УДК 004.056
DOI: 10.31673/2409-7292.2019.033641

В.В. Ткаченко, Ю.М. Щебланін

ОСНОВНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В SMART GRID СИСТЕМАХ НА ОСНОВІ СТАНДАРТІВ ISO/IES 27001 ТА 27005

Наведенні результати огляду основних загроз інформаційної безпеки, які притаманні Smart Grid системам. Надано перелік керівних вимог інформаційної безпеки які необхідно враховувати при проектуванні інтелектуальних мереж.

Ключові слова: інформаційна безпека, інтелектуальні мережі, загрози

Постанова проблеми

Згідно проекту "Енергетична стратегія України на період до 2030 року та подальшу перспективу" реалізація принципу “інтелектуальних мереж” (Smart Grid) є одним з пріоритетів розвитку електроенергетичної галузі. З урахуванням того що на даній час концепція “інтелектуальних мереж” не є остаточно сформованою, визначення загальних вимог до інформаційної безпеки Об’єднаної енергосистеми України (ОЕУ) є пріоритетним завданням по забезпеченню загальної керованості, надійності та безпеки ОЕУ.

Основні матеріали дослідження

Згідно проекту "Енергетична стратегія України на період до 2030 року" [1] пріоритетами розвитку електроенергетичної галузі стануть оптимізація структури генеруючих потужностей з урахуванням особливостей залучення до енергетичного балансу відновлюваної енергетики та розвиток мереж електропостачання, що передбачає зниження ступенів трансформації та наближення високовольтних мереж до споживача, підвищення гнучкості системи шляхом реалізації принципу "інтелектуальних мереж". Однак, не дивлячись на актуальність і популярність, концепція інтелектуальних мереж все ще не має загальноприйнятого визначення.

У світовій енергетичній сфері існують різні трактування поняття «інтелектуальні мережі» (Smart Grid). У загальному понятті «інтелектуальна» мережа – це електрична мережа, що на основі сучасних інноваційних технологій обладнання ефективно координує та управляє дією всіх підключених до неї об'єктів – від різних систем генерації, передачі та розподілу електроенергії до її споживачів з метою створення економічно рентабельної та стабільної енергосистеми з низькими втратами і високим рівнем надійності та якості енергопостачання.

Відповідно до Європейської технологічної платформи Smart Grid – це «електричні мережі, що задовольняють вимогам енергоефективного та економічного функціонування енергосистеми шляхом скоординованого управління за допомогою сучасних двосторонніх комунікацій між елементами електричних мереж, електричних станцій та споживачів електроенергії» [2] .

Інститутом інженерів електротехніки і електроніки США (IEEE) та Міністерством енергетики США визначення Smart Grid сформульовано як концепції повністю інтегрованої, саморегульованої і самовідновної електроенергетичної системи, що має мережеву топологію і включає в себе всі генеруючі джерела, магістральні і розподільчі мережі, а також споживачів електричної енергії, об’єднаних двостороннім потоком енергії та інформації, керованих єдиною мережею автоматизованих пристроїв у режимі реального часу [2].

Із проведеного огляду випливає, що перш за все Smart Grid трактується сьогодні в усьому світі як концепція інноваційного оновлення електроенергетики, що дозволяє за рахунок використання новітніх технологій, інструментів і методів значно підвищити ефективність роботи енергетичних систем.

Державні структури більшості розвинених зарубіжних країн розглядають технології Smart Grid як основу національних програм розвитку електроенергетики, компанії-виробники обладнання на основі нових технологій та енергетичні компанії – як базу для забезпечення стійкої інноваційної модернізації та розвитку енергетичної інфраструктури.

На загальносвітовому рівні концепції Smart Grid поєднують ряд сучасних напрямів і технологій, серед яких:

– системи управління режимами електросистем та енергоспоживанням, у тому числі «інтелектуальні» системи управління при централізованій та розподіленій генерації електроенергії, включаючи альтернативні джерела енергії;

– системи автоматизації розподілу електроенергії для середніх і низьких класів напруг (Distribution automation);

– «розумний» облік – технології «інтелектуальних» систем обліку і розрахунків (Smart metering) та режимного управління навантаженням;

– системи абонентського обліку та білінгу в галузі енергопостачання та комунального обслуговування (Customer Information System);

– системи зарядки електромобілів тощо.

У рамках реалізації концепції Smart Grid мають бути врахованими вимоги усіх зацікавлених сторін – держави, генеруючих, мережевих і енергозбутових компаній, споживачів і виробників обладнання тощо.

В рамках концепції, різноманітні вимоги усіх заінтересованих сторін, можливо виділити ключові групи цінностей нової електроенергетики [3]:

– доступність – забезпечення споживачів енергією згідно необхідних їм параметрам часу, місця та якості;

– надійність – можливість протистояння енергосистеми фізичним і інформаційним негативним впливам без тотальних відключень або високих витрат на відновлювальні роботи, а також її максимально швидке відновлення (самовідновлення);

– економічність – оптимізація тарифів на поставку та зниження загальносистемних витрат на генерацію та розподілення електричної енергії;

– ефективність – максимізація ефективності використання всіх видів ресурсів і технологій при виробництві, передачі, розподілі та споживанні електроенергії;

– органічність з навколишнім середовищем – зниження негативного впливу на навколишнє середовище;

– безпека – недопущення ситуацій в електроенергетиці, потенційно небезпечних для людей і навколишнього середовища.

Принципово важливо розглядати усі вимоги як рівні, їх порядок виконання може бути індивідуальним для кожного суб'єкту співвідношень.

Виконання цих вимог призводить до виникнення нових особливостей системи: самовідновлення, мотивація активності споживача, супротив негативним впливам, забезпечення надійності електропостачання, різноманіття типів електричних станцій, розширення енергетичних ринків, оптимізація керування активами.

З точки зору Міністерства енергетики США, інтелектуальним мережам притаманні такі атрибути [4]:

– здатність до самовідновлення після збоїв в подачі електроенергії;

– можливість активної участі споживачів;

– стійкість до фізичного і кібернетичного втручання зловмисників;

– забезпечення необхідної якості переданої електроенергії;

– забезпечення синхронної роботи джерел генерації та вузлів зберігання електроенергії;

– підвищення ефективності роботи енергосистеми в цілому.

Однією з актуальних проблем в галузі створення інтелектуальних мереж є проблема забезпечення їх інформаційної безпеки. У даній статті пропонується розглянути можливі загрози системи захисту інформації для мережі Smart Grid.

Для розробки системи захисту Smart Grid пропонується проводити оцінку ризиків інформаційної безпеки з урахуванням наступних основних аспектів:

– менеджмент - захист конфіденційної інформації з точки зору управління персоналом, розглядаються загрози, пов'язані з навмисними або випадковими діями співробітників Smart Grid;

– програми та бази даних - захист від загроз, що виникають на рівні додатків і баз даних;

– мережа - захист від загроз, які можуть виникнути в зв'язку з використанням LAN і WAN мереж, в тому числі загроз з мережі Інтернет;

– мобільні пристрої - захист від загроз, пов'язаних з використанням GSM-мереж і мобільних телефонів.

Для аналізу загроз і розробки заходів протидії виявленим загрозам були обрані два базових методи: SREP і CORAS, розроблених відповідно до міжнародного стандарту ISO / IEC 27001 [5].

SREP (Security Requirements Engineering Process) - метод, метою якого є розробка вимог до системи захисту інформації [6]. Реалізація методу включає:

1. Введення основних визначень.
2. Вибір критичних / вразливих джерел інформації.
3. Постановку цілей для системи захисту інформації.
4. Визначення загроз.
5. Визначення ризиків.
6. Розробку вимог до системи захисту.
7. Упорядкування вимог за важливістю.
8. Перевірку відповідності існуючої системи розробленим вимогам.
9. Розробку контрзаходів.

CORAS - метод проведення аналізу інформаційних ризиків [7]. Метод складається з:

1. Підготовки до проведення аналізу.
2. Вибору об'єктів захисту.
3. Опису об'єктів захисту за допомогою діаграм.
4. Постановки цілей.
5.Ідентифікації ризиків за допомогою діаграм загроз.
6. Визначення ризиків по діаграмах загроз.
7. Оцінки ризику з використанням діаграм ризиків.
8. Розробки контрзаходів з використанням діаграм контрзаходів.

Дані методи були обрані як найбільш підходящі для досягнення поставлених цілей. За допомогою CORAS здійснено аналіз ефективності системи захисту з точки зору додатків, баз даних і мережі. За допомогою SREP здійснено аналіз ефективності системи захисту з точки зору менеджменту та мобільних пристроїв.

Оцінка можливого ризику відбувалася відповідно до методології, запропонованої в стандарті ISO / IEC 27005 [8] з урахуванням моделей зрілості системи [9].

В результаті аналізу були виділені три види інформаційних ресурсів, що підлягають захисту:

1. Персональні дані користувачів Smart Grid.
2. Технічна інформація, яка надходить від клієнтів мережі.
3. Інформація про системні збої і помилки, які відбуваються при роботі мережі.

До вимог, які повинна реалізовувати система захисту, були віднесені:

– запобігання неавторизованого розкриття інформації, що захищається (конфіденційність);

– забезпечення постійного доступу користувачів до інформації, що захищається (доступність);

– запобігання несанкціонованої зміни інформації, що захищається (цілісність).

В результаті дослідження були виділені основні загрози інформаційної безпеки Smart Grid, наведені у таблиці 1.

Таблиця 1

Загрози інформаційної безпеки Smart Grid-мереж

№	Загрози
	Менеджмент
1	Неавторизоване розкриття / зміна / позбавлення доступу до персональних даних / технічних даних про відмови в результаті неправильного розподілу прав доступу до Smart Grid систем
2	Неавторизоване розкриття / зміна / позбавлення доступу до персональних даних в результаті збою / не оновлення систем, що функціонують в Smart Grid системах
3	Неавторизована зміна / позбавлення доступу до технічних даних / даних про відмови в результаті збою /не оновлення систем, що функціонують в Smart Grid системах
4	Неавторизоване розкриття персональних даних в результаті недбалого ставлення працівників до своїх обов'язків
5	Неавторизована зміна / позбавлення доступу до персональних даних / технічних даних / даних про відмови в результаті закупівлі або встановлення непотрібних систем безпеки
6	Неавторизоване розкриття / зміна / позбавлення доступу до персональних даних / технічних даних / даних про відмови в результаті безпечності або некомпетентності адміністратора SCADA систем
	Додатки та бази даних
7	SQL-ін'єкції в систему інформування клієнтів, SCADA систему, платіжну систему
8	XSS атаки на систему інформування клієнтів
9	Атаки на неавторизовану аутентифікацію в системі інформування клієнтів
10	Атаки на SSL
11	Backdoor'и, трояни і інші шкідливі програми
12	Підбір пароля методом «грубої сили»
13	DDoS атака на систему інформування клієнтів / SCADA систему
	Мережа
14	Перехоплення пакетів системи інформування клієнтів
15	Сканування портів
16	Підміна IP-адрес системи інформування клієнтів / SCADA системи
17	Крадіжка TCP-пакетів системи інформування клієнтів
18	Атака типу відмова в обслуговуванні системи інформування клієнтів / SCADA системи
19	TCP SYN-атака на систему інформування клієнтів
20	Смурф-атака на систему інформування клієнтів / SCADA систему
	Мобільні пристрої
21	Неавторизоване розкриття / зміна персональних даних / технічних даних / даних про відмови в результаті вилучення інформації з загубленого / вкраденого пристрою
22	Неавторизоване розкриття / зміна персональних даних / технічних даних / даних про відмови в результаті використання списаного / невірно оновленого пристрою
23	Неавторизоване розкриття / зміна персональних даних / технічних даних / даних про відмови в результаті збою / не оновлення мобільного пристрою

Для усунення зазначених загроз пропонується виділити наступні вимоги з безпеки Smart Grid. Перелік основних вимог до системи інформаційної безпеки Smart Grid наведено в таблиці 2.

Таблиця 2

Перелік основних вимог до інформаційної безпеки Smart Grid-мереж

№	Вимоги
	Менеджмент
1	Повинна бути задокументована персональна відповідальність за виконання всіх дій всіма користувачами Smart Grid
2	Повинні бути чітко вказані ролі користувачів Smart Grid
3	Повинні бути вказані алгоритми автоматичного присвоєння ролей для нових користувачів Smart Grid
4	Повинні бути вказані дії, дозволені для кожної ролі
5	Повинно бути зазначено, що дозволяється / забороняється робити за замовчуванням для всіх користувачів Smart Grid
6	Повинні бути вказані процедури при припиненні терміну дії ролі
7	Повинно бути забезпечено ефективне інвестування в системи безпеки Smart Grid
8	Процес пошуку і оцінки загроз повинен проводитися регулярно
	Додатки та бази даних
9	Дані, які використовуються в SQL-запитах до системи інформування клієнтів / SCADA / платіжної системи, повинні ретельно перевірятися
10	Дані, які вводяться на сайті системи інформування клієнтів повинні ретельно перевірятися
11	В системі інформування клієнтів повинні використовуватися протестовані методи автентифікації, засновані на власному способі автентифікації клієнтів
12	Все мандати доступу до системи інформування клієнтів повинні зберігатися в хешованому вигляді
13	Повинна використовуватися ефективна система захисту Smart Grid від шкідливого програмного забезпечення
14	Повинна бути забезпечена доступність системи інформування клієнтів і SCADA систем
	Мережа
15	Зміст переданих пакетів має захищатися і верифікуватися
16	Повинні бути розроблені мандатні управлінські функції для системи інформування клієнтів / SCADA системи
17	Повинно використовуватися тільки перевірене і ефективне програмне забезпечення
18	Повинні застосовуватися методи автентифікації при доступі до DNS-серверу
19	Повинно використовуватися захищене TCP з'єднання
	Мобільні пристрої
20	Повинно бути забезпечено безпечне видалення важливої (чутливої) інформації
21	Повинні бути розроблені дії, які необхідно застосовувати в разі списання пристрою
22	Повинна бути розроблена система захисту інформації від несанкціонованого розкриття та модифікації важливої (чутливої) інформації
23	Програмне забезпечення повинно своєчасно оновлюватися

Висновки

Smart Grid є новий перспективний клас енергомереж. У наші дні відбувається перетворення існуючих енергомереж відповідно до тих вимог, які виникають при модернізації цих мереж в мережі класу Smart Grid. В даний час не існує формалізованої методології розробки систем захисту інформації для подібних інтелектуальних мереж. У

даній роботі здійснено аналіз захищеності мереж Smart Grid, наведено типові загрози і вразливості, яким схильна основна частина мережі Smart Grid та основні вимоги до системи інформаційної безпеки Smart Grid систем.

Перелік посилань

1. Енергетична стратегія України на період до 2030 року [Електронний ресурс] // – Режим доступу: http://www.niss.gov.ua/public/File/2014_nauk_an_rozrobku/ Energy%20Strategy%202035.pdf (02.10.2019).

2. Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці [Електронний ресурс] // – Режим доступу: https://ua.energy/wp-content/uploads/2018/01/2.-SMART-GRID.pdf (02.10.2019).

3. European Smar tGrids Technology Platform [Електронний ресурс] // – Режим доступу: http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf (9.10.2019).

4. Estimating the Costs and Benefits of the Smart Grid [Електронний ресурс] // – Режим доступу: http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf (16.10.2019).

5. ISO / IEC 27001: 2013 [Електронний ресурс] // – Режим доступу: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr (18.10.2019).

6. List of Known Meshlocals [Електронний ресурс] // – Режим доступу: https://docs.meshwith.me/meshlocals/existing/ (14.10.2019).

7. Shifttstas. Hyperboria [Електронний ресурс] // – Режим доступу: https://habr.com/post/181862/ (14.10.2019).

8. ISO / IEC 27005 : 2018 [Електронний ресурс] // – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en (18.10.2019).

9. Щебланін Ю.М. Аналіз використання моделей зрілості процесів в ході оцінювання рівня інформаційної безпеки / Ю.М. Щебланін, А.Б. Гребенніков // Сучасний захист інформації. - №1(33), 2018.- с.33-37.

Надійшла: 15.08.2019 Рецензент: д.т.н., доцент Легомінова С.В.