

Іванна ЩУРКО

здобувачка освітньо-професійної програми
«Публічне управління та адміністрування», ЗУНУ
Науковий керівник – к. е. н., доцент, доцент кафедри
менеджменту, публічного управління та персоналу ЗУНУ
Лідія КРУП'ЯК

ОСОБЛИВОСТІ ЗАПРОВАДЖЕННЯ МЕТОДІВ ЗАХИСТУ КАДРОВОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ ОРГАНУ МІСЦЕВОГО САМОВРЯДУВАННЯ

Постійний розвиток інформаційних технологій в сучасному світі та невпинне зростання впровадження трансформаційних процесів цифрової інтеграції діяльності публічної служби вимагають від органу місцевого самоврядування удосконалення захисту кадрової інформації.

Останні роки в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним впровадженням новітніх інформаційних технологій, не є винятком публічні процеси та управління персоналом в органах місцевого самоврядування. Швидке зростання цифровізації вимагає від органів публічної влади підвищення рівня інформаційної безпеки, оскільки крім безперечних переваг, виникає ряд ризиків витоку конфіденційної інформації та даних. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Зазначимо, що захист інформації кадрової служби в органах місцевого самоврядування є важливим аспектом для забезпечення конфіденційності, правового захисту та ефективності публічного управління. Враховуючи те, що кадрові служби зберігають значні обсяги конфіденційних даних, впровадження сучасних методів захисту надасть змогу уникнути ризиків витоку інформації, несанкціонованого доступу та кібератак.

Масштаби збирання та спільного використання персональних

даних суттєво зросли. Технології дозволяють як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності [3].

Персональні дані в органах місцевого самоврядування можуть зберігатися як на папері, так і в інформаційних системах або на інших носіях. Оскільки сьогодні майже вся інформація оцифровується, ризик витоку даних в електронній формі значно вищий. При цьому загрозу може становити, як зовнішній злам системи з віддаленого комп'ютера (так звана хакерська атака), так і недбалість чи навмисні дії з боку службовців ОМС, тобто коли до протиправного поширення даних причетні самі працівники [1].

Масштаби й діапазон роботи з інформацією в кожному ОМС різняться. Водночас принципи та алгоритми захисту інформації залишаються єдиними, оскільки типові ризики її втрати, знищення чи неконтрольованого витоку достатньо давно відомі та описані. Поняття «ризик» не слід пов'язувати лише з «людським фактором», адже до виникнення інцидентів інформаційної безпеки можуть призвести й інші чинники. Повністю уникнути ризиків й убезпечити зібрану інформацію в умовах сучасного цифрового світу складно. Водночас передбачити потенційні загрози, своєчасно виявляти, мінімізувати та певною мірою навіть управляти ними - цілком можливо [2].

У відділах кадрів, діловодства та архівах зберігаються особові справи працівників органу місцевого самоврядування і депутатів місцевих рад, які містять, окрім їхніх особистих даних, ще відомості про склад сім'ї тощо. Здебільшого в органах місцевого самоврядування не організовані безпечні умови обробки спеціальної категорії даних, які можуть становити особливі ризики для людини - небезпеку переслідування, тиску, фізичної розправи або порушення інших прав та свобод. Переважна частина проблем, з якими стикнулися органи місцевого самоврядування у воєнний час, не є новою або притаманною лише сьогодні. Недоліки в організації роботи із захисту персональних даних існували й до

повномасштабної війни, проте саме виклики воєнного часу загострили їх, почасти зробивши їх такими, що безпосередньо впливають на життя та безпеку людини [1].

Отже, захист кадрової інформації в процесі роботи кадрових служб в органах місцевого самоврядування стає необхідним кроком в умовах викликів сьогодення, враховуючи законодавчі вимоги , високий ризик кіберзагроз , потребу в підвищенні ефективності управління людськими ресурсами. Це не лише обов'язок з дотримання діючого законодавства, але й необхідна складова побудови довірливих відносин між працівниками і роботодавцем, особливо в органах місцевого самоврядування.

Список використаних джерел

1. Шадська У., Олексіук Т., Батчаєв В. Захист персональних даних в органах місцевого самоврядування: стандарти і кроки впровадження: посібн. Київ, Асоціація УМДПЛ, 2022. 58 с.
2. Шадська У.С. Аналіз ризиків під час обробки персональних даних: що важливо знати?б: посіб. К.: Компринт, 2021. 68 с.
3. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text