УДК 621.316.925

ПРОБЛЕМИ ЦИФРОВИХ ПІДСТАНЦІЙ ПО ЗБЕРЕЖЕННЮ ІНФОРМАЦІЙНИХ ПОТОКІВ ДАННИХ

Лобода О. І., к.т.н. aleks.loboda27@gmail.com
Таврійський державний агротехнологічний університет імені Дмитра Моторного

Актуальність та постановка проблеми. В даний час одним з напрямків розвитку світової електроенергетики є застосування на енергетичних об'єктах цифрових пристроїв релейного захисту, протиаварійної автоматики, контролерів автоматизованої системи керування, систем комерційного обліку і контролю якості електроенергії. У світі почалося масове реалізація технології керування Smart Grid, впровадження рішень класу цифрових підстанцій, на базі стандартів серії МЕК 61850. Взагалі цифрова підстанція є принципово новим об'єктом з позиції систем керування. У ній забезпечується глибокий моніторинг первинного обладнання і всіх вторинних систем, спрощується процес контролю і керуванню. З позиції концепції Smart Grid, цифрова підстанція - це ефективний енергетичний елемент, що має властивості спостережливості, адаптивності і інтелекту. Проте, створення цифрових підстанцій в енергосистемах викликає велику кількість питань. Найбільш гострі і не до кінця вирішені - це питання кібербезпеки.

Основні матеріали дослідження. Цифрова підстанція виконує ту ж саму задачу як і традиційна підстанція, але існують деякі особливості, наприклад: використання цифрових і оптичних трансформаторів струму і напруги; заміна більшості фізичних аналогових і дискретних трактів цифровими; використання потужних сучасних мікропроцесорних пристроїв, що приведе до збільшення додаткових виконаних функцій і зменшення кількості інших інтелектуальних пристроїв. [1,2]

Слабкою ланкою цифрової підстанції є комунікаційні мережі і канали, а для існуючих підстанцій - системи оперативного постійного струму. В якості можливих загроз з позиції кібербезпеки для цифрових підстанцій можна відзначити наступні: атаки ззовні, через зовнішні цифрові канали зв'язку; невиявлені помилки в програмному забезпеченні пристроїв; внутрішні дефекти програмного забезпечення мікропроцесорних пристроїв, також людський фактор - помилки оперативного та експлуатаційного персоналу.

Для порівняння, зазначимо основні загрози в традиційних підстанціях: порушення ізоляції, що приведе до коротких замикань в ланцюгах; порушення контактів, обрив кабельних зв'язків; пошкодження обладнання; електромагнітна несумісність; помилки оперативного та експлуатаційного персоналу енергооб'єкта.

У традиційних підстанціях основними засобами підвищення надійності і живучості є: дублювання - установка декількох однакових пристроїв; функціональне резервування - реалізація однакових або схожих функцій з використанням різних фізичних принципів; декомпозиція - поділ різних функцій між різними пристроями, фізичне рознесення кабелів і пристроїв, виділення окремих кернів для поділу ланцюгів різних пристроїв; спрощення - застосування простих, зрозумілих і однозначних алгоритмів керування.

При переході від традиційних підстанцій до цифрові на основі стандарту МЕК-61850 відбудеться відмова від таких принципів: від функціонального резервування, тому що комунікаційні мережі (включаючи комутатори і маршрутизатори) працюють

на одному і тому ж принципі; відмова від декомпозиції, тому що комунікаційні мережі (включаючи комутатори і маршрутизатори), що забезпечують шини процесів і шини об'єктів, виконують функції доставки інформації до будь-яких пристроїв моніторингу та керування; відмова від спрощення, тому що алгоритми передачі та обробки цифрової інформації з комунікаційних мереж досить складні.

Для забезпечення надійності та живучості цифрових підстанцій застосовують тільки: дублювання пристроїв; дублювання мереж і каналів зв'язку; функціональне резервування і декомпозиція виключно на рівні електроенергетичних функцій, але не на рівні цифрових технологій.

Складно стверджувати, чи достатньо вищеперелічених способів для забезпечення надійності та живучості цифрових підстанцій. Більш того, можна відзначити, що комунікаційні мережі та мікропроцесорні пристрої цифрових підстанцій універсальні, і без істотної переробки можуть вирішувати будь-які інформаційні завдання в тому числі, не пов'язані з електроенергетикою (наприклад, виконувати свідомо шкідливі функції в процесі кібератаки), чого не можна було сказати про пристрої на традиційних підстанціях (особливо на електромеханічної базі).

Виходячи з аналізу роботи мікропроцесорних пристроїв і систем [3] пропонуються наступні заходи щодо підвищення кібербезпеки цифрових підстанцій і об'єктів електроенергетики в цілому:

- застосування симплексних каналів з односторонньою передачею інформації там, де це досить для виконання прикладної функції;
- поділ інформаційних потоків різних підсистем на фізично не пов'язані, сегменти комунікаційних мереж передачі даних всередині підстанції;
- використання тільки протоколів Ethernet і TCP / IP в комунікаційних технологіях цифрової підстанції;
- застосування для виконання відповідальних функцій керування спеціалізованих протоколів обміну інформацією, що дозволяють передавати тільки ту інформацію, яка потрібна для вирішення конкретного завдання;
- створення виділених сегментів комунікаційних мереж, що використовують для налаштуванню і перебудови мікропроцесорних і комунікаційних пристроїв;
- застосування міжмережевих екранів, які фізично не дозволять виконувати несанкціоновані функції.

Висновок.

В тезах представлені деякі актуальні проблеми в області кібербезпеки електроенергетичних об'єктів та систем, що стає важливим в зв'язку з появою цифрових підстанцій у світлі можливості подальшої реалізації концепцій Smart Grid.

Запропоновано ряд підходів, які, дозволять вирішити частину проблем кібербезпеки.

Список використаних джерел

1. Чичёв С. И., Калинин В. Ф., Глинкин Е. И. Методология проектирования цифровой подстанции в формате новых технологий. М: Издательский дом "Спектр", 2014. 228 с.

2. Шабад М. А. Автоматизация распределительных электрических сетей с использованием цифровых реле: Учебное пособие. СПб.: Изд. ПЭИпк, 2002.

3. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов.М.: Горячая линия-Телеком, 2006. 544 с.