УДК 004.056:005.8

Лазарев Л.Д., магістрант, 2 р.н., гр. ЕПМ-21, ФБСО
Науковий керівник – к.е.н., доц. Ткачук В.О.
Державний університет «Житомирська політехніка»

Місце цифрової безпеки в системі заходів безпеки підприємства

Цифрова безпека відіграє дедалі важливішу роль у загальній стратегії безпеки підприємства через постійне розширення цифрових каналів комунікації та напрямів роботи. Важливим викликом стає динамічність кіберзагроз, яка вимагає постійного інвестування в інноваційні технології, такі як штучний інтелект для виявлення аномалій та блокчейн для захисту даних, що дозволяє компаніям бути на крок попереду кіберзлочинців. В умовах сучасності все більшого значення набувають процеси впровадження засобів цифровізації в діяльність підприємств. Однак недостатньо дослідженими залишаються питання впливу цієї практики на безпеку підприємств та відповідно обґрунтування необхідності подальшої імплементації діджитал-трансформацій у різні сфери.

Зростання темпів адаптації підприємств до нових форм ризиків в умовах цифровізації та збільшення використання хмарних сервісів, Інтернету речей (IoT) і мобільних пристроїв не лише призводить до оптимізації бізнес-процесів, а й змушує підприємства постійно переглядати свою стратегію та мати чітке розуміння середовища ведення діяльності [1].

За даними Cybersecurity Ventures, глобальні збитки від кіберзлочинності можуть досягти 10 трлн дол. на рік до 2025 р., а це означає щорічне зростання на 15 %. Підвищення рівня цифрових загроз є ключовим викликом, що підштовхує підприємства до зміцнення кібербезпеки на рівні корпоративної стратегії [2]. Крім фінансових збитків, кібератаки створюють ризики для репутації підприємств, а також втрати довіри з боку клієнтів і партнерів.

Цифрова безпека гарантує захист критично важливих активів підприємства, таких як фінансова інформація, інтелектуальна власність та персональні дані клієнтів і співробітників. Також цифрова безпека сприяє підвищенню оперативної ефективності, дозволяючи швидше і безпечніше обробляти дані та оптимізувати процеси.

Аналітика ризиків, шифрування, управління доступом та навчання співробітників – це основні компоненти цифрової безпеки. Вона дозволяє ідентифікувати потенційні загрози, прогнозувати ризики і встановлювати пріоритети захисту. Шифрування даних гарантує, що інформація буде недоступною для несанкціонованих осіб навіть у разі її викрадення.

Зростаючий обсяг і складність кіберзагроз вимагають адаптації існуючих стратегій безпеки. Підприємства стикаються з такими викликами, як брак кваліфікованих фахівців з кібербезпеки, що створює труднощі для постійного оновлення засобів захисту. У зв’язку з цим, навчання співробітників є критичним, оскільки людський фактор залишається однією з найслабших ланок кібербезпеки. Проведення регулярних тренінгів з кібербезпеки допомагає зменшити ризики фішингових атак, атак соціальної інженерії та інших видів шахрайства.

Формування цифрової культури на підприємствах є важливим завданням для керівництва, оскільки дозволяє підвищити обізнаність і відповідальність працівників щодо загроз кібербезпеки. Розробка інноваційних програм для розвитку кібернавичок серед співробітників сприяє створенню стійкої організаційної культури кібербезпеки.

Важливо зосередитись на складовій кібербезпеки підприємств як зсередини, так і ззовні, оскільки ефективна цифрова безпека є не лише технологічним, але й стратегічним елементом для захисту активів підприємства від сучасних кіберзагроз, а її інтеграція у стратегічні ініціативи забезпечує високий рівень адаптивності та стійкості, що допомагає мінімізувати потенційні фінансові та репутаційні збитки.

Отже, цифрова безпека повинна бути частиною загальної бізнес-стратегії, оскільки забезпечує безперервність бізнесу, допомагає будувати довіру клієнтів і дозволяє адаптуватися до мінливого бізнес-середовища. Стрімкі темпи діджиталізації призводять до зміни обсягів і трансформації структури витрат і доходів підприємств та мають суттєвий вплив на їх економічну безпеку. Все це вимагає доповнення переліку факторів та нового погляду на представлення статистичних моделей оцінювання рівня економічної безпеки підприємств.

Список використаних джерел

1. Яценко В.В. Діджиталізація – сучасний фактор розвитку бізнес-процесів [Електронний ресурс]. Ефективна економіка : електронний журнал. 2022. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=10042. – Дата звернення: 26.10.2024.

2. Morgan S. Cybercrime To Cost The World 9,5 trillion USD annually in 2024. Cybercrime Magazine [Електронний ресурс]. – Режим доступу : https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024. – Дата звернення: 28.10.2024.