УДК 004.056:621.311

Катков А.О., здобувач,
Покляченко О.В., старший викладач
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ ЕЛЕКТРОЕНЕРГЕТИКИ

Сучасні об'єкти електроенергетики функціонують на основі комп'ютеризованих систем управління, зокрема SCADA-систем, автоматизованих систем диспетчерського керування та локальних підсистем контролю технологічних процесів. Поглиблення цифровізації, інтеграція таких систем у корпоративні мережі та використання віддаленого доступу підвищують ефективність керування енергетичними об'єктами, проте одночасно суттєво збільшують рівень кіберризиків. Наслідком реалізації кіберзагроз можуть стати порушення технологічних режимів, зниження надійності електропостачання, пошкодження обладнання та виникнення масштабних аварійних ситуацій.

До основних кіберзагроз для комп'ютеризованих систем управління в електроенергетиці належать несанкціонований доступ, шкідливе програмне забезпечення, атаки типу відмови в обслуговуванні, компрометація каналів передачі даних, а також цілеспрямовані атаки на об'єкти критичної інфраструктури. Особливу небезпеку становлять складні тривалі цільові атаки, які характеризуються прихованим проникненням у систему, закріпленням у мережі та подальшим впливом на технологічні процеси або інформаційні ресурси.

Метою дослідження є аналіз основних підходів до забезпечення кібербезпеки комп'ютеризованих систем управління об'єктами електроенергетики та визначення ефективних методів підвищення їх захищеності. Базовими напрямами захисту є сегментація мережевої інфраструктури, впровадження засобів виявлення та запобігання вторгненням, застосування криптографічного захисту даних, регулярне оновлення програмного забезпечення, а також реалізація рольового контролю доступу до ресурсів системи.

Одним із ключових принципів побудови захищеної інфраструктури є концепція багаторівневого захисту Defense in Depth, що передбачає формування декількох взаємодоповнювальних рубежів безпеки. Такий підхід дає змогу зменшити ймовірність успішної реалізації атаки навіть у разі компрометації окремого елемента системи. Додаткового значення набувають засоби моніторингу в реальному часі, аналізу журналів подій та виявлення аномальної активності, зокрема із застосуванням методів

машинного навчання, що підвищує оперативність виявлення потенційних інцидентів.

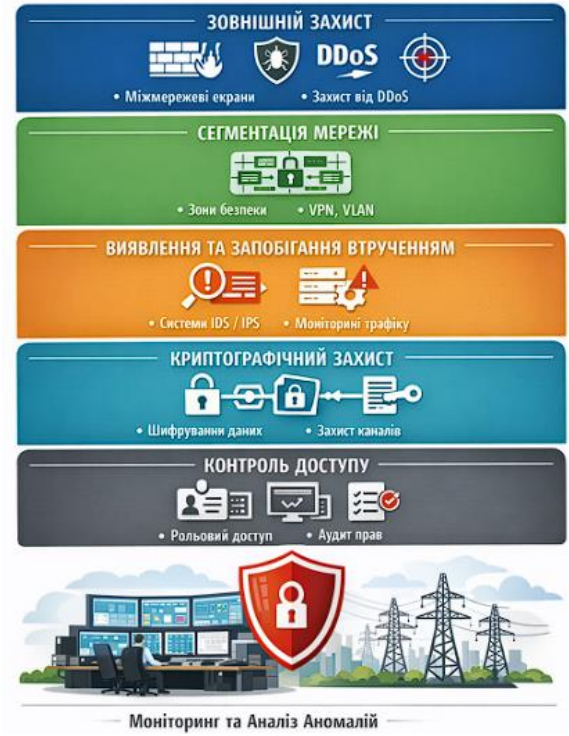

Рис.1. Ключові рівні багаторівневого кіберзахисту систем керування в електроенергетиці

Забезпечення кібербезпеки комп’ютеризованих систем управління в електроенергетиці є комплексним науково-технічним завданням, яке потребує узгодженого поєднання технічних, програмних та організаційних заходів. Реалізація сучасних підходів до захисту сприяє підвищенню стійкості енергетичної інфраструктури, надійності функціонування об’єктів електроенергетики та зниженню ризику кіберінцидентів.

Список використаних джерел:

1. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., Prokop, L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering, 2024.