НАПРЯМ 8. ПІДПРИЄМНИЦТВО, ТОРГІВЛЯ ТА БІРЖОВА ДІЯЛЬНІСТЬ

Іполітов Євгеній Миколайович
аспірант;

Соснов Ігор Ігорович
кандидат технічних наук,
доцент кафедри підприємництва, торгівлі і логістики,
Навчально-науковий інститут економіки,
менеджменту і міжнародного бізнесу
Національного технічного університету
«Харківський політехнічний університет»

DOI: https://doi.org/10.36059/978-966-397-566-5-39

МОНІТОРИНГ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ЕКОНОМІЧНИЙ АСПЕКТ

Інформаційна складова посідає провідне місце в структурі економічної безпеки підприємства, оскільки інформація становить критично важливий ресурс для забезпечення його конкурентоспроможності та фінансової стійкості. Відсутність належної системи інформаційного захисту може призвести до втрати стратегічних конкурентних переваг, а в окремих випадках і до банкрутства суб'єкта підприємництва.

Доцільність дослідження інформаційної безпеки підприємства в контексті економічної безпеки обґрунтовується низкою чинників. По-перше, інформація є одним із визначальних виробничих ресурсів у сучасній економіці знань. По-друге, інформаційні загрози здатні завдати суттєвих фінансових та репутаційних збитків суб'єктам господарювання. По-третє, імплементація комплексної системи інформаційної безпеки дозволяє мінімізувати ризики несанкціонованого доступу до конфіденційних даних і знизити ймовірність економічних втрат. По-четверте, на опрацювання

інформаційної компоненти економічної безпеки сприяє розробці дієвих механізмів захисту інформаційних активів підприємства.

Таким чином, дослідження інформаційної складової системи економічної безпеки підприємства характеризується багато-аспектністю, водночас воно є необхідною передумовою для забезпечення стабільного функціонування як окремих господарюючих суб'єктів, так і національної економіки загалом.

В цьому контексті забезпечення інформаційної безпеки підприємства варто розглядати з позиції здійснення системного моніторингу інформаційних загроз і раціонального управління витратами на безпеку. Питання економічної ефективності моніторингу інформаційних загроз активно досліджуються у працях зарубіжних і вітчизняних науковців. Зокрема, Gordon L A. та Loeb M. P. розробили модель оптимізації інвестицій у кібербезпеку, довівши, що витрати на захист не повинні перевищувати третини очікуваних збитків від інцидентів [1]. Böhme R. у власній праці підкреслює, що економіка інформаційної безпеки ґрунтується на співвідношенні вартості загроз і вигід від їхнього запобігання [2]. Kshetri N. розглядає глобальні тенденції розвитку кіберзлочинності та їхній вплив на фінансову стійкість підприємств [3]. Серед українських авторів Шостак Л., Федонюк А., Помазун О. зазначають, що в системі формування бізнес-моделі підприємства в умовах цифровізації суспільства кібербезпека відіграє провідну роль, але потребує формування інноваційних систем захисту вітчизняного бізнесу [4]. Бабічев А. В., Самородов Б. В., в свою чергу, запропонували концептуальну модель оцінки і аналізу інформаційної компоненти економічної безпеки підприємства, в якій безпека розглядається як сукупність усіх потоків робіт, даних та процесів, які є включеними у модель [5].

Метою роботи є аналіз економічного аспекту моніторингу загроз інформаційної безпеки підприємства, а також визначення вимог до формування ефективної системи моніторингу, що забезпечує зниження фінансових ризиків та підвищення рівня цифрової стійкості бізнесу.

Моніторинг загроз інформаційної безпеки – це систематичний процес виявлення, оцінки, аналізу та реагування на ризики, які

можуть вплинути на цілісність, доступність і конфіденційність інформаційних ресурсів підприємства [3]. Його економічна ефективність полягає у мінімізації витрат, пов'язаних із ліквідацією наслідків інцидентів, та запобіганні непрямим збиткам, що виникають через репутаційні ризики або втрату клієнтів. Більше половини малих і середніх підприємств, які зазнали серйозних кібератак, припиняють діяльність протягом року після інциденту. Це підтверджує необхідність створення систем раннього виявлення загроз і підвищення ефективності процесів реагування.

Вимоги до формування системи моніторингу загроз інформаційної безпеки підприємства:

- комплексність – охоплення всіх рівнів управління інформаційними потоками: технічного, організаційного та аналітичного;
- безперервність спостереження – моніторинг має здійснюватися у режимі реального часу із застосуванням систем автоматичного виявлення аномалій;
- інтегрованість з економічною аналітикою – фінансові показники мають бути інтегровані у процес управління ризиками;
- ризик-орієнтований підхід – розподіл ресурсів відповідно до потенційних економічних наслідків загроз;
- людський фактор – формування корпоративної культури безпеки через навчання;
- адаптивність і гнучкість – система повинна оперативно реагувати на появу нових загроз, використовуючи аналітику великих даних і машинне навчання;
- відповідність міжнародним стандартам ISO/IEC 27001:2022 та NIST Cybersecurity Framework.

Отже, моніторинг загроз інформаційної безпеки виступає невід'ємною складовою економічної політики підприємства. Ефективна система моніторингу, побудована з урахуванням комплексності, адаптивності та економічної доцільності, забезпечує баланс між витратами на безпеку та фінансовими вигодами від запобігання інцидентам. Такий підхід підвищує цифрову стійкість, сприяє сталому розвитку бізнесу й формує стратегічну перевагу у конкурентному середовищі.

Таким чином, інформаційна безпека є невід'ємною складовою частиною економічної безпеки підприємства, виступаючи одним із ключових елементів системи корпоративного захисту. Витік конфіденційної фінансової інформації, комерційної таємниці чи стратегічних планів може призвести до прямих економічних збитків, втрати конкурентних переваг та зниження ринкової вартості компанії. Кібератаки на інформаційні системи підприємства загрожують не лише технічними збоями, а й фінансовими втратами через зупинку виробництва, штрафи регуляторів та компенсації клієнтам. Водночас економічна нестабільність підприємства часто обмежує інвестиції в сучасні системи інформаційного захисту, створюючи замкнене коло вразливості. Ефективна система управління повинна інтегрувати інформаційну безпеку в загальну стратегію економічного захисту, розглядаючи її як стратегічний пріоритет, а не операційні витрати. Захист інформаційних активів стає критичним фактором економічної стійкості в умовах цифрової трансформації бізнесу. Саме тому без належного рівня інформаційної безпеки неможливо досягти комплексної економічної безпеки підприємства.

Список використаної літератури:

1. Gordon L A., Loeb M. P. The economics of information security investment. *ACM Transactions on Information and System Security*. 2002. № 5 (4). P. 438–457. DOI: https://doi.org/10.1145/581271.581274

2. Böhme R. The Economics of Information Security and Privacy. Springer. 2013. DOI: https://doi.org/10.1007/978-3-642-39498-0

3. Kshetri N. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Springer. 2010. DOI: https://doi.org/10.1007/978-3-642-11522-6

4. Шостак Л.В., Федонюк А.А., Помазун О.О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024. № 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-37

5. Бабічев А. В., Самородов Б. В. Концептуальна модель оцінки й аналізу інформаційної компоненти економічної безпеки підприємства. *Проблеми економіки*. 2023. № 3 (57). С. 157–167. URL: https://www.problecon.com/export_pdf/problems-of-economy-2023-3_0-pages-157_167.pdf