Сучасне підприємство характеризується великою кількістю внутрішніх і зовнішніх інформаційних потоків, що функціонують в межах його діяльності. Особливістю є те, що потоки містять великі об'єми різнорідної інформації, які необхідно правильно обробляти і виокремлювати ті дані, які будуть сприяти правильному та ефективному керуванню підприємством на всіх рівнях. Особливо це актуально для промислових підприємств з огляду на активний розвиток і широке впровадження концепції Industry 4.0.

Застосування філософії Industry 4.0 при організації роботи промислового підприємства вимагає створення Smart Factory, що не можна реалізувати без цифрових двійників виробництва, хмарних технологій, кіберсистеми тощо. Оскільки сучасне виробництво має високий ступінь автоматизації, то характеризується інформаційними потоками, що містять важливу промислову інформацію. Особливістю промислових автоматичних систем є відкритість їх протоколів і невисока степінь захищеності промислових мереж. Тому в умовах високої конкуренції і кризи, яка назріває через війну в Україні, захист промислової інформації, як складової ефективного функціонування підприємства, має надзвичайне значення. Одним з варіантів вирішення питань безпеки є проектування та впровадження інформаційної автоматизованої системи (ІАС) захисту промислової інформації [1]. Основою задачею якої є забезпечення різними методами і засобами захист інформації різної цінності та призначення від найпоширеніших загроз, таких як виток, злом тощо.

Фактично проектування інформаційної автоматизованої системи захисту промислової інформації буде включати етапи, передбачені стандартами ГОСТ 34.601-90 [2] та ISO/IEC 12207 [3].

Але слід зазначити, що для забезпечення захисної складової розроблюваної системи з урахуванням тенденцій Industry 4.0 на відповідних етапах проектування повинно бути враховане наступне: етап формування ІАС – аналіз систем промислового захисту та аналіз інтеграції із суміжними та зовнішніми системами; розробка концепції ІАС – класифікація автоматичних систем, які є на виробництві, та визначення інформації, яка підлягає захисту, й визначення усіх загроз безпеки, розробка вимог до цифрових двійників; ескізний проект – розробка моделі загроз, розробка проєкта захисту і модернізації існуючих автоматичних систем, створення та впровадження цифрового двійника.

Отже, зміни, які вносять тенденції Industry 4.0 та нова філософія ведення виробництва вимагає внесення змін в процес проектування інформаційних систем. Надважливим є забезпечення захисту промислової інформації для забезпечення ефективної роботи виробничого підприємства в умовах конкуренції.

Список літератури

1. Власенко Л.О. Кібербезпека як ключовий чинник впровадження Industry 4.0 / Л.О. Власенко, Т.В. Савченко, М.В. Сашньова // Глобалізаційні виклики розвитку національних економік : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. – Київ : Київ. нац. торг.-екон. ун-т, 2021. – С. 259-261.

2. ГОСТ 34.601-90 Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Автоматизовані системи. Стадії створення. Режим доступу – http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=53626

3. ISO/IEC 12207 – Information Technology – Software Life Cycle Processes. Режим доступу – https://www.iso.org/standard/35263.html