Лунгол Ольга Миколаївна,
кандидат педагогічних наук, доцент,
доцентка кафедри оперативно-розшукової
діяльності та інформаційної безпеки
факультету підготовки фахівців для
підрозділів кримінальної поліції Донецького
державного університету внутрішніх справ

АКТУАЛЬНІ ПІДХОДИ ДО ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ В УМОВАХ ІНДУСТРІЇ 4.0

Індустрія 4.0 – це концепція технологічної революції, що охоплює виробничі процеси та виробничі підприємства, яка базується на використанні передових цифрових технологій для автоматизації та оптимізації виробничих процесів. Дана концепція включає в себе ряд технологій, таких як Інтернет речей (IoT), штучний інтелект (AI), аналітика даних, доповнена реальність (AR), віртуальна реальність (VR), хмарні технології тощо. Впровадження кіберфізичних систем – це один із ключових аспектів Індустрії 4.0. Кіберфізичні системи поєднують в собі кібернетичні (інформаційні та комунікаційні) та фізичні (реальні) складники, створюючи єдину систему, де комп'ютеризовані системи взаємодіють з фізичними процесами в реальному часі. Ці системи дозволяють підприємствам отримувати більше даних з виробничих процесів за допомогою датчиків та IoT-пристроїв, а потім аналізувати ці дані за допомогою аналітики та штучного інтелекту для прийняття кращих управлінських рішень. Імплементація кіберфізичних систем у бізнес-процеси галузей економіки дозволяє взаємодіяти віртуальним і фізичним процесам в інформаційній мережі в режимі он-лайн, віддалено управляти ними та здійснювати контроль, приймати організаційні та управлінські рішення для оптимізації виробничих процесів, знижувати витрати, підвищувати продуктивність та якість продукції, а також покращувати умови праці [1 – 3].

Захист кіберфізичних систем у бізнес-процесах галузей економіки є вельми актуальною та важливою задачею, особливо в умовах воєнного стану. Кіберфізичні системи, які поєднують в собі цифрові та фізичні

компоненти, є невід'ємною частиною роботи бізнесу у багатьох сферах, включаючи виробництво, транспорт, медицину, енергетику тощо. Захист цих систем є критично важливим, оскільки вони відповідають за автоматизацію та оптимізацію бізнес-процесів.

Уразливість кіберфізичних систем може призвести до серйозних проблем і загроз для підприємств. Якщо кіберфізичні системи не захищені належним чином, вони можуть стати мішенню для кібератак. Атаки можуть призвести до втрати конфіденційної інформації, порушення роботи системи або навіть втрати контролю над фізичними процесами. Помилки в роботі кіберфізичних систем через кібератаки або програмні помилки можуть призвести до зупинки виробництва або інших бізнес-процесів, що призводить до фінансових втрат. В деяких галузях, таких як виробництво або енергетика, недостатній захист кіберфізичних систем може стати загрозою для безпеки працівників. Втрата даних або недоступність системи може призвести до стресу та психологічного тиску на співробітників, що впливатиме на продуктивність.

Отже, захист кіберфізичних систем у бізнес-процесах є актуальним питанням сьогодення для забезпечення стабільності та безпеки підприємства. Даний процес включає в себе використання сучасних методів шифрування, захисту від кібератак, регулярне оновлення програмного забезпечення та впровадження строгих правил безпеки для працівників. Захист кіберфізичних систем – це інвестиція в майбутнє підприємства, яка дозволяє уникнути серйозних проблем і зберегти репутацію та стабільність у галузях економіки.

В роботах вітчизняних науковців відображено низку сучасних рекомендацій із способів та засобів захисту кіберфізичних систем. Так, Погасій С. [4] описує метод оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтери «хижак-жертва». Метод ґрунтується на базі запропонованого класифікатора загроз з урахуванням їхньої гібридності та синергізму. Науковець описує в своїх дослідженнях [4] структуру класифікатора, що відображає гібридність та синергізм загроз. Пропонований метод, на відміну від існуючих, дозволяє надавати оцінку рівня безпеки кіберфізичних систем і систем безпеки, що розвиваються, тобто виробляти динамічне оцінювання, а не

статичне. Ярощук І. [5] проводить дослідження з удосконалення технології оцінки ризиків інформаційної безпеки кіберфізичних систем та наводить у своїх дослідженнях рекомендації щодо оцінки ризиків при прототипуванні кіберфізичних систем та мінімізації ризиків при їх експлуатації.

Актуальні підходи до захисту кіберфізичних систем стають все більш важливими в умовах зростаючої кількості кіберзагроз та широкого впровадження цифрових технологій у всі сфери життя. Для забезпечення надійності та безпеки кіберфізичних систем використовуються різноманітні підходи, серед яких можна виділити такі: шифрування даних, яке дозволяє захистити інформацію від несанкціонованого доступу; використання мультифакторної аутентифікації, коли для входу в систему потрібно підтвердити свою особу за допомогою кількох методів, наприклад, пароля та SMS-коду; IDS системи дозволяють вчасно виявляти несанкціонований доступ або аномальну активність в мережі; ACS системи регулюють доступ до різних частин кіберфізичних систем залежно від рівня доступу користувача; регулярне оновлення програмного забезпечення та встановлення важливих патчів безпеки; тестування на проникнення (penetration testing) задля виявлення слабких місць в системі та вжиття заходів для їх усунення тощо.

Актуальність розвитку та удосконалення цих підходів полягає у постійному розвитку кіберзагроз та швидкому розвитку технологій. Впровадження найсучасніших методів захисту дозволяє підприємствам та організаціям ефективно захищати свої кіберфізичні системи від потенційних загроз і забезпечувати надійність та безпеку своїх бізнес-процесів.

Список використаних джерел:

1. Чміль Г.Л. Економічна взаємодія суб'єктів споживчого ринку в умовах індустрії 4.0. Цифрова економіка та інформаційні технології: матеріали міжнар. наук.-практ. конф., 15-16 квітня 2021р. Київ: Видавничий центр ДУІТ, 2021. С. 200 – 202.
2. Храпкіна В. Інституціональні аспекти цифрової трансформації та розвитку цифрової економіки України. Цифрова економіка та економічна безпека. 2024. № 1 (10). С. 103-107. https://doi.org/10.32782/dees.10-19
3. Чміль Г. Л. Ґенеза економічної думки концепції «Індустрія 4.0» в умовах цифрової трансформації. Вісник Сумського національного аграрного університету. 2020. Вип. 4 (86). С. 71-75.
4. Погасій С. Моделі і методи захисту інформації в кіберфізічних системах. Ukrainian Scientific Journal of Information Security. 2022. № 28(2). С. 67-79.
5. Ярощук І.В. Оцінка ризиків кіберфізичних систем на базі мікроконтролерів: дипломна робота магістра за спеціальністю «125 – кібербезпека». Тернопіль : ТНТУ, 2020.