Шкрібинець І. Ф
студентка ПДЕБ-21 юридичного факультету,
Західноукраїнський національний університет
Ронська О.Г.
к.е.н, доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет

ІНФОРМАЦІЙНІ РИЗИКИ ТА МЕТОДИ ЇХ ОЦІНКИ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Інформаційні ризики є однією з ключових загроз сучасному бізнесу, оскільки вони безпосередньо впливають на стабільність функціонування підприємства, збереження комерційних та технічних секретів, фінансові результати діяльності та репутацію організації. У глобалізованому середовищі, де інформація стала основним стратегічним ресурсом, її захист визначає рівень конкурентоспроможності підприємства.

Інформаційні ризики — це ймовірність виникнення подій, які можуть призвести до порушення конфіденційності, цілісності або доступності інформації. Їхня реалізація здатна викликати фінансові збитки, втрату ринку, витік комерційної таємниці, порушення ділових зв’язків чи зниження довіри партнерів [1, с. 48].

З розвитком цифрових технологій масштаби інформаційних ризиків постійно зростають. Основні фактори, що зумовлюють їх виникнення, — використання глобальних мереж, віддаленого доступу до корпоративних систем, хмарних сховищ, автоматизації бізнес-процесів і великих обсягів даних. В умовах кіберзлочинності, фішингових атак, програм-вимагачів і соціальної інженерії захист інформаційних ресурсів стає невід’ємною складовою економічної безпеки підприємства [2, с. 133].

Класифікація інформаційних ризиків передбачає їх поділ за джерелом походження (внутрішні й зовнішні), характером дії (випадкові, навмисні),

об’єктом впливу (дані, програмне забезпечення, технічні засоби, персонал) та масштабом можливих наслідків. До внутрішніх ризиків належать недбалість персоналу, порушення політик безпеки, помилки адміністрування, а до зовнішніх — кібератаки, шкідливе ПЗ, хакерські дії, технічні збої чи стихійні лиха [3, с. 92].

Оцінка інформаційних ризиків є фундаментальним елементом системи управління економічною безпекою. Її метою є визначення рівня загрози, ймовірності її реалізації та потенційних наслідків для підприємства. Процес оцінки охоплює кілька етапів:

1. Ідентифікація ризиків — виявлення джерел загроз, об’єктів захисту та можливих сценаріїв порушення інформаційної безпеки.
2. Аналіз ризиків — оцінювання вразливостей та рівня імовірності виникнення інцидентів.
3. Кількісна та якісна оцінка — визначення потенційних збитків у грошовому й нематеріальному вимірі.
4. Розроблення стратегії реагування — вибір заходів зі зниження або усунення ризиків (прийняття, уникнення, мінімізація, передача ризику).

У практиці управління інформаційними ризиками застосовують кілька методів їх оцінювання: експертний, статистичний, аналітичний, імітаційний і комплексний. Експертний метод базується на думці фахівців у сфері безпеки, тоді як статистичний спирається на аналіз даних про попередні інциденти. Імітаційні моделі, зокрема метод Монте-Карло, дозволяють прогнозувати можливі сценарії розвитку ситуацій і визначати ймовірність реалізації загроз [4, с. 57].

Для ефективної оцінки інформаційних ризиків необхідно також використовувати сучасні стандарти та методики, зокрема ISO/IEC 27005, COBIT, NIST SP 800-30. Вони дають змогу системно оцінювати вразливість інформаційних активів, впроваджувати систему безперервного

моніторингу й формувати політику управління ризиками на рівні всієї організації.

Зменшення інформаційних ризиків потребує комплексного підходу, що поєднує технічні, організаційні та кадрові заходи. До технічних належать міжмережеві екрани, системи запобігання вторгненням, антивірусний захист, шифрування даних і контроль доступу. Організаційні заходи включають розроблення внутрішніх нормативних документів, політик конфіденційності, створення резервів даних, регулярний аудит безпеки та навчання персоналу.

Кадрова складова відіграє важливу роль у мінімізації ризиків, оскільки саме працівники часто стають джерелом витоку чи ненавмисного порушення правил захисту інформації. Тому важливо формувати культуру інформаційної безпеки, проводити інструктажі, тренінги та тестування знань персоналу [5, с. 278].

Держава також відіграє значну роль у створенні умов для ефективного управління інформаційними ризиками. Законодавче закріплення вимог щодо захисту персональних даних, електронних документів, кібербезпеки та захисту комерційної таємниці сприяє зменшенню ризиків як на мікрорівні (підприємства), так і на макрорівні (економіки держави). В Україні правові засади цього напрямку визначаються Цивільним кодексом України, Законами «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про основні засади забезпечення кібербезпеки України».

Отже, управління інформаційними ризиками є невід'ємною складовою системи економічної безпеки. Своєчасна ідентифікація загроз, їх об'єктивна оцінка та впровадження дієвих заходів мінімізації гарантують стабільність розвитку підприємства, його конкурентоспроможність та стійкість до зовнішніх і внутрішніх викликів інформаційного середовища.

ЛІТЕРАТУРА:

1. Бандурка О. М. *Економічна безпека підприємства.* — Київ: Центр учбової літератури, 2021. — 336 с.

2. Васильців Т. Г. *Економічна безпека підприємництва в Україні.* — Львів: Арал, 2020. — 386 с.

3. Копитко М. І. *Безпека підприємства: організація та управління.* — Львів: ЛДУВС, 2019. — 320 с.

4. Ліпкан В. А. *Інформаційна безпека України.* — Київ: КНТ, 2021. — 468 с.

5. Козаченко Г. В. Управління ризиками в системі економічної безпеки підприємства. — Київ: Наука і освіта, 2022. — 352 с.