1. Европейская комиссия Генерального директората по энергетике. Директорат B. Техническое задание Европейским организациям по стандартизации (EOC) на разработку стандартов для обеспечения внедрения европейской интеллектуальной электросети. M/49 EN. – c.10. -2011. – Режим доступу: http://www.smartgrid.ru/smartgrid/analytics/2012/analytics56/centercolumn/permanent/SmartgridArticleBrief/SmartgridArticleInnerCollection/0/0/text_files/file/tech.pdf .- Дата доступу: грудень 2012. – Назва з екрану.
2. *M. He, S.Murugesan, J.Zhang*. "Multiple Timescale Dispatch and Scheduling for Stochastic Reliability in Smart Grids with Wind Generation Integration". – 2010. - Режим доступу: http://arxiv.org/pdf/1008.3932v2.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
3. *Е.С.Вентцель*. Исследование операций. – М. «Советское радио», 1972, 552 с.
4. *Sommerstad T*. A framework and theory for cyber security assessment./ Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. – Royal Institute of Technology, Stockholm, Sweden. – 2012.- 42 p.

Поступила 25.02.2013р.

УДК 004.056.5

О.Ю. Юдін, м.Київ

АНАЛІЗ МОЖЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ СТВОРЕННІ SMART GRID СИСТЕМ

Abstract. The paper describes the determination of concept of the Smart Grid and the analysis of mechanisms of protection of the information which must be used in the Smart Grid.

Вступ

Останнім часом в інформаційному просторі України все частіше з'являються відомості щодо доцільності побудови Smart Grid системи. Актуальність створення такої системи викликана зростаючою необхідністю забезпечення енергетичної безпеки, тобто спроможністю держави забезпечити максимально надійне, технічно безпечне, екологічно прийнятне та обґрунтовано достатнє енергозабезпечення економіки й населення, а також гарантоване забезпечення можливості керівництва держави у формуванні і здійснені політики захисту національних інтересів у сфері енергетики без надмірного зовнішнього та внутрішнього тиску в сучасних та прогнозованих умовах [1]. Проте в середовищі фахівців досі не сформована єдина думка в визначенні самого поняття Smart Grid. Враховуючи той факт, що це поняття виникло на теренах США пропонується в статті використовувати цей термін в значенні яке використовується в U.S. Department of Energy, а саме: Smart Grid

це електрична мережа яка використовує інформаційні та комунікаційні технології, а також інформацію про поведінку постачальників та споживачів, з метою автоматизації процесу покращення продуктивності, надійності, економічності і стійкості виробництва та розповсюдження електричної енергії. Виходячи з цього визначення можливо припустити що Smart Grid це складна детермінована відкрита система.

Відповідно до прийнятої в Україні термінології [2, 3], будемо розглядати Smart Grid систему як сукупність підсистеми передачі електричної енергії та інформаційно-телекомунікаційної підсистеми.

Пошук проблемних питань

З метою пошуку проблемних питань в сфері захисту інформації, які можуть виникнути при створенні Smart Grid системи необхідно визначити її головні відмінності від існуючих електроенергетичних систем. Основні відмінності [4, 5], можливо викласти у вигляді таблиці 1.

Таблиця 1

Відмінності електроенергетичних систем від Smart Grid систем

Існуючи електроенергетичні системи	Smart Grid системи
Однонаправлений канал передачі даних або його відсутність	Двонаправлений канал передачі даних
Централізований видобуток енергії	Розподілений видобуток енергії
Реагування на наслідки аварії	Реагування з метою недопущення аварії
Ручне відновлення	Автоматичне відновлення
Схильність системним аваріям	Недопущення розвитку системних аварій
Перевірка обладнання за місцем функціонування	Віддалений моніторинг обладнання

Також, слід зауважити, що для забезпечення інформаційного обміну в Smart Grid системі передбачено використання цифрових комунікаційних мереж та інтерфейсів обміну даними, а однією з найважливіших цілей є забезпечення безперебійного керованого балансу між попитом та пропозицією електроенергії. Для цього елементи системи повинні постійно здійснювати між собою обмін інформацією про параметри електроенергії, режими споживання та видобутку, кількості енергії яка запланована до споживання і вже спожита [6]. Обмін інформацією повинний здійснюватись в режимі реального часу по всьому ланцюгу – від компанії які виробляють електроенергію до пристроїв що її споживають.

Аналізуючи наведені відмінності та особливості можливо зробити висновок, що в Smart Grid системі висуваються підвищені вимоги до стійкості від відмов, часу реагування на події, оперативності збору інформації щодо стану системи та її керованості. Виходячи з цього доцільно припустити що дієвим механізмом реалізації частини зазначених вимог є забезпечення таких властивостей як цілісність та достовірність інформації яка циркулює в системі.

Крім того необхідно зазначити, що Smart Grid система, як і сучасні

електроенергетичні системи України [7], може складатись з обладнання (підсистем) яке відрізняється за формою власності (приватна, комунальна і державна), а інформація яка обробляється в системі може бути відкритою або з обмеженим доступом [8], що в свою чергу теж накладає відбиток на засоби захисту інформації які доцільно застосовувати. Цей фактор впливає на вибір та можливість використання засобів що забезпечують конфіденційність інформації (засоби криптографічного захисту секретної, службової або конфіденційної інформації).

Враховуючи зазначене вище та з урахуванням вимог [2] щодо необхідності забезпечення операційної безпеки функціонування об'єднаної енергетичної системи і зважаючи на інші вимоги [9, 10] стосовно захисту інформації спробуємо проаналізувати механізми захисту інформації які необхідно застосовувати в Smart Grid системі. За базові документи для аналізу приймемо нормативні документи які описують механізми захисту інформації в Smart Grid системах, або за відсутності таких, документи щодо захисту інформації в інформаційно-телекомунікаційних системах [11, 12, 13, 14]. Аналіз будемо здійснювати за такими властивостями як цілісність, достовірність, доступність та конфіденційність.

Забезпечення цілісності (integrity) та достовірності (reliability)

Одним із самих ефективних механізмів забезпечення цілісності є обчислення імітовставки, яка є функцією від повідомлення x, M=f(x). За допомогою імітовставки можливо підтвердити цілісність та достовірність інформації.

В таблиці 2 наведемо приклади алгоритмів що реалізують імітовставку та застосовуються в Україні, США та Росії.

Таблиця 2

Порівняльна таблиця алгоритмів обчислення імітовставки

Україна	США	Росія
ДСТУ ГОСТ 34.311-95 ГОСТ 28147-89 в режимі вироблення імітовставки	Secure Hash Algorithm (SHA) SHA-256, SHA-384, and SHA-512	ГОСТ Р 34.11-94

Механізмом забезпечення достовірності та цілісності є електронний цифровий підпис.

В таблиці 3 наведений перелік національних алгоритмів України, США та Росії які реалізують електронний цифровий підпис.

Таблиця 3

Порівняльна таблиця алгоритмів електронного цифрового підпису

Україна	США	Росія
ДСТУ ГОСТ 34.310-95	Digital Signature Algorithm (DSA) RSA digital signature algorithm (RSA) Elliptic Curve Digital	
ДСТУ 4145-2002	Signature Algorithm (ECDSA)	ГОСТ Р 34.10-2001

Забезпечення доступності (availability)

Забезпечення доступності досягається вирішенням організаційно-технічних питань, таких як:

- створення систем безперебійного електроживлення;
- здійснення резервування та дублювання каналів зв'язку;
- здійснення резервування потужностей;
- розробка планів забезпечення безперервності процесів функціонування, та інших.

Хоча в Україні, США та Росії існують свої власні нормативно-правові акти щодо забезпечення захисту об'єктів інформаційної діяльності та інформації, яка в них циркулює, проте механізми захисту майже однакові. Єдиною суттєвою різницею в підходах до захисту інформації організаційно-технічними шляхами є методологія прийняття рішення. Ця різниця полягає в тому, що в США для прийняття рішення використовується модель визначення ризику як співвідношення ймовірності реалізації загрози до можливих фінансових втрат (система оцінки ризиків), а в Україні та Росії всі питання щодо захисту інформації з обмеженим доступом регулюються адміністративно, не зважаючи на те, яким є згадане вище співвідношення.

Забезпечення конфіденційності (confidentiality)

В таблиці 4 надані приклади алгоритмів які реалізують механізм конфіденційності інформації і застосовуються в Україні, США та Росії.

Таблиця 4

Порівняльна таблиця алгоритмів симетричного шифрування

Україна	США	Росія
ГОСТ 28147-89 (інші алгоритми визначені державою для захисту інформації з обмеженим доступом)	Advanced Encryption Standard (AES) AES-128, AES-192, AES-256	ГОСТ 28147-89 (інші алгоритми визначені державою для захисту інформації з обмеженим доступом)

За результатами аналізу даних наведених в таблицях 2-4 можна зробити висновок що алгоритми криптографічного захисту, які застосовуються в зазначених країнах відрізняються, що в свою чергу унеможливлює їх використання в одній системі.

Висновки

З урахуванням наведеного та спираючись на той факт, що сьогодні електроенергетичні системи України, Російської Федерації, Республіки Молдова, Республіки Білорусь, Польщі, Словаччини, Угорщини, Румунії дуже тісно пов'язані та працюють разом з електроенергетичними системами інших країн Східної Європи: Болгарії, Чехії, східній частині Німеччини [9] можливо виділити наступні актуальні проблеми стосовно захисту інформації в Smart Grid системі:

1. Неможливість підтвердження цілісності та достовірності на міждержавному рівні. Причиною є використання різних криптографічних алгоритмів що визначені як обов'язкові до застосування.

2. Відсутність єдиних підходів до створення системи прийняття рішень. В країнах ЄС та США використовуються системи аналізу ризиків, а в Україні та Росії застосовується підхід безумовного виконання директив.

Визначені проблеми можливо подолати шляхом вирішення завдання щодо:

- захисту на міждержавному рівні інформаційних ресурсів (механізми електронного цифрового підпису, шифрування);

- пошуку та знаходження єдиного підходу до визначення оцінки ризиків в різних системах, та як наслідок створення систем прийняття рішень які працювали за єдиними правилами.

Таким чином вирішення зазначених питань дозволить забезпечити інтероперабельність електроенергетичних систем на базі яких буде побудована Smart Grid система.

1. Енергетична безпека України: стратегія та механізми забезпечення / [Шевцов А. І., Земляний М. Г., Бараннік В. О. та ін.] / За ред. А. І. Шевцова. - Дніпропетровськ: Пороги, 2002. – 264 с.
2. Україна. Закони. Про електроенергетику : офіц. текст : [прийнятий Верховною Радою 16 жовтня 1997 р.]. - К.: Відомості Верховної Ради України, 1998, № 1.
3. Україна. Закони. Про захист інформації в інформаційно-телекомунікаційних системах : офіц. текст : [прийнятий Верховною Радою 5 липня 1994 р.]. - К.: Відомості Верховної Ради України, 1994, №31.
4. The path of the smart grid / *H. Farhangi*. // IEEE Power and Energy Magazine, - 2010. - Vol. 8, № 1. – P. 18-28.
5. A vision for the Modern Grid [Електронний ресурс] / The National Energy Technology Laboratory. - 2007. Режим доступу: http://www.bpa.gov/energy/n/smart_grid/docs/Vision_for_theModernGrid_Final.pdf. - Назва з екрану.
6. *Кобец Б. Б.* Инновационное развитие электроэнергетики на базе концепции Smart Grid / Б. Кобец, И. Волкова. - М.: ИАЦ Энергия, 2010. – 207 с.
7. Електроенергетика України: стан і тенденції розвитку // Національна безпека і оборона. – 2012. № 6 (135). – С. 2-42
8. Україна. Закони. Про інформацію : офіц. текст : [прийнятий Верховною Радою 2 жовтня 1992 р.]. - К.: Відомості Верховної Ради України, 1992, №48.
9. Україна. Розпорядження Кабінету Міністрів України. Про схвалення Енергетичної стратегії України на період до 2030 року : офіц. текст : [схвалена розпорядженням Кабінету Міністрів України від 15 березня 2006 року].
10. Україна. Постанови Кабінету Міністрів України. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : офіц. текст : [затверджена Кабінетом Міністрів України від 29 березня 2006 року].
11. NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements // National Institute of Standards and Technology. – 2010. – 289 p.
12. НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації в комп'ютерних системах від несанкціонованого доступу : офіц. текст : [затверджений наказом Адміністрації Держспецзв'язку 24 липня 2009 року № 172].

13. Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації : офіц. текст : [затверджений наказом Адміністрації Держспецзв'язку 12 червня 2007 року № 114].
14. Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005) : утв. приказом ФСБ Российской Федерации от 09.02.2005 № 66.

Поступила 18.02.2013р.

УДК 683.03

М.В.Коробчинський

МОДЕЛЮВАННЯ УПРАВЛЯЮЧИХ ПРОЦЕСІВ НА ОСНОВІ ВИКОРИСТАННЯ ЛОГІЧНИХ ЗАСОБІВ

Аннотация. Разрабатываются модели фрагментов управляющих процессов на основе использования средств математической логики. Приводится метод интерпретации значений логических переменных, которые используются в логических моделях. Исследуется точность аппроксимации логическими моделями процессов функционирования распределённой информационной управляющей системы.

Ключевые слова: модель, аппроксимация, логические средства, точность, интерпретация, система.

Оскільки в розподілених системах управління (IUS) мобільними компонентами (MK) розв'язується , в більшості випадків, одна спільна задача, то всі компоненти такої системи повинні бути логічно зв'язаними. Опис таких логічних залежностей реалізується в рамках логічних моделей $\mathcal{L} = \mathcal{F}(L_1, \dots, L_n)$. Доцільність використання логічних моделей для реалізації процесів управління в рамках IUS обумовлюється наступними факторами та причинами:

- в рамках логічних моделей окремих фрагментів задач $L_i \in \mathcal{L}$ розв'язується задача апроксимації подій, що виникають в процесі розв'язування у вигляді певної логічної схеми,
- логічна модель дозволяє на свєму рівні розв'язувати задачі виявлення суперечностей в процесі розв'язку, іще до моменту проявлення такої суперечності при реалізації в середовищі дій, що пов'язані з розв'язком задачі,
- визначення повноти логічних схем і окремої логічної схеми $L_i(x_{i1}, \dots, x_{in})$ дозволяє обгрунтувати можливість досягнення цілі при