УДК 004.056

С.Ф. Гончар, Київ
А.В. Ониськова, Київ

АНАЛІЗ СТАНДАРТІВ ПО ЗАБЕЗПЕЧЕННЮ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ SMART GRID

Abstract. This article summarizes, presents and briefly describes the basic standards that define the cybersecurity requirements that apply to Smart Grid.

Актуальність

Поява, існування та актуальність проблеми кібербезпеки новітніх і перспективних електроенергетичних систем, у тому числі із застосуванням інтелектуальних мереж Smart Grid визнається сучасною світовою енергетичною спільнотою. Дослідженню і розв'язанню цієї проблеми приділяється все більше уваги в багатьох передових країнах світу.

Впровадження технології інтелектуальних мереж з одного боку спрощує і прискорює управління, але з іншого боку відкриває доступ до можливих кібератак і неправомірного використанню даних.

Постановка задачі

Дослідженню проблеми забезпечення кібербезпеки інформаційних систем об'єктів енергетичного сектору присвячено значну кількість наукових робіт, зокрема [1, 2]. Разом з тим, питання кібербезпеки сучасних електроенергетичних об'єктів з використанням інтелектуальних мереж Smart Grid, оснащених цифровими системами моніторингу, управління, релейного захисту та протиаварійної автоматики стають дуже актуальними, через новизну і недостатнє дослідження проблеми. Необхідно провести аналіз стандартів, які стосуються питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid.

Вирішення задачі

На традиційних підприємствах порушення кібербезпеки в більшості випадків призводить до фінансових втрат, тоді як інші, більш серйозні наслідки є досить рідкими, на відміну від інтелектуальних мереж Smart Grid. Забезпечення кібербезпеки інтелектуальних мереж Smart Grid вимагає нових, багатопрофільних підходів, що поєднують різні технології та включають управлінські, політичні, правові аспекти тощо.

Комунікаційні протоколи є однією з найважливіших частин операцій енергосистеми, яка відповідає як за отримання інформації з польового обладнання, так і навпаки, для надсилання команд управління. Незважаючи на свою ключову функцію, до цих протоколів зв'язку рідко застосовуються будь-які заходи безпеки, включаючи захист від ненавмисних помилок,

 © С.Ф. Гончар, А.В. Ониськова

несправності обладнання енергосистеми, відмови обладнання зв'язку або навмисні диверсії. Оскільки ці протоколи були дуже спеціалізованими, “Security by Obscurity” є основним підходом по забезпеченню їх кібербезпеки. Адже керувати вимикачами із захищеного центру управління дозволено лише операторам.

Електроенергетична галузь є критичною інфраструктурою для всіх країн і тому привабливою мішенню для кібератак. Останнім часом кількість загроз кібербезпеки значно зросло. Окрім проблем національної безпеки, все більш поширеними є загрози промислового шпигунства. І бажання порушити роботу енергосистеми може породжуватися від простої підліткової бравади до конкурентної гри на електричному ринку до незадоволеного працівника, який прагне по тій чи іншій причині завдати шкоди компанії. Вирішальне значення для кібербезпеки мають не лише кіберзагрози. З роками зростає складність роботи енергосистеми, зробивши ймовірнішими відмови обладнання та експлуатаційні помилки, а їхній вплив збільшився за обсягом та вартістю. Стихійні лиха додають потребу не просто запобігати проблемам, але й розробляти плани подолання та заходи щодо відновлення. Позитивним моментом у цій ситуації є те, що ці самі плани подолання та відновлення можуть бути використані при відновленні роботи систем після кібератак.

Забезпечення кібербезпеки інтелектуальної мережі є необхідним для надійної роботи цієї нової форми електромережі. На думку експертів, у першу чергу слід застосовувати стандартизовані рішення та практику. В останні роки було опубліковано багато нових стандартів, пов’язаних із інтелектуальними мережами Smart Grid, що, призводить до певних труднощів у систематизації відповідної інформації.

Зв'язок між вимогами у стандартах які регламентують питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid приведено на рис. 1 [3].

Розглянемо більш детально деякі стандарти, які регламентують питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid [3].

– NISTIR 7628 [4]. Цей документ являє собою аналітичну базу, яку організації можуть використовувати для розробки ефективних стратегій кібербезпеки Smart Grid з урахуванням їх конкретних особливостей, ризиків та уразливостей. Такими організаціями можуть бути, наприклад, від комунальних служб, постачальників послуг з енергоменеджменту до виробників електромобілів та зарядних станцій. Даний документ представляє методи для оцінки ризику, а також визначення та застосування відповідних вимог безпеки. Вимоги кібербезпеки кожної організації повинні адаптивно розвиватися у відповідності до прогресу технологій, оскільки кіберзагрози інтелектуальних мереж неминуче збільшуються та урізноманітнюються.

У документі приводиться стратегія, архітектура та вимоги високого рівня Smart Grid, стратегія кібербезпеки включає довідкову інформацію про Smart Grid та важливість кібербезпеки для забезпечення надійності мережі та конфіденційності конкретної інформації. Обговорюється стратегія

кібербезпеки для Smart Grid та конкретні завдання в рамках цієї стратегії. Розглядається логічна архітектура, яка включає діаграму високого рівня і зображує складений вигляд високого рівня дійових осіб у кожному з доменів Smart Grid, а також включає загальну логічну опорну модель Smart Grid, включаючи всі основні домени, індивідуальні схеми для кожної з 22 категорій логічного інтерфейсу. Ця архітектура зосереджена на короткостроковому перегляді (1 – 3 роки) Smart Grid.

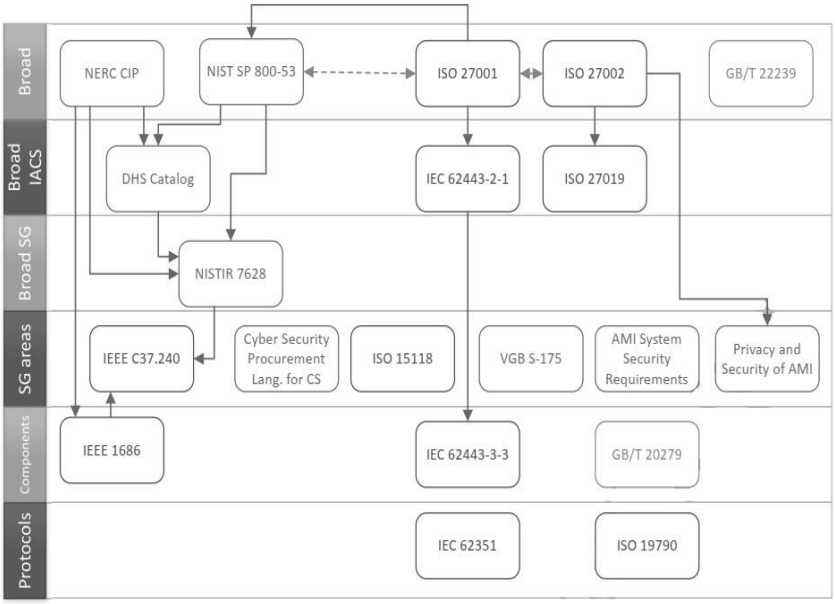

Рис. 1. Зв'язок між вимогами у стандартах

– ISO/IEC 27019 [5]. Область застосування ISO / IEC 27019 охоплює системи управління технологічними процесами, що використовуються енергетичною промисловістю для контролю та моніторингу генерації, передачі, зберігання та розподілу електроенергії, газу та тепла у поєднанні з керуванням допоміжними процесами. Зокрема, це включає такі системи, програми та компоненти:

– загальна технологія централізованого та розподіленого управління процесами, моніторингу та автоматизації, що підтримується IT, а також IT-системи, що використовуються для їх роботи, такі як пристрої програмування та параметризації;

– цифрові контролери та компоненти автоматизації, такі як пристрої управління та польові пристрої або ПЛК, включаючи цифрові датчики та елементи приводу;

– всі додаткові підтримуючі IT-системи, що використовуються в домені управління процесами, наприклад для додаткових завдань візуалізації даних та для контролю, моніторингу, архівації даних та цілей документації;

– загальну комунікаційну технологію, що використовується в домені управління процесом, наприклад мереж, телеметрії, програм управління та технології дистанційного керування;

– цифрові вимірювальні пристрої, наприклад для вимірювання значень споживання, генерації або викидів енергії;

– цифрові системи захисту та безпеки, наприклад реле захисту;

– розподілені компоненти майбутніх середовищ Smart Grid;

– все програмне забезпечення та додатки, встановлені на вищезгаданих системах.

Поза межами ISO / IEC 27019 залишається обладнання, яке не є цифровим, тобто суто електромеханічні або електронні системи моніторингу та управління процесами. Крім того, системи управління енергетичними процесами в приватних домогосподарствах також перебувають поза сферою стандарту ISO / IEC 27019.

– IEC 62443 [6]. Метою застосування стандартів 62443 серій є підвищення безпеки, доступності, цілісності та конфіденційності компонентів або систем, що використовуються для промислової автоматизації та управління, а також забезпечення критеріїв для придбання та впровадження безпечних систем промислової автоматизації та управління. Відповідність вимогам стандартів 62443 серій призначена для поліпшення електронної безпеки та сприяє виявленню і усуненню вразливостей, зменшуючи ризик порушити конфіденційну інформацію або спричинити вихід з ладу апаратне та програмне забезпечення. Серія стандартів 62443 заснована на встановлених стандартах безпеки систем інформаційних технологій загального призначення (наприклад, серії ISO / IEC 27000), ідентифікуючи та вирішуючи важливі відмінності, наявні в промислових автоматизованих системах управління (АСУ ТП). Багато з цих відмінностей ґрунтуються на реальності того, що ризики кібербезпеки в АСУ ТП можуть мати наслідки для здоров'я, безпеки та навколишнього середовища. Елементи стандарту серії 62443 показані на рис 2, [6].

- IEC 62351 [7]. Сімейство стандартів 62351 регламентує керування енергетичними системами та пов’язаний з ним інформаційний обмін, безпеку даних та комунікацій, зображує архітектуру захищеної системи живлення та стандартизує її протоколи і компоненти.

Висновки

Проведено аналіз стандартів, які стосуються питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid. За результатами проведеного аналізу здійснено систематизацію, представлення та опис основних стандартів, які визначають вимоги до кібербезпеки, що застосовуються до інтелектуальних мереж Smart Grid.

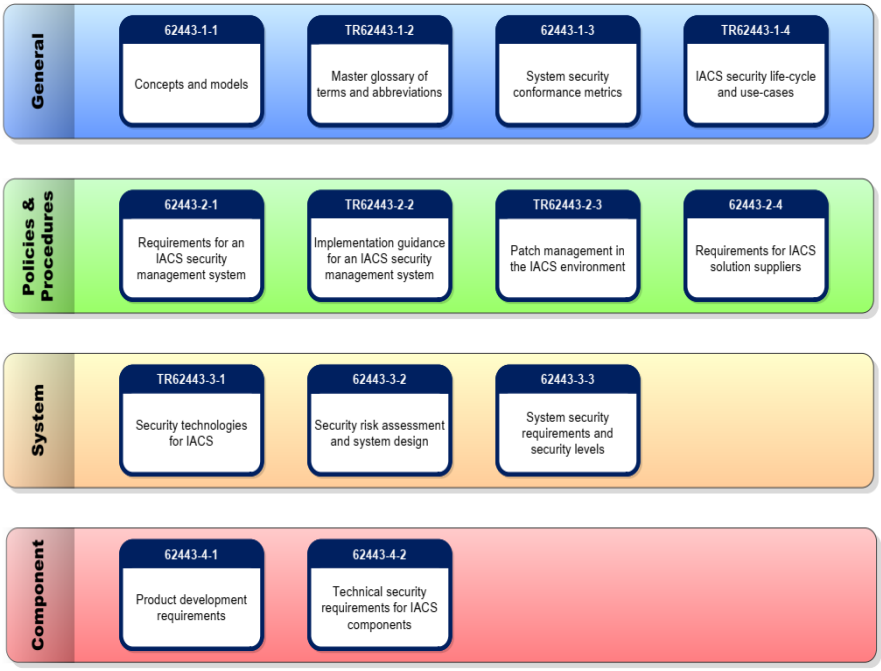

Рис. 2. Елементи стандарту серії 62443

1. *Mokhor V., Gonchar S.* The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers. Electronic modeling, 2018, Vol.40, no. 4, pp.107-111.
2. *Mokhor V., Gonchar S., Dybach O.* Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities. Nuclear and Radiation Safety, 2019, 2(82), pp.4-8.
3. *R. Leszczyna*. A Review of Standards with Cybersecurity Requirements for Smart Grid. // Computers & Security, 2018.
4. *Guidelines for Smart Grid Cyber Security*: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.
5. *ISO/IEC 27019.* Information technology – Security techniques – Information security controls for the energy utility industry.
6. *IEC 62443.* Cyber Security for Industrial Automation and Control Systems (IACS).
7. *IEC 62351.* Power systems management and associated information exchange – Data and communications security

http://doi.org/10.5281/zenodo.3859651

Поступила 26.09.2019р.