УДК 342.9
DOI 10.32782/2523-4269-2024-89-64-68

Онопрієнко Станіслав Григорович,
кандидат юридичних наук,
асистент проєкту
(Центр підтримки переселенців Євразія,
Програма прийому біженців у Сполучених Штатах Америки)
ORCID: https://orcid.org/0000-0002-5524-1798

ІНФОРМАЦІЙНА БЕЗПЕКА ВНУТРІШНЬОГО АУДИТУ ОРГАНІВ ВРЯДУВАННЯ (ДОСВІД РЕСПУБЛІКИ ПОЛЬЩА)

У статті на основі узагальнення та аналізу досвіду Республіки Польща визначено основні напрями вдосконалення інформаційної безпеки внутрішнього аудиту органів врядування. З'ясовано, що внутрішній аудит містить різні види інформаційної діяльності (збирання, одержання, використання інформації), що сприяє виникненню в процесі його здійснення інформаційних ризиків. Окреслено вектори розвитку методології внутрішнього аудиту в Республіці Польща. З'ясовано особливості інформаційного складника внутрішнього аудиту органів врядування. На підставі аналізу підходів, що сформувалися в польській науковій думці та практиці, визначено пріоритетні напрями забезпечення інформаційної безпеки внутрішнього аудиту органів врядування.
Ключові слова: *інформаційна безпека, інформаційні ризики, внутрішній аудит, органи врядування, Республіка Польща.*

Постановка проблеми. Кожне підприємство, установа, організація або орган влади (далі – організація) у своїй діяльності стикається з впливом негативних факторів, до яких належать неефективна робота персоналу, нераціональне витрачання ресурсів, розкрадання коштів, порушення в технологічних процесах тощо. Такі порушення безпосередньо впливають на безпеку діяльності організації та може призвести до неможливості виконання ним своїх функцій. Для того щоб оперативно запобігти можливим негативним наслідкам наявних порушень, запроваджено систему внутрішнього аудиту. Внутрішній аудит дає змогу оперативно здійснювати перевірку, оцінювання та моніторинг відповідності й функціонування систем бухгалтерського обліку та внутрішнього контролю, аналізує ситуації ризику й запобігання банкрутства; використовує ноу-хау для збільшення прибутку й ефективності нової технології, вживає інших заходів, що сприяють розвитку організації.

Водночас внутрішній аудит містить різні види інформаційної діяльності (збирання, одержання, використання інформації). Це сприяє виникненню в процесі здійснення внутрішнього аудиту певних інформаційних ризиків, які можуть негативно вплинути на діяльність організації. У період правового режиму воєнного стану в Україні такий негативний вплив може посилюватися, шкодячи системам національної, економічної, воєнної безпеки. Вказане підтверджує доцільність аналізу досвіду інших держав, які мають певні здобутки у сфері забезпечення інформаційної безпеки внутрішнього аудиту та зумовлює актуальність теми цієї статті.

Аналіз останніх досліджень і публікацій. Питання вдосконалення інформаційного складника внутрішнього аудиту в Республіці Польща розглядали в роботах таких учених, як Р. Бургемейстер, у працях якого визначено роль внутрішнього аудиту в розбудові систем врядування, зокрема його інформаційного складника. Автором акцентовано на тому, що в межах функцій управління ризиками та контролю внутрішній аудит відіграє особливу роль, забезпечує незалежне та об'єктивне підтвердження достовірності інформації на всіх рівнях організації. Внутрішні аудитори не лише підтверджують дотримання правил або процедур, а й оцінюють відповідність дизайну, операційну ефективність, точність і прозорість звітності про результати внутрішнього контролю відповідно до профілю ризику та стратегії підприємства. Тому функція внутрішнього аудиту повинна посідати особливе місце в організації, забезпечуючи чітке розуміння місії, бачення, стратегії та довгострокових цілей [1, с. 5]. Додамо, що такий підхід дає змогу відійти від вузького розуміння внутрішнього аудиту як процедури, що застосовується виключно для суб'єктів підприємницької діяльності з метою збільшення їх прибутків, і використати всі переваги означеного виду аудиту для підвищення ефективності органів публічної влади.

П. Лагодскі розглядає внутрішній аудит як незалежну, об'єктивну діяльність із надання достовірної інформації та консультування, спрямовану на підвищення цінності організації та покращення її діяльності. Внутрішній аудит, на думку науковця, підтримує організацію в досягненні її цілей, систематично й послідовно підвищуючи ефективність управління. Запровадження принципів внутрішнього аудиту може слугувати своєрідним інформаційним запобіжником проти корпоративних зловживань [2, с. 387]. Нам уявляється дуже важливим такий напрям внутрішнього аудиту, як визначення ступеня досягнення цілей організації, а також акцентування уваги на проблемі підвищення ефективності управління.

Досить цікавим уявляється підхід Б. Камінської-Чубали до проблем забезпечення інформаційної безпеки,

що розглядається в системному зв'язку з проведенням зовнішнього та внутрішнього аудиту. Авторка обстоює переваги, розробку та використання моделі цілісного оцінювання стану інформаційної безпеки «10 на 10», яка містить 100 стандартів у 10 сферах інформаційної безпеки в організації як інструмента для вимірювання рівня безпеки [3]. Перевагою цього підходу, на нашу думку, є алгоритмізація визначення актуального стану інформаційної безпеки організації. Водночас визначення конкретних критеріїв оцінювання стану інформаційної безпеки потребує попередньої кропіткої аналітичної роботи, результати якої періодично мають переглядатися у зв'язку із суттєвими змінами умов функціонування організації (які для України в умовах правового режиму воєнного стану постійно супроводжують функціонування всіх юридичних осіб).

Однак слід указати на недостатність висвітлення проблем інформаційної безпеки внутрішнього аудиту системи врядування як у дослідженнях польських науковців, так і у вітчизняних дослідженнях. У сукупності ці фактори є підтвердженням актуальності теми цієї статті.

Мета статті – на основі узагальнення та аналізу досвіду Республіки Польща визначити основні напрями вдосконалення інформаційної безпеки внутрішнього аудиту органів врядування.

Виклад основного матеріалу. Згідно з Міжнародним стандартом професійної практики внутрішнього аудиту останній розуміється як «незалежна, об'єктивна діяльність з надання впевненості та консультування, що має додавати вартості організації та покращувати її діяльність. Внутрішній аудит допомагає організації досягти поставлених цілей за допомогою систематичного, послідовного підходу до оцінки й підвищення ефективності процесів управління ризиками, контролю та корпоративного управління» [4].

Відповідно до методологічних підходів, що сформувалися в Республіці Польща, внутрішній аудит здійснюють працівники організації, що перевіряється. Для того щоб процес оцінки був об'єктивним і незалежним, його повинні проводити співробітники з іншого відділу, ніж той, що перевіряється. Це забезпечує неупередженість і зменшує можливість конфлікту інтересів. Співробітники, відповідальні за аудит, мають знання про діяльність організації та її процеси, що допомагає їм глибоко ідентифікувати всі порушення. Аудитори перевіряють та оцінюють дотримання компанією норм, правил, стандартів і внутрішніх процедур. Це процес незалежної та об'єктивної оцінки, який допомагає керівництву вдосконалювати діяльність, виявляти ризики та управляти ними [5]. Це породжує комплекс вимог до інформаційних складників професійної компетентності внутрішніх аудиторів: по-перше, вони мають бути належно інформовані про діяльність структурних ланок підприємства, які перевіряють, включно з нормативно-правовим складником їх функціонування та типові порушення й помилки, які при цьому виникають. По-друге, їх діяльність має бути убезпечено від комплаєнс-ризиків інформаційного характеру, пов'язаних із недодержанням вимог професійної етики при поводженні з масивами інформації, поширення якої може негативно вплинути на імідж підприємства або його структурного підрозділу (однак це не стосується випадків виявлення за результатами внутрішнього аудиту кримінальних правопорушень).

Ми погоджуємося з думкою, що внутрішній аудит не тільки допомагає мінімізувати ризик невідповідностей і порушень, а й захищає репутацію та імідж організації. Інформація та рекомендації, отримані під час внутрішнього аудиту, можуть бути використані для внесення змін і вдосконалень у функціонування організації, що сприяє підвищенню операційної ефективності та досягненню стратегічних цілей. Внутрішній аудит також спрямований на забезпечення прозорості організації завдяки незалежній оцінці та зворотного зв'язку щодо діяльності організації. Звіти та результати внутрішнього аудиту зазвичай представляють керівництву та іншим зацікавленим сторонам. Це сприяє більшій прозорості та уможливлює підзвітність керівництва за свої рішення й ефективне управління організацією [5].

Отже, внутрішній аудит сприяє підвищенню ефективності діяльності організації завдяки пошуку порушень фінансового законодавства, виявлення фактів нераціонального використання ресурсів підприємства, знаходження можливостей заощадження коштів. У масштабі діяльності органів врядування інформаційний складник внутрішнього аудиту дає змогу своєчасно отримувати відомості та дані про відхилення від заданих стратегічними документами параметрів, а також знаходити нові шляхи поставлених цілей. Слід погодитися з позицією Я. Пшибильської відносно того, що сучасний внутрішній аудит, зосереджений на перевірці ефективності діяльності суб'єкта господарювання, має допомагати керівництву. Окрім безпосереднього виявлення проблем, він дає змогу краще зрозуміти функціонування підрозділу [6, с. 48]. Детальні процедури внутрішнього аудиту охоплюють весь його процес, зокрема, планування аудиту та оцінки ризиків, інформування про його результати шляхом звітування, а також подальші дії, що містять оцінку виконання аудиторських рекомендацій. Це знайшло своє втілення в книгах та картах процедур внутрішнього аудиту, які затверджуються в Республіці Польща на місцевому рівні [7].

Аудитор базує свою роботу на оцінці ризику суттєвих помилок та ризиків у сферах діяльності підприємства та підпорядкованих йому незалежних структурних підрозділів, які підлягають внутрішньому аудиту. Ризик у польській доктрині внутрішнього аудиту розуміється як імовірність виникнення будь-якої події, дії або бездіяльності, яка може призвести до завдання шкоди активам або іміджу компанії та підпорядкованих їй відокремлених структурних підрозділів чи перешкоджати досягненню поставлених цілей і завдань [8]. М. Татой справедливо зауважує, що оцінка ризиків (визначення сфер ризику та їх аналіз) у діяльності суб'єкта сектору державних фінансів, яку виконує внутрішній аудитор, є непростим завданням. Воно вимагає хорошої предметної підготовки (кваліфікації) у сфері теорії внутрішнього аудиту, а також, і, можливо, насамперед, великого професійного досвіду, відповідних особистісних якостей, знання суб'єкта господарювання та володіння методами виявлення факторів і зон ризику, а також його аналізу [9, с. 285].

Слід сказати, що ризики діяльності підприємства або органу владу є різноплановими, і не всі з них пов'язані з питаннями інформаційної безпеки. Однак можна виокремити групу інформаційних ризиків, які можуть бути предметом внутрішнього аудиту. Їх ідентифікація потребує кропіткої підготовчої роботи, під час якої уявляється важливим визначити, у яких саме сферах діяльності організації такі інформаційні ризики виникають, а також ранжувати їх залежно від ступеня впливу на загальну ефективність суб'єкта. Цей процес вимагає і залежить від знань внутрішнього аудитора, розуміння

їм цілей, діяльності, організаційної структури офісу, а також підпорядкованих незалежних організаційних одиниць, сфери відповідальності окремих працівників чи від його інтуїції [10].

Розвиток інформаційних технологій сприяє широкому використанню автоматизованих методів оцінки ризиків у діяльності підприємств та органів публічного адміністрування, зокрема з використанням штучного інтелекту. Це дає змогу здійснювати частину процесів у внутрішній аудиторській діяльності дистанційно, що має значення в разі знаходження структурних підрозділів організації в різних географічних регіонах. Однак процес визначення інформаційних ризиків у діяльності органа врядування вимагає застосування креативних методів, які потребують застосовування здібностей людини.

Зауважимо, що застосування аудитором своєї інтуїції не має правового характеру й не може бути регламентовано методологією правової науки. Завданням правових досліджень, на нашу думку, має бути саме виокремлення інформаційних ризиків діяльності органу врядування, а також визначення серед них найбільш пріоритетних. Слід також додати, що в умовах повномасштабної збройної російської агресії проти України майже всі інформаційні ризики можуть розглядатися і в аспекті національної та воєнної безпеки, оскільки всі вразливості інформаційних та інформаційно-комунікаційних систем можуть бути використані противником. Прикладом такого використання слабких місць українських систем обміну відомостями та даними, утвореними в процесі функціонування органів врядування, стала кібератака на державні реєстри України в грудні 2024 року. З огляду на це важливості набуває виявлення помилок та ризиків на найраніших етапах внутрішнього аудиту, щоб недоліки у функціонуванні інформаційних та інформаційно-комунікаційних систем не накопичувалися, а своєчасно коригувалися.

Крім того, слід звернути увагу на визначення польськими дослідниками важливості зворотного зв'язку між аудитором та замовником. Оцінювання внутрішнього аудиту надає аудиторам інформацію про те, чи має їхня робота вимірювану цінність для одержувачів аудиторських послуг. Думки об'єктів аудиту та одержувачів звітів мають бути враховані в наступних аудитах [11, с. 339]. Використання зворотного зв'язку для вдосконалення систем інформаційної безпеки містить низку дій, пов'язаних як із визначенням задоволеності керівництва органу врядування результатами аудиту, так і з визначенням задоволеності персоналу заходами вдосконалення функціонування їх підрозділів після проведення аудиту, а також установлення впливу здійснених змін на задоволеність і довіру з боку громадян, якщо йдеться про користування певними публічними послугами.

Отже, нині розвиток методології внутрішнього аудиту в Республіці Польща відбувається за двома основними векторами: 1) визначення технік та методів, що дадуть змогу своєчасно проводити ідентифікацію та оцінку наявних і ймовірних ризиків; 2) розробка дієвих методик та технологій, які допоможуть побудувати систему раннього попередження ризиків та оцінку ефективності діяльності організації. Для органів врядування важливими векторами розвитку внутрішнього аудиту є встановлення відповідності між їх цілями, місією, візією та спрямованістю практичної діяльності, а також визначення впливу реалізації певних стратегій, програм, планів на динаміку рівня довіри з боку громадян.

Висновки. На підставі аналізу підходів, що сформувалися в польській науковій думці та практиці, можна визначити пріоритетні напрями забезпечення інформаційної безпеки внутрішнього аудиту органів врядування. До них належать визначення відповідності цілей, місії та візії організації її практичній інформаційній діяльності; встановлення рівня врегульованості найбільш важливих аспектів інформаційних правовідносин на законодавчому, підзаконному та локальному рівні; визначення наступності в оцінюванні рівня інформаційної безпеки організації на підставі попередніх аудитів чи інших перевірок; виокремлення, структурування та ранжування інформаційних ризиків, які можуть утворювати вагому небезпеку для діяльності організації та досягнення її цілей; додержання вимог інформаційного та цивільного законодавства відносно цифрових продуктів, особливо – вимог авторського права; убезпечення діяльності внутрішніх аудиторів від комплаєнс-ризиків; динаміка рівня довіри до організації у зв'язку з виконанням нею вимог щодо транспарентності, доступу до публічної інформації та захисту персональних даних.

Список використаних джерел

1. Burgemejster S. Rola audytu wewnętrznego w budowaniu ładu. Warszawa: Instytut Audytorów Wewnętrznych IIA Polska, 2019. S. 5–13.

2. Łagodzki P. Audyt wewnętrzny : wybrane zagadnienia. *Internal Audit Selected Issues*. 2011. № 32. S. 387–395.

3. Kamińska-Czubała B. Efektywność wybranych metod ewaluacji bezpieczeństwa informacyjnego. *Bezpieczeństwo informacyjne w dyskursie naukowym* / pod redakcją naukową Hanny Batorowskiej i Emilii Musiał. Kraków : Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją, 2017. S. 54–68.

4. Definicja audytu wewnętrznego, Kodeks Etyki, Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego, poradniki (2011), Stowarzyszenie Audytorów Wewnętrznych IIA Polska, Warszawa. URL: https://www.iia.org.pl/o-nas/dokumenty/

5. Audyt wewnętrzny – cele, rodzaje i znaczenie audytu. Warszawa: Akademię Leona Koźmińskiego, 2023. URL: https:// www.kozminski.edu.pl/p l/review/audyt-wewnetrzny-cele-rodzaje-i-znaczenie-audytu.

6. Przybylska J. Audyt wewnętrzny w sektorze publicznym (wyd. III), Warszawa: CeDeWu, 2023. 232 s.

7. Księga procedur audytu wewnętrznego: Załącznik do Zarządzenia Nr 51/2016 Burmistrza Miasta Gorlice z dnia 1 marca 2016 r. w sprawie wprowadzenia Księgi Procedur Audytu Wewnętrznego w Urzędzie Miejskim w Gorlicach. URL: https://bip.malopolska.pl/e,pobierz,get.html?id=1388440#:~:text=Ksi%C4%99ga%20Procedur%20Audytu%20 Wewn%C4%99trznego%20(zwana,opis%20stosowanej%20metodyki%20audytu%20wewn%C4%99trznego.

8. Karta audytu wewnętrznego miasta Luboń. Załącznik nr 1 do Zarządzenia nr 61/2014 Burmistrza Miasta Luboń z dnia 17.10.2014 roku. URL: https://archiwum-bip.lubon.pl/cms_inc/61_2014_Karta_audytu_wewn%C4%99trznego459c. doc?id=2823&dok_id=5780

9. Tatoj M. Ocena ryzyka na potrzeby audytu wewnętrznego jednostek sektora polskich finansów publicznych. *Zeszyty teoretyczne rachunkowości*. 2009. T. 53. № 109. S. 271–288.

10. Mazurek A., Piołunowicz M. Audyt wewnętrzny w sektorze publicznym w Polsce – Diagnoza i propozycje zmian. Wydawnictwo Fundacja FOR, Warszawa, 2008. 35 s.

11. Czerwiński K. Audyt wewnętrzny. Warszawa: InfoAudit Sp. z o.o., 2004. 450 s.

References

1. Burhemeyster, S. (2019). Rol′ vnutrishn′oho audytu v rozbudovi ladu [The role of internal audit in building order]. Warshava: Instytut vnutrishnikh audytoriv IIA Pol′shcha, 5–13. [In Polish]

2. Lahodzki, P. (2011). Vnutrishniy audyt: vybrani pytannya [Internal audit: selected issues]. Vybrani pytannya vnutrishn′oho audytu [Internal Audit Selected Issues], 32: 387–395. [In Polish]

3. Kamins′ka-Chubala, B. (2017) Efektyvnist′ obranykh metodiv otsinky informatsiynoyi bezpeky [Effectiveness of selected information security evaluation methods]. Informatsiyna bezpeka v naukovomu dyskursi [Information security in scientific discourse]/ za red. Hanny Batorovs′koyi ta Emiliyi Musyal. Krakiv: Pedahohichnyy universytet Krakova Komisiya narodnoyi osvity. Instytut bezpeky ta hromadyans′koyi osvity. Kafedra informatsiynoyi kul′tury ta informatsiynoho menedzhmentu, 54–68. [In Polish]

4. Vyznachennya vnutrishn′oho audytu [Definition of internal audit]. Kodeks etyky, Mizhnarodni standarty profesiynoyi praktyky vnutrishn′oho audytu, posibnyky (2011), Asotsiatsiya vnutrishnikh audytoriv IIA Pol′shcha, Warshava. URL: https://www.iia.org.pl/o-nas/dokumenty/ [In Polish]

5. Vnutrishniy audyt – tsili, vydy ta znachennya audytu [Internal audit – objectives, types and importance of audit] (2023). Warshava: Akademia Leona Koźmińskiego. URL: https://www.kozminski.edu.pl/pl/review/audyt-wewnetrzny-cele-rodzaje-i-zdrowie-audytu. [In Polish]

6. Przhybyl′s′ka, YA. (2023). Vnutrishniy audyt u derzhavnomu sektori [Internal audit in the public sector] (3-ye vyd.), Warshava: CeDeWu, 232. [In Polish]

7. Knyha protsedur vnutrishn′oho audytu [Book of internal audit procedures] (2016): Dodatok do Rozporyadzhennya № 51/2016 mis′koho holovy Horlyts′ vid 1 bereznya 2016 roku pro zaprovadzhennya Knyhy protsedur vnutrishn′oho audytu v mis′komu ofisi Horlyts′. URL: https://bip.malopolska.pl/e,pobierz,get.html?id=1388440#:~:text=Ksi%C4%99ga%20Procedur%20Audytu%20Wewn%C4%99trznego%20(nazva, opys %20%20metodolohiya,%20vykorystana%20dlya%20vnutrishn′o-ho%C4%99audytu. [In Polish]

8. Kartka vnutrishn′oho audytu m. Lyubon′ [Internal audit card of the city of Luboń] (2014). Dodatok No1 do rozporyadzhennya Lyubons′koho mis′koho holovy No61/2014 vid 17.10.2014. URL: https://archiwum-bip.lubon.pl/cms_inc/61_2014_Karta_audytu_wewn%C4%99trznego459c.doc?id=2823&dok_id=5780 [In Polish]

9. Tatoy, M. (2009). Otsinka ryzykiv dlya tsiley vnutrishn′oho audytu pidrozdiliv sektoru derzhavnykh finansiv Pol′shchi [Risk assessment for the needs of internal audit of Polish public finance sector entities]. Zoshyty z teoretychnoho obliku [Theoretical accounting notebooks], 53, 109: 271–288 [In Polish]

10. Mazurek, A. (2008). Piolunovich M. Vnutrishniy audyt u derzhavnomu sektori v Pol′shchi – Diahnostyka ta propozytsiyi shchodo zmin [Internal audit in the public sector in Poland – Diagnosis and proposals for changes]. Vydavnytstvo Fundacja FOR, Warshava, 35. [In Polish]

11. Czerwiński, K. (2004). Vnutrishniy audyt [Internal audit]. Warshava: InfoAudit, 450. [In Polish]

Onopriienko Stanislav,
Candidate of Legal Sciences,
Project Assistant
(RSC Eurasia, USRAP)
ORCID: https://orcid.org/0000-0002-5524-1798

INFORMATION SECURITY IN THE INTERNAL AUDIT OF GOVERNMENT BODIES (EXPERIENCE OF THE REPUBLIC OF POLAND)

The purpose of the article is to identify the main directions for improving information security in the internal audit of government bodies based on generalization and analysis of the experience of the Republic of Poland.

Internal audit has been found to include various types of information-related activities, including the collection, receipt, and use of information.This contributes to the emergence of certain information risks in the process of internal audit, which may adversely affect the activities of the organization. During the legal regime of martial law in Ukraine, such a negative impact may increase, causing damage to the systems of national, economic, and military security.

The development of the internal audit methodology in the Republic of Poland is currently substantiated to be progressing along two main vectors: 1) determination of techniques and methods that will allow timely identification and assessment of existing and probable risks; 2) development of effective methods and technologies that will allow building an early warning system of risks and assessing the effectiveness of the organization. For governance bodies, important vectors of internal audit development are to establish compliance between their goals, mission, vision, and focus of practical activities, as well as to determine the impact of the implementation of certain strategies, programs, and plans on the dynamics of the level of public trust.

The author identifies the priority areas of ensuring information security in the internal audit of government bodies based on the analysis of the approaches developed in Polish scientific thought and practice. These include the following: determining whether the goals, mission, and vision of the organization are consistent with its practical information activities; establishing the level of regulation of the most important aspects of information relations at the legislative, by-law, and local levels; determining the continuity in assessing the level of information security of the organization based on previous audits or other inspections; Identification, structuring, and ranking of information risks that may pose a significant threat to the organization's activities and achievement of its goals; compliance with the requirements of information and civil legislation in relation to digital products, especially copyright requirements; protecting the activities of internal auditors from compliance risks; dynamics of the level of trust in the organization in connection with its compliance with the requirements for transparency, access to public information and protection of personal data.

Key words: *information security, information risks, internal audit, government bodies, Republic of Poland.*

Надіслано до редколегії 19.12.2024