МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОМИСЛОВИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Ляшенко О.С., Гольцев Д.О., Мосєйкін А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день функціонування будь-якого промислового підприємства неможливо уявити без автоматизованої системи управління технологічними процесами (АСУТП). Сучасні АСУТП представляють собою апаратно-програмні комплекси, які обробляють інформацію з різного роду джерел та використовують для її обробки різні інформаційні технології. Інформаційні технології активно розвиваються в різних сферах людської діяльності і автоматизовані системи управління виробництвом не є винятком. Впровадження уніфікованих технологій дозволило вивести промислові системи управління на новий, більш високий рівень. Все це привело не тільки до зростання економічних показників, але і до підвищення ймовірності реалізації існуючих інформаційних загроз, а також появи нових. Варто зазначити, що протягом останніх десятиліть атаки на АСУТП стають привабливою метою, спостерігається значне зростання цілеспрямованих атак на промислові інформаційні системи з метою промислового шпигунства, шахрайства та порушення функціонування підприємства [1].

Метою роботи є побудова моделі, яка дозволяє враховувати особливості промислових комп'ютерних систем, які використовуються в АСУТП та забезпечення відповідного рівня безпеки інформації [2, 3]. В роботі запропоновано підхід для побудови моделі, яка буде враховувати різні види інформаційних загроз. Основою забезпечення безпеки є коректне визначення загроз. Використання даного підходу дозволяє виділити три основних класу загроз безпеки в АСУТП. Порушення промислової безпеки: реалізація погроз безпосередньо впливає на промислову безпеку, може бути причиною техногенної катастрофи. Зниження ефективності виробничого процесу: реалізація погроз явно знижує кількісні економічні показники процесу, що автоматизується за допомогою АСУТП. Інші порушення безпеки і надійності: реалізація загроз безпосередньо не впливає на промислову безпеку і надає опосередкований вплив на якісні або кількісні показники ефективності, надійності і безпеки.

Список літератури

1. Ляшенко С.А., Фесенко А.М., Ляшенко А.С., Создание открытого программно-технического комплекса управления безопасными технологическими процессами в выпарном отделении сахарного завода. Вісник ХНТУСГ ім. П. Василенка. 2015. № 156. С. 593–601.

2. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.

3. Jakobson G. Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions. International Conference on Cyber Conflict, CYCON. 2013. P. 1-18.