Ружніков Р. Є., канд. екон. наук Скрипник Н. Є.
Дніпровський національний університет імені Олеся Гончара (Україна)

КІБЕРБЕЗПЕКА ПРОМИСЛОВИХ СИСТЕМ ЯК СКЛАДОВА ЧАСТИНА СТРАТЕГІЇ ІННОВАЦІЙНОГО РОЗВИТКУ

Сьогодні розвиток економіки характеризується цифровою трансформацією виробничих процесів, яка зумовлює інтеграцію інформаційних технологій у промислові системи управління. Впровадження концепції Індустрії 4.0, автоматизація виробництва, використання інтернету речей, штучного інтелекту та хмарних технологій значно підвищують ефективність функціонування підприємств. Водночас зростає рівень кіберзагроз, які можуть призводити до порушення стабільності виробничих процесів, втрати конфіденційних даних або навіть зупинки критичної інфраструктури.

Розвиток цифрових технологій сприяв формуванню нової моделі промислового виробництва, яка базується на використанні кіберфізичних систем, великих даних та автоматизованих виробничих комплексів. У межах концепції Індустрії 4.0 підприємства впроваджують інтелектуальні технології, які забезпечують підвищення ефективності управління виробничими процесами. Як зазначають С. Отрода та К. Петренко, «Індустрія 4.0 представляє собою четверту промислову революцію, яка базується на використанні цифрових технологій та кіберфізичних систем» [1, с.70].

Використання цифрових технологій дозволяє підприємствам оптимізувати виробничі процеси та підвищувати конкурентоспроможність продукції. Разом із тим, інтеграція інформаційних систем у виробничі процеси створює нові ризики, пов’язані з кіберзагрозами. У зв’язку з цим виникає необхідність формування систем кіберзахисту промислових мереж, які здатні забезпечити безперебійну роботу підприємств у цифровому середовищі.

Промислові системи управління є важливим елементом сучасного виробництва, оскільки вони забезпечують контроль технологічних процесів, автоматизацію обладнання та моніторинг виробничих параметрів. Водночас такі системи часто використовують мережеві технології, що робить їх потенційною мішенню для кібератак. Дослідники Ю. Самойленко, Я. Смітюх та О. Мариненко

підкреслюють, що захист промислових систем управління від кіберзагроз є одним із основних завдань сучасної інформаційної безпеки [2].

Однією з головних проблем є те, що багато промислових систем були розроблені у період, коли питання кібербезпеки не мало критичного значення. Внаслідок цього вони часто мають низький рівень захисту та можуть бути вразливими до несанкціонованого доступу. З метою підвищення рівня безпеки промислових систем застосовуються різні технологічні рішення, серед яких:

– використання міжмережевих екранів;

– впровадження систем виявлення вторгнень;

– сегментація промислових мереж;

– контроль доступу до інформаційних ресурсів;

– моніторинг мережевої активності.

Як зазначає Н. В. Резнікова, В. А. Вовк та Л. В. Пташенко, «кібербезпека стає невід'ємним елементом стратегічного управління конкурентоспроможністю, оскільки вразливість цифрової інфраструктури може призвести до втрати довіри партнерів, клієнтів і інвесторів» [3, с. 439]. У цьому контексті кібербезпека виконує декілька важливих функцій: забезпечує безперервність виробничих процесів, захищає інформаційні ресурси підприємства та підвищує інвестиційну привабливість підприємств.

Формування ефективної системи кіберзахисту потребує застосування технологічних, організаційних та правових заходів. Серед основних напрямів розвитку кібербезпеки промислових систем можна виділити:

– впровадження сучасних технологій захисту інформації;

– використання штучного інтелекту для виявлення кіберзагроз;

– підготовку кваліфікованих фахівців;

– удосконалення нормативно-правового регулювання.

Отже, кібербезпека промислових систем є складовою стратегії інноваційного розвитку сучасної економіки. Впровадження цифрових технологій у виробничі процеси створює нові можливості для підвищення ефективності діяльності підприємств, проте одночасно зростає рівень кіберризиків. Аналіз наукових досліджень свідчить про те, що забезпечення кібербезпеки є необхідною умовою стабільного функціонування промислової інфраструктури та реалізації

інноваційних стратегій розвитку. Підвищення рівня кіберзахисту промислових систем потребує впровадження сучасних технологій захисту інформації, розвитку національної системи кібербезпеки, удосконалення правового регулювання та підготовки висококваліфікованих фахівців.

Список використаних джерел:

1. Отрода С. С., Петренко К. В. Індустрія 4.0 та її вплив на конкурентоспроможність української промисловості. Міжнародне науково-технічне співробітництво: принципи, механізми, ефективність. XXI (XXXIII) Міжнародна науково-практична конференція: збірник наукових праць. Секція 3. Національні інноваційні системи та індустрія-4.0: проблеми формування та ефективності. 2025. С. 70-72.
2. Самойленко, Ю. О., Смітюх Я. В., Мариненко О. В. Кібербезпека промислових систем управління на основі комутованого доступу. Наукові здобутки молоді – вирішенню проблем харчування людства у XXI столітті: матеріали 88 Міжнародної наукової конференції молодих учених, аспірантів і студентів. Київ: НУХТ, 2022. Ч. 2. С. 276.
3. Резнікова Н. В., Вовк В. А., Птащенко Л. В. Формування міжнародної конкурентоспроможності ІТ-сектору: стратегічні чинники та кіберризики. *European scientific journal of Economic and Financial innovation*. 2025. No 1 (15). С. 439-449.

Рязанова М. В.

Дніпровський національний університет імені Олеся Гончара (Україна)

УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ НЕСТАБІЛЬНОСТІ ЗОВНІШНЬОГО СЕРЕДОВИЩА

У сучасних умовах розвитку економіки підприємства функціонують у складному та динамічному зовнішньому середовищі, яке характеризується високим рівнем невизначеності. Економічні кризи, глобалізаційні процеси, технологічні зміни, посилення конкуренції та нестабільність фінансових ринків суттєво впливають на діяльність підприємств. У таких умовах питання управління ризиками набуває особливої актуальності, оскільки саме ефективне управління ризиками дозволяє підприємствам адаптуватися до змін та забезпечувати стабільність своєї діяльності.

Ризик у підприємницькій діяльності можна визначити як імовірність виникнення подій, що можуть негативно вплинути на результати діяльності підприємства. В умовах нестабільного зовнішнього середовища рівень ризику