Колесник В.С., здобувач
Науковий керівник: Тростенюк Т.М.,
доктор філософії, доцент,
Державний університет «Житомирська політехніка»

ПРАВОВЕ РЕГУЛЮВАННЯ ТА БЕЗПЕКОВІ ВИКЛИКИ ЦИФРОВІЗАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ ПУБЛІЧНИХ СЛУЖБОВЦІВ

У контексті європейської інтеграції та широкої цифрової модернізації публічного сектору особливо важливим є забезпечення високого рівня інформаційної безпеки та кіберстійкості в державних установах. Впровадження автоматизованих інформаційно-аналітичних систем, а також розширення електронного зв'язку між різними адміністраціями, очевидно, вимагає створення надійних механізмів захисту – як нормативних, так і технічних – персональних даних державних службовців. Актуальність цього питання випливає з необхідності переосмислення традиційних механізмів забезпечення конфіденційності та встановлення ефективних інституційних гарантій захисту даних у цифровому середовищі. Сучасний етап розвитку державного управління в Україні характеризується комплексною цифровою трансформацією, впровадженням електронного урядування та електронних публічних послуг. Швидке поширення інформаційних технологій неминуче несе з собою підвищений ризик для кібербезпеки та захисту даних, особливо для працівників державних органів. Такі аспекти, як правова база конфіденційності, гармонізація національного законодавства з європейськими стандартами та ефективний захист персональних даних, мають стратегічне значення для стабільного функціонування інститутів публічного управління.

Міжнародні стандарти формують фундаментальну основу для створення системи захисту персональних даних, у якій ключову роль відіграє Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція № 108). Європейські стандарти чітко визначають базові поняття права на приватне життя, права суб'єктів даних, обов'язки володільців та розпорядників даних, а також гарантії захисту громадянських прав як у судовому процесі, так і на міжнародному рівні [1].

На національному рівні нормативно-правову базу формують базові закони України, які регулюють інформаційні відносини. Ядро цієї системи утворюють Закони «Про захист персональних даних» та «Про інформацію», а також положення Цивільного кодексу України, проте українське законодавство все ще потребує системної кодифікації та адаптації до вимог Регламенту (ЄС) 2016/679 (GDPR) [6].

Правове регулювання захисту персональних даних ґрунтується на фундаментальних принципах, що гарантують ефективний захист прав суб'єктів даних у цифрову епоху [7].

Таблиця 1. **Ключові принципи захисту персональних даних**

Принцип обробки даних	**Зміст та практичне значення**
Законність	Обробка даних здійснюється суворо на підставах, передбачених законом
Справедливість і прозорість	Суб'єкт чітко інформується про мету, обсяги та способи використання його даних
Цільове обмеження	Збір інформації відбувається лише для конкретних, заздалегідь визначених цілей.
Мінімізація	Обсяг даних обмежується виключно мінімально необхідним для надання послуги
Точність	Забезпечення актуальності даних, їх своєчасне виправлення чи видалення
Обмеження зберігання	Дані зберігаються не довше, ніж цього вимагає мета їх обробки
Цілісність та конфіденційність	Гарантування безпеки від несанкціонованої обробки, втрати чи пошкодження

**Джерело:* складено автором на основі джерела [7].

Процеси цифровізації охоплюють не лише надання послуг громадянам, а й внутрішню діяльність державних установ, зокрема управління людськими ресурсами (HR-системи, електронний документообіг, дистанційна робота). Цифровізація трудових відносин у публічному секторі породжує специфічні правові виклики, оскільки вимагає балансу між потребою держави контролювати робочі процеси та ризиком надмірного цифрового стеження та порушення приватності працівників [4].

Системи управління персоналом в публічному управлінні стають привабливою мішенню для кібератак, оскільки вони містять конфіденційні дані про кадровий склад, його кваліфікацію, декларації та службову діяльність. Захист даних у цій сфері вимагає врахування нових європейських норм щодо кіберстійкості та використання штучного інтелекту [3].

Практичне впровадження послуг електронного урядування виявляє низку системних адміністративних та правових проблем. Серед основних викликів – постійна відсутність обов'язкової оцінки впливу на захист даних для впровадження нових публічних платформ, невідповідності в обміні інформацією між міжвідомчими реєстрами та невідповідність національних процедур вимогам європейського законодавства [2].

Для подолання цих викликів доцільно спиратися на передовий міжнародний досвід у побудові електронного урядування та наданні публічних послуг. Аналіз практики цифрового управління в країнах ЄС підкреслює необхідність встановлення чітких правових норм та регуляторних гарантій для захисту конфіденційності та даних громадян і державних службовців [8].

В умовах комплексної цифровізації публічного управління та переходу державних установ на електронний документообіг та хмарні сервіси, захист персональних даних виходить за межі суто нормативно-правових рамок. Практична кібербезпека державних установ значною мірою залежить від щоденної поведінки співробітників та дотримання ними основних протоколів безпеки [5]. Хакери все частіше вибирають державних службовців як головні цілі для атак (наприклад, за допомогою соціальної інженерії або фішингу), враховуючи, що їхні офіси надають доступ до конфіденційних державних реєстрів та чутливих баз даних.

Для ефективного захисту інформаційних ресурсів та пристроїв у публічному секторі необхідно реалізовувати комплексну технічну та організаційну модель, що охоплює кілька ключових рівнів:

Безпека облікових записів та надійна автентифікація:

обов'язкове впровадження багатофакторної автентифікації (2FA) для всіх корпоративних облікових записів, електронної пошти та державних електронних систем, що створює додатковий рівень захисту, навіть якщо пароль було скомпрометовано;

використовуйте складні та унікальні паролі довжиною щонайменше від 12 до 16 символів, які містять великі та малі літери, цифри та спеціальні символи;

регулярно змінюйте свої паролі, а також суворо заборонено записувати паролі на папері або ділитися ними з кимось;

Технічний захист робочих пристроїв та мережевої інфраструктури:

своєчасне та регулярне встановлення оновлень безпеки (патчів) для операційних систем, браузерів та всього офісного програмного забезпечення, оскільки застаріле програмне забезпечення є основною вразливістю до кібератак;

повна заборона на підключення та використання USB-накопичувачів, зовнішніх жорстких дисків або інших сторонніх та неперевірених носіїв інформації до робочих станцій державних установ;

обов'язкове та виключне використання ліцензованого антивірусного програмного забезпечення та захищених, зашифрованих каналів зв'язку (VPN) під час віддаленої роботи;

Заходи захисту від кіберзагроз, кібератак та фішингу:

будьте надзвичайно обережні під час обробки вхідних електронних листів: ретельно перевіряйте адресу відправника, не відкривайте підозрілі вкладення (стиснуті файли, документи з невідомих джерел) та не натискайте на сумнівні посилання;

негайно припиніть роботу та повідомте відділ кібербезпеки вашої установи, якщо помітите найменші ознаки незвичайної поведінки комп'ютера або спроб несанкціонованого входу;

Правила збереження та резервного копіювання даних (Стандарт 3-2-1):

створити щонайменше три копії критично важливих робочих документів та масивів даних, зберігаючи їх на двох різних типах носіїв;

обов'язкове віддалене зберігання щонайменше однієї копії в захищеному хмарному середовищі установи у разі надзвичайних ситуацій або збоїв локального обладнання;

періодичне тестування процедур відновлення інформації для забезпечення безперервності діяльності державного органу.

Дотримання цих правил сприяє створенню сильної внутрішньої культури кібербезпеки в публічному секторі, мінімізує ризик витоку персональних даних громадян та забезпечує стабільне функціонування державних установ [5].

Підсумовуючи, результати дослідження свідчать про те, що цифровізація публічних послуг вимагає збалансованого підходу, з одного боку, впровадження найсучасніших електронних сервісів, а з іншого, забезпечення надійного захисту персональних даних – як юридично, так і технічно. Створення ефективної національної системи захисту конфіденційності та даних залежить від гармонізації національного законодавства з європейськими стандартами та від суворого дотримання фундаментальних принципів обробки даних, таких як законність, прозорість, цільове обмеження, мінімізація та конфіденційність.

Особливу увагу необхідно приділяти управлінню персоналом та внутрішньому електронному документообігу в публічних установах, оскільки впровадження цифрових інструментів для моніторингу робочих процесів не повинно порушувати конституційне право працівників на недоторканність приватного життя. Водночас, зростаюча інтенсивність кіберзагроз робить персонал та бази даних потенційними цілями, що вимагає вищого рівня захисту. Крім того, впровадження цифрових державних послуг виявляє низку адміністративних та правових прогалин, зокрема відсутність систематичної оцінки впливу на захист даних на етапі розробки програмного забезпечення, а також конфлікти в обміні інформацією між різними державними органами. Ці недоліки можна усунути, застосовуючи передовий міжнародний досвід у секторі електронного урядування.

Однак, нормативні положення створюють лише правову базу, тоді як фактична безпека інформаційних ресурсів значною мірою залежить від людського фактору. Впровадження багатофакторної автентифікації, регулярні оновлення програмного забезпечення, пильність щодо фішингових електронних листів та систематичне резервне копіювання даних за принципом «3-2-1» формують основу надійної кібергігієни. Лише поєднання належного правового регулювання та сильної культури кібербезпеки серед працівників державного управління може гарантувати цілісність персональних даних та забезпечити високий рівень довіри громадян до цифрових інституцій держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: правове регулювання та практичні аспекти. Науково-практичний посібник. URL: https://rm.coe.int/168059920c

2. Волошанівська Т.В. Персональні дані в цифрових державних сервісах та адміністративно-правові виклики їх захисту. URL: https://www.researchgate.net/publication/410671234_.

3. Жуляєв В.В. Захист даних у системі управління персоналом в умовах викликів та кіберзагроз для інформаційної приватності. Економіка та суспільство. URL: https://economyandsociety.in.ua/index.php/journal/article/view/7267.

4. Малюга Л.Ю, Шкрібляк К.П. Особливості захисту персональних даних у процесі цифровізації трудових відносин в Україні: теоретико-правовий аналіз. Науковий вісник Ужгородського національного університету. Серія: Право. URL: https://visnyk-pravo.uzhnu.edu.ua/

5. Національне агентство України з питань державної служби - Як убезпечити робочі дані та пристрої: гайд Держспецзв'язку. URL: https://nads.gov.ua/news/yak-ubezpechyty-robochi.

6. Осика Ю.В. Правове регулювання використання персональних даних. Державний податковий університет. URL: https://ojs.dpu.edu.ua/index.php/.

7. Правове регулювання захисту персональних даних в Україні 9401 - статті - consultant.net.ua. «Консультант» Юридичний маркетплейс: послуги юриста онлайн - consultant.net.ua. URL: https://consultant.net.ua/consultant-article/9401.

8. Проданюк Н.Б. Правові основи надання цифрових послуг: національний та міжнародний досвід. Академічні візії. URL: https://academy-vision.org/index.php

Коломацька А.С., здобувач
Науковий керівник:Кучменко В.О.,
доктор наук з державного управління, кандидат економічних наук, доцент;
Державного університету «Житомирська політехніка»

ДИСТАНЦІЙНЕ ЗАЛУЧЕННЯ ОСІБ ДО ДИВЕРСІЙНО-ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ: СУЧАСНІ МОДЕЛІ ТА ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОЇ ОЦІНКИ

Повномасштабна збройна агресія Російської Федерації проти України супроводжується залученням громадян України до диверсій, терористичних актів, підпалів та інших суспільно небезпечних діянь. Цифрові засоби комунікації змінили не лише спосіб встановлення контакту з потенційними виконавцями, а й організаційну модель такої діяльності – організатор може дистанційно здійснювати пошук особи, передавати інструкції, контролювати виконання та розраховуватися з виконавцем, одночасно приховуючи власну належність і загальний задум операції. Значна частина таких контактів відбувається з використанням месенджера «Телеграм».

За результатами аналізу наявної інформації щодо диверсійно-терористичних проявів на території України протягом 2024-2026 років можна виокремити кілька моделей дистанційного залучення виконавців. Найпростішою є вербування на матеріальній основі, коли особі під виглядом «легкого заробітку» пропонують винагороду за конкретне протиправне завдання, зокрема підпал майна [2]. Виконавець може не знати справжнього замовника або загального задуму, однак усвідомлює фактичний характер власних дій. Складнішою є модель, за якої застосовуються обман, психологічний тиск або використання уразливого стану, внаслідок чого змінюється не лише обсяг доступної виконавцю інформації, а й його уявлення про мету завдання.

Особливе місце посідає залучення «під чужим прапором». У 2026 році Служба безпеки України неодноразово фіксувала випадки, коли представники російських спецслужб під час дистанційного контакту приховували свою справжню належність і діяли від імені українських правоохоронних органів. Після встановлення такого контакту особам пропонували або нав'язували виконання різних за характером завдань – від спостереження за визначеними об'єктами та переміщення предметів до дій, пов'язаних із підпалами, вибуховими пристроями та підготовкою терористичних чи диверсійних проявів [3]. Показовий випадок було також оприлюднено СБ України у вересні 2026 року: контакт із потенційною виконавицею російський представник установив під легендою українського правоохоронця, після чого їй було передано завдання, пов'язане з підготовкою терористичного акту [4].

Принципова особливість такої моделі полягає в тому, що особа помиляється щодо фактичної належності того, від кого отримує завдання, та того, в чиїх інтересах фактично діє. Виконавець може розуміти фізичний зміст своїх дій – наприклад, усвідомлювати факт підпалу чи переміщення певного предмета (зазвичай, гранат або саморобних вибухових пристроїв), – але водночас бути переконаним, що виконує завдання українського правоохоронного органу та сприяє захисту держави. Отже, однаковий об'єктивний результат не обов'язково означає однаковий зміст умислу.