Анчис А. О., магістрант,
Бродський Ю. Б., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ЗАХИСТ ТА АВТОМАТИЗАЦІЯ ПРОМИСЛОВИХ ЛІНІЙ ВИРОБНИЦТВА

У сучасному виробництві автоматизація відіграє ключову роль у підвищенні ефективності та конкурентоспроможності підприємств. Застосування автоматизованих систем управління дозволяє оптимізувати виробничі процеси, зменшує ймовірність людських помилок та забезпечує стабільність продукції.

Промислові контролери є ключовими компонентами в автоматизації промислових ліній виробництва. Вони відіграють важливу роль у керуванні різноманітними процесами та системами, забезпечуючи автоматизоване управління виробництвом.

Програмовані логічні контролери (Programmable Logic Controller, PLC) використовуються для автоматизації та керування процесами у виробництві, вони здатні обробляти великий обсяг вхідних сигналів та виконувати відповідні дії на вихідних пристроях.

У сфері промислової автоматизації компанії є Siemens Allen-Bradley, Mitsubishi Electric, Omron та інші. Вони спеціалізується на розробці та виробництві надійного та ефективного обладнання для автоматизації виробничих процесів.

Проте, разом з розвитком технологій зростає і кількість кіберзагроз для автоматизованих систем. Захист від цих загроз стає надзвичайно важливою задачею для будь-якого виробничого підприємства. Підвищення свідомості про кібербезпеку та використання захисту може допомогти у запобіганні можливим атакам та забезпеченні безпеки промислових систем.

Кіберзагрози для автоматизованих систем є серйозними загрозами безпеці, які можуть призвести до різноманітних негативних наслідків. Вони включають віруси, атаки на мережу, внутрішні загрози, втручання в програмне забезпечення та витік конфіденційної інформації. Зловмисники можуть використовувати різні методи, щоб завдати шкоди автоматизованим системам, включаючи неправомірний доступ до системи, зміну програмного забезпечення та крадіжку конфіденційних даних.

Впровадження систем кіберзахисту, які включають в себе заходи з протидії кібератакам та викраденню даних, стає ключовим завданням для підприємств. Розробка та використання програмних та апаратних засобів для захисту від несанкціонованого доступу до систем управління та захисту інформації процесів виробництва стають невід'ємною частиною безпеки.

Узагальнюючи, автоматизація промислових ліній виробництва та забезпечення їхньої безпеки завжди стоять перед виробничими підприємствами як пріоритетні завдання, щоб забезпечити ефективну та безпечну роботу систем управління та виробничих процесів.

Більш детально про засоби захисту та їх застосування в автоматизованих системах виробництва, включаючи заходи безпеки, буде представлено в доповіді. Основні аспекти цих технологій, включаючи їх переваги та можливості, будуть розглянуті, а також будуть висвітлені методи захисту від потенційних загроз та кібератак. Буде описано різні види промислових контролерів та їх роль в процесі виробництва, з особливим акцентом на заходи безпеки, спрямовані на захист автоматизованих систем від небезпек та кіберзагроз.

Список використаних джерел

1. Технологія програмування промислових контролерів [Електронний ресурс]. Режим доступу до ресурсу: https://publish.nure.ua/catalog/download/55/32/141?inline=1

2. Технології забезпечення безпеки мережевої інфраструктури [Електронний ресурс]. Режим доступу до ресурсу: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

3. PLC [Електронний ресурс]. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/PLC

4. Контролери Siemens [Електронний ресурс]. Режим доступу до ресурсу: https://www.siemens.com/ua/uk/produkty/avtomatyzatsiya-promyslovosti/prohramne-zabezpechennya-dlya-promyslovosti/prohramne-zabezpechennya-dlya-avtomatyzatsiyi/tia-portal.html

5. Засоби захисту ПЛК Siemens [Електронний ресурс]. Режим доступу до ресурсу: https://support.industry.siemens.com/cs/attachments/109798583/SecurityConcept_TIA_V17_en.pdf