АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КФС НА ОСНОВІ СТАТИСТИЧНИХ МЕТОДІВ

Фурсов І.І.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

У роботі розглянуто питання підвищення інформаційної безпеки кіберфізичних систем (КФС) за допомогою статистичних методів. Досліджено застосування методів дисперсійного аналізу, кореляційного аналізу, одно факторного дисперсійного аналізу у питаннях визначення порушень безпеки КФС на прикладі роботи вітрових електрогенераторів, що являються основою Smart Grid систем розумного електропостачання новітніх енергосистем. Актуальність роботи обумовлена великими збитками енергетичних компаній при інформаційній атаці на енергосистеми, загрозами виходу з ладу важливих елементів інфраструктури та об'єктів забезпечення життєдіяльності людини, загрозами навколишньому середовищу та життю людини та відносною легкістю порушення безпеки КФС що обумовлена великою кількістю каналів даних, до яких потенційних зловмисник має прямий доступ. Застосовані у даний час методи визначення фальсифікації даних у інформаційному потоці КФС, а саме метод нейронних мереж, метод само подібності процесів складних систем та ін., не надають надійної інформації про стан інформаційного потоку КФС, оскільки не аналізують вхідний потік даних, базуються на знаннях про стан атаки на КФС, тому не можуть виявити нові типи атак. Для усунення даних недоліків існуючих методів було запропоновано використання статистичних методів виявлення фальсифікованих даних у інформаційному потоці КФС, що не були достатньо розглянуті у науковій літературі. Статистичні методи дозволяють проводити комплексний аналіз зміни параметрів навколишнього середовища викликаний низкою факторів, що можуть бути використані як індикатори для виявлення фальсифікованих даних. Інформація про поводження певних змінних при впливі окремих факторів є унікальною для кожної КФС, тому може слугувати основою методу визначення атак на КФС. А комбінація методу нейронних мереж з попереднім статистичних аналізом дозволить досягти підвищення рівня розпізнання атак, що складає близько 80% на даний момент. У роботі було запропоновано алгоритм виконання аналізу вхідного потоку даних системи КФС вітрового генератора, що складається з таких етапів:

1) збір та первинна обробка даних КФС вітрогенератора з вхідними параметрами: «час замру», «сила вітру», «кут вітру».
2) збір описових статистик вхідного потоку: моди, медіани, дисперсії;
3) однофактроний дисперсійний аналіз даних;
4) розробка регресійної моделі роботи вітрогенератора відносно параметру «потужність» з вхідними параметрами: «час замру», «сила вітру», «кут вітру».