РЕГУЛЯТОРНІ ВИМОГИ ДО УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Пасічник Р.М., Кочорба В.Ю.
Харківський національний університет імені В.Н. Каразіна, м. Харків

У сучасному фінансовому секторі питання кібербезпеки, стійкості до ризиків та відповідності нормативним вимогам набувають критичного значення. Розглянемо ключові напрями регуляторних вимог, спрямованих на забезпечення стійкості, безпеки та прозорості операцій в умовах цифрової трансформації банківського сектору. Базове місце у формуванні стратегії цифрової безпеки в Європейському Союзі посідає регуляторний акт DORA (Digital Operational Resilience Act) [1], який зобов'язує банки здійснювати системне управління ризиками у сфері інформаційно-комунікаційних технологій шляхом регулярних оцінок загроз, а також розробки та тестування планів реагування на кіберінциденти. Одним з ключових елементів стає інтеграція інструментів штучного інтелекту для детекції аномалій у реальному часі, що дає змогу оперативно виявляти потенційні атаки. Важливу роль також відіграє забезпечення резервних систем, які дозволяють мінімізувати простої та втрати у разі збоїв. Ефективне управління даними передбачає відстеження, аналіз та захист даних клієнтів, що стає можливим завдяки використанню практик Data Governance. Це включає автоматизацію процесів дотримання нормативних вимог, таких як складання звітності для регуляторів. Особливу увагу приділяють дотриманню норм GDPR та інших вимог конфіденційності, що забезпечується шляхом шифрування даних та контролю доступу до них. В умовах активної співпраці банків із фінтех-компаніями важливо впроваджувати систему управління ризиками третіх сторін. Це включає проведення due diligence до укладення партнерських угод, а також постійний моніторинг діяльності контрагентів з використанням frameworks для vendor risk management. Для забезпечення відповідності партнерів регуляторним вимогам дедалі ширше застосовуються RegTech-рішення, що автоматизують процес перевірки. Зростаюча складність фінансового середовища потребує гнучких стратегій управління ризиками, здатних адаптуватися до змін у законодавстві та технологіях. Це передбачає застосування аналізу майбутніх загроз, зокрема за допомогою ШІ у сфері кредитування та оцінки поведінки клієнтів. З огляду на технологічну складність нових викликів, виникає потреба у навчанні персоналу роботі з моделями машинного навчання та системами кіберзахисту. Також актуальним є залучення експертів у сферах квантових обчислень і блокчейн-технологій для формування політики управління ризиками. Таким чином, сучасна стратегія управління ризиками у банківському секторі повинна спиратися на нормативне регулювання, технології та кадровий потенціал.

Література:

1. Digital Operational Resilience Act (DORA). URL: https://www.digital-operational-resilience-act.com