

**МІНІМІЗАЦІЯ РИЗИКІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗА РАХУНОК
ОПТИМАЛЬНОГО РОЗПОДІЛУ РЕСУРСІВ ЗАХИСТУ**

Аналіз ризиків – це насамперед їх визначення та оцінка. Оцінка інформаційного ризику включає визначення обсягу шкоди, якої він може завдати суб'єктові господарювання. У процесі контролю за інформаційними ризиками виявляють умови, за яких такі ризики можуть бути мінімальними, суттєвими або значними. Питання мінімізації ризику втрати інформації дуже актуальне для банків. Тому установи повинні вживати відповідних заходів, диференціюючи їх відповідно до певних загроз. Серед таких заходів насамперед мають бути:

- формування правових умов захисту інформації безпосередньо і банку;
- створення системи захисту інформації, яка функціонує в банківській інформаційній мережі;
- забезпечення контролю за носіями інформації;
- запровадження надійної системи документообігу в банку, яка б виключала можливість несанкціонованого доступу до банківських документів, їх втрати, знищення чи модифікації;
- забезпечення надійної охорони банків, особливо з точки зору виключення можливості несанкціонованого доступу до документів чи електронних носіїв інформації;
- ретельний підбір персоналу, зокрема управлінського, з урахуванням таких його характеристик, як професіоналізм, компетентність, креативність, конформізм, конструктивність мислення, колективізм, самокритичність, відповідальність;
- формування інформаційної бази прийняття управлінських рішень на основі таких принципів, як актуальність, достовірність, надійність, релевантність, цілеспрямованість та інформаційна єдність даних, повнота відображення змісту, зрозумілість;
- використання не одного, а декількох надійних інформаційних джерел для підвищення якості інформаційного забезпечення;
- використання додаткової інформації у разі недостатності наявної для прийняття обґрунтованих рішень;
- нагромадження, аналіз та ефективне використання інформації про досвід діяльності зарубіжних підприємств, науково-технічні досягнення.

Зазначимо, що частина з цих заходів вимагає значних фінансових ресурсів. Тому прийняття рішення щодо вибору способів зниження інформаційного ризику повинно враховувати: вартість здобуття додаткової інформації; важливість інформації, яку захищають; величину збитків, які може спричинити втрата інформації; ефективність інформаційної системи і системи захисту та їх відповідність вартості.