на положенні про те, що своєчасне отримання заробітної плати є конституційним правом працівника. Ним пропонується посилити захист права на оплату праці, передбачити компенсацію за затримку виплат, підвищити відповідальність роботодавців та запровадити механізм гарантійної установи для захисту працівників у разі неплатоспроможності роботодавця [4, с. 313].

Прийняття запропонованих змін мінімізує ризики затримок в оплаті праці та забезпечить працівників надійним страховим механізмом на випадок банкрутства власника. Це не лише покращить стан соціально-економічного захисту громадян, а й дозволить Україні максимально наблизити регулювання трудових відносин до стандартів Європейського Союзу.

Отже, публічно-правові засади оплати праці в умовах воєнного стану поєднують державне регулювання із збереженням базових трудових гарантій та їх адаптацією до умов війни. Держава виступає гарантом своєчасної та справедливої оплати праці, забезпечуючи баланс між економічними можливостями та соціальним захистом. Водночас подальше вдосконалення законодавства спрямоване на посилення гарантій своєчасної виплати заробітної плати та підвищення рівня захисту працівників.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Кодекс законів про працю України від 10 грудня 1971 року № 322-VII. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text
3. Про оплату праці: Закон України від 24 березня 1995 р. № 108/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/108/95-%D0%B2%D1%80#Text
4. Клайда Н. Я. Правове регулювання оплати праці в умовах воєнного стану: трудові гарантії, обов'язки роботодавця та межі відповідальності. Вісник національної асоціації адвокатів України. 2025. Т. 11, вип. 116. С. 34–35. URL: https://unba.org.ua/assets/uploads/news/vidannya/2025-12-04-vidannya-v-snik-11-2025_69313e20cabb2.pdf
5. Маньгора Т. В., Мелешин А. В. Особливості відповідальності за порушення законодавства про оплату праці в умовах воєнного стану. Наукові інновації та передові технології. Київ, 2023. Т. 13, вип. 27. С. 302–314. URL: https://socrates.vsau.org/repository/getfile.php/34892.pdf

Дідняк Анастасія Валеріївна,

здобувачка вищої освіти четвертого курсу інженерно-енергетичного факультету Миколаївського національного аграрного університету

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНИХ РЕЄСТРІВ В УМОВАХ ВОЄННИХ ЗАГРОЗ

Інформаційна безпека є ключовою передумовою ефективного функціонування системи громадського управління, оскільки сучасна держава все більше спирається на використання цифрових технологій, електронних інформаційних ресурсів та мережевих каналів комунікації. За таких умов порушення цілісності, конфіденційності чи доступності інформаційних даних неминуче спричиняє дестабілізацію роботи органів державної влади та ускладнює виконання їх функцій. У сфері публічного управління інформаційна безпека виконує системоутворюючу роль [1, с. 134], забезпечуючи належний рівень стабільності процесів прийняття управлінських рішень, надійний захист персональних даних громадян, а також безперервність і якість надання державних послуг.

В межах системи електронного урядування, де громадяни здійснюють подання заяв на отримання соціальних виплат або реєстрацію підприємницької діяльності через онлайн-платформи, порушення конфіденційності даних може спричинити випадки шахрайства. У разі отримання злодіями доступу до державних реєстрів виникає ризик модифікації або знищення критично важливих записів, що суттєво ускладнює функціонування адміністративних органів. В окремих випадках це може призвести до їх часткової чи повної дезорганізації [2, с. 45]. Тимчасова недоступність системи реєстрації актів громадянського стану внаслідок кібератаки унеможливлює для громадян оформлення актів народження, шлюбу чи отримання необхідних офіційних довідок, що, в свою чергу, спричиняє соціальну напругу та негативно впливає на рівень довіри населення до державних інституцій.

Забезпечення захисту інформаційних систем органів місцевого самоврядування є необхідною умовою їхнього стабільного функціонування [3, с. 202]. У разі втрати міською радою контролю за власними базами даних внаслідок вірусної атаки можуть виникати суттєві перебої у діяльності комунальних служб, процесах бюджетного розподілу, а також у плануванні та реалізації інфраструктурних проєктів. Навіть короткочасне порушення інформаційної безпеки здатне спричинити значні фінансові втрати, а також призвести до затримок у впровадженні соціально важливих програм розвитку.

Слід враховувати й загрози кіберрозвідки та дезінформаційних кампаній. Поширення неправдивої інформації через зламані офіційні акаунти органів влади можуть спричиняти паніку серед населення або впливати на політичну стабільність. Тому захист інформаційних каналів комунікації держави є не менш важливим, ніж захист технічної інфраструктури [4, с. 475].

Кіберзагрози справляють істотний вплив на функціонування державних інформаційних ресурсів, оскільки сучасна система державного управління все більшою мірою ґрунтується на використанні цифрової інфраструктури, електронних баз даних та інтегрованих інформаційних систем. Порушення їхньої роботи внаслідок кібератак здатне спричинити масштабні збої в діяльності органів державної влади, призвести до втрати або викрадення інформаційних даних, а також обумовити тимчасову чи повну недоступність критично важливих сервісів для громадян.

Найпоширеним проявом кіберзагроз є атаки типу ransomware, під час яких шахраї здійснюють шифрування даних державних установ та висувають вимогу викупу за їх подальше відновлення. У разі компрометації інформаційних систем міністерства або органів місцевого самоврядування подібним програмним забезпеченням може бути заблоковано доступ до реєстрів соціальних виплат чи податкових даних, що фактично призводить до припинення надання адміністративних послуг населенню. Навіть нетривала недоступність інформаційних ресурсів спричиняє накопичення адміністративних затримок та порушує стабільне функціонування державного апарату.

Ще одним аспектом впливу кіберзагроз є витоки конфіденційної інформації, що виникають у разі компрометації державних інформаційних систем [5, с. 26], зокрема у сфері охорони здоров'я. Можливе несанкціоноване розголошення персональних даних пацієнтів, включаючи медичні діагнози, історії лікування та іншу ідентифікаційну інформацію, що становить порушення права громадян на приватність. Водночас створюються передумови для можливого шантажу чи дискримінаційного ставлення.

Окрему загрозу становлять кібератаки на виборчі та адміністративні цифрові платформи [6, с. 27]. У разі здійснення атак під час виборчого процесу на інформаційні системи, які забезпечують реєстрацію виборців або підрахунок голосів, виникають обґрунтовані сумніви щодо достовірності отриманих результатів. Це, у свою чергу, може призводити до загострення політичної ситуації, формування соціальної напруги.

Уразливість цифрових систем державного управління наголошує на необхідності неперервного удосконалення механізмів кіберзахисту, впровадження сучасних технологічних рішень у сфері інформаційної безпеки, а також підвищення рівня цифрової стійкості державних інституцій. Це зумовлено зростанням складності кіберзагроз та

розширенням залежності державних органів від цифрової інфраструктури, що потребує системного та комплексного підходу до забезпечення безпеки інформаційних ресурсів.

В умовах посилення кіберзагроз та поглиблення процесів цифровізації державного управління забезпечення захисту державних інформаційних ресурсів ґрунтується на базових засадах [7, с. 239], спрямованих на підтримання їх цілісності, конфіденційності та доступності. Важливою передумовою ефективного функціонування такої системи є впровадження багаторівневого кіберзахисту, що дає змогу суттєво зменшити ризики несанкціонованого доступу до критично важливих даних. Реалізація цього підходу передбачає застосування сучасних механізмів автентифікації користувачів, впровадження систем виявлення вторгнень, а також використання технологій шифрування інформації, що зберігається в державних реєстрах.

Важливою складовою забезпечення інформаційної безпеки є підтримання неперервності функціонування інформаційних систем навіть в умовах виникнення кіберінцидентів. У разі здійснення кібератаки на систему податкової служби необхідним є завчасне впровадження резервних серверів та механізмів відновлення даних. Це дає змогу мінімізувати тривалість простою та запобігти втраті критично важливої інформації. У разі порушень у роботі системи електронної ідентифікації громадян має забезпечуватися можливість альтернативного доступу до державних послуг, оскільки це дозволяє уникнути дестабілізації та повного паралічу адміністративних процесів.

Важливим є контроль доступу до інформаційних ресурсів. Він передбачає чітке розмежування прав користувачів [8, с. 262]. Працівники різних підрозділів органів державної влади повинні мати доступ лише до тієї частини даних, яка потрібна для виконання їх функціональних обов'язків. Це зменшує ризик внутрішніх витоків інформації.

Отже, сучасні кіберзагрози можуть призводити до порушення роботи державних інформаційних систем, витоку конфіденційних даних та дестабілізувати процес надання адміністративних послуг. Особливого значення набувають впровадження сучасних засобів шифрування, резервного копіювання даних та систем оперативного реагування на кіберінциденти. Підвищення рівня цифрової стійкості державних інституцій сприятиме захисту національних інтересів та зміцненню довіри громадян до органів державної влади.

Список використаних джерел:

1. Kurepin V. M. The eu black sea strategy as a tool for shaping regional securhty: analysis of approaches to containing russia. Maritime security of the Baltic-Black Sea region: challenges and threats: V International scientific conference : conference proceedings (November 26, 2025, Odesa, Ukraine). Riga, Latvia : «Baltija Publishing», 2025. С. 132-135. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/24225.

2. Іваненко В.С. Фактори вразливості об’єктів перед терористичними нападами та шляхи їх подолання. Problems of Emergency Situations : матеріали міжнар. наук.-практ. конф., м. Черкаси, 14 травня 2025 р. Черкаси : Національний університет цивільного захисту України, 2025. С. 44-46. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/21484.

3. Іваненко В.С. Штучний інтелект у системах безпеки. Інформаційні технології в сучасному світі : матеріали міжнар. наук.-практ. конф. здобувачів вищої освіти і молодих учених, м. Харків, 29 квітня 2025 р. / Державний біотехнологічний університет. Харків, 2025, С. 200-203. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/21614.

4. Самойленко О. О., Бацуровська І. В., Курепін В. М. Кібергігієна та безпека життєдіяльності як ключові елементи цифрової компетентності здобувачів освіти. Національні інтереси України. 2025. № 11(16). С 461-477. DOI:https://doi.org/10.52058/3041-1793-2025-11(16)-461-476.

5. Власова Н. Цифрові освітні платформи крізь призму кібербезпеки. Освіта в умовах цифрової трансформації: сучасний стан та перспективи розвитку: Матеріали І Всеукраїнської студентської науково-практичної конференції (м. Кам’янець-Подільський, 26 лютого 2026 р.). Кам’янець-Подільський : Навчально-реабілітаційний заклад вищої

освіти «Кам'янець-Подільський державний інститут», 2026. С. 25-27. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/24545.

6. Іваненко В. С. Макроекономічні аспекти економічної безпеки підприємств аграрного профілю. Управління механізмами гарантування фінансово-економічної безпеки соціально-економічних систем різних рівнів функціонування : матеріали IV всеукраїнської науково-практичної конференції (м. Миколаїв; 26–28 листопада 2025 р.). Миколаїв : МНАУ, 2025. С. 27-28. https://dspace.mnau.edu.ua/jspui/handle/123456789/23929.

7. Іваненко В.С., Курепін В.М. Розвиток комунікативної компетентності фахівців цивільного захисту в умовах цифрової трансформації освіти. Українська мова та культура в сучасному гуманітарному часопросторі: аспекти міжмовної комунікації та формування комунікативної компетентності сучасного фахівця : збірник матеріалів міжнародної науково-практичної інтернет-конференції пам'яті філолога, журналіста та захисника України Володимира Мукана (м. Ірпінь – Ломжа, 20 лютого 2026 року). Ломжа : MANS w Łomży, 2026 С 232-242. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/24764.

8. Курепін В. М., Самойленко О. О., Бацуровська І. В. Кібербезпека цифрового освітнього середовища як складова системи безпеки праці та життєдіяльності. Суспільство та національні інтереси: журнал. 2025. № 11(19). С 255-268. https://doi.org/10.52058/3041-1572-2025-11(19)-255-267.

Добрянська Наталія Валеріївна,
професор кафедри державно-правових і гуманітарних наук
Таврійського національного університету імені В. І. Вернадського,
кандидат юридичних наук, професор

ЗАПОБІГАННЯ КОНФЛІКТУ ІНТЕРЕСІВ У ПУБЛІЧНІЙ СЛУЖБІ: ЗАГАЛЬНО-ТЕОРЕТИЧНІ АСПЕКТИ

Конфлікт інтересів у публічній службі є однією з ключових проблем, що впливають на ефективність державного управління та довіру громадян до державних інституцій. Конфлікт інтересів визначається як ситуація, в якій особисті інтереси службовця можуть вплинути на неупередженість виконання ним службових обов'язків. Така ситуація може виникати через фінансові, сімейні чи інші особисті зв'язки, що можуть вплинути на об'єктивність прийняття рішень.

Юридичні аспекти запобігання конфлікту інтересів регулюються законодавством, яке встановлює обов'язки та обмеження для державних службовців. В Україні, таким нормативно-правовим актом є Закон України «Про запобігання корупції» від 14 жовтня 2014 року № 1700-VII, який містить положення щодо запобігання конфлікту інтересів, зокрема, обов'язок декларування майна та доходів, а також обмеження на подарунки та інші форми винагороди [1].

Аналізуючи нормативні та доктринальні дефініції конфлікту інтересів, Р. Дутка, звертає увагу на існування трьох складових конфлікту інтересів. На думку автора, ними є: 1) приватний інтерес; 2) службові чи представницькі повноваження; 3) суперечність між приватним інтересом і службовими чи представницькими повноваженнями [2, с. 137].

Однак, дослідник цілком логічно підкреслює той факт, що відповідальність за порушення норм, спрямованих на врегулювання і запобігання конфлікту інтересів може настати виключно у випадку, коли такий конфлікт інтересів є реальним [2, с. 138].

Як зауважують, А. С. Голуб та М. С. Ковтун, загалом проблематика запобігання та врегулювання конфлікту інтересів є доволі гострою для публічної служби. Натомість, науковці акцентують на тому, що сам по собі конфлікт інтересів не є корупційним діянням. Однак, якщо існуючий конфлікт інтересів між приватною та публічною складовою цього питання не вирішується вчасно і в належний спосіб, він може перерости у корупційне