УДК 621.31

КУЛЬБОВСЬКИЙ І.І., к.т.н., доцент,
ГОЛУБ Г.М., аспірант (Державний економіко-технологічний університет транспорту)

Аналіз нормативно-технічної бази впровадження інтелектуальних енергетичних систем на основі технологій SMART GRID

Подано аналіз вимог і норм, що встановлюються нормативними документами, які забезпечують надійність, контроль, діагностику, визначення параметрів та інформаційну безпеку інтелектуальної електроенергетичної системи на основі концепції Smart Grid систем. Розглянуто питання впровадження систем стандартизації, подано ієрархію стандартів інтелектуальних мереж.
Ключові слова: *інформаційна безпека, Smart Grid, міжнародний стандарт, інтелектуальна електрична мережа, кібербезпека, інтелектуалізація.*

Постановка задачі

Розвиток електроенергетики у світі характеризується виникненням цілого ряду факторів, що визначають необхідність кардинальних перетворень в електроенергетиці, серед яких, з одного боку, подальше економічне зростання, що нерозривно пов'язане зі збільшенням обсягу енергоспоживання і підвищенням вимог до якості і рівня надійності енергопостачання, а з іншого — значний негативний вплив електроенергетики на навколишнє середовище та проблеми зі створенням потужного енергетичного обладнання. Вони і призвели до необхідності визначення нової концепції розвитку електроенергетики. Тобто концепція інноваційного перетворення електроенергетики передбачає побудову повністю інтегрованої, саморегульованої та самовідновлюваної системи, що має мережну топологію і включає в себе всі генеруючі джерела, магістральні та розподільні мережі та всі види споживачів електричної енергії, які керуються єдиною мережею автоматизованих пристроїв у реальному часі [1].

Під терміном Smart Grid будемо розуміти інтелектуальну електричну мережу, яка використовує інформаційні та комунікаційні технології, а також інформацію про поведінку постачальників і споживачів з метою автоматизації процесу поліпшення продуктивності, надійності, економічності і стійкості виробництва і розповсюдження електричної енергії. Визначення Smart Grid відображають низку можливостей інтелектуалізації електроенергетики, відповідно до особливостей та завдань розвитку країни, які стоять перед енергетичним комплексом кожної із країни. Необхідно відмітити, що впровадження Smart Grid систем спрямоване на забезпечення енергетичної безпеки України, тобто здатності держави забезпечити максимально надійне, технічно безпечне, екологічне та обґрунтовано достатнє енергозабезпечення економіки та населення [2].

У статті будемо розглядати Smart Grid систему як інтелектуальну електроенергетичну систему залізниць, яка являє собою якісно нову сукупність взаємно - інтегрованих електричних тягових мереж і розподілених комп'ютерних засобів та технологій керування ними, споживачів, генеруючих потужностей та засобів захисту, об'єднаних на основі сучасних принципів єдиного інформаційного простору, саморегулювання, самовідновлення, принципу підтримки єдиної моделі первинних даних, принципу синхронної інформаційної взаємодії [3]. На основі цього здійснюватимемо дослідження існуючих нормативних документів, застосовуваних для забезпечення інформаційної безпеки в проектах інтелектуальної мережі електропостачання на основі сучасної Smart Grid системи.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій показав, що на сьогоднішній день приділяється велика увага розробці технічних та нормативних документів, які описують норми та вимоги для забезпечення інформаційної безпеки Smart Grid систем. Основою нормативно-технічної складової створення інтелектуальної електроенергетичної системи, яка описує та регламентує вимоги, завдання, питання з стандартизації, що ставляться перед системою, є ряд директив та технічних завдань:

- Директива 2004/22/ЄС про вимірювальні прилади (скорочено - Директива M1D);
- Директива 2006/32/ЄС про ефективність кінцевого використання енергії та енергетичні послуги;
- Директива 2004/8/ЄС про просування когенерації на внутрішньому енергетичному ринку;

• Директива про стимулювання використання енергії з відновлюваних джерел (2009/28/ЄС);

• Директиви 2009/72/ЄС і 2009/73/ЄС («Третій енергетичний пакет»);

• Технічне завдання зі стандартизації M/468 від 29 червня 2010 р. щодо питань зарядки електричних транспортних засобів;

• Директива 2002/58/ЄС Європейського парламенту та Ради про обробку персональних даних і захисту конфіденційності у сфері електронних комунікацій;

• Директива про утримання даних (Директива 2006/24/ЄС);

• Директива про правові основи використання електронних підписів;

• Директива 1999/5/ЄС про кінцеве обладнання телекомунікаційних ліній і радіозв'язку; Комюніке COM (2010) 245 про Європейську програму впровадження цифрових технологій (Digital Agenda for Europe) та ін. [4].

Необхідно відзначити, що Європейський комітет стандартів, Європейський комітет зі стандартизації в електротехніці та Європейський інститут стандартів електрозв'язку працюють над нормативною базою, що дозволяє європейським організаціям зі стандартизації безперервно покращувати і удосконалювати стандарти в галузі інтелектуальних електромереж, забезпечуючи взаємну узгодженість і сприяючи безперервній інновації.

Актуальність проведення дослідження зарубіжних нормативних документів, що стосуються інформаційної безпеки, викликана тим, що на сьогодні у світі Smart Grid системи починають створюватися і розвиватися, а в Україні вони нормативно не закріплені і не описані.

Формулювання мети

Метою роботи є аналіз нормативно-технічної бази, в тому числі нормативної та нормативно – технічної документації, які використовуються для забезпечення інформаційної безпеки Smart Grid систем, і будуть основою забезпечення інформаційної безпеки інтелектуальної електроенергетичної системи залізниць України, зокрема компонентів корпоративної комп'ютерної системи моніторингу та діагностики на кожному з рівнів ієрархії, які повинні забезпечуватись відповідними комплексами інформаційного захисту, або системи інформаційної безпеки, що є передумовою подальшого використання інфраструктури системи для комплексного автоматизованого керування режимами енергопостачання.

Виділення не розв'язаної раніше частини загальної проблеми

Залізничний транспорт є одним із найбільших споживачів електроенергії країни, безперебійність і якість постачання якої впливає на експлуатаційні характеристики силового електричного обладнання, наприклад, зменшення строку служби ізоляції електричних машин і трансформаторів, погіршення роботи батарей конденсаторів для компенсації реактивної енергії, збої в роботі систем керування, релейного захисту та автоматики, телемеханіки. Тому однією із стратегічних цілей технічної політики в цьому плані є безперебійне і якісне постачання електроенергії на тягу поїздів, що є основою безпеки руху [5].

Концепція інноваційного перетворення тягових електричних мереж залізниць передбачає створення єдиної інформаційної моделі, яка забезпечує глибоку взаємну інтеграцію електромережної та інформаційної комп'ютерної інфраструктури управління для організації всережимної системи керування з повномасштабним інформаційним забезпеченням, зміни в реальному часі параметрів і топології тягової електричної мережі за поточними режимними умовами, оптимізації планування мережі, регулювання навантаження, безперервного моніторингу, обліку та аналізу виникнення і розвитку техпорушень, розширення ринкових можливостей і, на їх базі, формування культури споживання та стимулювання економічного розвитку [5]. На основі дослідження існуючих нормативних документів, застосовуваних для забезпечення інформаційної безпеки інтелектуальної мережі електропостачання Smart Grid систем і автоматизованих систем управління ними, можна зробити висновок, що інтелектуальні мережі електропостачання на основі сучасної Smart Grid системи тільки починають свій шлях розробки та розвитку в Україні і нормативно не закріплені і не описані, тому досвід Європейського Союзу та США стане основою для опису та закріплення нормативно-технічної документації, яка б орієнтувалася на пробазові механізми захисту електричних підстанцій та інтелектуальних пристроїв, на опис безлічі об'єктів і суб'єктів Smart Grid, їх взаємодії і механізмів захисту, на забезпечення інформаційної безпеки систем. Такий підхід відкриває можливість накопичувати в електроенергетиці нові «знання», що дозволяють різко підвищити ефективність функціонування тягової електричної мережі, забезпечити інформаційну безпеку системи для забезпечення можливості саморегуляції і самовідновлення в реальному часі тягових електричних мереж.

Основний матеріал дослідження

Розвиток системи стандартизації та нормативно-технічного забезпечення в галузі електроенергетики, розробка та гармонізація комплексів стандартів та інших нормативно-технічних документів (НТД), які об'єднують безліч інтелектуальних цифрових обчислювальних і комунікаційних технологій та

електричних архітектур, а також пов'язані з ними встановлені норми і процедури, процеси і послуги, які функціонально та інформаційно повинні бути сумісні і забезпечувати необхідні показники надійності, безпеки і якості, різноманітні інтелектуальні електромережі, достатньо гнучкі для їх інтегрування в майбутні розробки. Необхідно відзначити, що інтелектуальні системи відрізняються від інших самодіагностикою і саморегулюванням і повинні відображати технічні та організаційні потреби в стійкій інформаційно-безпечній інтелектуальній електромережі з урахуванням конфіденційності. Учасники повинні отримати можливість збору, використання, обробки, зберігання, передачі та видалення всієї інформації. Це дозволить надавати послуги інтелектуальних електромереж на базі відповідної інформаційно - комунікаційної системи, яка за своєю природою буде захищеною в інфраструктурі мереж передачі і розподілу електроенергії, а також у під'єднаних пристроях.

Оскільки інвестиції в електрогенеруючі і мережні інфраструктури є сферами довгострокової прибутковості, вони вимагають стабільної нормативної бази. Для досягнення цілей в енергетиці необхідний новий глобальний підхід до виробництва, передачі, розподілу, вимірювання, поставок, накопичення і зберігання, а також споживання електроенергії. Буде потрібно широкомасштабне впровадження систем стандартизації з інтеграції технологій зберігання енергії. Стандарти енергоефективності стануть загальним вектором розвитку, попит – істотним фактором в енергосистемах, зростаюча електрифікація транспорту – одним із стратегічних завдань.

У ході проведення досліджень нормативних документів, що відносяться до забезпечення інформаційної безпеки систем управління, систем диспетчерського управління та збору даних (SCADA), автоматизованих систем управління технологічним процесом (АСУ ТП) і Smart Grid, були виділені наступні документи міжнародних та національних галузевих стандартів та поданий загальних опис даних документів [6]. Спочатку розглянемо міжнародні стандарти:

1. Institute of Electrical and Electronics Engineers (IEEE):

- IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security. Стандарт носить загальний характер і визначає основні підходи до планування, проектування, будівництва та експлуатації електричних підстанцій. Даний стандарт не містить детальних специфікацій щодо забезпечення інформаційної безпеки.

- IEEE 1686. IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities. Стандарт описує специфікації, які необхідно виконати для оцінки захищених інтелектуальних електронних пристроїв (ІЕП). Цей документ дає можливість оцінити функції забезпечення кібербезпеки як уже застосованих ІЕП, так і тих, які планується використовувати.

- IEEE P1711. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links. Документ описує механізм шифрування для асинхронного послідовного каналу зв'язку. Стандарт наказує використовувати криптографічні алгоритми, які затверджені NIST і реалізовані відповідно до федеральних стандартів FIPS PUB 140-2.

2. International Organization for Standardization (ISO) ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002. На сьогодні зазначений стандарт знаходиться в стадії розробки. Основним його призначенням буде деталізація загальних вимог ISO/IEC 27002 для підприємств енергетичної галузі, які експлуатують системи реального часу. Планується використовувати стандарт спільно з ISO/IEC 27002.

3. International Electrotechnical Commission (IEC):

- IEC TR 62210. Power system control and associated communications. Data and communication security. Цей документ є технічним звітом, що робить акцент на механізмах захисту комунікаційних протоколів, які застосовуються в мережах управління електричних систем. Також в документі наведено приклади вразливості систем та можливі шляхи їх блокування. У звіті приділено особливу увагу відсутності механізмів аутентифікації пристроїв.

- IEC 61784-4. Digital data communications for measurement and control – Profiles for secure communications in industrial networks. Стандарт описує можливі загрози та порядок аналізу наслідків їх реалізації, вимоги до систем безпеки зв'язку, порядок здійснення віддаленого доступу за допомогою модему, а також встановлює профілі безпеки керуючого центру, корпоративної мережі, мережі вищого рівня керуючого центру, віддаленого управління за допомогою мережі Інтернет або Інтранет.

- IEC 62443. Security for industrial process measurement and control – Network and system security. Даний стандарт розроблений на базі галузевих стандартів ANSI / ISA 99 і на сьогодні складається з таких частин:

- IEC/TS 62443-1-1. Industrial communication networks - Network and system security - Part 1-1: Terminology;

- IEC/TR 62443-3-1. Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems;

- IEC/PAS 62443-3. Security for industrial process measurement and control - Network and system security.

В цілому, стандарт описує основні поняття і терміни, які пов'язані з безпекою виробництва та системою управління; практичні рекомендації щодо складання планів, спрямованих на забезпечення безпеки; конкретні вимоги до безпеки виробництва та систем управління з урахуванням специфіки промислових мереж; життєвий цикл програмного забезпечення захисту систем управління, а також планування промислового виробництва.

- IEC 62351. Data and Communication Security. Стандарт розглядає питання інформаційної безпеки підсистем управління енергосистемами. Також документ говорить про необхідність модернізації низки стандартів, визначених IEC TC 57, для гарантування безпеки комунікаційних протоколів. Зокрема, мова йде про стандарти, які описують комунікаційні мережі енергосистем, а саме: IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968.

У стандарті вводиться базове поняття «кінцевої безпеки», під яким розуміється захист інформації в усьому тракті передачі, від пункту створення до пункту використання. Документ містить частини, які визначають механізми поліпшення безпеки комунікаційних профілів, присвячені питанням авторизованого доступу та забезпечення безпеки інформації під час її передачі між різними підсистемами.

На даний час можна представити деяку ієрархію стандартів інтелектуальних мереж, яка зображена на рис. 1.

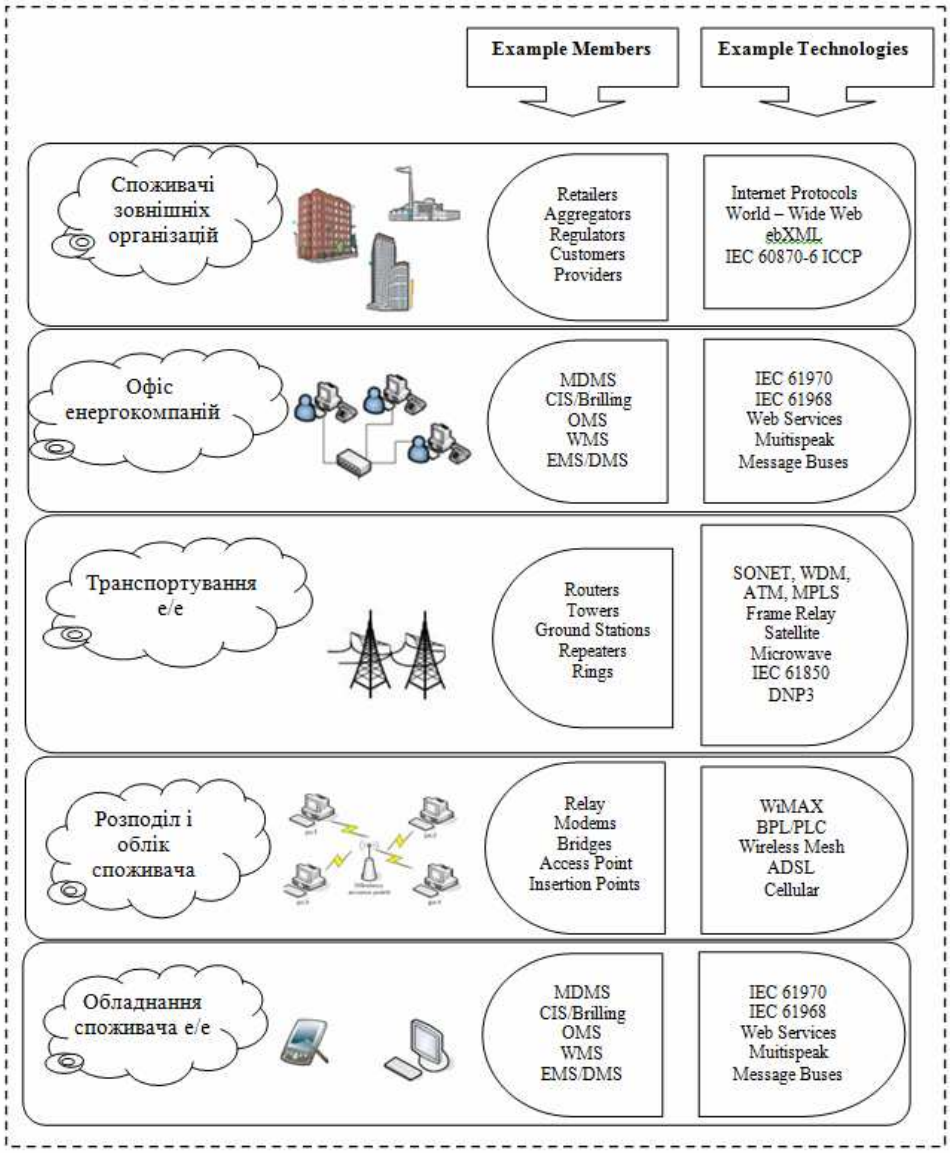

Рис. 1. Ієрархія стандартів інтелектуальних мереж

Розглянемо опис документів національних галузевих стандартів [5].

1. National Institute of Standards and Technology (NIST):

- NIST SP800-82. Guide to Industrial Control Systems (ICS) Security. Стандарт дає рекомендації щодо забезпечення безпеки систем промислового управління (ICS), в тому числі і SCADA, а також розподілених систем управління (DCS). У документі міститься огляд ICS і їх стандартних топологій, визначаються типові загрози та вразливості.

NIST SP800 - 82 складається з декількох розділів, які описують:

- огляд SCADA та інших ICS, а також обґрунтування необхідності забезпечення їх безпеки;
- відмінності між ICS та інформаційно - телекомунікаційними системами;
- загрози, вразливості та інциденти;
- процес розробки та впровадження програмного забезпечення ICS;
- рекомендації щодо інтеграції механізмів забезпечення безпеки в мережних архітектурах ICS;
- висновки з управління, оперативних і технічних засобів контролю, які описані в NISTSP800 - 53, а також вказівки про те, як ці засоби забезпечення безпеки застосовуються в ICS.

- NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations. Документ регламентує забезпечення безпеки систем управління типу SCADA федеральних інформаційних систем і орієнтований на широку аудиторію - від розробника до постачальника послуг. У стандарті дано докладний опис профілів безпеки та механізмів їх забезпечення. Також слід зазначити, що даний документ є одним із серії стандартів, спрямованих на реалізацію управління ризиками.

Стандарт NIST виходить з двох основних принципів побудови системи стандартів, специфікацій і посібників: першочерговість створення стандартів з функціональної сумісності ставить на перше місце взаємозв’язок і взаємозумовленість основних складових інтелектуальної системи; відкритість обговорення проектів стандартів і пропозицій і зауважень до них; орієнтація на застосування створених стандартів у міжнародному масштабі. Виходячи з основних складових інтелектуальної системи (генерація, передача, розподіл, ринки, операції, сервісний провайдер і клієнт), пріоритетними галузями, які підлягають стандартизації, є: широкозонна ситуаційна обізнаність, реакція попиту та енергоефективність для клієнтів, акумулювання електроенергії, кіберзахищеність, мережна система зв'язку, удосконалення інфраструктури вимірювання енергоспоживання, управління мережею розподілу електроенергії.

- NISTIR 7628. Guidelines for Smart Grid Cyber Security. Даний нормативний документ описує кібербезпеку в Smart Grid системах. Як і IEC 62351 і NIST SP800-53, він встановлює профілі безпеки, а також призводить у відповідність профілі безпеки по відношенню до NIST SP800-53 і NERC CIP.

Також в NISTIR 7628 дано опис безлічі об'єктів і суб'єктів, які належать позначеним доменам, і визначено взаємозв'язки між ними. Причому взаємозв'язки об'єктів і суб'єктів описані з точки зору необхідності забезпечення цілісності, конфіденційності та доступності. Ще однією цікавою обставиною є те, що NISTIR 7628 описує вимоги до криптографічних механізмів захисту інформації. Ці вимоги викладені з урахуванням подальшої перспективи розвитку (2030) систем безпеки.

2. Industrial Automation and Control Systems Security (ISA) ISA SP-99. Цей галузевий стандарт описує підходи до забезпечення інформаційної безпеки системи виробництва і управління виробництвом. Варто відзначити, що на базі ANSI/ISA-62443 розроблений стандарт IEC 62443. Security for industrial process measurement and control - Network and system security. Таким чином, ISA-99 повністю увійшов в IEC 62443 і розвивається як ANSI / ISA і IEC.

3. American Gas Association (AGA). Стандарт є пакетом документів, який пропонує практичні рішення, пов'язані із захистом SCADA від кібератак. Акцент робиться на забезпеченні конфіденційності зв'язку як механізму авторизації користувача. На сьогодні ці документи описують механізми шифрування асинхронних послідовних протоколів, захисту мережних систем та захисту вбудованих компонент SCADA.

Сучасні стандарти управління та інформаційного обміну між рівнями Smart Grid подано на рис. 2.

Слід зазначити, що AGA 12 пропонує використовувати криптографічні алгоритми, затверджені NIST і відповідні FIPS PUB 140-2 .

4. North American Electric Reliability Corporation (NERC).

Документ складається з нормативних актів, що регламентують питання забезпечення кібербезпеки в SCADA та інших критично важливих об'єктів інфраструктури електросистем.

Стандарт описує практично всі рівні забезпечення безпеки від фізичної охорони до захисту систем управління. У той же час необхідно відзначити, що ступінь деталізації цих вимог досить низький, а самі вимоги носять декларативний характер:

- NERC CIP-002. Cyber Security - Critical Cyber Asset Identification;
- NERC CIP-003. Cyber Security - Security Management Controls;
- NERC CIP-004. Cyber Security - Personnel & Training;

- NERC CIP-005. Cyber Security - Electronic Security Perimeter(s);
- NERC CIP-006. Cyber Security - Physical Security of Critical Cyber Assets;
- NERC CIP-007. Cyber Security - Systems Security Management;
- NERC CIP-008. Cyber Security - Incident Reporting and Response Planning;
- NERC CIP-009. Cyber Security - Recovery Plans for Critical Cyber Assets;
- NERC CIP-010. Cyber Security - Configuration Change Management and Vulnerability Assessments;
- NERC CIP-011. Cyber Security - Information Protection.

Також він визначає мінімальні вимоги необхідні для забезпечення відповідності та надійності електросистем.

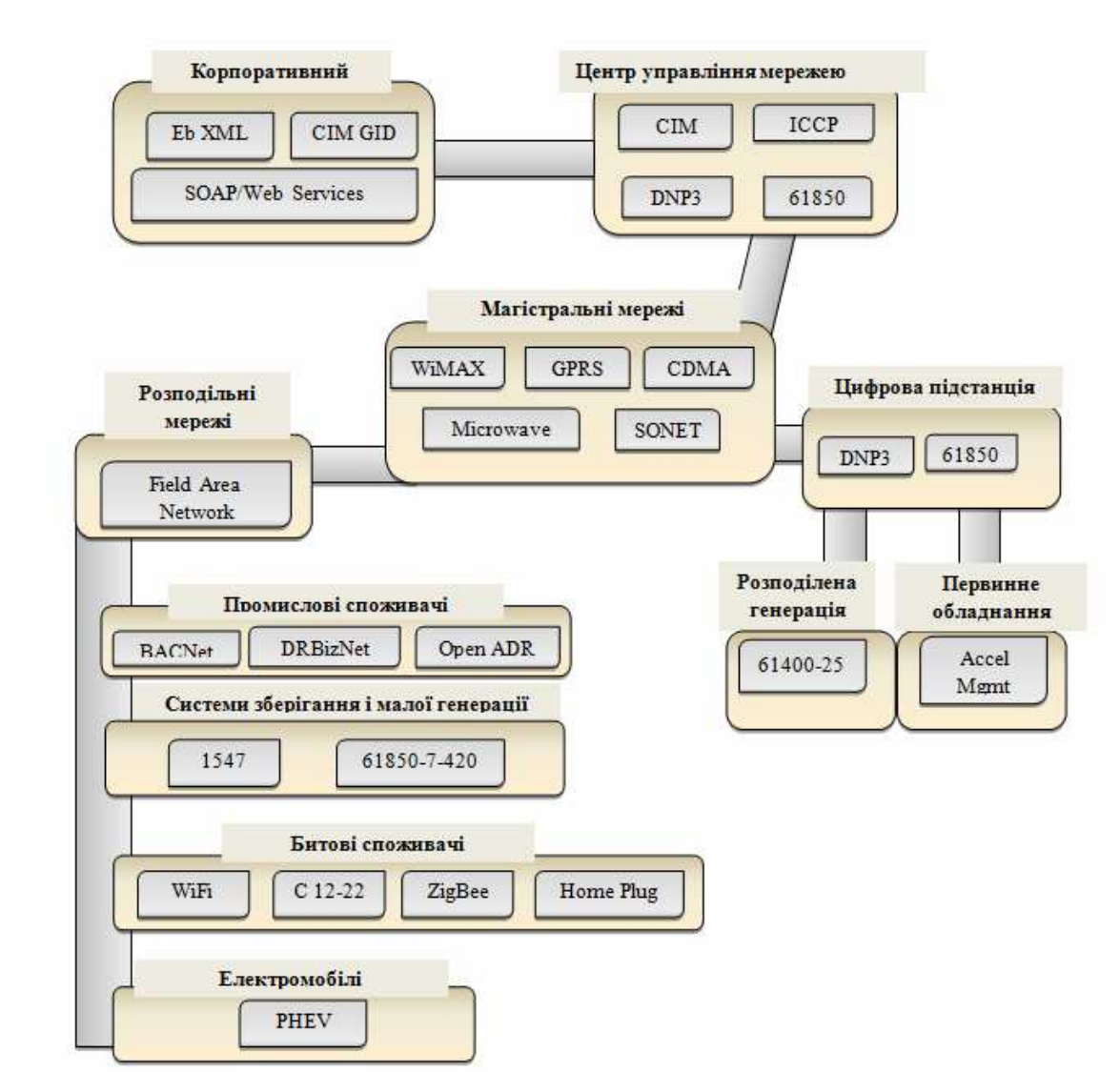

Рис. 2. Стандарти управління та інформаційного обміну між рівнями Smart Grid

На основі проведеного аналізу розглянуто вимоги та норми інформаційної безпеки, діагностики, контролю, надійності інтелектуальних систем на базі концепції Smart Grid, впровадження і розвиток якої вже здійснюється багатьма країнами світу. А для реалізації даної концепції в енергетиці України, в тому числі системи електропостачання залізничного транспорту та практичного впровадження, потрібно вирішення організаційних та технічних засобів, а також системи стандартизації.

Висновки

1. На основі досліджень було проведено аналіз нормативних документів, що відносяться до забезпечення інформаційної безпеки систем управління, систем диспетчерського управління та збору даних (SCADA), автоматизованих систем управління технологічним процесом (АСУ ТП) і Smart Grid.

2. Досліджено норми та вимоги, які мають бути в основі документів, що починають свій шлях дослідження та розвитку в країні і стануть основою забезпечення інформаційної безпеки інтелектуальної електроенергетичної системи залізниць України, зокрема компонентів корпоративної комп'ютерної системи моніторингу та діагностики на кожному з рівнів ієрархії, які повинні забезпечуватись відповідними комплексами інформаційного захисту або системи інформаційної безпеки, що є передумовою подальшого використання інфраструктури системи для комплексного автоматизованого керування режимами енергопостачання.

3. Проаналізовано норми та вимоги щодо стандартизації технологій, які описують питання безпеки в системах електропостачання на основі поняття кібербезпеки.

4. Подано ієрархію стандартів інтелектуальних мереж та стандарти управління з інформаційним обміном між рівнями Smart Grid.

Література

1. Стогній, Б.С. Еволюція інтелектуальних електричних мереж та їхні перспективи в Україні [Текст] / Б.С. Стогній, О.В. Кириленко, А.В. Праховник, С.П. Денисюк // Технічна електродинаміка. – 2012. – № 5. – С. 52–67.
2. The part of the smart grid/H. Farhangi//IEEE Power and Energy Magazine, - 2010. – Vol.8, №1. – P. 18-28.
3. Стасюк, О.І. Математичні моделі і комп'ютерно-орієнтовані методи моніторингу і ідентифікації аварійних режимів тягових мереж [Текст] / В.Л. Тутик, Л.Л. Гончарова, Г.М. Голуб // Інформаційно-керуючі системи на залізничному транспорті: наук.-техн. журнал. – Харків: УкрДУЗТ, 2015. – № 2. – С.7-13.
4. Джинчарадзе, А. Роль стандартизации в обеспечении разработки и внедрения интеллектуальной электроэнергетической системы [Текст] // А. Джинчарадзе, И. Миль // Информационные ресурсы России. – 2013. – №1.
5. Стасюк, О.І. Методи комп'ютерної інтелектуалізації режимів функціонування тягових мереж залізниць [Текст] / О.І. Стасюк, Л.Л. Гончарова, В.Ф. Максимчук, Г.М. Голуб // Інформаційно-керуючі системи на залізничному транспорті: наук.-техн. журнал. – Харків: УкрДУЗТ, 2013. – № 5. – С.29-36.
6. Юдин, А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности Smart Grid систем [Текст] / А. Юдин, Г. Пирогов // Правове, нормативне та метрологічне забезпечення системами захисту інформації в Україні. – 2013. – №1(25). – С. 88-95.

Kulbovskyy I.I, Golub G.M. Analysis of normative and technical base of the introduction of Intelligent energy systems based on SMART GRID technology. Analyze the requirements and standards that are established by normative documents, which provide reliability, control, diagnosis, determination of the parameters and information security intellectual power system based on the concept of Smart Grid systems.

Investigated the existing normative documents that apply to information security in the intellectual power network projects on the basis of Smart Grid systems concept, which is a qualitatively new set of mutually - integrated electric traction networks and distributed computing resources and management technologies, customers, generation capacity and means protection combined based on modern principles of a common information space, self-regulation, self-healing, support the principle of a single model of primary data, the principle of simultaneous information exchange.

The questions of application of standardization system, shows the hierarchy standard of intelligent network

This article contains an overview of the documents of international and industry standards related to information security management systems, supervisory control and data acquisition systems - the SCADA, automated process control systems - Process Automation and Smart Grid. Including documents Standards National Institute of Standards and Technology, which describe safety issues and introduce the concept of cyber security in SCADA and Smart Grid systems.

Key words: information security, Smart Grid, an international standard, smart grids, cyber security, intellectualization.

Кульбовский И.И., Голуб Г.М. Анализ нормативно-технической базы внедрения интеллектуальных энергетических систем на основе технологий SMART GRID. Приведен анализ требований и норм, устанавливаемых нормативными документами, которые обеспечивают надежность, контроль, диагностику, определение параметров и информационную безопасность интеллектуальной электроэнергетической системы на основе концепции Smart Grid систем. Рассмотрены вопросы внедрения

систем стандартизации, приведена иерархия стандартов интеллектуальных сетей.
Ключевые слова: информационная безопасность, Smart Grid, международный стандарт, интеллектуальная электрическая сеть, кибербезопасность, интеллектуализация.

Рецензент Стасюк Олександр Іонович, доктор технічних наук, професор, лауреат Державної премії в галузі науки і техніки, завідувач кафедри «Автоматизація та комп'ютерно-інтегровані технології транспорту», (Державний економіко-технологічний університет транспорту).

Надійшла 19.04.2016 р.

***Кульбовський Іван Іванович**, к.т.н., Доцент кафедри «Будівельні конструкції та споруди», Державний економіко-технологічний університет транспорту, Київ, Україна.*
***Голуб Галина Михайлівна**, аспірант кафедри «Автоматизація та комп'ютерно-інтегровані технології транспорту», Державний економіко-технологічний університет транспорту, Київ, Україна.*

***Kulbovskyy I.I.**, candidate of engineering, associate professor of "Building design and construction", State Economy and Technology University of Transport, Kyiv, Ukraine.*
***Golub G.M.**, graduate faculty " Automation and computer-integrated technologies of transport ", State Economy and Technology University of Transport, Kyiv, Ukraine*