Технічні науки

УДК 338.45:657

Курилик Олександр Володимирович
студент кафедри електричних мереж та систем
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
Курылык Александр Владимирович
студент кафедры электрических сетей и систем
Национального технического университета Украины
"Киевский политехнический институт имени Игоря Сикорского"
Kurylyk Olexandr
Student of Electric Networks and Systems Department
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Науковий керівник:
Буслова Наїна Володимирівна
кандидат технічних наук, доцент кафедри електричних мереж та систем
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"

ДОСЛІДЖЕННЯ ВУЗЬКИХ МІСЦЬ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ТА ОБЛІКУ ЕЛЕКТРОЕНЕРГІЇ
ИССЛЕДОВАНИЕ УЗКИХ МЕСТ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ И УЧЕТА ЭЛЕКТРОЭНЕРГИИ
RESEARCH PROBLEM SPACES OF SECURITY IN AUTOMATED ELECTRICITY CONTROL AND ACCOUNTING SYSTEM

Анотація. *У статті розглянуто проблему інформаційного захисту автоматизованої системи контролю та обліку електроенергії (АСКОЕ). В останні роки спостерігається зростання вартості електроенергії, яке, в свою чергу, вплинуло на реорганізацію енергообліку в усіх галузях промисловості, транспорту та житлово-комунального господарства. Адже споживачі чітко розуміють, що вони повинні платити за використання енергоресурсів не за умовними нормами, отримуючи дані із морально застарілих лічильників, в результаті не маючи чіткої картини електроспоживання (в зв'язку з цим часто спостерігається факт розкрадання електроенергії), а на основі даних із сучасних та високоточних приладів. Саме таким ''приладом'' і є АСКОЕ. Із зростанням популярності даної системи, значно знизився показник розкрадання електроенергії на підприємствах але підвищився інтерес до самого програмного комплексу так званих хакерів. Оскільки система обліку експлуатується відносно не довго і знаходиться в процесі оптимізації, в даній статті було розглянуто загрози можливих атак.*

Ключові слова: *АСКОЕ, система розподілу, безпека, електромережа Smart Grid.*

Аннотация. *В статье рассмотрена проблема информационной защиты автоматизированной системы контроля и учета электроэнергии (АСКУЭ). В последние годы наблюдается рост стоимости елктроенергии, которое, в свою очередь, повлияло на реорганизацию энергоучета во всех отраслях промышленности, транспорта и жилищно-коммунального хозяйства. Ведь потребители четко понимают, что они должны платить за использование энергоресурсов не по условным нормам, получая данные с морально устаревших счетчиков, в результате не имея четкой картины*

электропотребления (в связи с этим часто наблюдается факт хищения электроэнергии), а на основе данных из современных и высокоточных приборов. Именно таким "прибором" и является АСКУЭ. С ростом популярности данной системы, значительно снизился показатель хищения электроэнергии на предприятиях, но повысился интерес к самому программного комплексу так называемых хакеров. Поскольку система учета эксплуатируется относительно недолго и находится в процессе оптимизации, в данной статье были рассмотрены угрозы возможных атак.

Ключевые слова: *АСКУЭ, системы распределения, безопасность, электросеть, Smart Grid.*

Summary. *The article deals with the problem of information protection of the automated control system and accounting of electricity (ACSAE). In recent years, there has been an increase in the cost of electricity, which in turn has influenced the reorganization of energy accounting in all sectors of industry, transport and housing and communal services. After all, consumers clearly understand that they have to pay for the use of non-conditional energy resources, obtaining data from outdated meters, as a result of not having a clear picture of electricity consumption (in this regard, the fact that electricity is often stolen), and based on data from modern and high-precision instruments. It is this " device " that is the ACSAE. With the increasing popularity of this system, the rate of theft of electricity in enterprises has decreased significantly, but the interest in the software complex of so-called hackers has increased. Because the accounting system has been in operation for a relatively long time and is in the process of being optimized, this article examines the threats of possible attacks.*

Key words: *ACSAE, distribution system, security, electricity, Smart Grid.*

Постановка проблеми. Енергетична галузь є важливим стратегічним об'єктом кожної країни, характеризується високою надійністю електросистеми для забезпечення безперервного електропостачання споживачів різних категорій, перерва в постачанні яких може призвести до масштабних збитків.

Аналіз останніх досліджень і публікацій. Дослідження складають праці таких фахівців в енергетичній галузі як: В.В. Кирик [1], Коротких Н.Е. [2], В.Е. Воротніцький [3].

Формулювання цілей статті (постановка завдання). Аналіз наукових праць, досліджень та інтернет джерел. Систематизування загроз інформаційній безпеці системи обліку та поділення їх на зони.

Виклад основного матеріалу. За способом призначення АСКОЕ бувають трьох видів:

- АСКОЕ широкого використання, розробляється для серійного виробництва у вигляді завершених виробів.
- АСКОЕ вузького використання, розробляється для одиничного або повторного з невеликим партіями виробництва.
- АСКОЕ цільового використання, які проектуються для конкретних об'єктів.

За принципом організації існуючі АСКОЕ розділяють на три типи: локальні, регіональні та національні. Локальна АСКОЕ включає в себе лічильники електричної енергії і потужності, пристрої збору та передачі даних (телесуматори, мультиплексори, концентратори і т. п.), сервер опитування пристроїв збору та передачі даних (ПЗПД) і сервер бази даних, робочі місця технологів або енергетиків, які підключені до локальної обчислювальної мережі підприємства. В тих випадках, коли необхідно організувати збір і обробку даних від декількох локальних АСКОЕ,

створюється регіональна АСКОЕ, яка являє собою багаторівневу систему. Верхні рівні цієї системи створені вузлами, з'єднаних між собою лініями зв'язку, що мають відповідну каналоутворюючу апаратуру. До нижнього рівня відносять локальні АСКОЕ, від яких надходить інформація про використання електричної енергії. Національна АСКОЕ будується на тих самих принципах, що й регіональна, але охоплює територію всієї держави.

За способом опитування лічильників електроенергії АСКОЕ поділяють на сильнозв'язні та слабкозв'язні системи.

В сильнозв'язних (синхронних) системах опитування лічильників виконується циклічно із заданою частотою (зазвичай один раз за 1 або 3 хвилини). Такий принцип характерний для АСКОЕ, що мають лічильники електроенергії з число імпульсним виходом без запам'ятовування інформації.

Слабкозв'язні (асинхронні) системи будуються на базі лічильників електроенергії з цифровим інтерфейсом і можливістю зберігання даних в них. Опитування лічильників може здійснюватися як циклічно, так і за ініціативою лічильників або ПЗПД.

За функціональним призначенням розрізняють АСКОЕ для комерційного і технічного обліку електроенергії. Багатофункціональні АСКОЕ можуть проводити обидва обліки одночасно.

Структурна схема ОРЕ України зображено на Рис. 1.

В даний час спостерігається зростання кількості споживачів електроенергії та енергоємних підприємств. Зростаюча кількість втрат електроенергії, а також груба апроксимація процесу енергоспоживання не влаштовує ні споживачів, ні постачальників електроенергії.

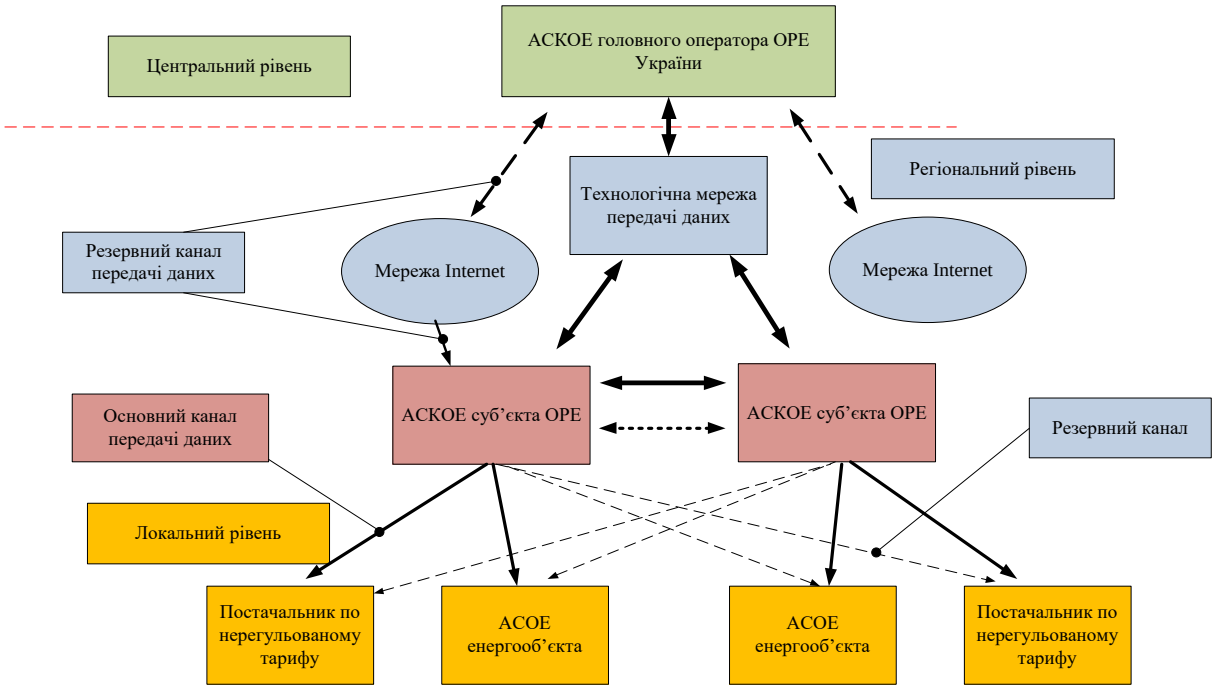

Рис. 1. Структурна схема АСКОЕ України

Інтелектуальні мережі (Smart Grid) - мережі електропостачання, що використовують комунікаційні канали, інформаційно-аналітичні і програмно-технічні системи для збору інформації про енерговиробництво та енергоспоживання з метою підвищення ефективності, надійності виробництва та розподілу електроенергії. Розвиток інтелектуальних мереж є важливим напрямком стратегії розвитку енергетики України [1].

Сьогодні концепція Smart Grid в Україні представлена в якості активно-адаптивної мережі, яку можна охарактеризувати за наступними ознаками:

- насиченість мережі активними елементами, призначеними для зміни топології мережі;
- велика кількість вимірювальних приладів;
- наявність системи впливу на активні елементи мережі;
- наявність автоматизованої системи збору, обробки та передачі даних;

Остання характеристика це не тільки задача автоматизації опитування вимірювального приладу, але й забезпечення інформаційного обміну між компонентами об'єкта енергозбереження, а також оперативної обробки даних енергоспоживання. Це привело до розвитку автоматизованих систем комерційного обліку електроенергії (АСКОЕ), які призначені для вирішення цих задач.

Більшість АСКОЕ можна розділити на три рівня:

- Уровень виміру - сукупність програмно-технічних засобів, що здійснюють вимірювання параметрів енергообліку, а також здійснюють їх первинну обробку в сигнал уніфікованого виду. Часто ці пристрої називають первинними вимірювальними приборами, в якості яких виступають електролічильники, що надають інтерфейс доступу до інформації по даній точці енергообліку.
- Інформаційно-вимірювальний комплекс сукупність функціонально об'єднаних програмно-технічних засобів, призначених для збирання та обробки даних з одного або декількох пристроїв першого рівня. Часто до другого рівня відносять: пристрої збирання та передачі даних, автоматизовані робочі місця і комунікаційні канали між пристроями.
- Рівень керування включає в себе сервери з спеціалізованим ПЗ, які здійснюють збір інформації з пристроїв другого рівня, кінцеву обробку цієї інформації, документування та відображення в зручному для аналізу вигляді. Автоматизована система контролю та обліку електроенергії (АСКОЕ) оперує великим об'ємом даних про енергоспоживання клієнтів і, відповідно, вимагає високого ступеню довіри до інформації в системі. Саме це робить актуальним питання інформаційної безпеки [2].

Класичні системи забезпечення інформаційної безпеки зазвичай не підходять для інсталяції на промислових підприємствах із-за недостатньої

надійності. Тому потрібні спеціалізовані засоби захисту, здатні працювати в таких умовах [3].

Інтеграція IT-рішень в автоматизовані системи управління технологічним процесом (АСУ ТП) привела до того, що промислові системи, які здавалися до цього безпечними, виявилися під загрозою ціле направлених кібератак. Інциденти з використанням спеціалізованих вірусів, таких як Stuxnet, Flame, BlackEnergy, знайдених на комп'ютерах великих промислових систем, вже кілька років є однією з найбільш обговорюваних тем на заходах, присвячених інформаційній безпеці. Велика кількість компаній, з надання засобів захисту інформації, аудит безпеки, розслідування інцидентів, відкриває для себе новий ринок промислової кібербезпеки. Експерти також визнають, що ризики цілеспрямованих атак на АСУ ТП критично важливих об'єктів промисловості (КВО) зростають з кожним роком [4].

Специфіка промислових систем (високий пріоритет доступності інформації та безперервності технологічного процесу) сильно затрудняє впровадження класичних засобів забезпечення інформаційної безпеки. Таке уповільнення інтеграції, а також неготовність і не усвідомлення проблеми призводить до росту кількості інцидентів інформаційної безпеки, які є причиною несправності промислових систем більш, ніж в третині випадків [5].

Якщо звернутися до статистики інцидентів по галузям промисловості RISI, то можна помітити, що енергетика - одна з найбільш небезпечних і підвергнутих загрозам галузь (див. Рис. 2).

Рис. 2. Кількість інцидентів інформаційної безпеки по галузям промисловості

Це зумовлено високим ступенем розподілу структури енергетичних об'єктів та її велика гетерогенність, що підвищує кількість можливих векторів атаки.

Інформаційна безпека Smart Grid та АСКОЕ. Питання інформаційної безпеки АСКОЕ заторгують не тільки класичні поняття конфіденційності, цілісності та доступності інформації, але також поняття стійкості енергосистем, надійності електропостачання і енергетичної ефективності.

Інформаційний обмін в АСКОЕ здійснюється як в межах одного рівня (між однорідними пристроями), так і між рівнями. В обох випадках присутні точки впливу на систему з боку хакерів.

Поняття Smart Grid охоплює, в основному, АСКОЕ, а також системи управління підстанціями, релейного захисту і автоматики. Для таких систем розвивається стандарт МЕК 61850, що регламентує обмін даними між елементами підстанцій. У завданнях, пов'язаних із забезпеченням безпеки інформаційного обміну, стандарт відсилається до документа МЕК 62351, який, в свою чергу, описує механізми захисту, в тому числі таких протоколів, як МЕК 60870-5, МЕК 61850-8-1 (GOOSE).

Але незважаючи на наявність захищених протоколів, багато АСКОЕ використовують небезпечні протоколи мережевого обміну польових пристроїв: ModBus, або дочірні протоколи на основі ModBus від виробника електролічильника. Якщо на польовому рівні АСКОЕ не передбачено базових методів захисту інформації, то для атакуючого не важко буде впливати на систему. Отримавши доступ до автоматизованого робочого місця або пристроїв збору та передачі даних, також можна реалізувати крадіжку або підміну даних, привести систему в неробочий стан. Подібні атаки можуть бути причиною неправомірного доступу до управління електролічильників: атакуючий зможе змінити, наприклад, коефіцієнт трансформації трансформатора струму або напруги, а також тимчасово приховати наслідки паралельного зловмисного впливу на елементи РЗА. Вразливе ПО на третьому рівні моделі АСКОЕ та незахищені канали зв'язку також є точками входу для атакуючого [6].

При аналізі загроз було виділено основні, та складено перелік з розподіленням на зони, що наведений нижче:

№ п/п	Загрози
Адміністративна зона	
1	отримання неправомірного доступу до керуючого сегменту
2	підвищення привілеїв в системі
3	використання ідентифікації / аутентифікації, заданої за замовчуванням
4	неправомірне ознайомлення з захищеною інформацією
5	розкриття інформації про стан, параметри, складу системи, а також про топології мережі
6	використання ПЗ, не призначеного для забезпечення працездатності системи, на АРМ
7	отримання неправомірного доступу до технічних даних системи в результаті недбалого ставлення працівників до своїх обов'язків
8	отримання неправомірного доступу до технічних даних системи в результаті некомпетентності адміністраторів системи
Програмна зона	
9	DoS / DDoS-атака на сервери системи управління / інформування
10	отримання доступу до інформації в результаті передачі даних в відкритому / незашифрованому вигляді (plaintext)
11	отримання неправомірного доступу через відсутність механізмів аутентифікації
12	XSS-атаки на систему управління / інформування
13	SQL-ін'єкції в систему управління / інформування
14	підбір паролів методами "грубої сили" або з використанням словників
15	неправомірне підключення до мережі управління / інформування на фізичному рівні
16	перехоплення даних систем управління / інформування
17	підміна даних систем управління / інформування, переданих по мереж
18	атаки підміни IP-адресів вузлів систем управління / інформування

Висновки. При дослідженні АСКОЕ можна впевнено сказати, що впровадження даної системи дозволить зменшити втрати енергії та отримати з найменшими затратами інформацію про те в якому обсязі електроенергія поступає в мережу та інформацію про її якість.

Дослідження проблеми інформаційної безпеки АСКОЕ і інтелектуальних систем електропостачання Smart Grid показало важливість забезпечення інформаційної безпеки таких систем, так як виявлені високі показники ризику і потенційного збитку, зростання кількості інцидентів і

складність впровадження систем захисту інформації. Для повного розуміння проблеми в забезпечені безпеки системи АСКОЕ можна навести в приклад інцидент кінця 2015 року, що стався з оператором системи розподілу «Прикарпаттяобленерго», в результаті якого на великій території Івано-Франківської області була відключена електроенергія, і більше 230 тисяч чоловік залишилися без світла та тепла.

Література

1. Кирик В.В. Інтелектуальні технології управління та імітаційного моделювання в складних системах // Навч. посібник. 2009. С. 88-90.
2. Коротких Н. Е. Системи комерційного контролю і обліку електроенергії / Інформатизація та системи управління в промисловості, 2013. №6.
3. Воротніцький В.Е. Зниження втрат електроенергії - найважливіший шлях енергозбереження в електричних мережах // Енергозбереження. 2014. № 3. С. 61-64.

   Резолюція четвертої конференції «Інформаційна безпека АСУ ТП критично важливих об'єктів» // Інформаційна безпека АСУ ТП КВО. Всерос. конф. (Москва, 17-18 березня 2016 р.). Москва, 2016. С. 6. The Repository of Industrial Security Incidentsю URL: http://www.risidata.com/Database/