУ БІЗНЕСУ»

5-6 листопада 2020 року
м. Житомир

Продовження дод. Е

Міністерство освіти і науки України,
Інститут модернізації змісту освіти,
Департамент агропромислового розвитку та економічної політики
Житомирської обласної державної адміністрації,
Управління культури та туризму Житомирської обласної державної адміністрації,
Закарпатський угорський інститут імені Ференца Ракоці II,
Київський національний університет імені Тараса Шевченка,
Причорноморський науково-дослідний інститут економіки та інновацій,
Львівський торговельно-економічний університет,
ННЦ «Інститут аграрної економіки»,
Національній університет водного господарства та природокористування,
Університет державної фіскальної служби,
Харківський державний університет харчування та торгівлі,
Інститут економіки і торгівлі Таджицького державного університету комерції (Таджикистан),
Таджицький державний університет права, бізнесу і політики (Таджикистан),
Барановичський державний університет (Республіка Білорусь),
Брестський державний технічний університет,
Білоруський державний економічний університет (Республіка Білорусь),
Гродненський державний університет імені Янки Купали (Республіка Білорусь),
Вища школа менеджменту в Лігниці (Польща),
Технологічний інститут Західної Македонії (Греція),
Господарська академія імені Д.А. Ценова (Болгарія),
Каршинський інженерно-економічний інститут (Узбекистан),
Вища школа економічна (Чеська Республіка)

ТЕЗИ

МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ
«СУЧАСНІ ВИКЛИКИ СТАЛОГО РОЗВИТКУ БІЗНЕСУ»

5-6 листопада 2020 року
м. Житомир

Продовження дод. Е

УДК 005.9 М50

Друкується за рішенням Вченої ради Державного університету «Житомирська політехніка» (Протокол № 12 від 07.12.2020 р.)

М50

Сучасні виклики сталого розвитку бізнесу: тези виступів Міжнар. наук.конф. – Житомир: Житомирська політехніка, 2020. – 404 с.

ISBN

В даному збірнику представлені матеріали досліджень українських та зарубіжних вчених і науковців, які доповідалися на Міжнародній науковій конференції «Сучасні виклики сталого розвитку бізнесу»

За точність викладення матеріалу та достовірність використаних фактів відповідальність несуть автори

УДК 005.9

ISBN

УДК 342.721

Save Data21

Захист персональних даних в цифровій економіці

Серед основних принципів політики «цифровізації України» відзначається положення про те, що цей процес «має супроводжуватися підвищенням довіри і безпеки при використанні інформаційно-комп'ютерних технологій». Тобто фактично аргументується необхідність вживання заходів, спрямованих на зміцнення довіри користувачів Інтернет до джерел інформації, включаючи інформаційну безпеку, кібербезпеку, захист конфіденційності персональної інформації.

Потреба захисту персональних даних не є примхою людини, яка не бажає розголошувати забагато інформації про себе в цифровому середовищі, – персональні дані користувачів (клієнтів) стають головним джерелом конкурентоспроможності суб'єкта господарювання. 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. Разом із тим, будучи одним із ключових цифрових трендів, персональні дані актуалізують реальну проблему їх захисту.

Підхід Європейського Союзу до забезпечення захисту персональних даних базується на розвитку «цифрових знань» і «цифрової грамотності», які мають підвищити рівень безпеки обороту персональних даних в цифровому середовищі. Також «цифрові знання» покликані поглибити розуміння користувачами інтернет-ресурсів непублічних персональних даних і можливих наслідків їх просочування у відкритий доступ.

Загалом захист – це заходи, що здійснюються системою для контролю доступу, захисту даних (конфіденційність, цілісність, доступність), опис процесів і процедур, захисту від атак, технічної підтримки, тренування та підготовка персоналу. Захист персональних даних є сукупністю правових, організаційних і технічних заходів, спрямованих на недопущення неправомірних дій з персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми персональними даними.

Забезпечення захисту персональних даних у базах персональних даних покладається на володільця персональних даних. Згідно із Законом України «Про захист персональних даних» №2297-VI від 01.06.2010 р., володілець персональних даних представляє собою фізичну або юридичну особу, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки. Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, зокрема від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них.

Такий захист важливий із погляду на значну кількість персональних даних, що обробляються володільцями персональних даних за допомогою управляючих елементів веб-ресурсів у мережі Інтернет. Найчастіше персональні дані із використанням веб-ресурсів обробляються у межах таких процесів, як:

– заповнення відвідувачами веб-ресурсів анкет;
– реєстрація та отримання логіна та пароля;
– реєстрація з використанням облікового запису соціальної мережі;
– надання електронної адреси відвідувача для зворотного зв'язку.

При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних персональних даних, які одночасно є відомостями про особу, яка ідентифікована, до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися у процесі ідентифікації особи: відомостей про оплату послуг з використанням платіжних карт, логіни та паролі, записи у соціальній мережі, номери телефонів, електронні адреси тощо.

Щоб захистити свої персональні дані від протиправних посягань, особа може використовувати будь-які не заборонені законом засоби. Зокрема, у випадку незаконної обробки персональних даних та втручання в особисте життя особи, суб'єкт персональних даних вправі звернутися до володільця та/або розпорядника персональних даних з вмотивованою вимогою: заборонити таку обробку; внести зміни до своїх персональних даних (у випадку їх недостовірності); вимагати їх видалення (знищення).

Отже, в умовах цифрової трансформації економіки та пов'язаного з цим збільшення обороту персональних даних в цифровому середовищі суб'єкту персональних даних важливо моніторити відкрити персональні дані про себе та вчасно застосовувати засоби їх захисту.

Продовження дод. Е

Продовження дод. Е

Наукове видання

Сучасні виклики сталого бізнесу
тези Міжнародної наукової конференції

Відповідальний за випуск: к.е.н., доц. О.П. Пащенко

Комп'ютерний набір та верстка: к.е.н., доц. О.П. Пащенко

Відповідальність за зміст матеріалів несуть автори

Редакційна колегія може не поділяти думок авторів