ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Іпполітов Є.М.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Інформаційна безпека (ІБ) є невід'ємною складовою загальної системи управління ризиками підприємства. Ефективне управління ризиками, пов'язаними з ІБ дозволяє не лише попередити виникнення кіберзагроз, а й забезпечує стійкість бізнес-процесів, зменшуючи потенційні збитки від ризикових інцидентів. Цифровізація бізнес-процесів, впровадження хмарних технологій, використання великих даних, штучного інтелекту та Інтернету речей призводять до збільшення кількості та складності інформаційних ризиків підприємств. У таких умовах ризик-менеджмент повинен враховувати не тільки традиційні загрози, але й кіберризики, пов'язані з витоком даних, кібератаками, збоєм систем або людським фактором.

Формування ефективної стратегії управління ризиками ІБ є ключовим фактором стабільного функціонування підприємства в умовах цифрових трансформацій. Стратегія має враховувати перелік потенційних загроз, ймовірність їх настання, наслідки, а також забезпечувати цілісну систему захисту інформаційних активів підприємства. Відповідно до міжнародних стандартів ISO/IEC 27001:2022 та ISO 31000:2018, стратегія управління ризиками повинна базуватися на принципах системності, адаптивності, превентивності та безперервного вдосконалення [1; 2]. Тому, пропонується така послідовність етапів формування стратегії управління ризиками ІБ:

1. Ідентифікація ризиків, пов'язаних з потенційними інформаційними загрозами і вразливостями у внутрішньому та зовнішньому середовищі.
2. Оцінювання ризиків – здійснюється аналіз ймовірності виникнення ризику та його можливих наслідків шляхом якісних і кількісних методів оцінки.
3. Вибір стратегії реагування на ризикові події – уникнення ризику, зниження ризику, передача ризику, прийняття ризику.
4. Розробка та впровадження заходів безпеки, спрямованих на зменшення рівня ризиків інформаційної безпеки.
5. Моніторинг, аудит і коригування стратегії – своєчасне виявлення потенційних загроз, оцінювання ефективності заходів, спрямованих на забезпечення інформаційної безпеки та внесення коректив в існуючу стратегію.

Таким чином, інтеграція інформаційної безпеки в систему ризик-менеджменту підприємства сприяє підвищенню надійності та його конкурентоспроможності.

Література:

1. ISO/IEC 27001:2022. Information technology. Security techniques. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 16.04.2025).
2. ISO 31000:2018. Risk management. Guidelines. URL: https://www.iso.org/standard/65694.html (дата звернення: 16.04.2025).