of existing forms of documentation for inventories' accounting, namely, their movements. Therefore, one should introduce new forms of primary documentation to ensure the timely movement of inventories that will improve the level of accounting and control of their use.

In General, summing up, we can say that the inventories' accounting at the investigated transport companies is not organized quite in accordance with the requirements. The disadvantages of the investigated transport enterprises in accounting practice are: general accumulation of information on the accounts which requires details with the purpose of obtaining necessary data for making managerial decisions regarding the flow of inventories; use for inventories' accounting adapted free forms of primary documents, characterized by a high complexity in their processing; absence of rationing of inventories use.

The elimination of the aforementioned disadvantages will encourage transport companies to properly resolve problematic issues, which have been in accounting practices in the area of inventories' accounting.

Thus, although the recognition and evaluation of inventories has a variety of methods, the enterprise chooses the simplest one that most closely matches the industry and the legal framework.

УДК 657.6:004:341.24

Бунда О.М., к.е.н., доцент
Київський національний університет технологій та дизайну

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІЖНАРОДНИХ ДОГОВОРІВ

Глобалізація економіки та швидкий розвиток інформаційних технологій як в Україні, так і у світі вимагають не тільки організації належної інформаційної безпеки діяльності підприємств, але і аудиту інформаційної безпеки міжнародних договорів.

Інформаційна безпека – це одне з найважливіших завдань, що стоять перед підприємствами, що здійснюють міжнародне співробітництво. Необхідно сформувати таку систему інформаційної безпеки, щоб ради директорів чи інші органи управління підприємством розуміли ризики, спричинені кіберзлочинністю та могли оперативно впливати на їх усунення та запобігання.

Органи управління, без сумніву, відповідають за управління інформаційною безпекою стосовно захисту активів, чи то фідуціарних відносин з третіми сторонами або управління ризиками та дотримання законів та стандартів [1].

Управління сучасним бізнесом вимагає створення розподілених

інтелектуальних систем нового покоління, що автоматизують процеси прийняття рішень, побудованих не як традиційні закриті, централізовані, монолітні і послідовні системи інформаційних технологій, а як цифрові платформи «штучного інтелекту» і екосистеми розумних сервісів, здатних до автономного, асинхронного і паралельного функціонування, миттєвої реакції на події, можливість планування і погодження своїх дій в умовах наявності суперечливих інтересів і обмежених ресурсів, контролю виконання намічених планів в реальному часі. Сучасні підприємства використовують сучасні інформаційні технології DW (Data Warehouse) – сховища даних; BSC (Balanced Scorecard) – система збалансованих показників; технології, які відносять до класу інтелектуальних засобів підтримки бізнесу BI (Business Intelligence) – система бізнес-аналітики для формування аналітичних звітів та оцінки бізнес-процесів. Максимальний ефект отримується при інтеграції всіх цих технологій, що і забезпечує підтримку всіх складових управління підприємствами [2].

Аудит інформаційної безпеки міжнародних договорів – це комплекс аналітичних робіт з оцінки поточного стану інформаційних систем компанії і пошуку потенційних загроз для міжнародного співробітництва. Для проведення аналізу у фахівців є перелік критеріїв і стандартів, яким повинна відповідати інформаційна система [3].

Аудит може також призначатися для систематизації та впорядкування існуючих заходів захисту інформації або для розслідування інциденту, що стався, пов’язаного з порушенням інформаційної безпеки [4].

Зазвичай для проведення аудиту інформаційної безпеки міжнародних договорів залучаються зовнішні компанії, які надають консалтингові послуги в даній сфері. Ініціатором проведення аудиту інформаційної безпеки міжнародних договорів може стати керівництво компанії, або внутрішня служба інформаційної безпеки. Аудит інформаційної безпеки міжнародних договорів виконується групою експертів, чисельність і склад якої залежить від цілей і завдань конкретної перевірки.

Цілями проведення аудиту інформаційної безпеки міжнародних договорів є: аналіз ризиків, пов’язаних з можливістю здійснення загроз безпеки щодо ресурсів інформаційних систем; оцінювання поточного рівня захищеності інформаційних систем; визначення проблемних моментів в системі захисту інформаційних систем; визначення та оцінка відповідності інформаційних систем існуючим стандартам у сфері інформаційної безпеки міжнародних договорів; розробка рекомендацій щодо підвищення рівня захищеності та ефективності механізмів захисту інформаційних систем [5].

Розглянемо основні види аудиту інформаційної безпеки міжнародних договорів:

- експертний аудит безпеки міжнародних договорів, в процесі проведення перевірки виявляються недоліки в системі заходів захисту

інформації на основі досвіду залучених експертів;

- оцінка відповідності рекомендаціям міжнародного стандарту ISO 17799, а також вимогам керівних документів;
- інструментальний аналіз захищеності інформаційних систем, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи;
- комплексний аудит, який передбачає усі інші види аудиту інформаційної безпеки міжнародних договорів.

Отже, проведення аудиту інформаційної безпеки міжнародних договорів дозволить підприємству не тільки своєчасно виявляти і усувати загрози для інформаційного середовища, але й запобігати їх виникненню в майбутньому.

Література

1. Аудит інформаційної безпеки об'єктів приватної власності. Режим доступу: https://www.asterslaw.com/ua/press_center/publications/information_security_audit/

2. Огнєвий О. В. Методи створення мультиагентних систем управління інформаційними ресурсами у реальному часі [Текст] / О. В. Огнєвий, М. В. Заворотний, А. М. Огнева // Вісник Хмельницького національного університету. Технічні науки. – 2019. – №4. – С. 106-110.

3. Інформаційна безпека. Режим доступу: https://itlogica.com.ua/uk/services /informacionnaja-bezopasnost/

4. Рой Я.В. Аудит інформаційної безпеки-основа ефективного захисту підприємства / Я.В. Рой, Н.П. Мазур, П.М. Складанний // Кібербезпека: освіта, наука, техніка. - 2018. - № 1. - С. 86-93. - Режим доступу: http://nbuv. gov. ua/UJRN/cest_2018_1_11.

5. Бартко М.А., Кухарська Н. П. Методи аудиту інформаційної безпеки інформаційних систем. Режим доступу: https://sci.ldubgd.edu.ua/bitstream/handle/123456789/4900/1.pdf?sequence=1&isAllowed=y