УПРАВЛІННЯ КІБЕРРИЗИКАМИ В УМОВАХ ЦИФРОВІЗАЦІЇ БІЗНЕСУ

Башанова Н.Є.
ЗВО спеціальності 073 Менеджмент
Миколаївський національний аграрний університет

Сучасна цифрова трансформація підприємств забезпечує зростання ефективності, автоматизацію процесів і доступ до глобальних ринків, але водночас створює нові ризики. Активна інтеграція хмарних сервісів, Інтернету речей (IoT) і штучного інтелекту формує залежність бізнесу від інформаційних систем, що підвищує вразливість до кіберзагроз. У сучасних умовах кіберризики стають не лише технічною, а й економічною категорією, оскільки їх наслідки мають безпосередній вплив на фінансові результати та конкурентоспроможність підприємства.

Одним із найбільш поширених ризиків є витік даних. За звітом IBM Security (2024), середня вартість одного інциденту перевищує 4,45 млн доларів США, що включає прямі та непрямі збитки [1]. Іншим небезпечним видом загроз є програми-вимагачі, які блокують інформаційні ресурси. Приклад атаки на Colonial Pipeline у 2021 році продемонстрував масштабність проблеми — зупинка діяльності стратегічного підприємства та сплата викупу у 4,4 млн доларів [2].

Суттєву небезпеку становлять фішингові атаки та соціальна інженерія, що експлуатують людський фактор. За даними Verizon (2025), 82% інцидентів витоку даних пов’язані саме з діями працівників [3]. Не менш актуальними залишаються інсайдерські загрози, пов’язані з недбалим використанням прав доступу, та вразливості IoT-пристроїв і хмарних сервісів, які можуть бути використані як «вхідна точка» для атак.

Кібератаки мають комплексні наслідки: фінансові (прямі втрати, простої виробництва), операційні (зупинка процесів, порушення логістичних ланцюгів), репутаційні (втрата довіри партнерів) і правові (штрафи за порушення GDPR). У

цьому контексті кібербезпека стає стратегічним пріоритетом цифрового розвитку підприємства.

Для зниження кіберризиків доцільно формувати багаторівневу систему захисту, яка поєднує технічні, організаційні та правові заходи:

- впровадження систем виявлення вторгнень, брандмауерів і багатофакторної автентифікації;
- регулярне оновлення програмного забезпечення та шифрування даних;
- прогнозний аналіз кіберзагроз із використанням алгоритмів машинного навчання;
- навчання персоналу щодо розпізнавання фішингу та кіберетикету;
- створення планів реагування на інциденти та симуляційних тренувань;
- дотримання законодавства про кібербезпеку (зокрема, Закону України «Про основні засади забезпечення кібербезпеки України» [4]).

Ключовим елементом успішного управління кіберризиками є формування корпоративної культури безпеки, де кожен працівник усвідомлює власну роль у захисті даних. Підприємства, що інтегрують кібербезпеку у свою стратегію цифрової трансформації, отримують стійкі конкурентні переваги та підвищують довіру споживачів.

Отже, цифровізація відкриває нові можливості розвитку, але водночас вимагає усвідомлення і управління кіберризиками. Комплексний підхід, який поєднує технічні рішення, освітні програми та нормативне регулювання, є запорукою сталого розвитку бізнесу в цифрову епоху.

Список використаних джерел

1. IBM Security. *Cost of a Data Breach Report 2024*. IBM, 2024. URL: https://www.ibm.com/security/data-breach.

2. BBC News. *Colonial Pipeline: US recovers most of ransom paid to hackers*. BBC, 2021. URL: https://www.bbc.com/news/business-57394041.

3. Verizon. *2025 Data Breach Investigations Report*. Verizon, 2025. URL: https://www.verizon.com/business/resources/reports/dbir/.

4. Верховна Рада України. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України, 2017, №45, ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

5. Deloitte. *Cybersecurity Workforce Survey 2023*. Deloitte, 2023. URL: https://www.deloitte.com/global/en/services/consulting-risk/analysis/futureofcyber23.html.

Науковий керівник – Олійник Т. Г.,
канд. екон. наук, доцент кафедри економіки підприємств
Миколаївський національний аграрний університет

СТАТИСТИЧНЕ СПОСТЕРЕЖЕННЯ: СУТЬ, ВИДИ ТА ПРИКЛАДИ

Бобик Тіна Станіславівна,
ЗВО спеціальності 073 Менеджмент
Миколаївський національний аграрний університет

Статистичне спостереження – це планомірне, систематичне, науково організоване збирання даних про явища суспільного життя шляхом реєстрації їх істотних ознак. [1] Метою спостереження є здобуття достовірних даних, що стануть основою для прийняття обґрунтованих рішень. Без правильно організованих статистичних спостережень неможливо провести якісне дослідження, адже від них безпосередньо залежить точність і достовірність отриманих результатів.

Сутністю статистичного спостереження полягає в тому, що той хто досліджує інформацію фіксує поточний стан об’єктів дослідження, збираючи дані завчасно. Наприклад, якщо ми хочемо дізнатися середній результат навчання студентів в університеті, то статистичне спостереження передбачає