Іполітов Є. М.,
здобувач PhD, Національний технічний університет «Харківський політехнічний інститут», м. Харків
Науковий керівник: ***Мащенко М. А.,***
д-р екон. наук, професор, завідувач кафедри підприємництва, торгівлі і логістики

АУДИТ ТА МОНІТОРИНГ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Під час підвищених економічних ризиків та запровадження цифрової трансформації ефективне використання інформаційних технологій потребує надійного захисту інформаційних ресурсів, що забезпечується через системний аудит і безперервний моніторинг безпеки інформаційних систем. Удосконалення механізмів контролю та управління інформаційною безпекою сприяє підвищенню стійкості підприємств та ефективності їх управління в нестабільному макроекономічному середовищі [1]. Зростання кількості кіберзагроз, витоків даних, несанкціонованого доступу до інформаційних систем та порушень конфіденційності інформації актуалізує необхідність формування ефективної системи управління інформаційною безпекою підприємства.

Важливим елементом такої системи є аудит та моніторинг інформаційної безпеки, які забезпечують своєчасне виявлення вразливостей, оцінювання ефективності заходів захисту та підвищення рівня стійкості підприємства до внутрішніх і зовнішніх загроз. Саме тому дослідження підходів до організації аудиту та моніторингу системи інформаційної безпеки набуває особливого значення в умовах динамічного розвитку цифрового середовища та зростання ролі інформаційних ресурсів у діяльності підприємств. Ефективне функціонування системи управління інформаційною безпекою підприємства неможливе без постійного контролю стану захисту інформаційних ресурсів. У цьому контексті аудит та моніторинг виступають важливими інструментами оцінювання рівня безпеки інформаційних систем, а також засобами своєчасного виявлення та запобігання потенційним загрозам.

Метою дослідження є обґрунтування ролі аудиту та моніторингу в системі управління інформаційною безпекою підприємства.

Аудит інформаційної безпеки являє собою системний процес оцінювання стану захисту інформаційних ресурсів підприємства, перевірки відповідності політик, процедур і технічних засобів безпеки встановленим стандартам, нормативним вимогам і внутрішнім регламентам організації. Основною метою аудиту є виявлення слабких місць у системі захисту інформації, визначення рівня ризиків та розроблення рекомендацій щодо підвищення ефективності заходів безпеки. Проведення аудиту може здійснюватися як внутрішніми підрозділами підприємства, так і незалежними зовнішніми експертами, що дозволяє отримати більш об’єктивну оцінку стану інформаційної безпеки.

Моніторинг системи інформаційної безпеки передбачає безперервне спостереження за функціонуванням інформаційних систем, мереж та програмного забезпечення з метою своєчасного виявлення аномальної активності, потенційних загроз та інцидентів безпеки. Застосування сучасних програмних засобів моніторингу дозволяє здійснювати аналіз журналів подій, контролювати доступ до інформаційних ресурсів, виявляти спроби несанкціонованого втручання та своєчасно реагувати на інциденти.

З метою підвищення ефективності аудиту та моніторингу системи інформаційної безпеки підприємствам доцільно впроваджувати низку практичних заходів [2; 3]. Насамперед необхідно розробити комплексну політику інформаційної безпеки та регламент проведення регулярних перевірок системи захисту інформації. Важливим є використання сучасних автоматизованих систем моніторингу та аналізу подій інформаційної безпеки, що забезпечують оперативне реагування на потенційні загрози. Крім того, підприємствам слід підвищувати рівень обізнаності персоналу щодо правил інформаційної безпеки шляхом проведення навчальних програм і тренінгів. Доцільним також є інтегрування процесів аудиту та моніторингу з системою управління ризиками підприємства, що дозволить забезпечити комплексний підхід до управління інформаційною безпекою. Важливим напрямом удосконалення є також регулярне оновлення програмного забезпечення, застосування багаторівневих механізмів контролю доступу та впровадження міжнародних стандартів управління інформаційною безпекою.

Отже, аудит і моніторинг системи інформаційної безпеки є важливими складовими ефективного управління інформаційними ресурсами підприємства. Їх впровадження сприяє своєчасному виявленню потенційних загроз, оцінюванню рівня захищеності інформаційних систем та постійному вдосконаленню заходів безпеки. Комплексне застосування аудиту та моніторингу дозволяє знизити інформаційні ризики, підвищити стійкість підприємства до кіберзагроз та забезпечити надійний захист інформаційних ресурсів. У довгостроковій перспективі це буде створювати передумови для стабільного функціонування та сталого розвитку підприємства в умовах цифрової економіки.

Список використаних джерел:

1. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство.* 2023. DOI: https://doi.org/10.32782/2524-0072/2023-56-118.

2. Яремко С.М, Кузьміна О. М. Актуальні аспекти захисту інформаційних ресурсів бізнес-структур. *Вісник Хмельницького національного університету* 2020. № 5. С. 238−242. URL: http://nbuv.gov.ua/UJRN/Vchnu_ekon_2020_5_46 (дата звернеення 12.03.2026).

3. Кицюк В. М., Пупинін О. С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації.* 2024. № 2. С. 103−108. DOI: https://doi.org/10.31673/2409-7292.2024.020012.