

УДК 004.49:65:658

Михайлов Ю.С.¹, Комаров П.М.²

¹канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

² студ. гр. БТЕ-0414сп НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА МОДЕЛЕЙ УПРАВЛІННЯ БІЗНЕСОМ: ІНТЕГРАЦІЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В ЦИФРОВУ СТРАТЕГІЮ

В умовах стрімкої цифрової трансформації практично всіх галузей економіки питання кібербезпеки набуває особливого значення для сучасних бізнес-моделей. Дедалі більше підприємств стикаються з необхідністю інтеграції комплексних заходів захисту інформації в загальну систему корпоративного управління, переходячи від фрагментарного до системного підходу в управлінні кіберризиками. Ключовою особливістю сучасного етапу розвитку цифрових технологій є те, що кібербезпека перестає бути виключно технічним питанням і трансформується у важливий стратегічний компонент бізнес-моделей.

Аналіз актуальних досліджень демонструє, що впровадження ризик-орієнтованого підходу до кібербезпеки дозволяє компаніям не лише захистити наявні інформаційні активи, але й підвищити загальну стійкість бізнесу до зовнішніх та внутрішніх загроз. Інтеграція ризик-орієнтованого підходу передбачає кілька ключових етапів, серед яких: ідентифікація інформаційних активів та їх систематизація за критичністю для бізнесу;

визначення потенційних кіберзагроз та вразливостей; оцінка ймовірності реалізації загроз та потенційного впливу на бізнес; розробка та впровадження контрзаходів з урахуванням співвідношення витрат та потенційних втрат; постійний моніторинг та аудит ефективності заходів кібербезпеки.

Сучасні тенденції демонструють, що ефективні моделі інтеграції кібербезпеки в бізнес-стратегію мають базуватися на принципах адаптивності та проактивності. Компанії, які впроваджують ці принципи, застосовують такі інноваційні методи як предиктивна аналітика кіберзагроз, автоматизоване оцінювання ризиків на основі штучного інтелекту, безперервний моніторинг з використанням машинного навчання для виявлення аномалій, а також багаторівневі системи реагування на інциденти.

Особливу увагу в сучасних моделях управління бізнесом приділяють питанням кібербезпеки ланцюгів постачання, оскільки зростаюча інтеграція бізнес-процесів з контрагентами створює додаткові вектори кіберзагроз. Підприємства впроваджують комплексні програми оцінки кібербезпеки постачальників та партнерів, встановлюють стандарти захисту інформації для всіх учасників бізнес-екосистеми та розробляють спільні плани реагування на інциденти.

Цікавим аспектом трансформації бізнес-моделей під впливом вимог кібербезпеки є зміна підходів до оцінки ефективності інвестицій у захист інформації. Традиційні методики, такі як ROI (Return on Investment), поступаються місцем більш комплексним підходам, що враховують не лише прямі фінансові показники, але й вплив на репутацію, довіру клієнтів, конкурентоспроможність та загальну стійкість бізнесу. Компанії впроваджують методики ROSI (Return on Security Investment) та метрики, орієнтовані на вимірювання зниження ризиків та підвищення загальної стійкості бізнесу.

Важливою складовою сучасних моделей управління кіберризиками стає забезпечення відповідності нормативним вимогам у сфері захисту інформації та персональних даних. У зв'язку з посиленням регуляторного тиску в усьому світі бізнес змушений трансформувати процеси обробки інформації, забезпечуючи прозорість, підзвітність і належний рівень захисту. Ця тенденція стимулює впровадження концепції "privacy by design", що передбачає врахування вимог конфіденційності та безпеки даних на всіх етапах розробки та впровадження інформаційних систем.

Нові виклики для бізнес-моделей створює зростання загроз, пов'язаних з поширенням технологій Інтернету речей (IoT). Збільшення кількості пристроїв, що підключаються до корпоративних мереж, значно розширює поверхню потенційних атак. У відповідь компанії впроваджують архітектури нульової довіри (Zero Trust), які базуються на принципі "ніколи не довіряй, завжди перевіряй" та передбачають постійну автентифікацію та авторизацію

всіх користувачів та пристроїв незалежно від їх розташування відносно периметру корпоративної мережі.

З переходом до хмарних обчислень модель спільної відповідальності за кібербезпеку між провайдерами хмарних послуг та їх клієнтами потребує нових підходів до управління ризиками. Компанії впроваджують специфічні методики оцінки безпеки хмарних середовищ, використовують спеціалізовані інструменти для моніторингу безпеки в мультихмарних середовищах та розробляють плани забезпечення безперервності бізнесу з урахуванням особливостей хмарної інфраструктури.

Підсумовуючи, можна констатувати, що ефективна інтеграція ризик-орієнтованого підходу до кібербезпеки в моделі управління бізнесом стає конкурентною перевагою в умовах цифрової економіки. Цей підхід дозволяє компаніям не лише мінімізувати потенційні втрати від кіберінцидентів, але й забезпечує довіру клієнтів, партнерів та інвесторів, що в довгостроковій перспективі позитивно впливає на сталий розвиток бізнесу та його вартість.