УДК 005.95

**Матківська Х.С.**

ад’юнкт денної форми навчання

**Зачко О.Б.**

д.т.н., Заслужений діяч науки і техніки України, професор, професор кафедри права та менеджменту у сфері цивільного захисту

Львівський державний університет безпеки життєдіяльності

**УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ ЦИФРОВІЗАЦІЇ HR-ПРОЦЕСІВ В БЕЗПЕКО-ОРІЄНТОВАНИХ СИСТЕМАХ**

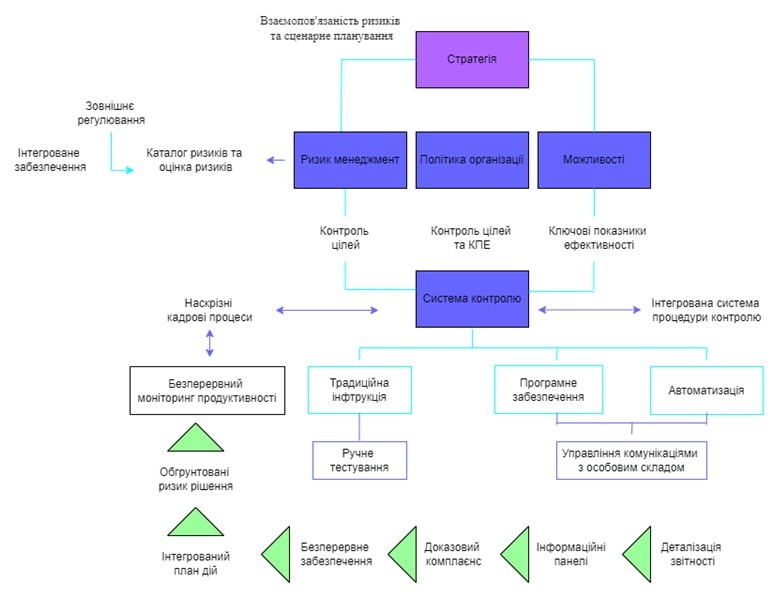
*Abstract. The relevance of the topic of risk management of security-oriented systems is more than ever present in the digitalization of the human resources sector, digital exchange and storage of personal and relevant information in our operations. There is an opportunity to add value to current risk management practices by integrating and automating risk management in government organizations. Such digitalization of risk management provides greater transparency, better risk decision-making, while reducing the required efforts and costs for government agencies.*

Управління ризиками є ключовою сферою діяльності державних установ для виявлення, оцінки та пом’якшення різних типів ризиків у кадрових процесах, таких як операційні, фінансові, регуляторні. Актуальність теми управління ризиками організації, як ніколи присутня при цифровізації кадрової сфери, цифрового обміну та зберігання особистої та актуальної інформації в наших операціях. Це може включати все: від особистих даних і зарплати до інформації про стан здоров’я, невикористану відпустку, про пільги, якими особовий склад може скористатись та результати роботи. Існують можливі ризики, пов’язані з впровадженням та посиленням цифровізації в державних установах, коли колеги можуть спричинити розкриття даних через свою щоденну цифрову діяльність. Тому ризик менеджмент є надзвичайно актуальним питанням, особливо враховуючи підвищений попит на захист даних і конфіденційність. [1-2]

Розглянемо кілька можливих ризиків пов’язаних з впровадженням та посиленням цифровізації в безпеко-орієнтованих системах:

* Випадкове надання облікових даних для входу: співробітник може випадково поділитися своїми обліковими даними для входу (ім’я користувача та пароль) іншому колезі. Потім цей колега може використовувати ці облікові дані для доступу до системи управління персоналом, щоб переглядати умови проходження служби і потенційно змінювати, видаляти або розкривати конфіденційну особисту інформацію.
* Несанкціонований доступ до робочих станцій: якщо працівник залишає свою робочу станцію незаблокованою та без нагляду, інший колега може отримати доступ до комп’ютера та потенційно відкрити систему управління персоналом. Це може призвести до розкриття конфіденційної інформації про проходження служби.
* Неправильне поводження з електронною документацією: працівник може надіслати повідомлення з вкладеними файлами, що містять конфіденційну кадрову інформацію, не тим одержувачам. Якщо електронний лист надійде колезі, який не повинен мати доступу до інформації, це може призвести до розкриття даних.
* Неправильна передача даних: під час передачі даних між HR-системами та іншими системами працівник може випадково надіслати інформацію не тому одержувачу або використати неправильні налаштування, що призведе до розкриття інформації. [3-4]

Існує можливість підвищити цінність поточних практик управління ризиками шляхом інтеграції та автоматизації управління ризиками в державних організаціях. Така цифровізація управління ризиками забезпечує більшу прозорість, прийняття кращих рішень щодо ризиків, водночас зменшуючи необхідні зусилля та витрати. Розглянемо послідовну блок-схему, що автоматизує та інтегрує процеси управління ризиками, контролю та надання впевненості на основі послідовного потоку даних. На діаграмі нижче показано інтегроване управління ризиками при цифровізації кадрових процесів безпеко-орієнтованих систем. [5]



На рис. 1 зображено відповідні компоненти інтегрованого циклу управління ризиками безпеко-орієнтованих систем.

Завдяки захищеній кадровій системі ризик потрапляння конфіденційної інформації в чужі руки зведений до мінімуму. Добре розвинена система управління ризиками призначена для захисту та керування великою кількістю конфіденційної інформації з якою працює особовий склад, включаючи особисті дані, зарплати і продуктивність.

Добре розвинена система управління персоналом використовує передові технології, включаючи шифрування та контроль доступу, щоб гарантувати, що лише авторизований персонал може отримати доступ до зазначеної інформації. Це забезпечує додатковий рівень безпеки, якого важко досягти при ручній обробці інформації. Завдяки системі управління персоналом державним структурам також легше і ефективніше дотримуватись правил захисту даних, оскільки система розроблена таким чином, щоб працювати згідно з цими правилами та автоматично керувати відповідністю.

ЛІТЕРАТУРА:

1. Балановська Т. І., Михайліченко М. В., Троян А. В. Сучасні технології управління персоналом: навч. посіб. Київ: ФОП Ямчинський О. В., 2020. 466 с.
2. Гуцуляк Н. П. Сучасні технології управління персоналом. Економіка і організація управління. 2019. № 3 (35). С. 111–118.
3. Дороніна О.А., Алярова А.В. Стратегія кадрового менеджменту в середовищі економіки знань. Економіка і суспільство. 2022. №42. С. 85-92.
4. Засуха І. П., Бушуєв С. Д., Бушуєва Н.С. Концентрична модель цифрового сліду проектів. Міжнародний науковий журнал «Грааль науки» № 8. 2021. С. 193–201.
5. Матківська Х.С., Зачко О.Б. Моделі цифровізації систем hr-менеджменту безпеко-орієнтованих організацій. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 5 (27). С. 98–113. DOI: <https://doi.org/10.30837/ITSSI.2023.26>