УДК 519.711

В.В. Ткаченко, Київ

# ОЦІНКА КІБЕРБЕЗПЕКИ SMART GRID СИСТЕМ

**Abstract.** The results of the review of the basic standards for information security assessment that are inherent in Smart Grid systems. The analysis of the possibility of applying information security requirements for assessing the cybersecurity of Smart Grid systems is given.

**Актуальність**

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 [1]. 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.

На загальносвітовому рівні концепції Smart Grid поєднують ряд сучасних напрямів і технологій, серед яких [2]:

– 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.

Однією з актуальних проблем в галузі створення «інтелектуальних мереж» є проблема забезпечення їх інформаційної безпеки.

**Постановка задачі**

У даній статті пропонується розглянути стандарти з інформаційної безпеки та визначити які з них можуть бути застосовані до оцінки кібербезпеки «інтелектуальної мережі».

**Вирішення задачі**

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 [4].

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». На рис. 1 наведена загальна сучасна конфігурація Smart Grid системи [2].

З точки зору споживачів, «інтелектуальні мережі» надають можливість активно контролювати енергоспоживання, користуючись гнучкими планами енергоресурсів і навіть стаючи дрібними постачальниками електроенергії. Що стосується постачальників енергоносіїв, то це дає змогу встановити ціни, що базуються на часі, покращити планування потужностей та використання енергії та більш гнучко пристосовуватися до потреб ринку. Мережа покращує управління передачею енергії та підвищує стійкість до відмов системи управління.

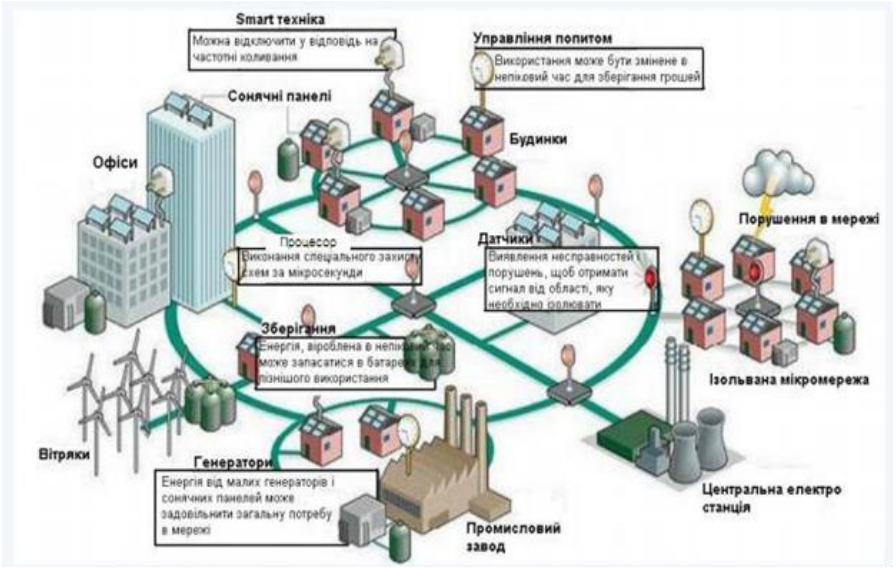


Рис. 1. Сучасна конфігурація Smart Grid системи.

Водночас інтенсивне використання інформаційно-комунікаційних технологій викликає багато нових проблем. «Інтелектуальні мережі» – це сукупність різних застарілих систем, оточених новими технологіями та архітектурними підходами, що відповідають різним стандартам і нормам, які всі повинні поєднувати в одну мережу зв'язку. Системи зв'язку «інтелектуальної мережі» мають багато вразливих місць, що відрізняються між мережами.

Взаємозв’язок «інтелектуальної мережі» з Інтернетом наражає мережу на нові типи ризиків, включаючи розширені постійні загрози (APT), розподілене-заборонене обслуговування (DDoS), ботнети та нульові дні, Stuxnet, Duqu, Red October або Black Energy – це лише кілька прикладів сучасних загроз, які з’явилися з 2010 року [4].

Впровадження «інтелектуальних мереж» вимагає мультидисциплінарного підходу, який поєднує різні технології та включає в себе управлінські, політичні, юридичні аспекти тощо. Вирішальну частину цього процесу формує оцінка безпеки, тобто оцінка рівня безпеки та виявлення потенційних вразливих місць, якими можуть скористатися зловмисники.

У літературі можна знайти кілька визначень оцінки безпеки. У цьому розділі представлені визначення з аналізованих стандартів. Визначення цих тез найбільш визнані серед експертів інформаційної безпеки.

IEC TS 62351-1 визначає оцінку безпеки як «круговий процес оцінки

активів для вимог безпеки, заснованих на ймовірних ризиках нападу, відповідальності за успішні атаки, і витрат на поліпшення ризиків і зобов'язань. [5].

NIST SP 800-53 прирівнюється до оцінки безпеки з оцінкою контролю безпеки та визначає це як «Тестування та / або оцінка управління, експлуатаційного, та технічний контроль безпеки в інформації система для визначення ступеня управління ними реалізовано правильно, функціонуючи за призначенням та виробляючи бажаний результат щодо забезпечення безпеки вимоги до системи» [6].

За даними Міністерства внутрішньої безпеки США (DHS), оцінки безпеки ґрунтуються на аналізі безпеки елементів управління в системі, «визначають елементи керування, виконані правильно, функціонуючи за призначенням, і досягнення бажаного результату щодо зустрічі вимоги безпеки для системи» [7].

NIST SP 800-115 визначає оцінку інформаційної безпеки як «процес визначення ефективності конкретної цілі безпеки, яку оцінюють (наприклад, хост, система, мережа, процедура, особа, відома як об'єкт оцінки)». Стандарт розрізняє три типи методів оцінювання, які можна використовувати для їх виконання це [8]:

– тестування – аналіз об'єктів оцінювання під визначеними умовами для порівняння реальної та очікуваної поведінки,

– експертиза – перевірка, огляд, спостереження, вивчення або аналіз об'єктів оцінювання з метою уточнити, зрозуміти або зібрати необхідні докази,

– інтерв'ю – обговорення з окремими особами чи групами в межах організації, щоб уточнити, зрозуміти чи визначити місце доказів.

Визначення дуже схожі. Їх спільний знаменник – розуміння оцінки безпеки як процес, заснований на аналізі активів з метою визначення якщо вони відповідають вимогам безпеки (або цілям безпеки). NIST SP 800-115 розширює визначення із включенням до нього методів оцінки безпеки.

Підсумовуючи, оцінка безпеки – це процес визначення наскільки ефективно відповідає організація, що оцінюється, конкретним цілям безпеки або вимогам безпеки. Це можна зробити за допомогою трьох типів методів: тестування, іспит та інтерв'ю.

Методи оцінки безпеки можна класифікувати на наступні групи:

− *Відгуки* – пасивні, зазвичай ручні, експертизи, що виконуються з метою виявлення вразливості безпеки. Вони включають огляд документації, журналу, правил та конфігурацій, перевірку відповідності, формальний аналіз, «обнюхування» мережі та перевірку цілісності файлів;

− Ідентифікація вразливості – ручний або автоматизований (як правило) пошук недоліків системи. Методи ідентифікації включають виявлення мережі, сканування портів, сканування вразливості, бездротове сканування та перевірку безпеки додатків;

− *Аналіз вразливості* – ручне або автоматизоване дослідження виявлених вразливостей для остаточного підтвердження їх існування та розробки подальших наслідків їх експлуатації. Методи включають в себе зламання паролів, проникнення, соціальну інженерію та тестування безпеки додатків;

− *Перевірка відповідності* визначає, чи відповідають системи цілям безпеки чи задовольняють вимогам безпеки. Мережеве нюхання – це інструмент, пасивний моніторинг мережевої комунікації та перевірка її вмісту для перевірки того, чи є вона достатньо захищеною. Перевірка цілісності файлу виявляє модифікації файлів на основі обчислення контрольних сум.

− *Формальний аналіз* використовує формальну логіку, дискретну математику та інші математично обґрунтовані методи для оцінки безпеки інформаційних систем. Оцінка вимагає підготовки формальних специфікацій аналізованих систем, які згодом можуть бути перевірені, подібно до перевірки математичних формул. Формальні методи часто оснащені логічним обчисленням, яке може систематично перевірятися автоматизованим інструментом;

− *Відкриття мережі* – це розпізнавання мережевої структури, яке зазвичай виконується за межами її межі. Сканування портів дозволяє ідентифікувати відкриті порти зв'язку, які найчастіше є першою мішенню зловмисників. *Сканування вразливості* шукає (зазвичай відомі) вразливості програмного забезпечення. Це допомагає помітити застарілі версії програмного забезпечення, відсутні патчі або неправильну конфігурацію. Бездротове сканування вивчає, чи можна отримати доступ до бездротових мереж чи комунікацій стороннім користувачем;

− *Злом паролів* спрямований на виявлення паролів на основі наявних даних з метою виявлення слабких паролів та політик щодо паролів. *Тестування на проникнення*, «злучення з червоним колективом» або «злом білого капелюха» чи інші так звані процедури «етичного злому», використовують підходи хакерів для аналізу вразливості системи. *Соціальна інженерія* покладається на те, щоб впливати на людей, щоб вони діяли, що призвело б до викриття системи зловмисникам, перевірки процедур безпеки та поведінки користувачів системи (обізнаність користувачів).

− *Експертиза безпеки тестування та тестування* підтверджує, якщо програмні продукти містять уразливості, працюють надійно, безпечно взаємодіють з користувачами, іншими програмами та середовищем його виконання.

Процес оцінки безпеки «інтелектуальної мережі», визначений у NIST SP 800-115 зображений на рис. 2 може застосовуватися для оцінки кібербезпеки Smart Grid систем.

**Висновки**

Аналіз показує, що стандарти для оцінки кібербезпеки поки що не визначені. Стандарти інформаційної безпеки для «інтелектуальної мережі» вирішують цю проблему різною мірою та різними способами, але дають

досить загальні вказівки без технічних характеристик. Вони можуть бути використані як орієнтир для заходів вищого рівня, таких як визначення політики оцінювання безпеки, присвоєння обов'язків або планування дій з оцінки безпеки.

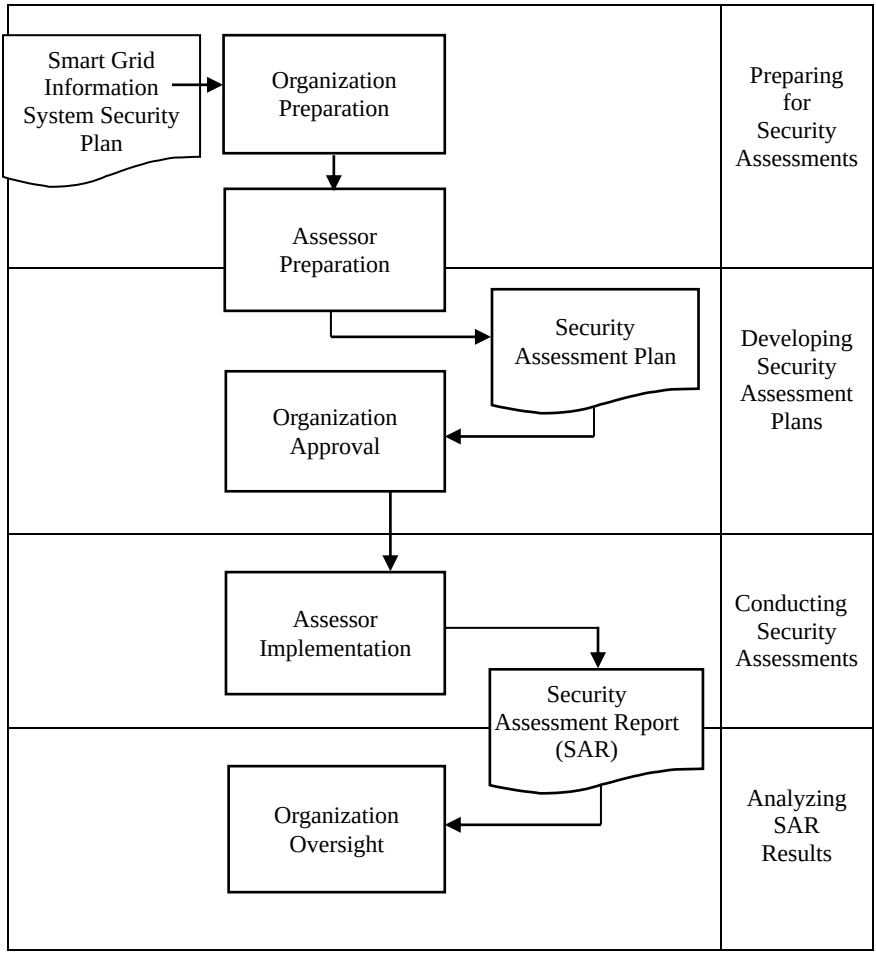


Рис. 2. Процес оцінки безпеки Smart Grid систем [8]

Ці стандарти можуть бути застосовані до корпоративного рівня «інтелектуальної мережі», а також до всіх її компонентів, які використовують комунікаційні технології та обробляють інформацію. Серед них NIST SP 800-115 виділяється як найповніше джерело настанов щодо оцінки безпеки. Він

визначає трирівневу методологію оцінювання безпеки, описує декілька методів оцінювання та надає посилання на подальшу літературу та підходи. Цей документ може стати основою для оцінки кібербезпеки в інформаційних системах «інтелектуальної мережі» та її компонентів.

1. Енергетична стратегія України на період до 2030 року [Електронний ресурс] – http://www.niss.gov.ua/public/File/2014_nauk_an_rozrobku/ Energy%20Strategy%202035.pdf.
2. Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці [Електронний ресурс] – https://ua.energy/wp-content/uploads/2018/01/2.-SMART-GRID.pdf.
3. European Smar tGrids Technology Platform [Електронний ресурс] – http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf.
4. Estimating the Costs and Benefits of the Smart Grid [Електронний ресурс] – http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf.
5. IEC / TS 62351-1: Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security Introduction to security issues.
6. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations.
7. DHS (2009). Catalog of Control Systems Security: Recommendations for Standards Developers. Technical report.
8. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.

**http://doi.org/10.5281/zenodo.3860750**

*Поступила 30.09.2019р.*

УДК 519.7-004.65

М.Ю. Комаров, Київ

## КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЇ, ЯКА ЦИРКУЛЮЄ В АВТОМАТИЗОВАНИХ ТА АВТОМАТИЧНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Abstract.** Threats, automatic systems, Sniffing, Hijacking, Denial-of-Service, DoS, Man-in-the-Middle.

**Актуальність**

На сьогоднішній день відомий достатньо широкий перелік загроз інформаційної безпеки, який містить сотні позицій. Перелік загроз, оцінки імовірності їх реалізації, а також модель порушника є основою для аналізу