УДК 005.95/.96:005.334:316.77
DOI https://doi.org/10.32782/CMI/2024-12-16

Водкевич В.Д.
аспірант,
Приватний вищий навчальний заклад «Європейський університет»
ORCID: https://orcid.org/0009-0007-8400-1252

Фетісов О.О.
аспірант,
Приватний вищий навчальний заклад «Європейський університет»
ORCID: https://orcid.org/ 0009-0002-7561-5555

Кузьмич А.В.
аспірант,
Приватний вищий навчальний заклад «Європейський університет»
ORCID: https://orcid.org/0009-0003-9982-0956

ОЦІНКА РИЗИКІВ БЕЗПЕКИ В УПРАВЛІННІ ПЕРСОНАЛОМ: РОЛЬ КОМУНІКАЦІЙНИХ АУДИТІВ ЯК ІНСТРУМЕНТУ ОЦІНКИ

Мета дослідження: проаналізувати роль комунікаційних аудитів як інструменту оцінки ризиків безпеки в системі управління персоналом організації та розробити рекомендації щодо їх ефективної інтеграції в існуючі протоколи безпеки. Методика дослідження: застосовано системний підхід до аналізу наукових джерел; використано методи теоретичного узагальнення, систематизації та порівняльного аналізу для визначення ключових компонентів комунікаційного аудиту та його впливу на безпеку організації. Результати: визначено основні ризики безпеки в управлінні персоналом та обґрунтовано роль комунікаційних аудитів у їх оцінці; розроблено структуровану методологію проведення комунікаційного аудиту; виявлено ключові проблеми та переваги використання аудитів для оцінки ризиків безпеки. Практична значущість: запропоновано механізм інтеграції комунікаційних аудитів у існуючі протоколи безпеки організації, що дозволяє підвищити ефективність управління ризиками та покращити загальну систему безпеки підприємства.

Ключові слова: *комунікаційний аудит, управління персоналом, ризики безпеки, оцінка ризиків, інформаційна безпека, організаційні комунікації, безпека персоналу, система управління безпекою.*

Vodkevych Vitalii, Fetisov Oleksii, Kuzmich Andrii
Private Higher Education Establishment “European University”

SECURITY RISK ASSESSMENT IN PERSONNEL MANAGEMENT: THE ROLE OF COMMUNICATION AUDITS AS AN EVALUATION TOOL

Purpose of the research: to analyze the role of communication audits as a security risk assessment tool in the organization's personnel management system and develop recommendations for their effective integration into existing security protocols. Research methodology: The study employs a systematic approach to analyzing the relationship between communication audits and security risk assessment in personnel management. A comprehensive theoretical framework was developed through the analysis of existing literature, focusing on the integration of communication practices with security protocols. The research methodology includes systematic review, comparative analysis, and theoretical generalization methods to evaluate the effectiveness of communication audits in risk assessment. Results: The study has identified several key findings that contribute to the understanding of communication audits' role in security risk assessment. First, the research established a clear correlation between effective communication protocols and enhanced security measures in personnel management. Critical security risks in human resource management were identified and categorized, including data breaches, internal threats, and mismanagement of confidential employee information. The study developed a structured methodology for conducting communication audits, incorporating security considerations at each stage of the audit process. Furthermore, the research revealed that successful implementation of communication audits significantly improves risk identification and assessment capabilities within organizations. The analysis also highlighted the importance of integrating communication audits with existing security protocols, demonstrating how this integration strengthens overall organizational security. Key components of effective communication audits were identified, including assessment of message clarity, communication channel effectiveness, and employee engagement levels. The study revealed both challenges and benefits of implementing communication audits as security measures, providing practical solutions for overcoming common obstacles while maximizing potential advantages. Practical significance: The research provides practical recommendations for organizations seeking to enhance their security risk assessment through communication audits. A comprehensive framework for integrating communication audits into existing security protocols has been developed, offering step-by-step guidelines for implementation. This framework includes specific measures for risk assessment, audit procedures, and evaluation metrics, making it applicable across various organizational contexts. The findings contribute to improving organizational security systems by providing practical tools for risk management and communication assessment, ultimately enhancing both personnel management and security protocols.

Keywords: *communication audit, personnel management, security risks, risk assessment, information security, organizational communications, personnel security, security management system, HR security protocols, communication risk analysis.*

Постановка проблеми. В сучасних умовах зростаючих загроз безпеці організацій особливої актуальності набуває проблема ефективної оцінки та управління ризиками в системі управління персоналом. Стрімкий розвиток інформаційних технологій, збільшення кількості кібератак, посилення конкуренції за кваліфіковані кадри та зростання випадків витоку конфіденційної інформації через людський фактор створюють нові виклики для організацій.

Традиційні методи оцінки ризиків безпеки в управлінні персоналом часто не враховують комунікаційну складову, яка може бути джерелом значних загроз для організації. Неефективні комунікаційні процеси, відсутність чітких протоколів передачі інформації, низький рівень комунікаційної культури можуть призвести до серйозних порушень безпеки, включаючи витік конфіденційних даних, порушення робочих процесів та зниження лояльності персоналу.

Комунікаційний аудит як інструмент оцінки ризиків безпеки в управлінні персоналом залишається недостатньо дослідженим у науковій літературі. Існує потреба у розробці методологічних підходів до проведення таких аудитів та їх інтеграції в загальну систему безпеки організації. Це завдання тісно пов'язане з важливими науковими та практичними проблемами:

- розробка ефективних механізмів забезпечення кадрової безпеки підприємств;
- вдосконалення методів оцінки ризиків в системі управління персоналом;
- підвищення ефективності організаційних комунікацій;
- захист конфіденційної інформації та комерційної таємниці;
- формування культури інформаційної безпеки в організації.

Актуальність дослідження підсилюється тим, що в умовах цифрової трансформації бізнесу та переходу до віддаленої роботи зростає роль ефективних комунікацій у забезпеченні безпеки організації. Це вимагає нових підходів до оцінки та управління ризиками, де комунікаційний аудит може стати дієвим інструментом виявлення та попередження потенційних загроз.

Аналіз останніх досліджень і публікацій. Питання безпеки в управлінні персоналом та роль комунікаційних процесів у забезпеченні організаційної безпеки активно досліджуються як українськими, так і зарубіжними науковцями. Фундаментальні аспекти кадрової безпеки та її ключових ознак грунтовно висвітлені у роботі О.В. Марченка [2], де автор систематизує підходи до визначення сутності кадрової безпеки. Значний внесок у розуміння проблематики економічної безпеки та інноваційного розвитку підприємств зробила Л.О. Волощук [3], розкриваючи комплексний підхід до управління безпекою.

Особливу увагу заслуговують дослідження Г.В. Назарової [4, 5], які детально розкривають загрози, ризики та методи управління кадровою безпекою підприємства, а також визначають передумови створення ефективної системи кадрової безпеки. Психологічні аспекти управління персоналом та їх вплив на безпеку організації досліджено в роботі Є.В. Гейко, Г.О. Горської та І.Г. Радул [6].

Методологічні основи проведення комунікаційних аудитів та їх роль у забезпеченні безпеки розглянуто в роботах С.В. Бардаша та В.О. Мисюка [8], які досліджують особливості організації аудиту в медіасфері. Важливий внесок у розуміння комунікаційної політики та її впливу на безпеку організації зроблено Ю. Булко [10]. Значущими є дослідження В.В. Зеліч [14], які розкривають роль комунікативного аудиту як чинника вибору стратегії комунікації в управлінні підприємством.

Аспекти інформаційної безпеки та оцінки ризиків детально висвітлені у роботі М.Д. Василенка та В.М. Слатвінської [1], де автори аналізують методологію оцінки ризиків у контексті соціальної інженерії. Практичні аспекти впровадження систем безпеки та проведення аудитів розглянуто в дослідженнях А. Рибидайла, Ю. Кірпічнікова, С. Васюхна та М. Петрушена [13].

Незважаючи на значну кількість наукових праць з питань безпеки персоналу та комунікаційних процесів, залишається потреба у поглибленому дослідженні ролі комунікаційних аудитів як інструменту оцінки ризиків безпеки, особливо в контексті сучасних викликів цифровізації та зростаючих загроз інформаційній безпеці організацій. Також недостатньо дослідженими залишаються питання методології проведення комунікаційних аудитів з урахуванням специфіки оцінки безпекових ризиків та їх інтеграції в загальну систему управління безпекою організації.

Формування цілей статті (постановка завдання). Метою статті є теоретичне обґрунтування та розробка практичних рекомендацій щодо використання комунікаційного аудиту як інструменту оцінки ризиків безпеки в системі управління персоналом організації.

Для досягнення поставленої мети визначено такі завдання:

1. Систематизувати та проаналізувати основні види ризиків безпеки в управлінні персоналом, визначити їх вплив на діяльність організації та роль HR-підрозділу у їх мінімізації.

2. Дослідити сутність та особливості комунікаційного аудиту як інструменту оцінки ризиків, визначити його ключові компоненти та місце в системі управління безпекою організації.

3. Розробити методологічний підхід до проведення комунікаційного аудиту з урахуванням специфіки оцінки безпекових ризиків у сфері управління персоналом.

4. Визначити основні етапи та особливості інтеграції комунікаційного аудиту в існуючі протоколи безпеки організації.

5. Виявити та проаналізувати проблеми і переваги використання комунікаційних аудитів для оцінки ризиків безпеки, запропонувати шляхи подолання виявлених проблем.

Виклад основного матеріалу дослідження. У сучасному ландшафті організаційного менеджменту інтеграція заходів безпеки в управління персоналом стала критичною проблемою, особливо тому, що підприємства стикаються з дедалі складнішим набором загроз. Розуміння загальних ризиків безпеки, властивих управлінню персоналом, таких як витік даних, внутрішні загрози та неправильне управління конфіденційною інформацією про співробітників, є життєво важливим для захисту активів організації та підтримки довіри зацікавлених сторін. Ці ризики не тільки ставлять під загрозу цілісність організації, але й суттєво впливають на її ефективність і репутацію. Отже, управління персоналом віді-

грає ключову роль у пом'якшенні цих вразливостей за допомогою стратегічного нагляду та проактивних заходів. Одним з ефективних інструментів, який привернув увагу в цій сфері, є комунікаційний аудит, який служить систематичним методом оцінки ефективності комунікаційних процесів в організації. Застосовуючи комунікаційні аудити, організації можуть виявити слабкі місця у своїх механізмах розповсюдження інформації та зворотного зв'язку, отримуючи таким чином уявлення про потенційні ризики безпеці, які можуть виникнути через неадекватну комунікаційну практику. Ключові компоненти аудиту ефективної комунікації включають оцінку чіткості повідомлень, ефективності каналів комунікації та рівня залученості співробітників. Крім того, наслідки комунікаційних аудитів виходять за межі простої оцінки ризику; вони відіграють важливу роль у формуванні загальних стратегій управління людськими ресурсами, які надають пріоритет безпеці. Впровадження аудиту зв'язку як заходу безпеки передбачає низку структурованих кроків, включаючи оцінку поточних протоколів зв'язку та інтеграцію результатів аудиту в існуючі структури безпеки. Однак організації можуть зіткнутися з труднощами в цьому процесі, такими як опір змінам і проблеми з розподілом ресурсів, які поєднуються зі значними перевагами, такими як посилена безпека та покращене залучення працівників. Ця стаття має на меті дослідити багатогранний зв'язок між ризиками безпеки в управлінні персоналом і роллю комунікаційних аудитів у забезпеченні надійної системи оцінки, зрештою підкреслюючи, як ефективна комунікація може служити наріжним каменем організаційної безпеки.

Розуміння ризиків безпеки в управлінні персоналом

Поширені ризики безпеки в управлінні персоналом. У сфері управління персоналом ризики безпеки є багатогранними та можуть серйозно вплинути як на організаційні операції, так і на добробут співробітників. Однією з головних проблем є управління ризиками економічної безпеки, що вимагає надійних стратегій управління ризиками для захисту активів і персоналу підприємства [1, с. 90]. Важливо відзначити, що ці ризики стосуються не лише фінансових активів, а й поширюються на людські ресурси, де розуміння стану інформаційної безпеки через призму людського фактору стає важливим [2, с. 338]. Тому управління персоналом має застосовувати комплексні методи, які підкреслюють захист конфіденційної інформації та безпеку окремих працівників, особливо в середовищах, сприйнятливих до зовнішніх загроз, таких як кібератаки чи військові дії [3, с. 250]. Зосередившись на цих основних аспектах, організації можуть краще підготуватися до пом'якшення потенційних ризиків безпеці, гарантуючи належний захист свого персоналу та конфіденційних даних.

Вплив цих ризиків на безпеку організації. Розуміння багатогранних ризиків, пов'язаних із безпекою персоналу, має ключове значення для забезпечення загальної безпеки організації. Внутрішні загрози, такі як працівники з девіантною поведінкою або ті, що належать до груп ризику, можуть суттєво поставити під загрозу безпеку персоналу, що призводить до потенційних загроз для діяльності та стабільності організації [4, с. 231]. Такі ризики не тільки впливають на безпеку персоналу, а й поширюються на економічну стабільність організації, оскільки несприятливі дії персоналу можуть призвести до фінансових наслідків [4, с.231]. Крім того, моральний клімат в організації відіграє вирішальну роль у підтримці безпеки персоналу. Погіршення такого клімату може знизити продуктивність співробітників, тим самим впливаючи на ефективність і безпеку організації [4, с. 232]. Тому вкрай важливо запровадити комплексну систему заходів щодо виявлення, запобігання та пом'якшення цих ризиків. Така система не лише усуває внутрішні загрози безпеці персоналу, але й готує організацію до боротьби із зовнішнім тиском, який може вплинути на її безпеку та фінансові результати [4, с. 233] [5, с. 55]. Зосереджуючись на управлінні безпекою персоналу, організації можуть значно підвищити свою стійкість проти передбачуваних і непередбачуваних загроз, захищаючи тим самим свої операційні та економічні інтереси [4, с. 236].

Роль управління персоналом у зниженні цих ризиків. Управління персоналом відіграє ключову роль у зменшенні ризиків, сприяючи безпечному та продуктивному робочому середовищу за допомогою систематичних і стратегічних практик. Впроваджуючи ретельні процеси перевірки, такі як перевірка репутації, референсів і перевірка кредитоспроможності, управління персоналом ефективно знижує ризики, пов'язані з наймом осіб, які можуть становити загрозу безпеці організації [6, с. 159]. Цей проактивний підхід не тільки захищає підприємство від потенційних внутрішніх порушень, але й підвищує загальну надійність робочої сили. Крім того, управління персоналом забезпечує постійне навчання працівників протоколам безпеки, наголошуючи на важливості захисту даних і активів компанії; це досягається за допомогою регулярних навчальних програм, які охоплюють гігієну кібербезпеки та спеціальні протоколи для обробки конфіденційної інформації [6, с. 160]. Таке навчання не тільки зменшує ризики, але й дає можливість співробітникам брати активну участь у підтримці системи безпеки організації. Крім того, впровадження сучасних технологій управління персоналом автоматизує різні аспекти управління персоналом, тим самим мінімізуючи ризики, пов'язані з ручними процесами та людськими помилками [6, с. 160]. Ці технології сприяють більш ефективному моніторингу та оцінці персоналу, що має вирішальне значення для підтримки високих стандартів безпеки та продуктивності. У сукупності ці практики підкреслюють невід'ємну роль управління персоналом у зниженні ризиків і підтримують довгострокову стійкість і зростання організації.

Роль комунікаційних аудитів в оцінці ризиків

Використання аудит зв'язку для оцінки ризиків безпеки. Аудит комунікацій служить життєво важливим інструментом для оцінки ризиків безпеки шляхом систематичної оцінки комунікаційних систем і протоколів організації. Однак одним із критичних аспектів проведення ефективного комунікаційного аудиту є необхідність визначення меж аудиту на початковому етапі. Це гарантує, що аудит залишається цілеспрямованим і ресурсоефективним, дозволяючи аудиторам зосередитися на найбільш значущих сферах ризику, не будучи перевантаженими масштабами всієї комунікаційної інфраструктури [7]. Цей цільовий підхід особливо важливий, оскільки певні підсистеми, незважаючи на те, що вони є критичними, можуть бути виключені з аудиту

через пріоритетність ресурсів у бік більш вразливих областей, які представляють вищий ризик для безпеки організації [7]. Крім того, доступ до певних підсистем може бути обмежений через міркування конфіденційності, що може суттєво вплинути на точність оцінки ризиків безпеки [7]. Таким чином, комунікаційні аудити, незважаючи на те, що вони за своєю суттю корисні для виявлення та пом'якшення вразливостей безпеки, повинні бути стратегічно сплановані та виконані, щоб збалансувати повноту з конфіденційністю та обмеженнями ресурсів. Ця стратегічна спрямованість не тільки підвищує ефективність аудиту, але й гарантує, що будь-які виявлені ризики безпеки розглядаються за допомогою відповідних втручань, тим самим захищаючи комунікаційні мережі організації від потенційних загроз.

Ключові компоненти ефективного комунікаційного аудиту. Ефективний комунікаційний аудит складається з кількох критичних компонентів, які забезпечують комплексну оцінку комунікаційних процесів організації. Перш за все, розуміння конкретних цілей аудиту має вирішальне значення, оскільки це допомагає пристосувати аудит до конкретних сфер, які потребують вдосконалення або оцінки [8, с. 4]. Крім того, регулярне планування аудитів, наприклад, їх проведення кожні три місяці, є життєво важливим для постійного вдосконалення та адаптації до мінливих обставин всередині організації [9, с. 289]. Ця регулярність не тільки полегшує виявлення потенційних проблем, але й допомагає своєчасно впроваджувати коригувальні дії, тим самим підвищуючи загальну ефективність комунікаційних стратегій. Крім того, інтеграція інформації з рекламного та комунікаційного ринку, наприклад, тих, що спостерігаються в Україні, може надати цінні орієнтири та інноваційні практики, які можна застосувати для посилення комунікаційної структури організації [10]. Таким чином, комплексний комунікаційний аудит повинен не лише оцінювати внутрішні процеси, а й враховувати зовнішні тенденції та стандарти, щоб переконатися, що комунікація організації є ефективною та конкурентоспроможною на ширшому ринковому ландшафті. Ці компоненти спільно сприяють надійному аудиту зв'язку, що робить його незамінним інструментом для будь-якої організації, яка прагне оптимізувати свої канали зв'язку та стратегії.

Вплив комунікаційних аудитів на загальні стратегії управління персоналом. Комунікаційні аудити є критично важливим компонентом у формуванні стратегій, які використовує управління персоналом, оскільки вони забезпечують повний огляд поточних комунікаційних процесів в організації [11]. Систематично оцінюючи ефективність цих процесів, комунікаційні аудити допомагають виявити прогалини та неефективність, які можуть перешкоджати ефективному потоку інформації та співпраці між відділами. Такі аудити є інструментальними для мінімізації ризиків, пов'язаних із неправильним спілкуванням, що може призвести до ширших організаційних проблем, включаючи вплив на моральний стан працівників і продуктивність [12]. Крім того, комунікаційні аудити можуть запропонувати цілеспрямовані рекомендації, такі як ті, що містяться в аудитах ISMS, які пропонують впровадження передових технологій для покращення каналів зв'язку та оптимізації функцій HR [13, с. 74]. Оскільки стратегії управління персоналом значною мірою залежать від ефективної комунікації для управління стосунками, навчанням і розвитком співробітників, знання, отримані в результаті цих аудитів, дозволяють менеджерам з управління персоналом адаптувати свої підходи, щоб вони краще узгоджувалися з цілями організації та створювали більш згуртоване робоче середовище. Підсумовуючи, проведення регулярних комунікаційних аудитів є необхідним для того, щоб стратегії управління персоналом залишалися ефективними та адаптувалися до мінливих потреб робочої сили та організації в цілому.

Впровадження комунікаційних аудитів як заходу безпеки

Кроки комунікаційного аудиту. Комунікаційний аудит – це всебічний процес оцінки, який стосується багатьох аспектів організаційної комунікації, забезпечуючи цілісне уявлення про її ефективність і області для покращення. Одним із важливих кроків є аналіз особливостей мовної комунікації всередині організації, що включає вивчення того, як мова використовується в різних контекстах, щоб забезпечити ясність і узгодженість у повідомленні [14, с. 144]. Це доповнюється структурним аналізом як змісту, так і форм мовного обміну, що використовується в системі документообігу організації, підкреслюючи, як інформація організована та ділиться всередині [14, с. 144]. Виявляючи та аналізуючи як зовнішню, так і внутрішню інформацію про організацію, аудит оцінює фактори, що характеризують її репутацію та імідж, які є важливими для підтримки сталого суспільного сприйняття [14, с. 145]. Далі аудит поширюється на оцінку каналів комунікації та стосунків із співробітниками, щоб виявити внутрішні проблеми, які можуть перешкоджати ефективній комунікації [14, с. 146]. Крім того, процес також включає перегляд текстової, візуальної та аудіоінформації в чотирьох інформаційних потоках – зовнішньому, внутрішньому, вихідному та внутрішньому просторі – щоб переконатися, що всі форми комунікації узгоджуються з цілями організації [14, с. 146]. Зрештою, це ретельне обстеження допомагає організаціям ефективніше координувати та керувати інформаційними потоками, тим самим підвищуючи ясність і розуміння на всіх рівнях організації [14, с. 147]. Цей комплексний підхід не лише виявляє приховані проблеми, але й сприяє проактивній стратегії покращення комунікації, що має вирішальне значення для посилення організаційної узгодженості та ефективності.

Інтеграція аудиту зв'язку в існуючі протоколи безпеки. Інтеграція аудиту комунікацій в існуючі протоколи безпеки вимагає стратегічного підходу, який узгоджується зі структурою управління організації, гарантуючи, що ці аудити не погіршать їхню якість [15, с. 137]. Цей процес інтеграції починається з оновлення свідомості персоналу шляхом проведення регулярних аудитів безпеки мережі, які не тільки виявляють уразливості, але й підкреслюють важливість підтримки надійних протоколів безпеки. Крім того, інтерпретація результатів як зовнішнього, так і внутрішнього аудиту відіграє вирішальну роль у підтримці відповідності та зміцненні безпеки організації [16, с. 28]. Щоб досягти цього, організації повинні тісно співпрацювати з компетентними органами, включаючи навчання співробітників і регулярні аудити в свій протокол, таким чином сприяючи культурі постійного вдосконалення та пильності [17]. Узгодивши ці елементи, організації можуть

ефективно вбудувати аудит комунікацій у свої системи безпеки, забезпечуючи відповідність і захист конфіденційної інформації.

Проблеми та переваги використання аудиту комунікацій для оцінки ризиків безпеки. Проведення аудиту комунікацій для оцінки ризиків безпеці представляє як проблеми, так і переваги, які перетинають різні сфери управління безпекою. Однією з основних проблем є потреба в унікальному та зрозумілому методі оцінки, який узгоджується з процесом оцінки ризиків інформаційної безпеки. Ця складність ускладнюється необхідністю ідентифікувати та оцінювати зовнішню поверхню потенційних атак, перевіряти відповідність існуючим стандартам безпеки та досліджувати будь-які витоки даних, які можуть поставити під загрозу цілісність організації. Більше того, брак кваліфікованих фахівців, які б могли вміло орієнтуватися та вирішувати ці ризики, що розвиваються, створює значну перешкоду, особливо коли технології стають все більш інтегральними та стратегічними в бізнес-операціях [18]. Незважаючи на ці проблеми, комунікаційні аудити пропонують значні переваги, особливо в тестуванні безпеки, яке допомагає виявити вразливі місця в системах і надає програмістам інформацію, необхідну для вирішення та вирішення цих проблем. Крім того, впровадження ефективних засобів контролю має вирішальне значення для зменшення потенційної шкоди, що дозволяє аналітикам безпеки приймати обґрунтовані рішення щодо запобігання ризикам. Для підвищення ефективності комунікаційних аудитів важливо розробити комплексні методології оцінки ризиків, адаптовані до конкретних потреб різних організацій, включаючи малі та середні підприємства, забезпечуючи при цьому відповідність встановленим вимогам бізнесу щодо безпеки. Зрештою, цілеспрямовані зусилля для подолання цих проблем, такі як підвищення професійних навичок і вдосконалення методологій оцінки, є обов'язковими для повного використання переваг аудиту зв'язку в управлінні ризиками безпеки.

Висновки. У результаті проведеного дослідження комунікаційного аудиту як інструменту оцінки ризиків безпеки в системі управління персоналом організації встановлено, що сучасні організації стикаються з комплексними викликами у сфері безпеки персоналу, включаючи витік даних, внутрішні загрози та неправильне управління конфіденційною інформацією. Ці ризики мають прямий вплив на економічну безпеку та стабільність організації, що підкреслює важливість ефективних механізмів їх оцінки та управління.

В ході дослідження обґрунтовано роль комунікаційного аудиту як стратегічного інструменту оцінки ризиків безпеки. Встановлено, що систематичне проведення таких аудитів дозволяє виявляти вразливості в комунікаційних процесах організації ще до того, як вони призведуть до серйозних порушень безпеки. На основі проведеного аналізу розроблено структурований підхід до проведення комунікаційного аудиту, який включає аналіз мовної комунікації, оцінку документообігу, дослідження інформаційних потоків та аналіз каналів комунікації. Це забезпечує комплексну оцінку комунікаційних ризиків та їх потенційного впливу на безпеку організації.

У процесі дослідження визначено основні проблеми впровадження комунікаційних аудитів, серед яких виділяється потреба в унікальних методах оцінки, складність ідентифікації зовнішніх загроз та нестача кваліфікованих фахівців. Водночас виявлено суттєві переваги, включаючи посилення захисту конфіденційної інформації та покращення загальної системи безпеки. Запропоновано механізм інтеграції комунікаційних аудитів у існуючі протоколи безпеки організації, що передбачає регулярне оновлення процедур, навчання персоналу та співпрацю з компетентними органами.

Перспективи подальших досліджень у цьому напрямі пов'язані з розробкою методики кількісної оцінки ефективності комунікаційних аудитів у системі безпеки організації та дослідженням особливостей їх проведення в умовах віддаленої роботи та цифрової трансформації. Важливим напрямом майбутніх досліджень є вивчення можливостей автоматизації процесів комунікаційного аудиту з використанням сучасних технологій, аналіз галузевої специфіки та розробка відповідних рекомендацій. Окрему увагу варто приділити дослідженню впливу культурних факторів на ефективність комунікаційних аудитів у міжнародних організаціях.

СПИСОК ЛІТЕРАТУРИ

1. Василенко М. Д., Слатвінська В. М. Соціальна інженерія в контексті розуміння методології щодо аналізу оцінки ризиків у галузі інформаційної безпеки. Інформаційне суспільство: проблеми та перспективи : матеріали VII Всеукраїнської науково-практичної конференції (м. Одеса, 20 травня 2022 р.) / відп. ред. Н.І. Логінова. Одеса, 2022. С. 90–93.

2. Марченко О. В. Підходи до визначення сутності кадрової безпеки та її ключових ознак. *БізнесІнформ*. 2019. № 7. С. 337–344.

3. Волощук Л. О. Інноваційний розвиток та економічна безпека промислових підприємств: проблеми комплексного управління: монографія. Одеса : Апрель, 2015. 396 с.

4. Назарова Г. В. Кадрова безпека підприємства: загрози, ризики, функції та методи управління. *Формування ринкової економіки* : зб. наук. праць. Спец. вип. Проблеми сучасної економіки та інституціональна теорія. 2012. № 2. С. 230–240.

5. Назарова Г. Передумови створення системи кадрової безпеки підприємства. *Регіональні аспекти розвитку продуктивних сил України*. 2017. № 15. С. 54–63.

6. Гейко Є. В., Горська Г. О., Радул І. Г. Психологічні засади управління персоналом підприємства. *Науковий вісник Ужгородського національного університету. Серія: Психологія.* 2022. № 1. С. 158–162.

7. Аудит інформаційної безпеки. URL: https://amica.ua/audyt-informatsiinoi-bezpeky/ (дата звернення: 10.11.2024).

8. Бардаш С. В., Мисюк В. О. Аудит діяльності суб'єктів медіа ринку: необхідність та особливості організації. *Вісник Житомирського державного технологічного університету. Серія: Економічні науки*. 2016. № 4. С. 3–13.

9. Гальченко В. Г. Сучасні підходи до класифікації власного капіталу підприємства. *Збірник наукових статей магістрів*. Полтава : ПУЕТ, 2019. С. 288–292.

10. Булко Ю. Аналіз комунікаційної політики транснаціональної корпорації : кваліфікаційна робота. Київ : Національний університет «Києво-Могилянська академія», 2022. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/f0853cc8-114c-4237-8b17-625469933853/content (дата звернення: 11.11.2024).

11. Гірник О. М. Ризик-менеджмент закладу сфери охорони здоров'я в умовах нестабільності. 2022.

12. Гавриличенко Є. В. Внутрішній аудит : конспект лекцій для студентів денної і заочної форм навчання другого рівня (магістерського) рівня вищої освіти спеціальності 071–Облік і оподаткування. 2021.

13. Рибидайло А., Кірпічніков Ю., Васюхно С., Петрушен М. Порядок вибору та впровадження технологічних рішень для забезпечення функціонування інформаційної інфраструктури Міністерства оборони України: методичний підхід. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. 2024. С. 66–76.

14. Зеліч В. В. Комунікативний аудит як чинник вибору стратегії комунікації в комунікативному менеджменті підприємства. 2018. С. 143–148. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/24445 (дата звернення: 12.11.2024).

15. Petryk O. M., Sukhoversha V. O., Martsenko S. V. Дослідження мережевих архітектур для критичних інфраструктур. Актуальні задачі сучасних технологій. 2022. С. 137.

16. Лавренова Д. Л., Клименок Н. С. Інформаційно-керуюча система для цифрової підстанції. *Міжнародний науково-технічний журнал «Сучасні проблеми електроенерготехніки та автоматики»*. 2023. С. 27–30.

17. Землянська С. А. Удосконалення системи менеджменту в сфері обслуговування : магістер. кваліфікаційна робота. Дніпро : Дніпровський державний аграрно-економічний університет, 2024. URL: https://dspace.dsau.dp.ua/handle/123456789/9532 (дата звернення: 13.11.2024).

18. Оптимізація діяльності з внутрішнього аудиту в кризові часи / Міністерство фінансів України. URL: https://mof.gov.ua/storage/files/Оптимізація_діяльності_з_внутрішнього_аудиту.pdf (дата звернення: 13.11.2024).

REFERENCES

1. Vasylenko M. D., Slatvinska V. M. (May 20, 2022) Sotsialna inzheneriia v konteksti rozuminnia metodolohii shchodo analizu otsinky ryzykiv u haluzi informatsiinoi bezpeky [Social engineering in the context of understanding the methodology for risk assessment analysis in information security]. Informatsiine suspilstvo: problemy ta perspektyvy: materialy VII Vseukrainskoi naukovo-praktychnoi konferentsii. Odesa, pp. 90–93.

2. Marchenko O. V. (2019) Pidkhody do vyznachennia sutnosti kadrovoi bezpeky ta yii kliuchovykh oznak [Approaches to determining the essence of personnel security and its key features]. *BiznesInform*, no. 7, pp. 337–344.

3. Voloshchuk L. O. (2015) Innovatsiinyi rozvytok ta ekonomichna bezpeka promyslovykh pidpryiemstv: problemy kompleksnoho upravlinnia: monohrafiia [Innovative development and economic security of industrial enterprises: problems of complex management: monograph]. Odesa: Aprel. (in Ukrainian)

4. Nazarova H. V. (2012) Kadrova bezpeka pidpryiemstva: zahrozy, ryzyky, funktsii ta metody upravlinnia [Personnel security of the enterprise: threats, risks, functions and management methods]. *Formuvannia rynkovoi ekonomiky*: zb. nauk. prats. Spets. vyp. Problemy suchasnoi ekonomiky ta instytutsionalna teoriia, no. 2, pp. 230–240.

5. Nazarova H. (2017) Peredumovy stvorennia systemy kadrovoi bezpeky pidpryiemstva [Prerequisites for creating an enterprise personnel security system]. *Rehionalni aspekty rozvytku produktyvnykh syl Ukrainy*, no. 15, pp. 54–63.

6. Heiko Ye. V., Horska H. O., Radul I. H. (2022) Psykholohichni zasady upravlinnia personalom pidpryiemstva [Psychological principles of enterprise personnel management]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Psykholohiia*, no. 1, pp. 158–162.

7. Audyt informatsiinoi bezpeky [Information security audit]. Available at: https://amica.ua/audyt-informatsiinoi-bezpeky/ (accessed November 10, 2024).

8. Bardash S. V., Mysiuk V. O. (2016) Audyt diialnosti subiektiv media rynku: neobkhidnist ta osoblyvosti orhanizatsii [Audit of media market subjects: necessity and features of organization]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Ekonomichni nauky*, no. 4, pp. 3–13.

9. Halchenko V. H. (2019) Suchasni pidkhody do klasyfikatsii vlasnoho kapitalu pidpryiemstva [Modern approaches to the classification of enterprise equity]. Zbirnyk naukovykh statei mahistriv. Poltava: PUET, pp. 288–292.

10. Bulko Yu. (2022) Analiz komunikatsiinoi polityky transnatsionalnoi korporatsii [Analysis of the communication policy of a transnational corporation]: kvalifikatsiina robota. Kyiv: National University of Kyiv-Mohyla Academy. Available at: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/f0853cc8-114c-4237-8b17-625469933853/content (accessed November 11, 2024).

11. Hirnyk O. M. (2022) Ryzyk-menedzhment zakladu sfery okhorony zdorovia v umovakh nestabilnosti [Risk management of a healthcare institution in conditions of instability].

12. Havrylychenko Ye. V. (2021) Vnutrishnii audyt: konspekt lektsii [Internal audit: lecture notes].

13. Rybydailo A., Kirpichnikov Yu., Vasiukhno S., Petrushen M. (2024) Poriadok vyboru ta vprovadzhennia tekhnolohichnykh rishen dlia zabezpechennia funktsionuvannia informatsiinoi infrastruktury Ministerstva oborony Ukrainy: metodychnyi pidkhid [Procedure for selecting and implementing technological solutions to ensure the functioning of the information infrastructure of the Ministry of Defense of Ukraine: methodological approach]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU imeni Ivana Cherniakhovskoho*, pp. 66–76.

14. Zelich V.V. (2018) Komunikatyvnyi audyt yak chynnyk vyboru stratehii komunikatsii v komunikatyvnomu menedzhmenti pidpryiemstva [Communication audit as a factor in choosing a communication strategy in enterprise communication management]. Pp. 143–148. Available at: https://dspace.uzhnu.edu.ua/jspui/handle/lib/24445 (accessed November 12, 2024).

15. Petryk O. M., Sukhoversha V. O., Martsenko S. V. (2022) Doslidzhennia merezhevykh arkhitektur dlia krytychnykh infrastruktur [Research of network architectures for critical infrastructures]. Aktualni zadachi suchasnykh tekhnolohii, p. 137.

16. Lavrenova D. L., Klymenok N. S. (2023) Informatsiino-keruiucha systema dlia tsyfrovoi pidstantsii [Information control system for digital substation]. Mizhnarodnyi naukovo-tekhnichnyi zhurnal "Suchasni problemy elektroenerhotekhniky ta avtomatyky", pp. 27–30.

17. Zemlianska S. A. (2024) Udoskonalennia systemy menedzhmentu v sferi obsluhovuvannia [Improvement of the management system in the service sector]: mahister. kvalifikatsiina robota. Dnipro: Dnipro State Agrarian and Economic University. Available at: https://dspace.dsau.dp.ua/handle/123456789/9532 (accessed November 13, 2024).

18. Optymizatsiia diialnosti z vnutrishnoho audytu v kryzovi chasy [Optimization of internal audit activities in times of crisis]. Ministry of Finance of Ukraine. Available at: https://mof.gov.ua/storage/files/Оптимізація_діяльності_з_внутрішнього_аудиту.pdf (accessed November 13, 2024).