АНАЛІЗ УРАЗЛИВОСТЕЙ ТА ЗАГРОЗ У СИСТЕМАХ УПРАВЛІННЯ КІБЕРФІЗИЧНИМИ ОБ'ЄКТАМИ НА ПРИКЛАДІ РОЗУМНОЇ ЕЛЕКТРОМЕРЕЖІ

Чебурахін М.І., Балагура Д.С.

Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
Україна

E-mail: mykhailo.cheburakhin@nure.ua,
dmytro.balahura@nure.ua

Abstract

The work examines and analyzes threats and methods of penetration into control systems of cyber-physical objects using the example of a smart power grid, as well as methods for preventing them. Not a single industry in our time can do without methods for protecting confidentiality, integrity and availability, and the smart power grid is no exception, for which information protection is vital, because without information protection, the owner of the power grid can suffer large losses, both financially and and reputational.

Завдяки розвитку інформаційних технологій і впровадженню систем інформатизації у практично усі сфери життєдіяльності людини, кібербезпека стала одним із найпріоритетніших напрямків по забезпеченню безпеки існування і життєдіяльность людини. Однак, слід зазначити, що кібербезпека часто розглядається тільки у розрізі безпеки комп'ютерних систем та мереж. Насправді поняття кібербезпеки набагато ширше. Одним із напрямів кібербезпеки є кіберфізична безпека.

Розглянемо аспекти кіберфізичної безпеки на прикладі розумної електромережі. Розумна електромережа є однією з найскладніших кіберфізичних систем, яка поєднує фізичні та кібернетичні компоненти в критичній інфраструктурі.

Кіберфізична безпека розумної електромережі вимагає інтегрованого підходу, який враховує як фізичні, так і кібернетичні загрози та залежності. Атаки на зазначену систему є більш комплексними з точки зору методів, що застосовуються, а також елементів, на які зловмисник може вплинути під час атаки. До найбільш поширених атак на розумні електромережі відносяться:

1) Атаки на системи генерації: Атакуючи контролери швидкості турбін та частоти системи, зловмисники можуть спричинити нестабільність, перевантаження та знищення генераторів. Наприклад, атака Aurora використовує швидке відкриття та закриття вимикачів ліній, щоб розсинхронізувати генератори .
2) Атаки на системи передачі: Атакуючи вимірювальні дані, топологію та команди керування, зловмисники можуть викликати перевантаження ліній, каскадні відмови та масштабні збої. Наприклад, атака інтердикції вимикає критичні компоненти системи, щоб максимізувати втрати енергії та витрати оператора .
3) Атаки на системи розподілу: Атакуючи розумні лічильники та інші пристрої кінцевих користувачів, зловмисники можуть красти енергію, порушувати приватність, маніпулювати попитом та завдавати шкоди розподільчим трансформаторам. Наприклад, атака зміни навантажен-ня використовує фальшиві дані, щоб перерозподілити навантаження між автобусами та викликати перевантаження ліній .
4) Атаки на ринки електроенергії: Атакуючи інформацію про ціни, тарифи та торгові угоди, зловмисники можуть отримувати неправомірні прибутки, спотворювати сигнали ринку та порушувати економічну ефективність. Наприклад, атака переповнення

передачі використовує фальшиві дані, щоб викликати переповнення передачі та збільшити ціни на ринку.

Порівняння зазначених вище атак за різними критеріями наведено у таблиці 1.

Таблиця 1. Порівняння атак на розумна електромережа

Атака	Потенційні наслідки	Ефективність	Економічний вплив
Атаки на системи генерації	Мають потенціал призвести до нестабільності та навіть знищення генераторів, що може спричинити серйозні наслідки для електростанцій	Можуть бути ефективнішими через можливість призвести до фізичних пошкоджень та перебоїв у постачанні	Можуть мати серйозний економічний вплив через фізичні пошкодження та прямі втрати від перерв у постачанні
Атаки на системи передачі	Можуть викликати перевантаження ліній та каскадні відмови, що також може мати серйозні наслідки для електромережі	Також можуть бути ефективнішими через можливість призвести до фізичних пошкоджень та перебоїв у постачанні	Також можуть мати серйозний економічний вплив через фізичні пошкодження та прямі втрати від перерв у постачанні, але менщі за атаки на системи генерації
Атаки на ринки електроенергії	Хоча вони можуть порушити економічну ефективність, їх наслідки можуть бути менші в порівнянні з першими двома видами атак.	Можуть мати ефективність у вигляді спотворення сигналів ринку, але їх можливі наслідки не є такими серйозними, як у перших двох випадках.	Можуть вплинути на ціни на ринку, але їх економічний вплив не є великим
Атаки на системи розподілу	Може принести к фінансовим втратам, але наслідки менші порівняно з першими двома	Можуть спотворити системи розподілу, але ефективність не занчна порівняно з першими двома	Можуть спричинити втрату деякої кількості енергії, але якщо вчасно відреагувати. то втрат майже не буде

Отже, виходячи з цих критеріїв, можна зробити висновок, що атаки на системи генерації можуть вважатися найбільш небезпечними через свій потенціал призвести до серйозних фізичних пошкоджень та великих втрат в енергопостачанні. Це означає, що виявлення та захист від зазначених вище атак, та, особливо атаки на систему генерації, є завданням, що має вирішуватись у всіх розумних електромережах.

В цілому можна запропонувати різні методи для підвищення рівня захисту кіберфізичних компонентів розумної електромережі, такі як криптографічні протоколи, детектори аномалій, захищені мережеві архітектури, резервне живлення та фізична охорона. Також існують різні техніки для виявлення кіберфізичних атак, такі як аналіз залишків, аналіз статистичних властивостей, аналіз графів, аналіз взаємозв'язків та аналіз даних.

Крім того можна виділити декілька стратегій для зменшення наслідків кіберфізичних атак, такі як ізоляція атакованих компонентів, регулювання параметрів системи, застосування резервних ресурсів та використання адаптивних алгоритмів.

З усіх методів для відновлення нормальної роботи розумної електромережі після кіберфізичних атак можна виділити такі як: використання резервних копій даних, використання альтернативних каналів зв'язку, використання аварійних планів та використання самоорганізації.

Складнощі, які стоять перед розробкою та реалізацією ефективних захисних стратегій, такі як складність та гетерогенність кіберфізичних систем, неповна та неточна інформація про стан

системи, високі вимоги до швидкості та надійності відповіді, взаємозалежність та взаємодія різних секторів та недостатній рівень освіти та обізнаності.

Існує ряд можливостей для підвищення безпеки та стійкості розумної електромережі. Серед них - використання новітніх технологій, застосування інтелектуальних та розподілених алгоритмів, використання багаторівневих та гібридних моделей, впровадження стандартів та політик та активізація співпраці та координації.

Кіберфізична безпека майже не розглядається окремо, існує лише декілька документів, які безпосередньо спрямовані на стандартизацію цього питання:

ISA/IEC 62443: Це міжнародний стандарт, який спеціалізується на кіберзахисті індустріальних автоматизованих систем. Він надає практичні вказівки та вимоги для захисту критично важливих інфраструктур і промислових систем.

MITRE ATT&CK: Це набір знань та матриця тактик і методів, що використовуються кіберзлочинцями, розроблений MITRE Corporation. Він може бути використаний для аналізу та виявлення загроз у кіберфізичних системах.

IEC 62443: Цей стандарт розроблений Міжнародною комісією з електротехніки (IEC) і спрямований на кіберзахист систем автоматизації та керування, включаючи кіберфізичні об'єкти. Він містить вимоги та рекомендації щодо безпеки і кіберзахисту.

Але при цьому варто враховувати, що деякі загальні стандарти також певною мірою можуть застосовуватись для організації безпеки у кіберфізичних системах, серед них:

ISO 27001: Це міжнародний стандарт для управління інформаційною безпекою. Хоча він спрямований на загальну інформаційну безпеку, він також застосовується до кіберфізичних систем та може бути корисним для виявлення уразливостей із цього погляду.

NIST SP 800-53: Документ "Стандарт для керівництва безпекою інформації та кіберзахистом" від Національного інституту стандартів і технологій (NIST) США надає набір контрольних заходів і вказівок для забезпечення безпеки і кіберзахисту в інформаційних системах, включаючи кіберфізичні системи.

Розглянемо на прикладі розумної електромережі основні аспекти побудування захищеного кіберфізичного простору.

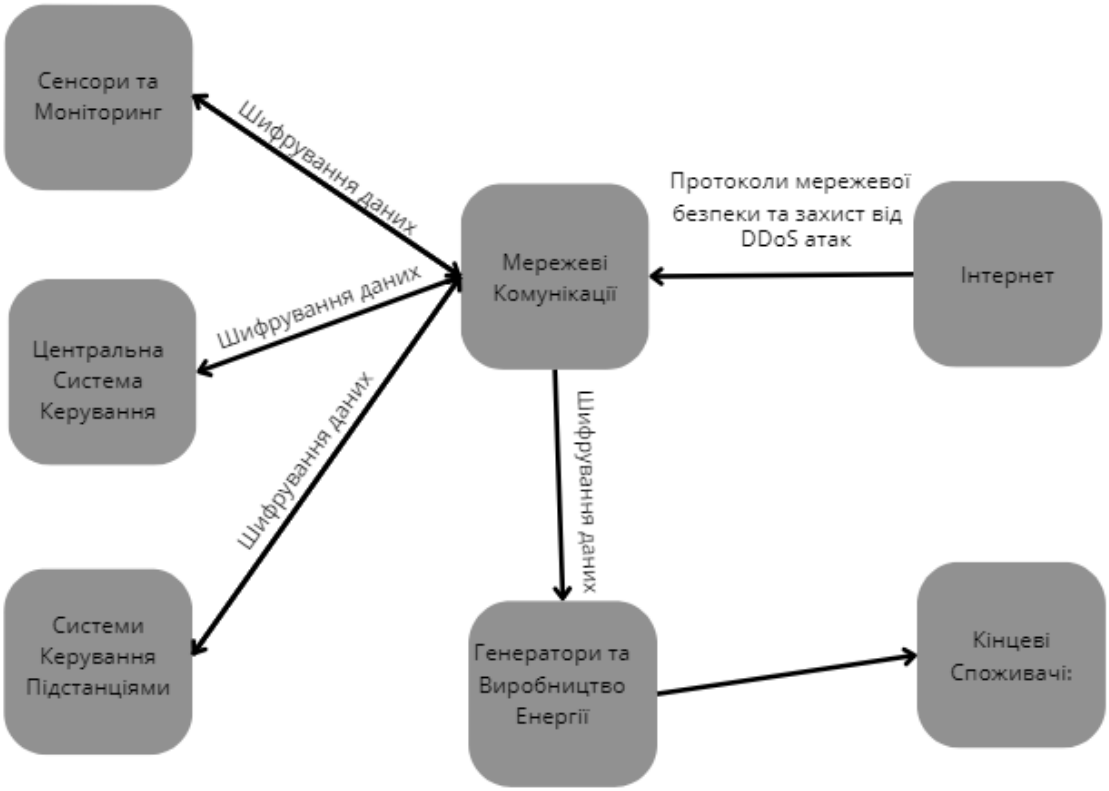

Рис. 1. Побудова розумної електромережі та її захист

Перелік приладів, що використовуються у розумній електромережі

- Сенсори та Моніторинг: Включають різноманітні сенсори, що вимірюють рівні споживання енергії, стан обладнання, температуру, напругу та інші фізичні параметри.
- Мережеві Комунікації: Забезпечують зв'язок між всіма компонентами розумної електромережі, дозволяючи обмін даними та комунікацію між сенсорами, керуючими системами та іншими частинами мережі.
- Центральна Система Керування**:** Це серце системи, що отримує дані від сенсорів, аналізує їх та приймає рішення про керування енергетичною мережею на основі зібраних даних.
- Системи Керування Підстанціями: Вони отримують команди від центральної системи керування та здійснюють контроль над окремими підстанціями електромережі.
- Генератори та Виробництво Енергії: Це джерела енергії, що постачають електроенергію в мережу.
- Кінцеві Споживачі: Це підприємства та особисті споживачі, які отримують енергію через розумну електромережу.

Також на рис. 1. зображені методи захисту, які потрібно використовувати для захисту розумної електромережі.

Захист

- Шифрування даних: Використання шифрування даних у всіх мережевих передачах для захисту конфіденційності та цілісності даних.
- Протоколи мережевої безпеки: Використання протоколів, таких як VPN (віртуальна приватна мережа), TLS/SSL (що забезпечують безпеку під час передачі даних через Інтернет), Firewalls та інших інструментів мережевої безпеки для захисту мережевих з'єднань та даних.
- Захист від відмов сервісу (DoS) та атак DDoS: Використання заходів для запобігання атак DoS та DDoS, що можуть перекрити роботу мережі.

Виходячи з вищезазначеного, необхідно обрати найкращий алгоритм для шифрування даних в розумній електромережі. Для цього порівняємо алгоритми шифрування для захисту розумної електромережі. Результати наведені в талиці 2.

Таблиця 2. Порівняння методів шифрування для захисту розумної електромережі

Алгоритм	Рівень захисту	Швидкість та продуктивність	Складність та вартість впровадження
AES (Advanced Encryption Standard)	Вважається одним з найбільш ефективних методів шифрування	5-10 мікросекунд на блок 128 біт	Досить поширений і підтримується в багатьох системах, але може вимагати спеціалізованого обладнання для швидкої обробки.
RSA (Rivest–Shamir–Adleman)	Має сильний захист, особливо в контексті асиметричного шифрування.	Швидкість шифрування RSA в мікросекундах на блок даних може значно варіюватися в залежності від конкретних обставин	Використання RSA може бути дорожчим та потребувати більше обчислювальних ресурсів.
ECC (Elliptic Curve Cryptography)	Також володіє високим рівнем захисту	Швидше **за** RSA але повільніший за AES, швидкість також може варіюватися в залежності від конкретних обставин	Його використання може бути меншим за рахунок використання менше обчислювальних ресурсів.

У контексті захисту розумної електромережі може бути корисним використання різних методів шифрування в залежності від конкретних вимог системи. Однак, для захисту розумної електромережі, кращим вибором може бути Advanced Encryption Standard (AES). Він є одним з найбільш ефективних та широко використовуваних методів шифрування в сучасних інформаційних системах та має кращу швидкість, якщо порівнювати з конкурентами.

Отже, слід розуміти, що кіберфізична безпека є надважливою частиною забезпечення безпеки інформаційних та фізичних середовищ. Відсутність уваги до ~~щієї~~цієї сфери може призвести до фатальних наслідків. У доповіді розглянуто загрози, які можуть бути небезпечними для розумної електромережі, наслідки до яких вони можуть призвести та способи їх усунення.

Література

1. Farhangi, H.:‘The path of the smart grid’,IEEE Power Energy Mag., 2010,8, (1),pp. 18–282.

2. Sridhar, S., Hahn, A., Govindarasu, M.:‘Cyber–physical system security for theelectric power grid’,Proc. IEEE, 2012,100, (1), pp. 210–2243.

3. Wood, A.J., Wollenberg, B.F.:‘Power generation, operation, and control’(JohnWiley & Sons, Hoboken, NJ, 2012, 3rd edn.)

4. National Institute of Standards and Technologies (NIST):‘Framework androadmap for smart grid interoperability standards–release v3.0’(NIST SpecialPublication, Gaithersburg, MD, 2014).

5. Gungor, V.C., Sahin, D., Kocak, T.,et al.:‘Smart grid technologies:communication technologies and standards’,IEEE Trans. Ind. Inf., 2011,7, (4),pp. 529–539

6. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT):‘Cyber-attack against Ukrainian critical infrastructure’. 2016. Режим доступа: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (дата звернення: 07.11.2023).

7. Anwar, A., Mahmood, A.N., Tari, Z.:‘Identification of vulnerable node clustersagainst false data injection attack in an AMI based smart grid’,Inf. Syst., 2015,53,pp. 201–212. Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0306437914001884 (дата звернення: 07.11.2023).

8. Liang, J., Sankar, L., Kosut, O.:‘Vulnerability analysis and consequences of falsedata injection attack on power system state estimation’,IEEE Trans. Power Syst.,2016,31, (5), pp. 3864–3872