ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ
ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ
ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: « **РЕАЛІЗАЦІЯ ДОКУМЕНТАЦІЙНИХ ПРОЦЕСІВ ЛОГІСТИЧНОГО ПІДПРИЄМСТВА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ»**

на здобуття освітнього ступеня бакалавра
зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітньо-професійної програми Документознавство та інформаційна діяльність

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Емілія ЄРЕМЕНКО

Виконав: Емілія ЄРЕМЕНКО
здобувачка вищої освіти
гр. ДЗД-41

Керівник: Леся КОВАЛЬСЬКА
доктор історичних наук, професор

Рецензент: Інна ПЕТРОВА
доктор історичних наук, доцент

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти бакалавр
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
Освітньо-професійна програма Документознавство та інформаційна діяльність

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Єременко Емілії Сергіївни

1. Тема кваліфікаційної роботи: Реалізація документаційних процесів логістичного підприємства та захист персональних даних, керівник кваліфікаційної роботи проф., д.і.н. Ковальська Леся Андріївна, затверджено наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56.

2. Строк подання кваліфікаційної роботи «16» травня 2025 р.

3. Вихідні дані до кваліфікаційної роботи
   Мета роботи – обґрунтувати потреби захисту персональних даних в умовах реалізації документаційних процесів логістичного підприємства.
   Об’єктом роботи є документаційні процеси та захист персональної інформації клієнтів логістичної компанії.
   Предметом дослідження виступає безпека персональної інформації в документаційних процесах логістичної компанії.
4. Перелік питань, які потрібно розробити:
   1 Особливості захисту персональних даних у документаційних процесах
   2 Аналіз сучасних засобів захисту персональних даних логістичного підприємства
   3 Потреби вдосконалення захисту персональних даних логістичної компанії
5. Перелік ілюстративного матеріалу: презентація, 18 рисунків, 1 таблиця.
6. Дата видачі завдання «26» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Визначення тематики, вибір наукового керівника, уточнення теми	18.09.2024	
2	Розроблення та складання плану кваліфікаційної бакалаврської роботи	26.09.2024	
3	Підготовка 1 розділу	07.11.2024	
4	Підготовка 2 розділу	22.04.2025	
5	Підготовка 3 розділу	01.05.2025	
6	Висновки	09.05.2025	
7	Підготовка остаточного варіанта роботи	12.05.2025	
8	Написання відгуку науковим керівником	14.05.2025	
9	Оформлення й представлення роботи на кафедру та перевірка на плагіат	16.05.2025	
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	20.05.2025	
11	Попередній захист роботи	26.05.2025	
12	Основний захист кваліфікаційної бакалаврської роботи	19.06.2025	

Здобувач вищої освіти _____ Емілія ЄРЕМЕНКО

Керівник
кваліфікаційної роботи _____ Леся КОВАЛЬСЬКА

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 74 стор., 14 рис., 1 табл., 55 джерел.

Мета роботи – обґрунтувати потреби захисту персональних даних в умовах реалізації документаційних процесів логістичного підприємства.

Об'єктом роботи є документаційні процеси та захист персональної інформації клієнтів логістичної компанії.

Предметом дослідження виступає безпека персональної інформації в документаційних процесах логістичної компанії.

Короткий зміст роботи: розкрито специфіку організації баз даних персональної інформації в умовах функціонування цифрової економіки; проведено аналіз юридичного унормування захисту даних нормами українського законодавства та світового досвіду захисту даних; встановлено механізми організації систем захисту персональної інформації установи, традиційні та інноваційні технології практичного захисту баз персональних даних; розкрито принципи функціонування електронної логістики, умови її роботи в умовах цифрової економіки, шляхи підвищення рівня захисту персональних даних клієнтів логістичної компанії «Нова пошта».

Ключові слова: база даних, система захисту, персональні інформація, документаційний процес, логістична інформаційна комунікація.

ЗМІСТ

ВСТУП

Актуальність теми. Активний процес цифровізації соціального простору передбачає використання її складових в усіх сферах суспільних відносин. Збільшення документованого текстового контенту, пов'язаного з підприємницькою діяльністю, які генерують бізнес-процеси, актуалізує необхідність комплексних заходів для класифікування, зберігання різноманітних документів і персональних даних та реалізації систем захисту даних. Захист процесу управління у вигляді документів на паперовому носії є доволі зрозумілий, але фізично обтяжливий. Управління в СЕД складніше, ніж просто перегляд документів. Це включає обмін, редагування та коментування документів, своєчасне повідомлення про зміни, пошук вмісту та описових даних, забезпечення віддаленого доступу, гарантування цілісності та достовірності документів, використання, запобігання втрат і що найважливіше в цих маніпуляціях – створення надійної системи захисту процесу управління.

Для реалізації ефективного процесу управління документами необхідною умовою виступає використання інноваційних моделей безпеки руху документованої інформації, що в свою чергу позитивно впливає на оптимізацію бізнесово-комунікаційних процесів установи. Дотримання вимог європейських стандартів документної безпеки є однією з найбільш актуальних проблем для всіх, хто має справу з персональними даними. Динамічність цифрових технологій і потреб маркетологів у персональній інформації ставить процес захисту персональних даних у залежність від рівня безпеки обігу інформації.

Значний внесок у розвиток теоретичних і прикладних аспектів документаційного забезпечення логістики зробили Г. Балабанова, М. Єрмолаєв, І. Анілова, які досліджують оптимізацію логістичних процесів, управління ланцюгами постачання та автоматизацію облікової документації. Вони розглядаються моделі управління логістичними операціями, а також важливість впровадження інформаційних технологій для підвищення ефективності документообігу. Окрема увага приділяється автоматизованим системам

управління документацією (СЕД), які дозволяють оптимізувати бізнес-процеси на підприємствах, включаючи логістичні. У працях О. Гуменюка, С. Ільченка, Л. Прокопенка простежено переваги використання цифрових систем обліку, збереження й обробки документів у логістиці, а також їх вплив на швидкість обробки замовлень, комунікацію між ланками ланцюга постачання та рівень сервісу. Тема захисту персональних даних у контексті логістичних підприємств постійно потребує вдосконалення, тому у роботах Н. Кавун, В. Шевченка, І. Сіроштан висвітлено питання відповідності законодавству щодо захисту персональної інформації, зокрема в контексті Закону України «Про захист персональних даних», Регламенту ЄС (GDPR), а також технологій криптографічного захисту й контролю доступу. Аналіз наукових досліджень свідчить, що проблема документаційно-інформаційного забезпечення логістичної діяльності стала вагомою проблемою документознавства та менеджменту інформації. Відсутність єдиного підходу пов'язана з багатогранністю логістичної діяльності та постійними викликами та вимогами, що висуваються до електронної торгівлі на реальному ринку і зумовила постановку мети роботи.

Мета роботи – обґрунтувати потреби захисту персональних даних в умовах реалізації документаційних процесів логістичного підприємства.

Реалізація мети дослідження передбачає вирішення наступних **завдань:**

- визначити особливості цифрової інформаційної комунікації;
- дослідити українське законодавство з питань захисту персональних даних і проаналізувати світовий досвід роботи у захисті даних;
- з'ясувати місце системи захисту персональних даних організації;
- дослідити потенціал традиційних заходів захисту персональних даних та розглянути інноваційні напрями захисту персональних даних;
- визначити основні принципи функціонування електронної системи баз даних логістичної компанії і виявити можливості системи захисту персональних даних логістичної компанії в умовах цифрової економіки;
- визначити шляхи захисту персональних даних клієнтів логістичної

компанії на прикладі документаційного забезпечення діяльності підприємства «Нова Пошта».

Об’єктом роботи є документаційні процеси та захист персональної інформації клієнтів логістичної компанії.

Предметом дослідження виступає безпека персональної інформації в документаційних процесах логістичної компанії.

Методологічну базу дослідження становлять принципи системності, об’єктивності, функціональності. В межах яких застосовано наукові методи аналізу та синтезу, системності, абстрагування, моделювання, порівняння. Використання методології уможливило провести комплексне дослідження систем документообігу та захисту персональних баз даних логістичних компаній в комунікаційному процесі обміну інформацією.

Апробація результатів дослідження. Наукові результати кваліфікаційного дослідження представлені на X Всеукраїнській науковій студентській конференції «Інформаційні технології і системи в документознавчій сфері» (Вінниця, 11 квітня 2025 р.).

Обумовлені метою і завданнями наукові **положення роботи виносяться на захист** у вигляді окремих тез. Аналіз функціонування систем документаційного забезпечення та захисту баз даних в умовах цифровізації потребує постійного вдосконалення норм безпеки інформації з використанням ефективних практик і світового досвіду захисту даних. Механізми побудови, традиційні й інноваційні технології організації систем документообігу і захисту баз даних персональної інформації відповідають технологічним змінам. В умовах інноваційних змін потребують підвищення рівня захисту документаційні процеси та персональні дані у сфері логістики.

Структура бакалаврської роботи визначена метою і завданнями, представлена вступом, трьома розділами і підрозділами в них, узагальненими висновками, переліком посилань. Основна частина роботи складає 62 сторінки, загальний обсяг роботи 74 сторінки.

РОЗДІЛ 1
ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДОКУМЕНТАЦІЙНИХ ПРОЦЕСАХ

1.1 Особливості цифрової інформаційної комунікації підприємство / клієнт

Нині майже кожна державна установа або приватна компанія мають справу з персональною інформацією клієнта. Особливо це питання стосується установ і компаній, які працюють з обробкою персональних даних кінцевого споживача. Персональними даними є інформація, яка стосується ідентифікованої або деідентифікованої особи. Різна інформація зібрана разом призводить до ідентифікації конкретної особи та містить її особисті дані. Персональні дані, які були де-ідентифіковані, зашифровані або псевдонімізовані, можуть бути використані для повторної ідентифікації особи, залишаються персональними даними та потребують відповідного системного захисту з боку держави та установи утримувача баз персональних даних. Персональні дані, які були передані анонімно, тобто таким чином щоб особа не була ідентифікована, більше не вважаються персональними даними.

Процес обробки персональних даних включає збирання, реєстрацію, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення, знищення персональних даних. Обробка персональних даних може бути здійснена як неавтоматичними засобами з носіїв (у тому числі паперових), що становлять будь-який структурований масив доступних персональних даних, так і з використанням інформаційних (автоматизованих) систем.

У процесі управління підприємства мають справу з великим обсягом інформації на різних матеріальних носіях, які становлять основу тісної взаємодії підприємство / клієнт. Повна інтегрована автоматизація управління передбачає охоплення наступних документаційних інформаційно-управлінських процесів: зв’язок, збір, зберігання і доступ до необхідної

інформації, аналіз інформації, підготовка тексту, підтримка індивідуальної діяльності, програмування і вирішення спеціальних задач. Важливим аспектом створення інформаційного середовища є вимога поєднати всі шість функцій системи автоматизації як в управлінському апараті центру, так і на кожному робочому місці. Сучасну систему управління неможливо уявити без засобів, що дозволяють оперативно опрацьовувати документну інформацію, необхідну для обґрунтування та прийняття управлінських рішень. Висока складність та надзвичайна мінливість зовнішнього середовища потребують відповідної швидкості обробки інформаційних сигналів. Для цього застосовуються певні технічні засоби, які допомагають скоротити витрати часу на технічні операції обробки інформації і тим самим збільшити його ресурси на творчі процеси, зробити управлінську працю більш інтенсивною і результативною.

Найпростіші засоби оргтехніки, призначені для роботи з паперовим документообігом, застосовуються досить широко (копіювальна техніка, різних видів папки і файли, каталоги). Однак збереження паперової документації як у великій установі, так і в установах середнього та малого розміру не принесе відчутного зменшення витрат на управління і майже не вплине на його ефективність. Деяка частка паперової документації є необхідною (зовнішній документообіг: платіжні доручення, договори, контракти, акти). Але використання технічних засобів тільки з метою прискорення роботи з паперовими носіями інформації – це використання лише двох з шести вище перерахованих функцій. Раціонально організована структура технічних засобів управління має допомогти звільнитися від паперової документації всередині організації і захистити інформацію збережену на ній. Тому сьогодні поряд із простими пристроями для полегшення управлінської роботи і захисту даних особливої популярності набули цифрові комунікаційні системи і технології. Для їх реалізації потрібні комп’ютери, комп’ютерні мережі, смартфони та інше устаткування, а також засоби програмного забезпечення, які дозволяють автоматизувати більшість рутинних операцій.

До персональних даних можна віднести будь-які відомості, за якими

ідентифікується або може бути ідентифікована фізична особа, зокрема: прізвище, ім'я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров'я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо; дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи (за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану із здійсненням функцій держави або органу місцевого самоврядування) тощо.

Вказаний перелік не є вичерпним. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може оброблятися в тому числі і поширюватись тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Для операційної маніпуляції інформацією баз даних потрібно отримати згоду власника на використання його персональних даних. Усі процеси, які стосуються персональних даних, необхідно зробити прозорими для власника: для чого використовуються дані, хто має до них доступ, де вони зберігаються.

Також необхідно за запитом власника протягом місяця надавати в повному обсязі його персональну інформацію, яка зберігається у компанії і за першою вимогою власника потрібно видаляти його персональну інформацію зі сховищ даних. Варто організовувати документообіг з використанням вимог українського законодавства і нормативного регулювання європейських структур щодо використання особистих даних. Важливе місце в цифровій комунікації посідає організація належного IT-захисту персональних даних, а при виявленні порушень конфіденційності у стислі терміни повідомляти про втрату даних власнику [8].

Типовими порушеннями у сфері захисту персональних даних згідно з результатами перевірок Уповноваженого ВРУ з прав людини є:

- невідповідність внутрішніх положень / документів володільця

персональних даних вимогам чинного законодавства про захист даних;

- відсутність повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних та про створення (визначення) відповідального структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, у випадку коли таке повідомлення вимагається відповідно до Закону «Про захист персональних даних»;
- відсутність обліку працівників, які мають доступ до персональних даних суб'єктів персональних даних, що передбачено п. 3.5 Типового порядку обробки персональних даних;
- не ведеться або ведеться частково / не в повному обсязі облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них, як це передбачено п. 3.11 Типового порядку;
- у працівників, які мають доступ до персональних даних не відбирається зобов'язання не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних обов'язків, що передбачено частиною третьою статті 10 Закону;
- майже всі володільці отримують згоду на обробку персональних даних від працівників для реалізації прав та обов'язків у сфері трудових відносин, в той час як обробка персональних даних працівників здійснюється на підставі дозволу, наданого володільцю персональних даних, відповідно до закону виключно для здійснення його повноважень, а тому, окрема згода на обробку таких відомостей згідно з Законом не вимагається;
- склад та зміст персональних даних, що обробляється в багатьох випадках є надмірним стосовно визначеної мети їх обробки;
- недотримання принципу строковості обробки / зберігання, а саме обробка персональних даних здійснюється довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися, що не відповідає вимогам частини восьмої ст. 6 Закону [31].

Запровадження політики захисту даних в адміністрації ЄС також ретельно контролюється шляхом регулярного обстеження показників ефективності, залучаючи всі установи та органи ЄС. Так, перевірка проведена Інспектором по захисту даних на вебсайтах в великих установ і органів ЄС виявила проблеми безпеки для захисту даних семи з десяти сайтів. Кожна із зацікавлених установ отримала рекомендації від Інспектора про те, як забезпечити повну відповідність їхніх вебсайтів правилам захисту даних, і відповідні установи відреагували на початок виправлення виявлених проблем.

Рисунок 1.1 – Типові порушення захисту персональних даних

Для перевірки інформації було відібрано десять публічних вебсайтів, включно ті, що експлуатуються найбільшими установами та органами ЄС. До перевірки було залучено вебсайти Європейського парламенту, Європейської Ради та Ради Європейського Союзу, Європейської Комісії, Суду ЄС, Європолу, Європейського банківського органу, Європейської ради з захисту даних, Міжнародної конференції з питань захисту даних та конфіденційності. Для проведення інспекції була розроблена програма, яка автоматично збирає інформацію про обробку персональних даних вебсайтами. Ця інформація включає використання файлів cookie, вебмаяків, елементів сторінки і безпеки зашифрованих з'єднань (HTTPS).

Інспекція показала, що деякі вебсайти не відповідали Регламенту або

Директиві про електронну конфіденційність і не дотримувалися Керівних принципів ЄКЗД щодо вебсервісів. Однією із проблем було відстеження третіх сторін без їх попередньої згоди. Це особливо проблематично у випадках, коли відповідна третя сторона діє в рамках бізнес-моделі на основі профілювання та подальшого поведінкового націлювання відвідувачів вебсайту. Інші проблеми, що виникли, включали використання трекерів для вебаналітики без попередньої згоди відвідувачів і подання даних, через вебформи, з використанням незашифрованих з'єднань. У результаті інспекції установи ЄС забезпечують безпечні з'єднання HTTPS і значно зменшили кількість трекерів, які вони використовують. Узагальнюючі висновки інспекції були представлені загалу та обговорювалися з мережею офіцерів із захисту даних в інституціях ЄС [11].

Конфіденційність при розробці та за замовчуванням є фундаментальними компонентами політики захисту персональних даних. Тому регулювання цифрових послуг має забезпечувати мінімізацію даних, їхню ціль обмеження та прозорість. Ігнорування компаніями конфіденційності та намагання отримати від споживача більше персональних даних, надання ними більше персональних даних, ніж необхідно, порушує юридичні норми українського національного та європейського законодавства. Маніпулювання споживачами та невпорядкований обмін їх особистими даними зменшує їх особисте автономне представництво, що загалом порушує фундаментальний принцип свободи вибору.

Дослідження норвезької Ради Споживачів показує і порівнює способи, якими великі компанії домагаються використання темних моделей. Дослідження фокусується на аналізі орієнтованого на користувача дизайну, який спрямований на створення інтерфейсу, заснованого на тому, що користувачі, швидше за все, будуть шукати, намагаючись передбачити, як це зробити максимально ефективно задовольняти свої потреби. Фінансові стимули компаній, які використовують такі моделі, перестали поважати право користувачів на вибір. Використовуючи скриті моделі, компанії сприяють тому, що люди не є автономними індивідами, а функціонують у технічно-

визначеному полі. Коли особи не сприймаються як особи, а лише як сукупність даних, які можуть бути оброблені в промислових масштабах для отримання прибутку деяких компаній, вони явно не поважають норми прав людини. Висунення такого образу людства не тільки ставить під сумнів найбільш фундаментальні соціальні цінності, але також зменшує довіру людей до цифрових послуг [37].

1.2 Нормативне-правове забезпечення захисту персональних даних в Україні

В Україні функції захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. Центральний апарат уповноваженого та його регіональні представництва контролюють виконання вимог законодавства в сфері захисту персональних даних. Законом України від 6 липня 2010 р. Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї. Україна взяла на себе зобов'язання забезпечити дотримання прав і свобод людини, зокрема, права на недоторканність приватного життя, передбаченого ст. 8 Конвенції про захист прав людини і основоположних свобод та гарантованого ст. 32 Конституції України.

Рисунок 1.2 – Вебпортал Уповноваженого ВРУ з прав людини

Зважаючи на гарантування Конституцією України права особи на невтручання у її особисте життя, правові відносини пов'язані із захистом і обробкою персональних даних були врегульовані Законом України «Про

захист персональних даних» [26]. Загальні вимоги щодо обробки та захисту персональних даних суб'єктів персональних даних визначені Типовим порядком обробки персональних даних затвердженим наказом Уповноваженого Верховної Ради України з прав людини [22].

Порядком обробки персональних даних визначено загальні вимоги до обробки та захисту персональних даних суб'єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів. Власники, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог, визначених Законом України «Про захист персональних даних» та Порядком [22, 26].

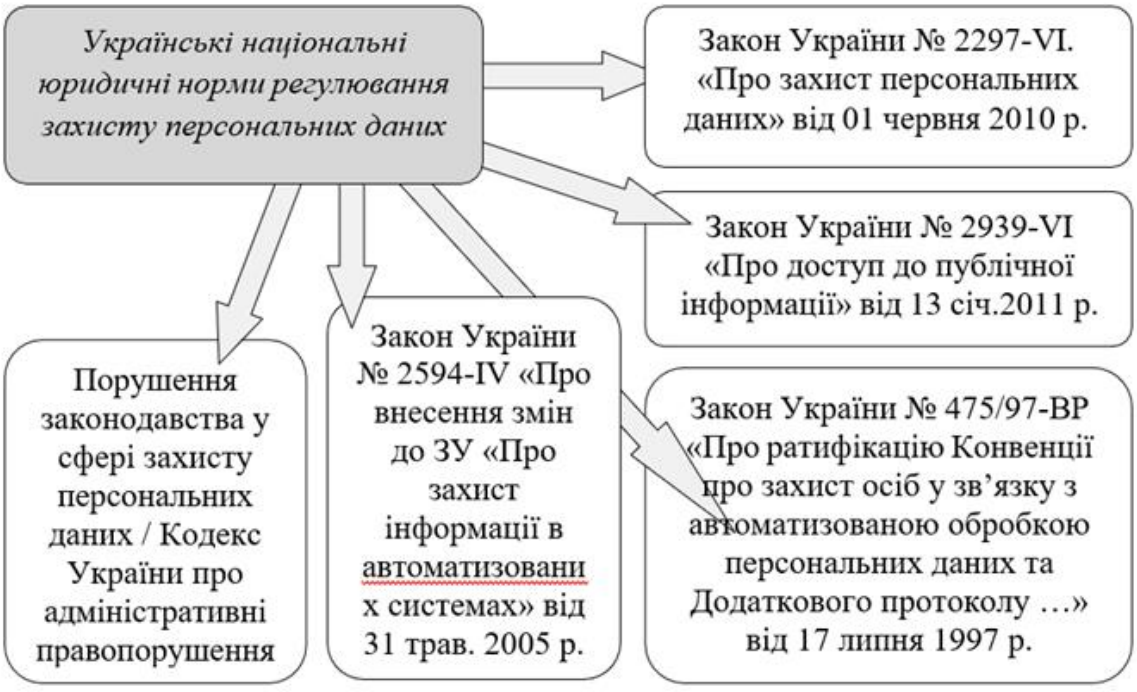

Рисунок 1.3 – Нормативна база у сфері регулювання дії та захисту систем персональних даних

Окремим аспектам обробки та захисту персональних даних (таким як надання згоди на обробку персональних даних, забезпечення реалізації окремих прав суб'єктів персональних даних) приділено додаткову увагу в Роз'ясненнях до Типового порядку обробки персональних даних. Багато документів

нормативно-правового характеру України регулюють відносини у справі захисту персональних даних, окремі з них наведено на рисунку 1.3 [16 - 18, 21 - 26, 29]. Для запровадження реальних механізмів реалізації взятого на себе зобов'язання Верховною Радою України ухвалено Закон України «Про захист персональних даних», який набув чинності 1 січня 2011 р. [26].

Згідно із ст. 23 Закону України «Про захист персональних даних» у сфері захисту персональних даних Уповноважений має повноваження: отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних у порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом; затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом; за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних; надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб; взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до

цього Закону організовують роботу, пов’язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб; звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних; надавати за зверненням професійних, самоврядних та інших громадських об’єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них; складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом; інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов’язки суб’єктів відносин, пов’язаних із персональними даними; здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних; організовувати та забезпечувати взаємодію з іноземними суб’єктами відносин, пов’язаних із персональними даними, виконанням Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних; брати участь у роботі міжнародних організацій з питань захисту персональних даних [26].

Уповноважений Верховної Ради України з прав людини також має включати до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних [31, 19].

Уповноваженим Верховної Ради України з прав людини роз’яснено окремі положення законодавства щодо захисту персональних даних. Щодо необхідності отримувати згоду на обробку персональних даних ст. 11 Закону визначений перелік підстав для обробки персональних даних, однією з яких є згода суб’єкта персональних даних на обробку його персональних даних [19]. Виключення поняття «згода на обробку персональних даних» із Закону не

позбавляє можливості використовувати інші механізми щодо забезпечення його застосування [31].

Відповідно до зазначених положень законодавства наказом Уповноваженого від 08.01.2014 р. № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» затверджено Типовий порядок обробки персональних даних, Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [22].

Зазначені нормативно-правові акти опубліковані на офіційному сайті Уповноваженого, до кожного з цих актів надано відповідні роз'яснення [31]. Зокрема, у роз'ясненнях до Типового порядку обробки персональних даних надано визначення поняття «згода на обробку персональних даних» та розтлумачено порядок її надання (отримання). Так, згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій чи електронній формі [22]. Отже, власникам та розпорядникам персональних даних отримувати згоду на обробку таких даних доведеться, зокрема, у тих випадках, коли існує потреба для обробки цих даних, а інші передбачені ст. 11 Закону підстави для обробки таких даних не поширюються на цей випадок обробки даних.

У п. 1.2 Порядку повідомлення визначено, що обробкою персональних даних, що становить особливий ризик для прав і свобод суб'єктів, є будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження,

реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно персональних даних про: расове, етнічне та національне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості; стан здоров'я; статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування щодо особи заходів в рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; вчинення щодо особи тих чи інших видів насильства; місцеперебування та/або шляхи пересування особи.

Таким чином, основним критерієм при визначенні того, чи становить певна обробка такий ризик, є те, які категорії персональних даних обробляються. Про це більш детально зазначено у роз'ясненнях основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, що додаються до Порядку повідомлення і опубліковані на офіційному сайті Уповноваженого [31, 19].

Щодо здійснення захисту персональних даних, про обробку яких повідомляти Уповноваженого не потрібно, то зобов'язання забезпечити захист персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, закріплено у частині першій ст. 24 Закону, поширюється на всіх володільців, розпорядників персональних даних та третіх осіб і не залежить від необхідності повідомляти Уповноваженого про обробку персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних.

Щодо реєстрації баз персональних даних, утворених до 01.01.2014 р., то відповідно до вимог чинної редакції Закону процедура реєстрації баз персональних даних замінена обов'язком володільців персональних даних повідомляти Уповноваженого про обробку персональних даних, яка становить

особливий ризик для прав і свобод суб'єктів персональних даних.

Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, покладається на Уповноваженого лише з набранням чинності Законом України від 03.07.2013 р. № 383-VII «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [16; 31]. Отже, Уповноваженим може бути складено протокол про притягнення до адміністративної відповідальності за ті діяння, які визнаються адміністративними правопорушеннями згідно з чинним законодавством і вчинені чи виявлені, відповідно, у строки, встановлені частиною другою ст. 38 Кодексу України про адміністративні правопорушення [16].

1.3 Ефективні практики реалізації захисту даних

Інститут захисту персональних даних сьогодні вже не є тією категорією, яку можна регулювати тільки національним правом. Найважливішою особливістю сучасних автоматизованих інформаційних систем є наднаціональність і вихід за межі кордонів держав.

Організаційно захист персональних даних представлений низкою світових і європейських структур, які проводять дослідження виконання вимог ЄС в цьому питанні. Регламентом про захист даних запроваджується посада європейського інспектора із захисту даних, регламентуються його повноваження та інституційна незалежність як контролюючого органу. Ця посада є незалежним наглядовим органом, чия головна мета полягає в гарантуванні європейськими інститутами влади поваги і дотримання прав на приватне життя і захист даних при обробці персональних даних, а також розробка політик в цій сфері. На практиці діяльність Інспектора можна розділити на три основні напрями: нагляд, консультації та співпраця [37].

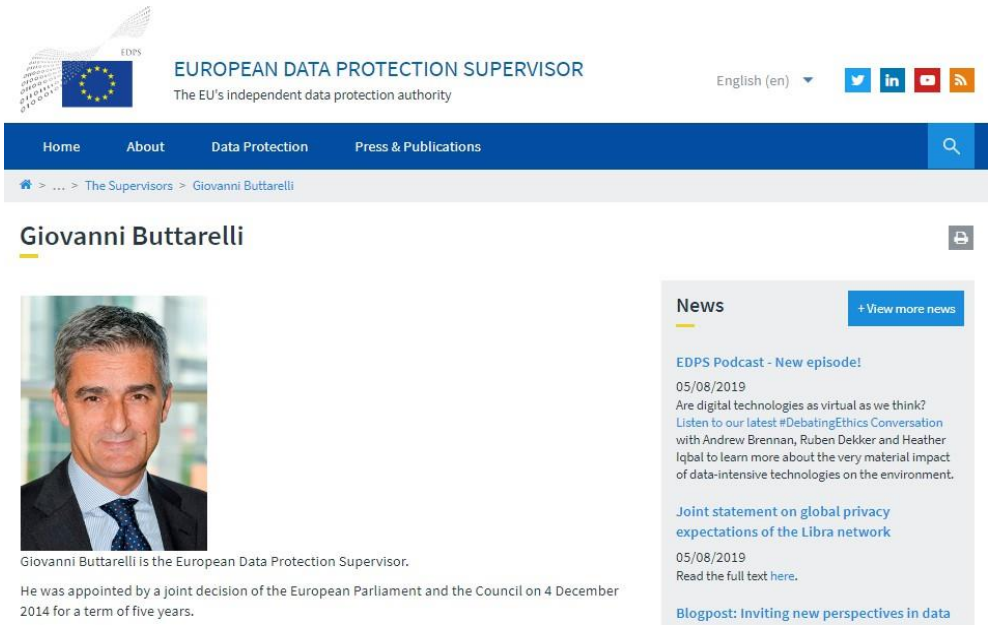

Рисунок 1.4 – Вебсайт європейського інспектора із захисту даних [37]

Головним завданням є контроль за обробкою персональних даних у європейських установах та органах, і робить це Інспектор у співпраці з посадовими особами із захисту даних присутніми в кожній європейській установі та органі. Інспектор аналізує повідомлення відповідно Регламенту про захист даних та видає висновок «попередньої перевірки», який у більшості випадків призводить до набору рекомендацій установі чи органу з вимогою забезпечення дотримання правил захисту даних.

Рисунок 1.5 – Вебпортал наглядового органу із захисту даних [37]

Наглядова роль також передбачає розслідування скарг, поданих працівниками ЄС або особою, яка вважає, що їхні особисті дані були порушені європейською установою чи органом. Приклади скарг включають ймовірні порушення конфіденційності, доступу до даних, права на виправлення, стирання даних, надмірне збирання, незаконне використання даних.

У консультативній ролі Інспектор надає відповідну інформацію Європейській Комісії, Європейському Парламенту та Раді Європейського Союзу щодо питань захисту даних у різних сферах політики. Ця роль стосується пропозицій щодо нового законодавства, а також інших ініціатив, які можуть впливати на захист персональних даних в ЄС. Технологічні розробки, що впливають на захист даних, також відстежуються як частина цієї діяльності.

Основною платформою для співпраці між органами захисту даних в Європі є Робоча група з питань захисту даних за ст. 29. ЄНОЗД бере участь у діяльності Робочої групи, яка відіграє важливу роль у рівномірному застосуванні Директиви про захист даних та замінених Загальних положень про захист даних (GDPR). ЄНОЗД та Робоча група ефективно співпрацювали з цілого ряду питань, але, зокрема, з питань імплементації Директиви про захист даних та проблем, які постають перед новими технологіями. Одним з найважливіших завдань спільної роботи є Eurodac, коли відповідальність за нагляд розподіляється з національними органами захисту даних.

Співпраця також відбувається шляхом участі у двох головних щорічних конференціях із захисту даних: Європейській конференції, яка збирає органи захисту даних країн-членів ЄС і Ради Європи, та Міжнародній конференції, в якій взяли участь широкий спектр експертів із захисту даних, як з боку державний та приватний сектори. Так, дев’ятнадцяте 17-18 травня 2017 р. в місті Тбілісі відбулася Конференція органів із захисту даних Центральної та Східної Європи (Central and Eastern Europe Data Protection Authorities).

Рисунок 1.6 – Конференція з питань захисту даних Центральної та Східної Європи (CEEDPA)» [34].

В Європейському Союзі склався комплексний механізм захисту персональних даних, який ґрунтується на таких головних елементах як, наявність загальноєвропейської нормативної бази, дія національних законодавчих актів, що регулюють питання персональних даних; правова чіткість основних принципів права щодо захисту ПД; наявність європейських консультативних і наглядових органів, а також створення національних адміністративних органів щодо захисту ПД; нормативна визначеність правового статусу – основних прав, свобод і обов'язків; наявність правової визначеності за умовами передачі ПД третім особам. Протягом останніх 25 років технології трансформували наше життя таким чином, що ніхто не міг собі уявити, щоб був необхідний перегляд правил. Захист персональних даних є основним правом, гарантованим ст. 8 Хартії ЄС про основні права [23-25].

Юридичні норми ЄС про захист даних вже давно вважаються золотим стандартом у всьому світі. Основними віхами поступу у світовому

законодавстві є низка юридичних норм, які частково представлені на рис. 1.7.

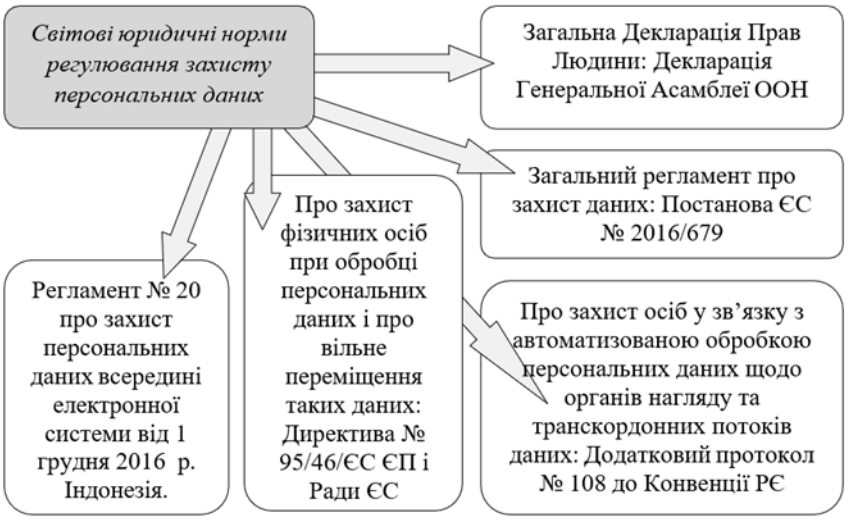

Рисунок 1.7 – Норми у сфері регулювання дії та захисту систем персональних даних

Конкретні правила щодо захисту даних в інституціях ЄС, а також обов'язки Європейського наглядового органу з питань захисту даних викладені в Регламенті (ЄС) 2018/1725. Ці правила замінили ті, що викладені в Регламенті (ЄС) № 45/2001 11 грудня 2018 р. [37].

Так, Загальна декларація прав людини від 10 грудня 1948 р. говорить про те, що «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [4].

Наступним особливо значущим документом, який регламентує відносини в сфері персональних даних, стала Конвенція про захист фізичних осіб при обробці персональних даних від 28 січня 1981 р. [23]. Цей документ унормовує основні принципи обробки персональних даних в державних та комерційних інформаційних системах. Метою Конвенції є забезпечення поваги прав і основних свобод кожної людини і особливо його права на недоторканність особистої сфери в зв'язку з автоматичною обробкою його персональних даних.

Згідно з Директивою Європейського Союзу 95/46 / ЕС2 введені наступні критерії обробки ПД: обробка можлива при наявності однозначної згоди

суб'єкта, або обробка необхідна для виконання договору, стороною якого є суб'єкт даних або з метою вжиття заходів щодо прохання суб'єкта даних до укладення договору; або обробка необхідна для дотримання юридичного зобов'язання, суб'єктом якого є оператор тощо [7].

У 2016 році ЄС ухвалив Загальний регламент захисту даних (GDPR), один з найбільших досягнень останніх років, який замінює застарілу Директиву про захист даних від 1995 р., що була прийнята в той час, коли інтернет перебував у зародковому стані [37]. З травня 2018 р. в Європейському союзі набув чинності згаданий Регламент захисту персональних даних. Це стосуватиметься будь-яких бізнес-процесів, які пов'язані з персональною інформацією клієнтів з ЄС. Така ситуація вимагає зміни підходів у підвищення рівня безпеки баз даних у фізичній та віртуальній площині, встановлення серверів, додаткових сховищ даних, програмного забезпечення та призначення відповідальних осіб.

Окрім європейської системи захисту, кожна країна пройшла свій шлях створення. Наприклад, в Німеччині перший закон в сфері захисту персональних даних був прийнятий ще у 1970 р в землі Гессен. А за сім років з'явився перший федеральний закон, що захищає персональні дані німців.

На початку 1970-х рр. уряд Франції прийняв Національний інформаційний план. Його метою стало створення банків даних. Уряд запустив проекти SIRENE і SAFARI, які видавали ідентифікаційні коди компаніям і приватним особам. Надалі їх планували використовувати, щоб встановлювати взаємозв'язки між різними базами даних. З 1974 р. діє «Французька національна комісія з обробки даних та громадянських свобод». Вона стала регулятором системи захисту персональних даних в країні. У 1978 р. уряд ухвалив закон «Про обробку даних, файли даних і індивідуальних свободах». У ньому, окрім визначення понять, встановлені покарання за порушення.

Система захисту персональних даних у Великій Британії почала формуватися пізніше, ніж у Франції та Німеччині, профільний закон був прийнятий в 1984 р. У ньому, крім основних положень, вказувалися вимоги до структур, які збирають і обробляють персональні дані. Для цього уряд створив

спеціальний Реєстр захисту даних. Невиконання цієї вимоги карається законом.

Активність європейців щодо захисту персональних даних спричинила аналогічні процеси в інших частинах світу. Так, 1 грудня 2016 р. міністр зв'язку та інформації Індонезії затвердив Регламент № 20 про захист персональних даних всередині електронної системи. Це законодавчо закріпило необхідність встановлення процедури захисту особистих даних, зібраних, збережених та використаних в електронній системі.

В умовах цифровізації соціальних та економічних процесів у суспільстві кожна установа або підприємство має справу з персональною інформацією клієнта. До персональних даних відносять інформацію за допомогою якою стає можливим ідентифікація особи та містить її особисті дані.

В Україні функції захисту персональних даних покладено на уповноваженого ВРУ з прав людини. Зважаючи на гарантування Конституцією України права особи на невтручання у її особисте життя, правові відносини пов'язані із захистом і обробкою персональних даних були врегульовані Законом України «Про захист персональних даних». Загальні вимоги щодо обробки та захисту персональних даних суб'єктів персональних даних визначені Типовим порядком обробки персональних даних затвердженим наказом Уповноваженого ВРУ з прав людини. Україна в питанні захисту персональних даних спирається на міжнародний досвід.

В ЄС склався комплексний механізм захисту персональних даних, який ґрунтується на наявності загальноєвропейської нормативної бази, національних законодавчих актів і європейських консультативних і наглядових органів. Проаналізувавши низку європейських юридичних документів, в яких позначені принципи захисту і обробки персональних даних в автоматизованих інформаційних системах можна виокремити такі головні юридичні підвалини їх функціонування як захищеність суб'єктів ПД від втручання в приватне життя, а також гарантія прав суб'єкта; фізична захищеність ПД від несанкціонованого доступу.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

2.1 Організація документаційних процесів логістичних компаній та їх системи захисту персональних даних

Визначення принципів захисту персональних даних працівників установи може забезпечити стабільність норм трудового законодавства про захист приватного життя працівника, усунути можливі протиріччя між ними, визначити пріоритети правового регулювання зазначених відносин. Необхідність закріплення принципів обробки персональних даних працівника обумовлена розвитком автоматизованих інформаційних систем, можливостями обмеження прав і законних інтересів працівників, заподіяння їм матеріального збитку і моральної шкоди. Основи захисту ПД повинні знаходити своє відображення в юридичних нормах національного та міжнародного законодавства [2].

Процедура роботи з персональними даними передбачає ознайомлення користувача з можливим використанням таких даних. Підставами для обробки персональних даних є:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних,

який передбачений законом;

6) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

На думку А. Дворецького, при роботі з документами, справами і базами даних відділу кадрів повинні дотримуватися такі основоположні вимоги до захисту персональних даних:

- особистої відповідальності працівників за збереження і конфіденційність відомостей про роботу відділу та персональних даних, а також носіїв цієї інформації;
- розбиття (дроблення) знань персональних даних між різними працівниками відділу;
- наявності чіткої дозвільної системи доступу працівників відділу до документів, справ і баз даних;
- проведення регулярних перевірок наявності традиційних та електронних документів, справ і баз даних у працівників відділу та кадрових документів в підрозділах підприємства [2].

В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню створюється / визначається структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, яка:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим ВРУ з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

У випадку не можливості самостійного захисту даних установи варто знайти відповідних спеціалістів. Пошук виконавця робіт з організації захисту

персональних даних важлива справа, яка потребує виконання певних умов.

Публікувати, передавати, розповсюджувати та / або надавати доступ – заходи, яким повинен дотримуватися постачальник електронної системи захисту. А саме: відображення, публікація, передача, розповсюдження та доступ до персональних даних повинні базуватися на згоді власника персональних даних, якщо інше не передбачено чинним законодавством, і тільки після його точності та відповідності цілям збору персональних даних були перевірені; використання та використання персональних даних повинні базуватися на згоді та узгоджуватися з метою отримання, збору, обробки та аналізу таких даних. Видалення персональних даних повинно відбуватися до такої міри, щоб видалені дані більше не було можливості відновити повторно, якщо власник персональних даних не надає нових даних [39].

Деякі документознавці виокремлюють значну кількість вимог захисту персональних даних. Вони відображають специфіку міжнародних актів, в деяких прямо перераховуються принципи правового регулювання. Оскільки принципи права відображають зміст елементарних норм, то використання принципів законодавчого регулювання відносин у зарубіжних країнах можливо або в якості порівняльного зіставлення з вітчизняними положеннями, або в разі значного подібності норм вітчизняного та іноземного права.

На думку І. Басаргіна, можна виділити три принципи захисту персональних даних працівника: 1) конфіденційність одержуваних персональних даних; 2) максимальне обмеження доступу посадових та інших осіб організації роботодавця, а також третіх осіб до зазначених відомостей; 3) достовірність персональної інформації [2].

Аналогічні вимоги до захисту персональних даних працівників установи виділяє С.Ю. Головіна [2]. Перші два зі згаданих вона об’єднує в єдине правило конфіденційності одержуваних персональних даних, обмеження доступу до них інших осіб, а третю вимогу доповнює правилом повноти персональної інформації.

Поряд з цими принципами авторами виділяється ще три: 1) цільовий

характер персональної інформації; 2) вільний доступ працівника до своїх персональних даних; 3) гарантованість суб'єктивних прав працівника, пов'язаних із захистом його персональних даних.

Для створення, впровадження та ефективного функціонування системи захисту персональних даних необхідно реалізувати комплекс заходів, який включає в себе наступні етапи:

Рисунок 2.1 – Створення і впровадження системи захисту персональних даних

Обстеження автоматизованих інформаційних систем установи включає:

- визначення переліку персональних даних установи, які підлягають захисту;
- визначення переліку інформаційних систем для роботи з персональними даними установи;
- визначення використовуваних засобів захисту персональних даних установи;
- аналіз внутрішніх нормативних документів, що регламентують порядок

обробки та захисту персональних даних;

- визначення ступеня участі персоналу в обробці персональних даних установи.

За результатами обстеження формується звіт, в якому містяться вихідні дані для класифікації інформаційних систем персональних даних і опис поточного стану захисту персональних даних.

На другому етапі робіт на основі інформації, зібраної під час обстеження, проводиться класифікація інформаційних систем персональних даних [2]. Для їх класифікації проводиться категоріювання наступних вихідних даних:

- категорія оброблюваних в інформаційній системі даних;
- обсяг оброблюваних персональних даних;
- задані оператором характеристики безпеки персональних даних;
- структура інформаційної системи;
- наявність підключень до мереж зв'язку загального користування;
- режим обробки персональних даних;
- місцезнаходження технічних засобів.

Розрізняють типові і спеціальні інформаційні системи персональних даних:

Рисунок 2.2 – Види інформаційних систем захисту персональних даних

До типових інформаційних систем персональних даних відносяться системи, в яких потрібне забезпечення тільки конфіденційності персональних даних. Спеціальні інформаційні системи персональних даних, в яких незалежно від необхідності забезпечення конфіденційності потрібно забезпечити хоча б одну з характеристик безпеки персональних даних, відмінну від конфіденційності (захищеність від знищення, перекручення, блокування, інших

несанкціонованих дій). Результати класифікації інформаційних систем персональних даних оформляються відповідним актом, що підписується керівником установи, з зазначенням всіх вихідних даних [2].

На сьогоднішній день, класифікація інформаційних систем персональних даних незважаючи на простоту використовуваної методики, є найбільш важливою і складною роботою. У більшості випадків, якщо є така можливість, буває економічно вигідніше залучити до класифікації інформаційних систем персональних даних експертів з питань персональних даних.

При необхідності застосування засобів криптографічного захисту розробляється «Модель порушника» відповідно до нормативних документів. Вимоги щодо забезпечення безпеки персональних даних при їх обробці в інформаційних системах персональних даних розробляються на підставі розроблених моделей загроз і порушника.

В рамках проектування системи захисту персональних даних виконуються наступні роботи:

Рисунок 2.3 – Етапи створення систем захисту персональних даних

На основі технічного завдання здійснюється розробка технічного проекту, що містить детальний опис конкретних програмно-технічних і організаційних

рішень, що забезпечують виконання встановлених вимог щодо захисту персональних даних в створюваній систем захисту персональних даних [2].

У процесі робочого проектування здійснюється розробка пакету експлуатаційної та організаційно-розпорядчої документації, що відповідає вимогам нормативних документів щодо захисту персональних даних і регламентує порядок забезпечення безпеки інформаційних систем персональних даних в організації.

На практиці володілець бази персональних даних повинен створити умови для захисту в інформаційній (автоматизованій) системі персональних даних та забезпечити захист цих персональних даних від незаконної обробки, а також від незаконного доступу до них. Умови для захисту персональних даних залежать від конкретних реальних загроз, природи персональних даних, які обробляються, технології обробки інформації та типу інформаційної системи, у рамках якої обробляються персональні дані.

Забезпечення умов для захисту в інформаційній (автоматизованій) системі персональних даних не вирішується реалізацією визначеної сукупності заходів, а є постійним процесом, який включає:

- розробку політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них, виходячи з характеристик діяльності організації, цілей, процесів та процедур, суттєвих для управління ризиком небажаних подій щодо обробки персональних даних з урахуванням серйозності наслідків таких небажаних подій;
- впровадження політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них та забезпечення функціонування заходів, процесів та процедур захисту персональних даних;
- оцінювання і вимірювання продуктивності процесів захисту персональних даних згідно з прийнятою політикою, цілями і практичним досвідом, підготовка пропозицій щодо коригувальних заходів.
- вживання коригувальних та запобіжних дій щодо захисту персональних даних на підставі результатів внутрішніх перевірок, періодичний перегляд

політики захисту персональних даних, постійне удосконалення заходів.

У разі, коли обробка персональних даних здійснюється в інформаційній (автоматизованій) системі, то створюється комплексна система захисту інформації відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

Комплексна система захисту інформації забезпечує захист персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до плану захисту інформації в системі, який містить:

- завдання захисту персональної інформації, класифікацію персональної інформації, опис особливостей технології обробки інформації;
- модель загроз для персональних даних у системі;
- вимоги щодо захисту персональних даних та правила доступу до них;
- перелік документів, згідно з якими здійснюється захист інформації в інформаційній системі.

Для захисту персональних даних важливо, щоб організаційні заходи та використовувані засоби захисту, що визначають рівень захисту, відповідали реальним конкретним загрозам, даним, які обробляються, та процесам обробки даних, які виконуються.

До основних факторів, які впливають на рівень захисту, що вимагається, відносяться:

- увага, яка приділяється суспільством до оброблюваних даних;
- рівень обізнаності персоналу Володільця та/або розпорядника бази персональних даних стосовно інформаційної безпеки, захисту персональних даних, поваги до авторських прав, тощо.
- тип інформаційно-телекомунікаційної системи, у рамках якої обробляються персональні дані.

Роботи зі створення системи захисту персональних даних можуть виконуватися операторами інформаційних систем як власними силами, так і з

залученням сторонніх фахівців. На завершальному етапі проводиться навчання співробітників та розробка проектів документів, необхідних для виконання контрольних заходів і, при необхідності, атестаційних випробувань. В рамках етапу також здійснюється проведення самих випробувань, а також оформлення Атестату відповідності.

2.2 Традиційні заходи реалізації захисту персональних даних

Визначення загроз безпеки персональних даних здійснюється на основі теоретичної базової моделі загроз безпеки персональних даних. Показник небезпеки в такій традиційній моделі має три значення:

Рисунок 2.4 – Шкала небезпеки в інформаційних системах персональних даних

Інформаційні системи, для яких порушення заданої характеристики безпеки персональних даних, які обробляються в них, не призводить до негативних наслідків для суб'єктів персональних даних. При використанні типових моделей загроз і відповідних для них вимог основні заходи з організації і технічного забезпечення безпеки персональних даних, які обробляються в інформаційних системах установ слід враховувати, що в ряді випадків можливості реалізації окремих загроз можуть бути вищими і вимагати

додаткових заходів захисту персональних даних.

Серед традиційних заходів захисту інформаційних систем персональних даних:

Рисунок 2.5 – Реалізація захисту інформаційних систем персональних даних

Суттєво зменшити обов’язкові вимоги і необхідні витрати на захист персональних даних можна шляхом знеособлення і сегментування інформаційних систем персональних даних, відключення сегментів систем від мереж загального користування, організації виділених ліній зв’язку тощо [26].

Найбільш ефективним є знеособлення в інформаційних системах персональних даних шляхом заміни прізвища / ім’я / по батькові суб’єктів персональних даних на їх особисті коди (табельні номери), використовувані для автоматизованого обліку в установі. Ефективно повне виключення з інформаційних систем персональних даних відомостей, що стосуються расової, національної приналежності, політичних поглядів, релігійних і філософських переконань, стану здоров’я, інтимного життя. За необхідності облік таких персональних даних слід здійснювати в формі анкет, довідок, особистих справ й інших документів тільки на паперових носіях [26].

Знеособлення інформаційних систем персональних даних дозволяє зберегти діючий порядок доступу користувачів, включаючи віддалений. При

цьому не можна обмежитися знеособлення нововведених персональних даних, а раніше накопленні залишити в тій же базі даних без зміни [26].

Знеособлення є найбільш прийнятним способом приведення у відповідність вимогам законодавства інтегрованих багатофункціональних і розподілених інформаційних систем персональних даних, що використовують для обміну даними мережі загального користування. Найбільш просто обмежити доступ до систем, в яких ПІБ використовувалися тільки в якості логінів або паролів для доступу до інформаційного системам забезпечення комунікаційного процесу. В цьому випадку достатньо змінити спосіб формування ідентифікаційних даних. Функціональність і порядок використання таких знеособлених інформаційних систем повністю зберігаються.

Рисунок 2.6 – Організація безпеки інформаційних систем персональних даних

Можливий також універсальний спосіб знеособлення і подальшої експлуатації недоступних для самостійної модернізації інформаційних систем персональних даних, які дозволяють виводити призначені для роздруківки бухгалтерські та інші документи в файл для подальшого редагування. Він полягає в розробці нескладної програми або макросу для автоматичної зворотної заміни особистих кодів на ПІБ в вивантажених з інформаційних систем персональних даних для роздруківки документах [8; 26].

Важливими перевагами зазначеного способу знеособлення інформаційних

систем персональних даних, крім універсальності, є:

- збереження функціональності і сервісного супроводу знеособлення діючих інформаційних систем персональних даних без їх програмної модернізації;
- використання єдиного кодифікатора ПІБ;
- можливість децентралізованого використання кодифікатора ПІБ на окремих комп'ютерах;
- забезпечення належного зберігання і використання кодифікатора ПІБ на захищеному вбудованому або окремому зовнішньому носії;
- можливість редагування і доповнення кодифікатора ПІБ відповідним програмним забезпеченням.

Сегментування полягає в поділі мережевої інформаційної системи персональних даних на кілька сегментів для зменшення вимог і спрощення захисту персональних даних [26]. Даний спосіб на практиці є одним з основних.

Альтернативним способом сегментування є використання сертифікованих міжмережевих серверних екранів. Однак на практиці обидва ці способи пов'язані з придбанням додаткового серверного обладнання та програмного забезпечення, підвищеними витратами на адміністрування і технологічний супровід сегментованої інформаційної системи персональних даних [26].

Підключення інформаційних систем персональних даних до мереж загального користування, в тому числі до мережі Internet, вимагає додаткових засобів захисту навіть в тому випадку, якщо передача персональних даних по ним не передбачена. Для зменшення вимог і витрат на захист інформації доцільно ізолювати від мережі Internet всі локальні мережеві інформаційні системи персональних даних [26].

Для забезпечення необхідного інформаційного взаємодії через мережі Internet (пересилання електронних платіжних документів, даних персоналізованого податкового обліку та ін.) рекомендується використовувати виділені автоматизовані робочі місця, які не підключені до локальних мережевих ІСПД [8]. Перенесення персональних даних між взаємодіючими в

мережі Internet виділеними комп'ютерами і локальними ІСПД доцільно здійснювати за допомогою маркованих знімних носіїв. В іншому випадку, необхідно додатково використовувати сертифіковані міжмережеві серверні екрани. З метою захисту персональних даних при передачі по каналах зв'язку учасниками інформаційного обміну застосовуються також засоби криптографічного захисту інформації, сертифіковані в установленому порядку.

2.3 Інноваційні напрями на шляху захисту персональних даних

Ключові проблеми у забезпеченні належного захисту персональних даних полягають у розробці відповідних процесів управління персональними даними та встановленні відповідальності за такі процеси. Для інноваційного шляху у захисті персональних даних необхідно мати досвід роботи у сфері права, інформаційної безпеки, відповідності нормативним вимогам та якості бізнес-процесів, а також умінь ефективного впровадження необхідних технічних та організаційних заходів, передових практик забезпечення дотримання захисту персональних даних [39].

Для запровадження захисту даних установи варто дотримуватися європейського регламенту захисту персональних даних. В першу чергу потрібен чіткий аналітичний огляд персональних даних, які знаходяться в установі, включаючи організовані записи обробки персональних даних, процеси обробку персональних даних, відповідно до протоколів та внутрішніх нормативних документів установи, визначити інформаційні процеси, які містять персональні дані та конкретні типи даних, та оцінити невідповідність між поточною ситуацією та необхідністю регулювання [39].

Мета обробки персональних даних повинна бути обґрунтована, для чого необхідно встановити відповідні періоди зберігання даних [39]. Тому варто використати наступні заходи:

- систематичний опис передбачуваної обробки та її мети, а також, де це доречно, законних інтересів, яких переслідує процесор;
- оцінку необхідності та пропорційності операцій обробки, що стосуються

її цілей;

- оцінка ризиків для прав і свобод суб'єктів даних;
- заходи, спрямовані на подолання ризиків (включаючи гарантії), заходи безпеки та механізми для забезпечення захисту персональних даних та демонстрації відповідності.

Класифікація витоків інформації систем персональних даних установи теоретично відбувається переважно двома канали витоку даних в інформаційних мережах: мережа передачі даних і мобільні пристрої, до них же слід відносити й мобільні носії даних [32].

Причини витоку можна умовно розділити на внутрішні і зовнішні. До зовнішніх витік відносять, наприклад, успішну DDoS атаку з подальшим проникненням всередину периметра корпоративної безпеки і отриманням доступу до шуканим даними. До внутрішніх витоків, а саме до них відноситься на сьогоднішній день більше 90 % всіх витоків даних, відносяться ситуації з умисними або ненавмисними діями співробітників компаній і організацій, в результаті яких конфіденційність даних була порушена [32].

Рисунок 2.7 – Шляхи витоків інформації систем персональних даних установи

На жаль, захистити критичні дані, в тому числі і персональні дані клієнтів і контрагентів, на 100 % не зможе жодна компанія. Нинішній розвиток технологій DLP дозволяє лише мінімізувати ризики. Один з підходів, який використовується в DLP–аналіз контенту.

Рисунок 2.8 – Причини витоків інформації систем персональних даних установи

Даний принцип не залежить від специфіки каналу витоків, і заснований на аналізі змісту файлів або потоків при передачі їх по мережі або при операціях збереження, копіювання або перенесення на різні носії інформації. Метою даного аналізу є локалізація конфіденційних даних і запобігання їх нелегального виходу за периметр безпеки [32].

Перш ніж говорити про DLP–системи, необхідно визначитися з поняттями – під DLP–системами прийнято розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Сама абревіатура DLP розшифровується як Data Leak Prevention, тобто, запобігання витокам даних. Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю витікаючу, а в ряді випадків і вхідну інформацію. Контрольованою інформацією повинен бути не тільки internet-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі захищається контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і тощо.

Оскільки DLP–система повинна перешкоджати витоку конфіденційної інформації, то вона в обов’язковому порядку має вбудовані механізми визначення ступеня конфіденційності документа, виявленого в перехоплений

трафік. Крім свого основного завдання, пов'язаної із запобіганням витоків інформації, DLP–системи також добре підходять для вирішення низки інших завдань, пов'язаних з контролем дій персоналу.

Визначення конфіденційного вмісту проводиться DLP–системою, як правило, за списком ключових слів, що складають основу конфіденційної інформації. Різні виробники по різному підходять до цього питання і реалізують ці механізми на основі алгоритмів фільтрації контенту, або контекстної фільтрації.

Більш досконала система заснована на принципі «грифування» електронних документів, названа так за аналогією грифу на паперовому документі. Технічно це реалізовано у вигляді позначки файлів, вміщаючи спеціальний тег в ім'я файлу. Найбільш ефективною виявилася техніка установки мітки всередину файлу. Однак такий спосіб значно обмежує роботу з документами і залишає лазівки для зловмисника [32].

Рисунок 2.9 – Створення DLP–систем захисту персональних даних

Для використання підходу грифування потрібно провести повний аналіз і класифікацію всіх електронних документів в організації і позначити всі секретні файли відповідним чином. Головним недоліком таких методів є те, що помітити все конфіденційні документи, як правило, дуже складно. Ще важче постійно підтримувати базу даних грифовані документів. Щоб вирішити цю проблему програма переносить грифи в нові файли зі старих документів при їх

трансформації і таким чином суттєво спрощує процес.

Одна зі складностей, з якими зіткнулася галузь інформаційної безпеки це те, що DLP–системою можна легко назвати антивірус, оскільки він дозволяє уникнути «троянів», які відсилають інформацію своїм замовникам, і програму для контролю пристроїв в операційній системі, оскільки вона бореться з витоками через мобільні пристрої і накопичувачі. Однак і антивірус, і система контролю пристроїв закривають лише один з каналів витоків [32]. Практично половина сучасних витоків відбувається в результаті крадіжки мобільних пристроїв. В цьому випадку єдиним ефективним способом захисту є шифрування даних. Це дозволяє надійно захистити дані на дисках мобільних пристроїв – ноутбуків, КПК, смартфонів, змінних носіїв тощо.

Отже, практично ідеальним засобом захисту персональних і конфіденційних даних в умовах реальної дійсності може бути рішення, яке комбінує основні підходи до аналізу і контролю контенту, дозволяє усунути витоку за класичними каналах, а також мінімізувати збиток від вкрадених мобільних пристроїв за рахунок шифрування дисків. У такому рішенні має бути присутня централізована система аудиту і доказова база всіх дій з конфіденційними документами. Крім того, рішення має враховувати специфіку організацій і бути підлаштовано під основні бізнес-процеси організацій [32].

Ключовою проблемою при впровадженні DLP–систем, стало те, що до моменту початку впровадження системи компанія замовник вже повинна мати чітке і ясне уявлення про те, які конфіденційні дані знаходяться в її розпорядженні, як і де вони зберігаються, які дії з ними проводяться.

Понад 70 % організацій взагалі не уявляють, які дані слід віднести до категорії критичних. В цьому випадку дуже може допомогти застосування DLP-систем, які мають функціональність при завданні правильного класифікатора даних за ступенем їх конфіденційності і визначенні чітких критеріїв ідентифікації цих даних, дозволить автоматично призвести процедуру аналізу всіх даних і дій над ними. DLP–система володіє такою функціональністю, яка дозволить спростити процес впровадження технології захисту від витоків.

Цілком зрозуміло, що для створення повноцінної комплексної системи захисту інформації (КСЗІ) потрібні значні кошти. Тому сьогодні в технічних рішеннях при створенні комплексу ТЗІ АСБД перевага надається заходам пасивного захисту інформації. Крім питання фінансового забезпечення ТЗІ АСБД (мова навіть не йде про вибір серверних рішень чи клієнт-серверних платформ), актуальним залишається питання компетенції працівників, які працюють з інформацією АСБД (внесення змін, передача даних тощо). Таким чином, на повноцінну реалізацію ТЗІ баз персональних даних значною мірою впливають: недоліки існуючого законодавства (зокрема ЗУ «Про захист персональних даних»); відсутність фінансування заходів ТЗІ АСБД бюджетами всіх рівнів (органи влади та місцевого самоврядування, комунальні підприємства) та комерційними структурами; людський фактор (надзвичайно низький рівень компетенції відповідальних осіб, які мають відповідати за безпеку використання АСБД).

Таблиця 2.1 - Процедура організації захисту баз персональних даних

Підготовка розпорядчих актів та документації	***Проектування комплексу ТЗІ***
Порядок обробки персональних даних в АСБД *Згода на обробку персональних даних* *Повідомлення про включення персональних даних до АСБД* *Зобов'язання щодо збереження інформації з обмеженим доступом* *Наказ про ведення АСБД* (визначення бази, затвердження Порядку обробки персональних даних, призначення відповідальних, внесення змін до положень про структурні підрозділи та посадових інструкцій працівників, діяльність яких пов'язана з використанням персональних даних тощо)	Виконання заходів ТЗІ

Незважаючи на всі зусилля, сьогодні більшість компаній все ж не готові

захищати наявні в їхньому розпорядженні дані.

Ефективне функціонування системи захисту персональних даних установи передбачає реалізацію багатоетапного комплексу заходів. Така система захисту персональних даних забезпечить конфіденційність операційних персональних даних, цільовий характер персональної інформації, обмеження доступу посадових до ПД, доступ до особистих ПД, гарантування прав і свобод користувача у сфері захисту ПД.

При використанні традиційних моделей загроз необхідно забезпечити функціонування відповідних для них вимог, реалізації традиційних заходів з організації і технічного забезпечення безпеки персональних даних установ. Серед традиційних заходів захисту інформаційних систем персональних даних: організація безпеки приміщення, контроль за використанням мікрофонну і динаміків, розстановка моніторів відвернутими від вікна/відвідувача, контроль використання бездротових пристроїв, запровадження парольного захисту тощо.

Практичним засобом захисту персональних даних в умовах реальної дійсності може бути інноваційне рішення, яке комбінує основні підходи до аналізу і контролю контенту, дозволяє усунути витоку за класичними каналах, а також мінімізувати збиток від вкрадених мобільних пристроїв за рахунок шифрування дисків. У такому рішенні має бути присутня централізована система аудиту і доказова база всіх дій з конфіденційними документами.

РОЗДІЛ 3
ПОТРЕБИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЛОГІСТИЧНОЇ КОМПАНІЇ

3.1 Основні принципи функціонування електронної системи персональних даних логістичного оператора

Нині сформувалася світова тенденція до інформатизації суспільних процесів про які говорять такі фактори як – цифровізація документаційно-інформаційної комунікації, поширення комп'ютерних технологій, утворення інформаційних хабів і баз даних, тощо. Розвиток цифрової економіки, електронного урядування й комерції ставить під питання цілісність національного й глобального інформаційного простору, потребу урегулювання й уніфікації вимог до утворення, функціонування і збереження цифрових баз даних, їх взаємної інтеграції, недоторканості особистої приватної інформації і персональних даних, узгодження систем безпеки ефективного функціонування.

Побудова системи захисту персональних даних логістичного оператора та її функціонування повинні здійснюватися відповідно до таких принципів:

Принципи організації захисту персональних даних		
	законність	гнучкість
	системність	професіоналізм
	комплексність	самоспостереження
	безперервність	спеціалізація
	своєчасність	самооцінювання
	спадкоємність і безперервність вдосконалення	знання своїх партнерів і працівників
	розумна достатність і адекватність	науково-технічна обґрунтованість
	персональна відповідальність	відкритість алгоритмів захисту
	мінімізація повноважень	обов'язковість контролю

Рисунок 3.1 – Принципи організації захисту персональних даних логістичного оператора [3]

За допомогою інтернет-технологій з’явилась можливість надати клієнтам ряд додаткових логістичних послуг: відстеження вантажів, довідкові дані, порівняння альтернативних варіантів, індивідуалізація обслуговування.

Захист персональних даних в документаційно-інформаційних системах логістичного оператора повинен ґрунтуватися на положеннях і вимогах існуючих законів, стандартів і нормативно-методичних документів щодо захисту персональних даних і враховує кращі світові практики. Системний підхід до побудови захисту персональних даних передбачає врахування всіх взаємопов’язаних, взаємодіючих і змінних в часі елементів, умов і факторів, істотно значущих для розуміння, вирішення проблеми забезпечення безпеки персональних даних. Безпека даних забезпечується комплексом програмно-технічних засобів і підтримують їх організаційних заходів, реалізованих логістичним оператором [1].

Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а самі персональні дані знаходять все ширше використання в найрізноманітніших сферах від бізнесу до політики. Їх використання стає багатоаспектнішим і, окрім допомоги в роботі та побуті, вони можуть слугувати для декого інструментом порушення прав та свобод людини, зокрема права на приватність. Застосування різних засобів і технологій захисту інформації має перекривати всі істотні (значущі) канали реалізації загроз безпеки персональних даних і не містити слабких місць в узгодженні застосовуваних засобів і технології захисту інформації. Повинен бути забезпечений галузевий підхід до розробки рекомендацій (вимог) щодо захисту персональних даних з урахуванням особливостей їх обробки в інформаційних системах даних логістичного оператора.

Володілець (підприємство, що займається роздрібною торгівлею) веде базу даних, в яку включаються такі категорії даних про клієнтів: 1) прізвище, ім’я та по батькові, 2) рік, дата народження та вік, 3) телефон/електронна адреса, 5) адреса проживання, 6) місце роботи (сфера зайнятості), 7) дані про склад сім’ї, 8) дані про придбані товари протягом останніх років. Доступ до бази даних

передбачається надавати на чотирьох рівнях: Керівник – доступ до всіх категорій даних; Спеціаліст-маркетолог (розробка та реалізація заходів щодо просування товарів володільця на ринку) – доступ до 2, 3, 6, 7, 8; Спеціаліст із закупівель – 8; Спеціаліст з продажу (прийняття замовлення та доставка товару) – доступ до 1, 2, 3 категорії даних; Спеціаліст по роботі з постійними клієнтами – доступ до 1–8 категорії даних.

Можна навести приблизний порядок обробки персональних даних. Володілець/розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про: – дату, час та джерело збирання персональних даних суб'єкта; – зміну персональних даних; – перегляд персональних даних; – будь-яку передачу (копіювання) персональних даних суб'єкта; – дату та час видалення або знищення персональних даних; – працівника, який здійснив одну із указаних операцій; – мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

Система захисту персональних даних повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення і несанкціонованого доступу до персональних даних, але і з урахуванням можливості підвищення рівня захисту в міру виявлення нових моделей безпеки для персональних даних, розвитку способів і засобів їх реалізації в інформаційних системах персональних даних.

Станом на сьогодні незаконне поширення персональних даних у мережі Інтернет залишається практично безкарним. Так, особу, яка поширила

персональні дані, як правило, просто неможливо встановити, оскільки доменне ім'я сайту, де незаконно поширені персональні дані, зареєстроване зазвичай в іншій державі. Інформація, надана хостинг-провайдером щодо особи, яка зареєструвала доменне ім'я, також не завжди відповідає дійсності.

У таких випадках є можливість заблокувати доступ до вебсторінки чи видалити її. Для цього наглядовий орган спочатку звертається до адміністрації сайту з вимогою (приписом) видалити інформацію, що порушує права суб'єкта на захист персональних даних. У випадку відсутності реакції наглядовий орган або самостійно блокує доступ до сторінки, де містяться незаконно поширені персональні дані, або звертається з цією метою до суду, який приймає відповідне рішення. При цьому, якщо наглядовий орган здійснює блокування самостійно, особа, яка розмістила відповідну інформацію на веб-сайті має право оскаржити такі дії до суду.

В Україні станом на сьогодні відсутні будь-які юридичні механізми такого характеру. Як наслідок, ні встановити особу, яка причетна до незаконного поширення інформації, ні заблокувати доступ до такої інформації немає можливості. Усвідомлюючи такий стан справ, правопорушники часто навіть не намагаються приховати незаконність розміщеної інформації. Звісно, надання таких повноважень наглядовому органу може призвести до суперечливих ситуації, коли адміністрація сайту вважатиме, що розміщена інформація не порушувала законодавство, а наглядовий орган доводитиме протилежне. Однак, саме для цього такі повноваження наглядового органу повинні здійснюватися під попереднім чи ретроспективним контролем суду. Таким чином, буде врівноважено право особи на захист її приватного життя та право адміністрації сайту на свободу висловлення поглядів та поширення інформації.

На даний час абсолютна безкарність поширення інформації в Інтернеті призводить до частих порушень права особи на приватність і відповідальність за такий стан справ повністю лежить на державі.

Система захисту персональних даних логістичного оператора будується на основі єдиної технічної політики, з використанням функціональних

можливостей інформаційних технологій, реалізованих в інформаційній системі і наявних систем і засобів захисту відповідно до розроблених типовими моделями загроз і профілями захисту. При створенні систем захисту персональних даних можуть використовуватися системи і засоби захисту інформації, які використовуються в організації для забезпечення безпеки комерційної таємниці та іншої конфіденційної інформації [9].

Захист персональних даних повинен забезпечуватися на всіх технологічних етапах обробки персональних даних і у всіх режимах функціонування, в тому числі при проведенні ремонтних та регламентних робіт. Вжиті заходи щодо забезпечення безпеки персональних даних повинні носити своєчасний попереджувальний характер. Логістичний оператор вживає необхідних заходів щодо захисту персональних даних до початку їх обробки, що має забезпечити належний рівень безпеки даних. Системи захисту персональних даних розробляються одночасно з розробкою і розвитком інформаційних систем персональних даних логістичного оператора, що дозволяє враховувати вимоги з безпеки при проектуванні і модернізації систем захисту персональних даних [14].

Наступність і безперервність вдосконалення інформаційних систем персональних даних повинно відбуватися на основі результатів аналізу функціонування вже існуючих систем захисту персональних даних з урахуванням виявлення нових способів і засобів реалізації безпеки, вітчизняного і зарубіжного позитивного досвіду в сфері захисту інформації. Логістичний оператор повинен визначати дії, необхідні для усунення причин потенційних невідповідностей вимогам з безпеки персональних даних з метою запобігти їх повторній появі. Заходи, що вживаються мають носити запобіжний характер і повинні передбачати можливі негативні наслідки.

Рівень достатності та адекватності дій має відповідати стану і вартості реалізації заходів захисту, порівнюватися з ризиками, пов’язаними з обробкою і характером персональних даних, що потребують підвищенню рівня безпеки. Аналіз ризиків порушення безпеки персональних даних проводиться з метою

визначення впливу системи захисту інформації на ймовірність реалізації загроз безпеки персональних даних з урахуванням вразливостей інформаційної інфраструктури логістичного оператора [9].

Програмно-технічні засоби захисту не повинні істотно погіршувати основні функціональні характеристики і продуктивність інформаційних систем персональних даних логістичного оператора. Персональна відповідальність за безпеку персональних даних в інформаційній системі логістичного оператора покладається на кожного працівника в межах його повноважень. Розподіл обов'язків і повноважень працівників логістичного оператора має забезпечувати виявлення винних осіб у випадках порушення безпеки персональних даних. Ролі та обов'язки співробітників повинні бути визначені і документально підтверджені відповідно до організаційної політикою в області захисту інформації [3].

Принцип мінімізації повноважень передбачає надання та використання прав доступу до персональних даних на обмеженому і керованому рівні. Користувачам необхідно мінімальні права доступу до персональних даних в ІСПД тільки відповідно з виробничою необхідністю. Доступ до персональних даних повинен надаватися тільки в тому випадку і обсязі, якщо це необхідно співробітнику для виконання його посадових обов'язків. Користувачеві повинні бути заборонені всі операції з персональними даними за винятком тих, які дозволені відкрито.

Принцип гнучкості в процесі функціонування інформаційних систем персональних даних дозволить змінювати її характеристики, а також обсяг і категорію оброблюваних логістичним оператором персональних даних. Для забезпечення можливості варіювання рівня захищеності персональних даних, система захисту персональних даних логістичного оператора повинна володіти гнучкістю.

Відкритість алгоритмів і механізмів захисту персональних даних дозволить відійти від традиційних моделей захисту, які здійснюються тільки за рахунок приховування структури, технологій і алгоритмів функціонування системи

захисту персональних даних. Знання зазначених характеристик системи захисту персональних даних не повинно давати можливості подолання захисту можливими порушниками безпеки персональних даних, включаючи розробників засобів захисту [1].

Рівень рекомендацій і вимог щодо захисту персональних даних повинен відповідати наявному рівню наукової обґрунтованості, технічної реалізація процесів, розвитку інформаційних технологій та засобів захисту інформації. При створенні і експлуатації системи захисту персональних даних необхідно орієнтуватися на кращі сучасні вітчизняні і зарубіжні технічні рішення і практику захисту інформації [3].

Реалізація заходів щодо забезпечення безпеки персональних даних і експлуатація систем захисту персональних даних повинна здійснюватися відповідно до спеціалізації та професійно підготовленими фахівцями логістичного оператора. Компанія повинна володіти інформацією про своїх партнерів, що дозволяє мінімізувати ймовірність реалізації негативних проявів в сфері безпеки інформаційних систем персональних даних, джерела яких пов’язані з людським фактором. Логістичний оператор повинен реалізовувати кадрову політику (ретельний підбір персоналу і мотивація працівників), що дозволяє виключити або мінімізувати можливість порушення безпеки персональних даних своїми працівниками [9].

Правила захисту персональних даних, які застосовуються в Європі, встановлені двома міжнародними інструментами. Конвенція Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних бере початок з 1981 року і була першим міжнародним документом, який встановив юридично обов’язкові правила захисту персональних даних. Більшість європейських країн, включаючи Україну, є сторонами цього документу. Конвенція була доповнена в 2001 році Додатковим протоколом, який встановлює правила щодо органів нагляду та транскордонних потоків даних.

Держави-члени Європейського Союзу також мають зобов’язання відповідно до Директиви ЄС «Про захист прав приватних осіб стосовно

обробки персональних даних та про вільний рух таких даних» 1995 р., яка містить у цілому схожі, але більш детальні положення, у порівнянні з Конвенцією. Відбувся швидкий розвиток інформаційних та комунікаційних технологій із часу прийняття цих інструментів і, відповідно, в даний час ведеться робота і Радою Європи, і Європейським Союзом із метою зробити їх інструменти з питань захисту персональних даних більш придатними до реагування на виклики двадцять першого століття.

В «Правилах надання та отримання телекомунікаційних послуг» (Постанова КМУ 11 квітня 2012 року №295) до персональних даних споживачів віднесено дані, які стосуються абонентів, містять інформацію про особисте життя фізичних осіб і пов'язані з правом на приватність: «відомості про абонента, отриманих під час укладання договору» і які згідно Закону України «Про захист персональних даних» є первинними джерелами відомостей про фізичну особу (видані на ім'я фізичної особи документи, підписані нею документи; відомості, які особа надала про себе).

Пропоновані логістичним оператором заходи щодо забезпечення безпеки персональних даних повинні бути сплановані так, щоб результат їх застосування був прозорий для користувачів послуг логістичної компанії і міг би бути оцінений державними органами влади, що здійснюють функції по контролю і нагляду в межах своїх повноважень. Невід’ємною частиною робіт по захисту персональних даних є оцінка ефективності системи захисту та контроль за всіма інформаційними процесами компанії.

3.2 Організація системи захисту персональних даних логістичної компанії в умовах цифрової економіки

Запровадження вимог захисту персональних даних національного законодавства і Загального регламенту Європейського Союзу про захист даних, є багатоетапним процесом. Особливо це позначається на організації систем захисту персональних даних логістичної компанії в умовах цифрової економіки. В першу чергу необхідно проаналізувати персональні дані інформаційної

системи логістичного оператора, якими він керує та обробляєте, включаючи організовані записи обробки персональних даних [39].

Разом з «оцифруванням» в диджитал трансформуються злочинність, вандалізм і війни. Зростання кількості кібератак провокують переклад інфраструктури і даних в хмару і розвиток Інтернету Речей (IoT). Постійно виявляються нові вразливості гаджетів і мобільних пристроїв. Smart-речі містять безліч подібних «лазівок», і це вже саме собою є проблемою. Адже кожна вразливість – це додаткова точка входу в хмарний сервіс або інфраструктуру для кіберзлочинців. Цілі зловмисників – скомпрометувати облікові записи користувачів, або отримати контроль над їхніми пристроями.

Необхідно знати, які дані надаються для обробки програмним забезпеченням, які дані надсилаються до зацікавлених сторін, які спеціальні категорії особистих даних зберігаються, як захищати ці дані тощо.

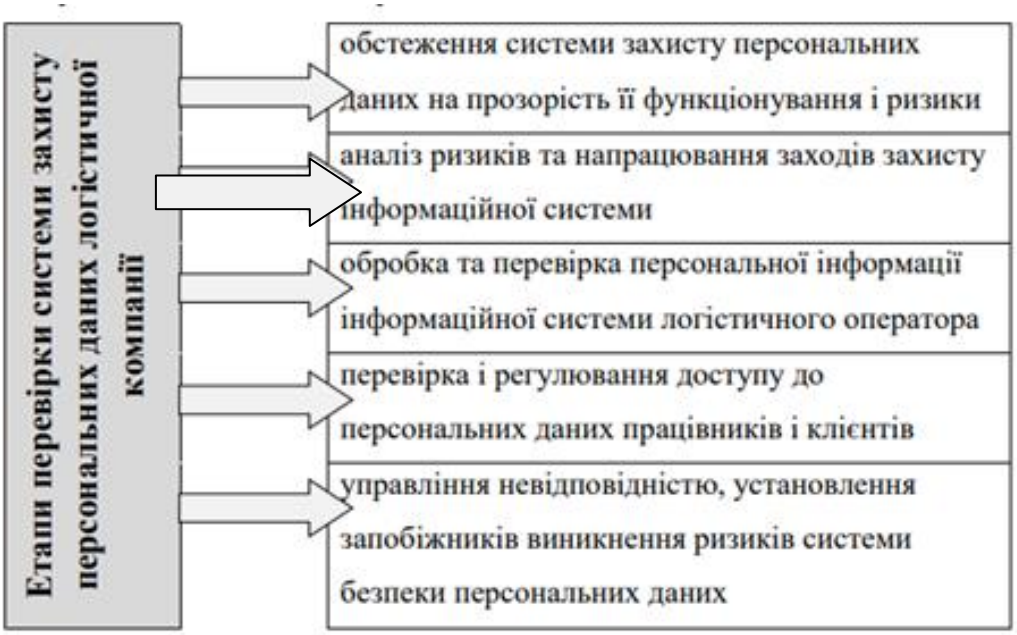

Рисунок 3.2 – Перевірка системи захисту персональних даних логістичної компанії

Тому всі сучасні й майбутні атаки будуть проходити від імені реальних облікових записів користувачів. Це так звана «загроза атаки інсайдера» в новому виконанні, коли зловмисник діє від імені підконтрольного йому облікового запису користувача або технічної служби. Щоб виявити скомпрометовані акаунти користувачів, варто в обов’язковому порядку відстежувати поведінку

облікових записів користувачів і призначених для користувача пристроїв. Розробникам ПЗ і IT-провайдерам варто подумати про максимальний захист власної інфраструктури і контроль вразливостей в ПЗ і сервісах. Варто враховувати, що IT і кібербезпека – це різні речі, часто навіть полярні. Спеціалізований аудит не буде зайвим навіть для най впевненішої в своїх силах компанії. Технології кіберзахисту змінюються. Боротьба з кіберзлочинністю давно припинила бути війною одинаків: абстрактні «айтішники» переходять на абонентське обслуговування в центрах комплексного управління загрозами (SOC), підписуються на індикатори загроз Threat Intelligence.

З метою планування наступних кроків необхідно зробити аналіз виявлених невідповідностей реальної ситуації і бажаного рівня захисту персональних даних. Під час аналізу перевіряється обробка даних регламентована локальними протоколами та внутрішніми нормативними документами, визначаються процеси, які містять персональні дані та конкретні типи даних, та оцінюються невідповідності між поточною ситуацією та тим, що вимагає регулювання і захисту. Аналіз невідповідностей призводить до переліку всіх процесів, оцінки очікуваного обсягу роботи та часу необхідного для:

- створення записів обробки даних;
- підготовка або адаптація планів класифікації;
- підготовка оцінок впливу.

Далі відбувається облік обробки персональних даних. Встановлюються записи діяльності з обробки персональних даних [39]. На основі аналізу розриву та переліку процесів ми розглядаємо:

- зміни до зазначених процесів, що вимагаються внутрішніми протоколами, на відміну від місцевих законів про захист персональних даних;
- управління базами даних, необхідними для обробки даних;
- властивості встановлених інтеграцій.

Наступним кроком вибудовується план класифікації та внутрішні правила. У разі необхідності готується або змінюється план класифікації. Мета обробки

персональних даних повинна бути обґрунтована, для чого необхідно встановити відповідні періоди зберігання даних у класифікаційному плані. Таким чином, переглядаються всі періоди зберігання і визначаються початок і тривалість періодів зберігання для всіх процесів. Якщо немає плану класифікації або існуючий план неповний, варто його підготувати або завершити з метою досягнення відповідності реального стану і бажаного рівня захисту. Крім того, якщо виявлено, що внесення змін до плану класифікації вимагає внесення змін до внутрішніх правил, необхідно підготувати або доповнити такі правила. Останнє застосовується, якщо адміністративні органи підтвердили свої внутрішні правила [39].

Оцінки впливу є важливими для обробки конкретних персональних даних і є доцільними для всіх інших обробок, якщо можливо, що тип обробки буде представляти значний ризик для прав і свобод людини. Підготовка оцінок впливу охоплює як мінімум:

- систематичний опис передбачуваної обробки та її мети, а також, де це доречно, законних інтересів, які переслідує організатор;
- оцінку необхідності та пропорційності операцій обробки, що стосуються її цілей;
- оцінка ризиків для прав і свобод суб’єктів даних;
- заходи, спрямовані на подолання ризиків (включаючи гарантії), заходи безпеки та механізми для забезпечення захисту персональних даних та демонстрації відповідності.

Необхідно перевірити чи співпрацює логістична компанія з надійними обробниками даних контракту та оцінюєте, чи потрібно оновити існуючі контракти з учасниками цього інформаційного процесу обміну персональними даним. І тут необхідно вказати наступну інформацію:

- зміст і тривалість обробки;
- характер і мету обробки;
- типи оброблюваних персональних даних;
- категорії суб’єктів даних;

- права та обов’язки учасників процесу обміну даними.

Паралельно з наведеними діями також розглядається завдання забезпечення відповідності ІТ–системи логістичної установи. Незважаючи на те, що питання відповідності спеціального програмного забезпечення може здаватися швидко і легко вирішеним, не варто його недооцінювати.

Ці та інші пов’язані з цим питання особливо важливі при прийнятті рішень щодо використання нових програмних рішень. Тут варто обирати відповідні сертифіковані інструменти та послуги. У будь-якому випадку, ви повинні знати про такі питання у світлі змін у ваших ІТ–системах або можливого обороту працівників або підрядників [39].

3.3 Захист інформаційної системи персональних даних клієнтів компанії «Нова пошта»

В логістичній компанії «Нова пошта» чинний внутрішній документ, який регламентує доступ працівників і клієнтів до інформації персональних даних. «Політика конфідеційності» встановлює порядок обробки персональних даних, зібраних за допомогою сайту і пов’язаних з ними послуг і інструментів. У всіх зазначених випадках Компанія обробляє персональні дані користувачів виключно в рамках вимог Закону України «Про захист персональних даних» та Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних [15].

Склад персональних даних на скріншотах, що в 2018 році було опубліковано у ЗМІ, відрізняється від тих даних, які обробляє «Нова пошта» за допомогою своєї інформаційної системи. Такими є результати перевірки компанії, що провели фахівці секретаріату уповноваженого Верховної Ради з прав людини щодо додержання законодавства про захист персональних даних, повідомляє прес-служба «Нової пошти». У системі «Нової пошти» фахівці не виявили інформації про заявників, щодо яких начебто був витік даних.

Пошук в інформаційній системі компанії можливий лише за номером експрес-накладної та/або номером телефону. Інформація про експедирування

зберігаються не більше 3 місяців, після чого програма видаляє їх автоматично.

Окремі випадки виявлено і в інших компаніях. Так співробітники кіберполіції затримали в Київській області екс-працівника Пенсійного фонду, який продавав в інтернеті персональні дані українців. На комп'ютері екс-чиновника поліцейські виявили більше 250 баз даних. Служба безпеки України тоді повідомила, що підозрює компанію Яндекс у державній зраді – за інформацією СБУ, менеджмент компанії незаконно збирав, накопичував і передавав в рф персональні дані українських громадян.

Які механізми використання отриманих даних зловмисниками. Перш за все, нав'язлива реклама, спам SMS і за електронною поштою, холодні дзвінки. Далі йдуть варіанти використання цих даних в якості компонента атак соціальної інженерії з різноманітними, далекосяжними наслідками.

Оперуючи поняттями кібербезпека та інформаційна безпека часто підміняють поняття та вводять людей в оману. Кібербезпека – це безпека IT систем (обладнання та програм). Інформаційна безпека – це безпека інформації, зазвичай організації чи компанії, у тому числі в IT системах. Кібербезпека є частиною інформаційної безпеки будь-якої організації.

Наскільки захищений домашній комп'ютер чи вебсайт від зламу хакерами – це питання кібербезпеки. Але стікер із записаним паролем від комп'ютера чи профайлу у соцмережі збережений / закріплений на екрані монітору – це вже питання персональної інформаційної безпеки.

Хакери – це, в основному, спеціалісти з кібербезпеки. Вони вивчають як побудовані різні IT системи, щоб знайти в них слабкі місця і використати їх для отримання вигоди, чи то фінансової, чи для інших цілей. Хакерам протидіють не тільки Білі Хакери (White Hats), які також знаходять вразливі місця в наших IT системах, але роблять це відкрито, аби допомогти нам закрити наявні проблемні місця, але й спеціалісти з інформаційної безпеки, тому що для проникнення в ту чи іншу організацію можуть використовуватись не тільки прямі методи зламу тієї чи іншої системи, але також і прості людські слабкості – збережені паролі у відкритих місцях, зайва балакучість співробітників,

фішинг, спам, прийоми соціальної інженерії по телефону, емейл і т.п.

Підприємство обробляє інформацію зібрану при реєстрації: при створенні користувачем облікового запису на сайті, компанія може вимагати певну інформацію, таку як дійсну адресу електронної пошти та пароль. Обліковий запис включає в себе таку інформацію про клієнта, як ім'я та прізвище, номер телефону і супутню інформацію, в тому числі фотографії, які можна завантажувати у свій обліковий запис [10].

Логістичний оператор може збирати інформацію сервісів, які використовують клієнти. Зокрема, ігри, реклама, звернення клієнтів тощо. Компанія може також збирати іншу інформацію про спілкування з користувачами, наприклад, будь-які запити до служби підтримки, що подаються користувачами, або будь-який зворотний зв'язок, що надається ними. Компанія може автоматично отримувати і реєструвати на своїх серверах інформацію з браузера користувача або будь-якого пристрою, включаючи IP–адресу, геолокацію, програмне забезпечення і апаратні атрибути, сторінки, які запитує користувач, дані, які містяться в базах даних браузера, включаючи SQL бази даних, мобільні ідентифікатори (включаючи ідентифікатори мобільних пристроїв, такі як Google Advertisement ID, IFA or IFV), інформацію про використання додатків, та / або інформацію про інші використовувані пристрої, або інформацію системного рівня [15].

Компанія може збирати та зберігати інформацію, що отримана в результаті опитувань, що можуть проводитись компанією, або залученими підрядниками, а саме інформацію щодо статі, віку, сімейного стану, особистих вподобань та ін. В процесі роботи сайту компанія може збирати певну інформацію за допомогою таких технологій як кукіс (куки, cookies), пікселі (pixels) та локального сховища (як у конкретному браузері або мобільному пристрої). Компанія не збирає і не обробляє персональні дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках та подібну інформацію [10].

Для надання своїх послуг компанія використовує інформацію, яку збирає і

розміщує для

- забезпечення обслуговування клієнтів, в тому числі для створення і управління обліковими записами користувачів, вирішення технічних труднощів і доступу до різних функцій;
- адаптації пропозицій і досвіду, в тому числі реклами на своїх сервісах або сервісах третіх осіб;
- контролю загальної та індивідуальної активності користувачів для управління трафіком на сайті;
- зв'язку з користувачами, в тому числі з питань сервісу, обслуговування клієнтів або дозволених маркетингових комунікацій через будь-які доступні канали зв'язку;
- проведення науково-дослідницької та аналітичної активності з метою поліпшення нашого сервісу;
- оцінки деяких факторів особистої інформації, зокрема, для аналізу та прогнозування особистих вподобань, інтересів, поведінки та місцезнаходження [11].

Логістична компанія може ділитися інформацією, яку вона збирає, крім тієї, що відноситься до персональних даних у розумінні Закону України «Про захист персональних даних», з афілійованими особами (компанії, що діють на основі права спільної власності або перебувають під загальним контролем кінцевих бенефіціарних власників ТОВ «Нова Пошта Інтернешнл»), розташованої в будь-якій третій країні. Компанія може надавати персональні дані користувачів на запити компетентних органів, оформлених відповідно до вимог чинного законодавства України. Компанія може передавати певну знеособлену інформацію (дані, які не дозволяють ідентифікувати користувачів окремо) стороннім постачальникам послуг, довіреним партнерам або авторизованим дослідникам з метою кращого розуміння, яка реклама або послуги можуть зацікавити користувачів, поліпшення загальної якості та ефективності послуг на сайті або сервісів, або для забезпечення свого внеску в наукові дослідження, які, на думку Компанії, можуть приносити велику

соціальну користь [11].

Користувачі, які створили обліковий запис на сайті компанії, можуть отримувати доступ, виправляти або видаляти інформацію, яку вони надають. Користувач несе відповідальність за точність наданих даних, або повідомлень на сайті. Вся інформація, яку збирає логістична компанія в розумних межах захищена технічними засобами і процедурами забезпечення безпеки з метою запобігання несанкціонованому доступу або використання даних [15].

Інформаційна система логістичного оператора є програмно-технічним комплексом, за допомогою якого «Нова Пошта» здійснює експедирування поштових відправлень. Пошук в інформаційній системі компанії можливий лише за номером експрес-накладної або номером телефону. Інформація про експедирування зберігаються не більше трьох місяців, після чого програма видаляє їх автоматично.

В результаті внутрішніх перевірок компанії та аудитів в систему внесено низку змін, що створили додаткові перешкоди можливим зловмисникам. При цьому проведений комплекс заходів не є остаточним, заплановано комплексні заходи із захисту персональних даних, внутрішнього та зовнішнього аудиту безпеки, зміни архітектури. Увага до проблеми безпеки даних дозволила логістичному оператору значною мірою розширити власну та залучити зовнішню експертизу, скористатися допомогою потужних компаній і структур з підтримки IT–безпеки [11].

Директор з інформаційних технологій логістичного оператора наголосив, що в планах є різні кроки щодо вдосконалення захисту персональних даних клієнтів, в яких особлива увага приділяється інформаційній безпеці, передовим механізмам захисту даних і моніторингу ризиків. Компанія впроваджує нову стратегічну IT–програму і планує запустити системи криптографічного захисту, анонімізації персональних і аналітичних даних клієнтів для підвищення інформаційної безпеки компанії [15].

Криптографічні методи захисту інформації – це методи захисту даних із використанням шифрування, головною метою якого захист від

несанкціонованого читання.

Системи криптографічного захисту (системи шифрування інформації) для on-line–систем можна поділити за ознаками:

за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

за способом реалізації (апаратний, програмний, програмно-апаратний);

за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачи);

за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо [11].

Додатковими механізмами криптозахисту є додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту. За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним, або програмно-апаратним.

Заходи з анонімізації даних являють собою метод видалення персональних даних з набору даних з метою захисту приватного життя фізичної особи або компанії, від яких ці дані були отримані. В міру розширення використання аналітики даних і технологій «великих даних», використання анонімізувати (знеособлених) наборів даних стало популярним. Ідея полягає в тому, щоб взяти конфіденційні дані і видалити будь-яку інформацію, яка може дозволити відновити їх зв’язок з конкретною людиною. Після цього дані можуть бути використані не ставлячи під загрозу недоторканність приватного життя людей.

Загалом, логістична компанія «Нова Пошта» піклується про безпеку особистих даних клієнтів і регулярно вдосконалює всі рівні захисту своїх баз.

Компанія розділяє Загальний регламент щодо захисту даних Європейського парламенту (GDPR) і орієнтується на викладені в ньому стандарти безпеки персональних даних [11].

Системність у створенні захисту персональних даних логістичного оператора передбачає функціонування її на низці визначених принципів, врахування всіх взаємопов'язаних, взаємодіючих і змінних в часі елементів, умов і факторів, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки персональних даних.

З метою своєчасного виявлення та припинення спроб порушення встановлених правил забезпечення безпеки персональних даних логістичного оператора повинні бути визначені процедури для постійного контролю використання систем обробки та захисту персональних даних, а результати контролю повинні регулярно аналізуватися. Логістична діяльність вимагає створення моделі захисту оперативних персональних даних заснованих на традиційних та інноваційних рішеннях, які є основою при прийнятті рішень щодо використання нових апаратних і програмних рішень. Для створення надійного захисту інформації логістичної компанії «Нова Пошта» та унеможливлення в майбутньому зловмисного проникнення в периметр безпеки її інформаційної системи необхідно здійснити кроки із апаратно-програмного вдосконалення системи захисту, криптографічного та анонімізаційного захисту, що створить надійний захист інформаційної системи та оперативних персональних даних компанії.

ВИСНОВКИ

Підсумовуючи розгляд теми бакалаврської роботи і послідовне виконання зазначених завдань стає можливим викладення узагальнених висновків:

В сучасних умовах цифровізації документаційних процесів кожна установа або підприємство має справу з персональною інформацією клієнта, зокрема з обробкою персональних даних кінцевого споживача. До персональних даних відносять інформацію за допомогою якою стає можливим ідентифікація особи та містить її особисті дані. Саме тому для унеможливлення маніпулювання й запобігання порушення прав і свобод людини персональні дані необхідно де-ідентифікувати, зашифрувати, або псевдонімізувати таким чином, щоб особа не була ідентифікована, такі дані більше не вважаються персональними. Українське законодавство передбачає процесуальні дії з персональними даними людини які включають в себе збирання, реєстрація, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення, знищення персональних даних.

Персональні дані, які можуть бути використані для повторної ідентифікації особи потребують відповідного системного захисту з боку національних та міжнародних установ. Загальні вимоги щодо обробки та захисту персональних даних суб'єктів персональних даних визначені Типовим порядком обробки персональних даних затвердженим наказом Уповноваженого ВРУ з прав людини. Україна в питанні захисту персональних даних спирається на міжнародний досвід.

Загальний регламент захисту даних, який діє у ЄС з 2016 р., встановлює безпосередньо застосовні правила щодо прав суб'єктів даних, обов'язки тих організацій, які вимагають обробки персональних даних, і тих, які здійснюють обробку, міжнародні передачі даних і повноваження наглядових органів. В ЄС склався комплексний механізм захисту персональних даних, який ґрунтується на наявності загальноєвропейської нормативної бази, національних

законодавчих актів і європейських консультативних і наглядових органів. Юридичні норми ЄС про захист даних вважаються в світі золотим стандартом.

Створення та ефективне функціонування системи захисту персональних даних установи передбачає реалізацію багатоетапного комплексу заходів. Запровадження таких заходів захисту забезпечить конфіденційність одержуваних персональних даних, максимальне обмеження доступу посадових і третіх осіб до зазначених відомостей, цільовий характер персональної інформації, вільний доступ працівника до власних персональних даних, гарантованість суб'єктивних прав користувача, пов'язаних із захистом його персональних даних.

При використанні типових моделей загроз необхідно забезпечити функціонування відповідних вимог, реалізації традиційних заходів з організації і технічного забезпечення безпеки персональних даних установ. Серед традиційних заходів захисту інформаційних систем персональних даних: організація безпеки приміщення, контроль за використанням мікрофонну і динаміків, розстановка моніторів, контроль використання бездротових пристроїв, запровадження парольного захисту BIOS, використання дротових або бездротових засобів мережевої взаємодії, заборона недозволених додатків.

В організації захисту інформаційної системи персональних даних слід враховувати, що в ряді випадків можливості реалізації окремих загроз можуть бути вищими і вимагати додаткових заходів захисту персональних даних. Сучасним інструментом створення DLP–систем захисту персональних даних установи, яка включає такі заходи як грифування ім'я файлів установи, міткування всередині файлу, автопролонгація грифування і міткування нових файлів, захист internet-трафіку, захист мережевих інформаційних потоків, захист мобільних носіїв інформації, захист мобільних пристроїв (ноутбуків, КПК, смартфонів, тощо).

Функціонування захисту повинно здійснюватися відповідно до таких принципів як законність, системність, комплексність, безперервність, своєчасність, спадкоємність і безперервність вдосконалення, розумна

достатність і адекватність, персональна відповідальність, мінімізація повноважень, гнучкість, професіоналізм, самоспостереження, спеціалізація, само оцінювання, знання своїх партнерів і працівників, науково-технічна обґрунтованість, відкритість алгоритмів захисту, обов'язковість контролю тощо.

Логістична діяльність і пов'язана з нею організація роботи документаційно-інформаційних систем персональних даних вимагає створення моделі захисту, яка відповідає традиційним та інноваційним рішенням. Паралельно розглядається завдання забезпечення відповідності ІТ–системи логістичної установи сучасним вимогам законодавства і технічного розвитку. Ці та інші пов'язані з цим питання особливо важливі при прийнятті рішень щодо використання нових апаратних і програмних рішень.

Для створення надійного захисту логістичної компанії «Нова Пошта» та унеможливлення в майбутньому зловмисного проникнення в периметр безпеки її інформаційної системи необхідно здійснити низку кроків з апаратно-програмного вдосконалення системи захисту. Реалізація криптографічного та анонімізаційного методів, а також вдосконалення програмного забезпечення створить надійний захист персональних даних компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Валькова Н.В. Електронна логістика: визначення та складові її інструментарію. Моделювання регіональної економіки. 2013. № 1. С. 119–128.

2. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів: ДСТУ 4163-2003. Чинний від 01.09.2003. К.: Держспоживстандарт України, 2003. 50 с. (дата звернення: 01.10.2024)

3. Єлетенко О.В. Структура логістичної інформаційної системи підприємства. Прометей. Вип. 1 (22). Донецьк. 2007. С. 204–206.

4. Загальна Декларація Прав Людини: Декларація Генеральної Асамблеї ООН від 10 грудня 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 01.10.2019)

5. Загальний регламент про захист даних: Постанова ЄС № 2016/679 від 27 квітня 2016 р. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення: 01.10.2024)

6. Загорецька О. М. Нормативне та методичне забезпечення організації діловодства й архівної справи в Україні. *Секретар-референт*. 2006. № 1. С. 19–24; № 2. – С. 18–22; № 3. – С. 27–30.

7. Палеха Ю.І. Загальне діловодство: навч. посібник– 2-ге вид. перероб. і доп. К.: Ліра-К, 2014. 623 с.

8. Козак А. Захист персональних данихв ЄС: що потрібно знати українським компаніям. Delo.ua. 10 квітня 2018 р. URL: https://delo.ua/business/zahist-personalnih-danih-v-jes-scho-potribno-znati-ukrajinskim-k-341115/ (дата звернення: 01.10.2024)

9. Колодізєва Т.О. Інноваційні технології в логістиці. Харків: Вид. ХНЕУ. 2013. 268 с.

10. Палеха Ю.І. Документально-інформаційні комунікації: навч. посібник. Ю. І. Палеха, Н.В. Мурейко, О.Г. Оксіюк. К. : Ліра-К, 2014. 532 с.

11. «Нова пошта»: офіційний сайт логістичної компанії. URL: https://novaposhta.ua (дата звернення: 01.04.2025)

12. Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини (ст. 18840): Кодекс України про адміністративні правопорушення. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.

13. Конституція України від 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

14. Павленко А.Ф., Кривещенко В.В. Логістичні інформаційні системи. Маркетингова освіта в Україні (спец.випуск). Київ. 2011. С. 291–299.

15. Політика конфіденційності ТОВ «Нова пошта»: офіційний сайт логістичної компанії. URL: https://novaposhtahelp.zendesk.com/hc/uk/articles/ (дата звернення: 01.10.2019)

16. Порушення законодавства у сфері захисту персональних даних (ст. 18839): Кодекс України про адміністративні правопорушення. Відомості Верховної Ради Української РСР. 1984, додаток до № 51. Ст. 1122.

17. Порушення недоторканності приватного життя (ст. 182): Кримінальний кодекс України. Відомості Верховної Ради України. 2001., № 25-26. Ст. 131

18. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини від 12 серпня 2013 р. № 18/02-13. URL: https://ips.ligazakon.net/document/view/MUS22979?an=1 (дата звернення: 01.10.2019)

19. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних: Лист Уповноваженого Верховної Ради України з прав людини від 03.03.2014 р. № 2/9-227067.14-1/НД-129. URL: http://www.ombudsman.gov.ua/ua/page/secretariat/docs/legislation/poriadok-

povidomlennia-ypovnovazsh.html (дата звернення: 01.11.2024)

20. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах»: Закон України від 31 трав. 2005 р. № 2594-IV. Відомості Верховної Ради України. 2005. № 26. Ст. 347.

21. Про доступ до публічної інформації: Закон України від 13 січ.2011 р. № 2939-VI. Відомості Верховної Ради України. 2011. № 32. Ст. 314.

22. Про затвердження документів у сфері захисту персональних даних: Наказ Уповноваженого ВР України з прав людини від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14 (дата звернення: 01.10.2024)

23. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 р. № 108. Страсбург. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 01.10.2024)

24. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива № 95/46/ЄС Європейського Парламенту і Ради ЄС від 24 жовтня 1995 р. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення: 01.10.2024)

25. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних: Додатковий протокол до Конвенції Ради Європи від 8 листопада 2001 р. № 108. Страсбург. URL: https://zakon.rada.gov.ua/laws/show/994_363 (дата звернення: 01.10.2024)

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

27. Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

28. Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27/28. Ст. 181.

29. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до

Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 17 липня 1997 р. № 475/97-ВР. Відомості Верховної Ради України. 2010. № 46. Ст.542.

30. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12 (дата звернення: 01.10.2024)

31. Уповноважений Верховної Ради України з прав людини. Київ. URL: http://www.ombudsman.gov.ua/ (дата звернення: 01.10.2024)

32. Швецова-Водка Г. Типологія документа: навч. посіб. для студ. інститутів культури. К.: Кн. Палата України, 2014. 180 с.

33. Чухрай Н.І., Гірна О.Б. Розвиток логістики в умовах Е-економіки Логістика. Львів. 2008. № 623. С. 272–278.

34. Central and Eastern Europe Data Protection Authorities (CEEDPA). Tbilisi. URL: https:// http://ceedpa.pdp.ge/ (Last accessed: 01.10.2024)

35. Consulting: Personal data protection compliance (GDPR). *MIKROCOP*. URL: https://www.mikrocop.com/digital-transformation-consulting/data-protection-compliance (Last accessed: 01.10.2024)

36. Dragan I. The E-Logistics System University. *EDUCONS.* URL: http://www.ien.bg.ac.rs/IEN1/images/stories/conferences/03/Ilic%20Dragan.htm (Last accessed: 01.10.2024)

37. European data protection supervisor. Brussels.URL: https:// edps.europa.eu/ (Last accessed: 01.10.2024)

38. Kovalska L. Information technologies as the newest social paradigm of the life of youth. International journal of new economics and social sciences. Warsaw, 2018. Vol. 7, No. 1. P. 335–347.

39. Personal data protection within electronic systems. Asia Business Live Journal. URL: https://www.vantageasia.com/personal-data-protection-within-electronic-systems/ (Last accessed: 01.10.2024)

40. Кулешов С. Г. Управлінське документознавство. К.: ДАКККіМ, 2003.

– 57 с.

41. Керування документаційними процесами : навч. посібник . М. В. Комова, А. М. Пелещишин, Т. М. Білущак. Львів : Видавництво Львівської політехніки, 2013. 188 с.

42. Комова М.В. Документознавство: навч. посіб. Львів: Тріада плюс, 2007. 296 с.

43. Термінологія документознавства та суміжних галузей знань / за заг. ред. В.В. Бездрабко. К.: Четверта хвиля, 2011. 271 с.

44. Шкіцька, І. Ю. Управлінське документознавство [Електронний ресурс] : навч. посіб. / І. Ю. Шкіцька. - 2-ге вид., оновл. і доповн. - Тернопіль : ТНЕУ, 2020. 382 с.

45. Левицька С. Критерії ефективності документаційних процесів. *Бухгалтерський облік і аудит*. 2012. № 1. С. 10-17. URL: http://nbuv.gov.ua/UJRN/boau_2012_1_3.

46. Корж А.В. Документознавство: зразки документів праводілової сфери: навчальний посібник; рекомендовано Міністерством освіти і науки України. вид. 2-ге, змін. та доп. К.: КНТ, 2007. 372с.

47. Антоненко І. Сучасні нормативно-правові акти з керування документаційними процесами (зарубіжний досвід) . Студії з архівної справи та документознавства. 2006. Т. 14. С. 48-58. URL: http://nbuv.gov.ua/UJRN/sasd_2006_14_10

48. Бабій І. В. Основи діловодства: навчально-методичне видання для курсантів та студентів 2–3 курсів. Львів: СПОЛОМ, 2020. 76 с.

49. Бєльська Т. В. Документообіг в публічному управлінні: конспект лекцій. . Харків: ХНУМГ ім. О. М. Бекетова, 2019. 40 с.

50. Матвієнко О., Цивін М. Основи організації електронного документообігу. К.: Центр учбової літератури. 2008. 112 с.

51. Тур О. М., Шабуніна В. В. Стандарти ISO, присвячені процесам оцифровування, конверсії та міграції документів. Документознавство. № 4. 2019. С. 54–61.

52. Чукут С.А. Блокчейн чи система електронного документообігу: сучасні тенденції впровадження в органах виконавчої влади України. *Інвестиції: практика та досвід*. 2018. № 1. С. 70–76.

53. Писаренко В. П. Шляхи вдосконалення організації керування електронними документаційними процесами в діяльності органів влади в Україні. *Теорія та практика державного управління і місцевого самоврядування*. 2018. № 2. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2018_2_25.

54. Кудлай В. О. Керування документаційними процесами в цифровій громаді. Актуальні проблеми науки та освіти : зб. матеріалів XXVI підсумкової наук.-практ. конф. викладачів МДУ, м. Київ, 22 лют. 2024 р. / за заг. ред. М. В. Трофименка. Київ : МДУ, 2024. С. 289–290.

55. Герасимюк, Л. (2016). Тенденції впровадження новітніх технологій керування документаційними процесами в умовах інформатизації суспільства. Інтегровані комунікації, (2), 102-105. https://doi.org/10.28925/2524-2644.2016.2.17

56. Публічний договір приєднання, умови надання послуг та приватність. URL: https://npshopping.com/faq/article/360021326791