НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

ЗАПРОШЕННЯ
ПРОГРАМА ТА МАТЕРІАЛИ

28 травня 2021 року

Київ – 2021

УДК [621.3+620.9]::004[056.53+42+94]
ББК 31
К-381

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 7 від 20 травня 2021 р.)

К-381 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : запрошення, програма та матеріали, 28 травня 2021 р. Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2021. 61 с.

Вельмишановний _____

_____

запрошуємо Вас прийняти участь в роботі науково-практичної конференції «Кібербезпека енергетики», яка буде проходити 28 травня 2021 року в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, м. Київ.

СПІВОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

АСОЦІАЦІЯ «ІНФОРМАТІО-КОНСОРЦІУМ»
ТОВ «ІНФОРМАТІО»

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор, директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, старший науковий співробітник

Куцан Юлій Григорович
доктор технічних наук, заслужений енергетик України

Гончар Сергій Феодосійович
доктор технічних наук, учений секретар Інституту

Гурєєв Віктор Олександрович
доктор технічних наук

Гільгурт Сергій Якович
доктор технічних наук, старший науковий співробітник

Богданов Олександр Михайлович
доктор технічних наук, професор

Борукаєв Зелімхан Харитонович
доктор технічних наук, старший науковий співробітник

Васильєв Всеволод Вікторович
член-кореспондент НАН України, доктор технічних наук, професор

Верлань Анатолій Федорович
доктор технічних наук, професор

Винничук Степан Дмитрович
доктор технічних наук, старший науковий співробітник

Владимирський Олександр Альбертович
доктор технічних наук, старший науковий співробітник

Євдокимов Віктор Федорович
член-кореспондент НАН України, доктор технічних наук, професор, почесний директор Інституту

Самойлов Віктор Дмитрович
доктор технічних наук, професор

Саух Сергій Євгенович
член-кореспондент НАН України, доктор технічних наук, професор

Яцишин Андрій Володимирович
доктор технічних наук, старший науковий співробітник

РЕГЛАМЕНТ
РОБОТИ КОНФЕРЕНЦІЇ

28 травня – п'ятниця

Час	Захід
10.00 – 11.00	Реєстрація учасників конференції
11.00 – 11.15	Відкриття конференції
11.15 – 13.00	Робота конференції. Виступи учасників
13.00 – 14.00	Перерва
14.00 –17.00	Робота конференції. Виступи учасників
17.00 – 18.00	Підведення підсумків роботи конференції. Прийняття рішень. Закриття конференції

Примітка: в регламенті роботи конференції можливі зміни.

ПРОГРАМА
РОБОТИ КОНФЕРЕНЦІЇ

28 травня. П'ятниця

11.00 – 11.15 ***ОФІЦІЙНЕ ВІДКРИТТЯ КОНФЕРЕНЦІЇ***

ВСТУПНЕ СЛОВО

Мохор Володимир Володимирович –
член-кореспондент Національної академії наук України, доктор технічних наук, професор, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

11.15 – 13.00 ***ПЛЕНАРНЕ ЗАСІДАННЯ - ДИСКУСІЇ***

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
Бакалінський Олександр Олегович,
Пахольченко Дмитро Віталійович,
Сапожнік Тетяна Михайлівна

ПРАВОВІ ЗАСАДИ ЗДІЙСНЕННЯ КІБЕРБЕЗПЕКИ В ПАЛИВНО-ЕНЕРГЕТИЧНОМУ КОМПЛЕКСІ УКРАЇНИ ЯК ФАКТОР НАДІЙНОСТІ ІСНУВАННЯ РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ
Бондаренко Степан Юрійович

ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В МЕРЕЖАХ 5G ДЛЯ КОНЦЕПЦІЇ SMART GRID
Одарченко Роман Сергійович,
Дика Тетяна Василівна

РАЗРАБОТКА СТЕНДА ДЛЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ ИСКРОБЕЗОПАСНЫХ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ
Владимирский Александр Альбертович,
Владимирский Игорь Альбертович,
Криворучко Игорь Петрович,
Анфимова Галина Викторовна

РЕГИСТРАЦИЯ СОПУТСТВУЮЩИХ СОБЫТИЙ В ИЗМЕРИТЕЛЕ ПАРАМЕТРОВ ДВИЖЕНИЯ
Владимирский Александр Альбертович,
Владимирский Игорь Альбертович,
Криворучко Игорь Петрович

ПІДХОДИ ДО ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ АТАК НА ПРОТОКОЛИ ЦИФРОВИХ ЕЛЕКТРИЧНИХ ПІДСТАНЦІЙ
Гільгурт Сергій Якович

ОГЛЯД ЕТАПІВ І НАПРЯМІВ ДОСЛІДЖЕНЬ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГАЛУЗІ ЕЛЕКТРОЕНЕРГЕТИКИ
Герасимов Ростислав Павлович,
Крук Ольга Миколаївна

13.00 – 14.00 ***ПЕРЕРВА***

14.00 –17.00 ***ПЛЕНАРНЕ ЗАСІДАННЯ - ДИСКУСІЇ***

РІЗНОВИДИ ЕКТОРІВ ПРИ АНАЛІЗУВАННІ ВРАЗЛИВОСТЕЙ СОЦІОТЕХНІЧНИХ СИСТЕМ ДО ВПЛИВІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ
Мохор Володимир Володимирович,
Цуркан Оксана Володимирівна,
Клименко Тетяна Михайлівна,
Яшенков Вадим Петрович
Цуркан Василь Васильович

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ ЕНЕРГЕТИКИ
Гончар Сергій Феодосійович

АНАЛІЗ ДИНАМІКИ ВИРОБНИЦТВА ЕЛЕКТРОЕНЕРГІЇ ТЕЦ В УМОВАХ НОВОГО РИНКУ ЕЛЕКТРОЕНЕРГІЇ В УКРАЇНІ
Джигун Олена Миколаївна

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОНЦЕПЦІЇ SMARTGRID
Заблоцький Костянтин Васильович,
Малик Святослав Васильович,
Чумаченко Богдан Сергійович
Одарченко Роман Сергійович

МЕТОД ДІАГНОСТУВАННЯ НЕЛІНІЙНИХ ДИНАМІЧНИХ ОБ'ЄКТІВ НА ОСНОВІ НЕПАРАМЕТРИЧНИХ ІНТЕГРАЛЬНИХ МОДЕЛЕЙ
Верлань Анатолій Федорович,
Митько Лідія Олексіївна,

ПОБУДОВА ПРОФІЛІВ ПРОТИДІЇ ЗАГРОЗАМ ЗА ДОПОМОГОЮ ПРИНЦИПУ ОПТИМУМУ Р. БЕЛМАНА В АС 1-3 КЛАСІВ
Потенко Олександр Сергійович

ПРОТИДІЯ ЗОВНІШНИМ АТАКАМ НА ІНФОРМАЦІЙНІ РЕСУРСИ ПІДПРИЄМСТВ ЕНЕРГЕТИКИ
Давиденко Анатолій Миколайович,
Довбня Сергій Якович,
Сулима Олександр Андрійович,
Кіслов Олексій Геннадійович

17.00 – 18.00 ***ПІДВЕДЕННЯ ПІДСУМКІВ РОБОТИ КОНФЕРЕНЦІЇ.***

ПРИЙНЯТТЯ РІШЕНЬ.

ЗАКРИТТЯ КОНФЕРЕНЦІЇ.

Примітка: в регламенті роботи конференції можливі зміни.

ПАНЕЛЬНІ ПРЕЗЕНТАЦІЇ

УДК 621.3::004.056.53

Бакалинський Олександр Олегович,
ІПМЕ ім. Г.Є. Пухова НАН України
канд. техн. наук, старш. наук співроб.
baov@meta.ua

Пахольченко Дмитро Віталійович,
ІПМЕ ім. Г.Є. Пухова НАН України
аспірант
dimapakholchenko@gmail.com

Сапожнік Тетяна Михайлівна,
Адміністрація ДССЗІ України
пров. спеціаліст
tanya.sapojnik@gmail.com

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: Методичні рекомендації можуть бути використані для організації та проведення робіт, що виконують уповноважені органи державної влади, відповідальні за сектор (підсектор) критичної інфраструктури, з метою визначення (ідентифікації) та категоризації об'єктів критичної інфраструктури, що віднесені до сфери його управління.

Abstract: The methodological recommendations can be used for the organization and implementation of works performed by authorized public authorities responsible for the sector (subsector) of critical infrastructure, in order to identify (identify) and categorize critical infrastructure objects that fall within its scope.

Віднесення об'єктів до об'єктів критичної інфраструктури є обов'язковою умовою для формування цілісної системи захисту критичної інфраструктури, зокрема й у контексті захисту її від загроз у кіберпросторі, зважаючи на роль інформаційних технологій у процесах забезпечення функціонування сучасних інфраструктурних об'єктів.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до вирішення завдань із захисту інфраструктурних об'єктів від сучасних загроз на загальнодержавному рівні вироблення критеріїв і визначення порядку віднесення об'єктів до об'єктів

критичної інфраструктури є першим кроком на шляху створення цілісної системи захисту критичної інфраструктури.

Головним критерієм віднесення об'єктів до об'єктів критичної інфраструктури є визнання того, що наслідки порушення сталого функціонування одного або низки об'єктів критичної інфраструктури можуть спричинити надзвичайні ситуації та/або мати негативний вплив на стан екологічної, енергетичної, економічної, фінансової безпеки, на стан обороноздатності держави, порушити систему управління нею. Тому передусім необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій.

Постанова Кабінету Міністрів України [1] визначає механізм і критерії віднесення об'єктів до об'єктів критичної інфраструктури, перелік секторів (підсекторів), основних послуг критичної інфраструктури держави та механізм віднесення об'єктів критичної інфраструктури до однієї з категорій критичності. Зазначену постанову розроблено з урахуванням вимог законодавства ЄС, зокрема:

Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу»;

Директиви Ради 2008/114/ЄС від 08 грудня 2008 року «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту».

Постанова Кабінету Міністрів України [1] затверджує:

Порядок віднесення об'єктів до об'єктів критичної інфраструктури (далі – Порядок);

Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави та уповноважених органів державної влади, визначених відповідальними за відповідний сектор (підсектор) критичної інфраструктури (далі – Перелік);

Методику категоризації об'єктів критичної інфраструктури (далі – Методика).

Порядок встановлює категорії критичності об'єктів критичної інфраструктури, механізм ідентифікації таких об'єктів уповноваженими органами державної влади, відповідальними за сектор (підсектор) критичної інфраструктури та їх категоризацію уповноваженими органами спільно з операторами основних послуг, а також визначає необхідність формування Національного переліку об'єктів критичної інфраструктури та секторальних переліків об'єктів критичної інфраструктури та посадових осіб, які будуть відповідальні за їх формування.

Перелік визначає перелік основних послуг, які надаються об'єктами критичної інфраструктури і є послугами та функціями, що надаються органами державної влади, державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України.

Перелік визначає також сектори та підсектори, об'єкти інфраструктури яких належать до критичної інфраструктури, за умови, що такі об'єкти надають основні послуги, визначені для такого сектору або підсектору. Треба зазначити, що перелік секторів (підсекторів), основних послуг гармонізовано з відповідним переліком, який наведено в Директиві ЄС 2016/1148.

Методика визначає процедуру віднесення об'єктів критичної інфраструктури до певної категорії критичності.

Для визначення категорії об'єкта критичної інфраструктури уповноважені органи у своїх секторах разом з операторами критичної інфраструктури проводять бальну оцінку критичності кожного об'єкта критичної інфраструктури за допомогою форм із секторальними та міжсекторальними критеріями визначення рівня негативного впливу.

Зазначені критерії враховують важливість об'єкта критичної інфраструктури на основі аналізу потенційної шкоди, яку суспільство, навколишнє середовище, економіка та національна безпека держави можуть зазнати внаслідок порушення або припинення функціонування об'єкта інфраструктури. Важливість об'єктів інфраструктури оцінюється за допомогою низки секторальних та міжсекторальних критеріїв.

Сума всіх балів, що отримується під час оцінки об'єкта критичної інфраструктури згідно із секторальними та міжсекторальними критеріями визначення рівня негативного впливу, використовується для розрахунку узагальненої нормованої оцінки рівня критичності об'єкта за формулою та правилом, які наведені у Методиці.

Методика та категорії критичності об'єктів критичної інфраструктури є необхідними механізмами процедури віднесення об'єктів до об'єктів критичної інфраструктури та призначені для мінімізації витрат суб'єктами господарювання на заходи з кіберзахисту та визначення оптимальної моделі віднесення об'єктів до об'єктів критичної інфраструктури, за якої об'єктам критичної інфраструктури різної категорії будуть висуватися вимоги з кіберзахисту, що є адекватними рівню негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України у випадку порушення їх функціонування або збоїв чи переривань у наданні (виконанні) основних послуг.

Зазначені рекомендації можуть бути використані для організації та проведення робіт, які проводяться уповноваженим органом державної влади, відповідальним за сектор (підсектор) критичної інфраструктури, з метою визначення (ідентифікації) та категоризації об'єктів критичної інфраструктури, що віднесені до сфери його управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кабінет Міністрів України. (2020, жовт. 9). Постанова № 1109 «Деякі питання об’єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

УДК 621.3::004.056.53

Бондаренко Степан Юрійович,
Київський інститут інтелектуальної власності та права Національного університету «Одеська юридична академія»,
лаборант кафедри кримінального права та процесу та криміналістики
bondarenko.stephan@ukr.net

ПРАВОВІ ЗАСАДИ ЗДІЙСНЕННЯ КІБЕРБЕЗПЕКИ В ПАЛИВНО-ЕНЕРГЕТИЧНОМУ КОМПЛЕКСІ УКРАЇНИ ЯК ФАКТОР НАДІЙНОСТІ ІСНУВАННЯ РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

Анотація: На теперішній час у багатьох чільних країнах світу вже сформовані загальнодержавні мережі кібернетичної безпеки в сфері ПЕК, які здатні досить швидко акумулювати сили та засоби державних органів і приватного сектору для протидії кіберзагрозам, тим самим забезпечуючи кібербезпеку своїх країн. Тому в роботі ставиться завдання вивчити та проаналізувати питання надійності комп'ютерних підсистем і кібербезпеки сучасних електроенергетичних об'єктів, оснащених цифровими системами моніторингу, управління, релейного захисту і протиаварійної автоматики, які стають дуже актуальними внаслідок новизни проблеми. У більшості публікацій і нормативних документах, присвячених питанням кібербезпеки об'єктів електроенергетики, основним способом її забезпечення бачиться застосування відповідних технічних засобів, аналіз чинних НПА, які забезпечують необхідний захист від різних несанкціонованих дій.

Abstract: Currently, many leading countries of the world have already formed National Cyber Security Networks in the fuel and energy sector, which are able to quickly accumulate the forces and resources of state bodies and the private sector to counter cyber threats, thereby ensuring the cybersecurity of their countries. Therefore, the paper aims to study and analyze the reliability of computer subsystems and cybersecurity of modern electric power facilities equipped with digital monitoring, control, relay protection and emergency automation systems, which are becoming very relevant due to the novelty of the problem. In most publications and regulatory documents devoted to cybersecurity issues of electric power facilities, the main way to ensure it is the use of appropriate technical means, analysis of existing regulations that provide the necessary protection against various unauthorized actions.

На теперішній час у багатьох чільних країнах світу вже сформовані загальнодержавні мережі кібернетичної безпеки в сфері ПЕК, які здатні досить швидко акумулювати сили та засоби державних органів і приватного сектору для проти дії кіберзагрозам, тим самим забезпечуючи кібербезпеку своїх країн.

Тому в роботі ставиться завдання вивчити та проаналізувати питання надійності комп'ютерних підсистем і кібербезпеки сучасних електроенергетичних об'єктів, оснащених цифровими системами моніторингу, управління, релейного захисту і протиаварійної автоматики, які стають дуже актуальними в наслідок новизни проблеми. У більшості публікацій і нормативних документах, присвячених питанням кібербезпеки об'єктів електроенергетики, основним способом її забезпечення бачиться застосування відповідних технічних засобів, аналіз чинних НПА, які забезпечують необхідний захист від різних несанкціонованих дій.

Цифрові технології, мікропроцесорна техніка зі значними обчислювальними ресурсами дозволяють створювати в рамках ПЕК досить складні і досконалі алгоритми управління як в рамках оперативно-диспетчерського управління нормальними режимами, так і протиаварійного управління[5, с. 134]. Це, в поєднанні з новим поколінням первинного обладнання, що має високі експлуатаційні характеристики, і володіє можливостями моніторингу та управління, дозволяє підвищити загальну надійність ПЕК. З іншого боку, цифровим технологіям і мікропроцесорній техніці властива можливість різкої зміни свого функціоналу шляхом перепрограмування, яка, при правильному застосуванні, дозволяє вдосконалювати технології і алгоритми управління без заміни обладнання. Але саме це і є основою нових видів загроз для ПЕК – загроз кібербезпеки.

Кіберзагрози в сфері ринку електроенергії за своєю суттю – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, які справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів; виконання непередбачених функцій, від несанкціонованої передачі інформації третім особам, до виконання шкідливих функцій, тобто по суті часткова або повна відмова системи управління енергооб'єктом [6].В свою чергу нагадаємо, шо ринок електричної енергії - система відносин, що виникають між учасниками ринку під час здійснення купівлі-продажу електричної енергії та/або допоміжних послуг, передачі та розподілу, постачання електричної енергії споживачам.

Альтернативним шляхом є перегляд структурної та функціональної схем цифрових підстанцій таким чином, щоб в принципі виключити багато з потенційно можливих кіберзагроз. Деяке поєднання цифрових, аналогових і механічних пристроїв може бути простим і ефективним засобом забезпечення кібербезпеки, так як істотно знижується масштаб наслідків від кібератаки, причому дане рішення буде повністю зрозумілим електроенергетикам.

Як було зазначено вище, успішність кібератаки залежить не тільки від якості технічних засобів, але і від слабокерованих процесів, таких як лояльність, наявність робочих НПА і людський фактор. Тому одним з найбільш важливих аспектів, який необхідно забезпечувати з позиції

кібербезпеки цифрових підстанцій, є те, щоб успішна кібератака не приводила до пошкодження дорогого або складно ремонтованого обладнання.

Варто зауважити, що національна система кібербезпеки в ПЕК України є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту ПЕК, адже вона належить до об'єктів критичної інформаційної інфраструктури [3].

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки ПЕК, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак на ПЕК та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, спрямованим на ПЕК, кібератакам та мінімізації їх наслідків [7].

Передусім розвиток у сфері боротьби з міжнародною та національною кіберзлочинністю започаткувала Конвенція Ради Європи про кіберзлочинність (Будапешт, листопад 2001 р.). При цьому її було ратифіковано більше ніж півсотнею країн, а серед країн-учасників були й країни, що не є країнами-членами РЄ, як-от США, Канада, Японія, Мексика, Австралія та багато інших. Розглянемо більш детально її основні положення. Зауважимо, що положення Конвенції діють не у всіх країнах, адже відомо, що чотири країни підписали, але не ратифікували її, та є противники підписання – Росія та Китай. Як зазначено у преамбулі, «Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це прописано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва» [1]. Конвенція передбачає впровадження кримінальної відповідальності на національному рівні за такі групи злочинів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями); комп'ютерні правопорушення (підробка та шахрайство із застосуванням комп'ютерів).

Невдовзі Генеральна Асамблея (ГА) ООН прийняла Резолюцію, зміст якої був пов'язаний саме з питаннями забезпечення кібербезпеки у сфері електроенергетики [3]. Зокрема, у Резолюції йшлося про конкретні заходи: про необхідність створення системи глобальної культури кібербезпеки. ГА ООН пропонувала державам-членам відповідно віднестися до створення глобальної культури кібербезпеки, зокрема, в рамках їхніх зусиль щодо розвитку у своїх суспільствах культури кібербезпеки при застосуванні та використанні інформаційних технологій. В Резолюції відзначалося також важливе значення міжнародного співробітництва для досягнення кібербезпеки шляхом підтримки національних зусиль, спрямованих на укріплення людського потенціалу, розширення можливостей в плані навчання і зайнятості, покращення державних послуг і підвищення якості життя за рахунок використання передових, надійних та безпечних інформаційно-комунікаційних технологій (ІКТ) і мереж, а також сприяння забезпеченню загального доступу [9]. Це сприяло прийняттю в наступному році (2003 р.) Женевської декларації [8], в якій зазначалася необхідність прискорення впровадження глобальної культури кібербезпеки в співробітництві з усіма зацікавленими сторонами і компетентними міжнародними органами. Такі зусилля мали спиратися на широке міжнародне співробітництво. У рамках глобальної культури кібербезпеки вважалося доцільним підвищувати безпеку і забезпечувати захист даних і недоторканності приватного життя (п. 35).

Практичною реалізацією Резолюції стало прийняття Туніської програми для інформаційного суспільства (п. 39), де наголошувалося таке: «Ми прагнемо підвищувати довіру і безпеку при використанні ІКТ шляхом зміцнення основи для довіри. Ми знову підтверджуємо необхідність далі просувати, розвивати і впроваджувати у співробітництві з усіма заінтересованими сторонами глобальну культуру кібербезпеки, як це викладено в резолюції 57/239 ГА ООН та інших відповідних регіональних основоположних документах. В ЄС у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security), яке функціонує й по теперішній час, спершу надаючи настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібербезпеки, виступаючи центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою [6]. Завдяки цьому кроку у більшості країн-членів було створено національні стратегії кібербезпеки та національні план із захисту інформаційної інфраструктури. Знаковою подією сталося ухвалення в рамках ЄС (2013 р.) Стратегії кібербезпеки, метою якої можна вважати

відкритий, надійний і безпечний кіберпростір у сфері електроенергетики. Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в електроенергетичному комплексі, розробляє та затверджує правила про безпеку постачання електричної енергії, які є обов'язковими для виконання всіма учасниками ринку.

Варто нагадати, що в 2016 році президентом був підписаний Указ Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", в якому містився ряд заходів, присвячений протидії та боротьбі із кібератаками на ПЕК України, зокрема було сказано, що метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [6].

Відповідно до Директиви, у разі виникнення несподіваної кризи на ринку електроенергії або у разі виникнення загрози фізичній безпеці, безпеці людей, обладнанню або об'єктам чи загрози цілісності системи, держави-члени можуть тимчасово вживати необхідних заходів безпеки. Застосування таких заходів повинно створювати якомога найменші порушення у функціонуванні внутрішнього ринку, і вони не повинні бути ширшими за масштабом, ніж необхідно для усунення труднощів, що виникли.

Відповідні держави-члени негайно повідомляють про ці заходи інші держави-члени та Комісію, які можуть прийняти рішення про те, що зазначені держави-члени повинні змінити або припинити застосування таких заходів настільки, наскільки вони викривляють конкуренцію та негативно впливають на торгівлю, що суперечить спільним інтересам[1].

Для досягнення цієї мети необхідними є: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством у сфері ПЕК, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також енергетичної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична енергетична інфраструктура).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Директива 2003/54/ЄС Європейського Парламенту та Ради Європейського Союзу стосовно спільних правил для внутрішнього ринку електроенергії від 26.03.2003 № 994_571. URL: https://zakon.rada.gov.ua/laws/show/994_571#Text (дата звернення: 24.04.2021).

2. Договір про заснування Енергетичного Співтовариства від 25.10.2005 № 994_926 URL: https://zakon.rada.gov.ua/laws/show/994_926#Text (дата звернення: 24.04.2021).
3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 № 994_326 URL: https://zakon.rada.gov.ua/ laws/show/994_326#Text (дата звернення: 24.04.2021).
4. Конвенція про кіберзлочинність від 23.11.2001№ 994_575 URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 24.04.2021).
5. Кириленко О. В., Сегеда М. С., Буткевич О. Ф., Мазур Т. А., Математичне моделювання в електроенергетиці: підручник; за ред. М. С. Сегеди. Львів : Вид-во Львів. політехніки, 2013, 608 с.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/ 2163-19#n 169 (дата звернення: 24.04.2021).
7. Про ринок електричної енергії: Закон України від 13.04.2017 № 2019-VIII URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text (дата звернення: 24.04.2021).
8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/ show/96/2016#n11 (дата звернення: 24.04.2021).
9. Про схвалення Енергетичної стратегії України на період до 2035 року “Безпека, енергоефективність, конкурентоспроможність”: Розпорядження КМУ від 18.08.2017 № 605-2017-р. URL: https://zakon.rada.gov.ua/ laws/show/ 605-2017-р#Text (дата звернення: 24.04.2021).
10. УГОДА ПРО АСОЦІАЦІЮ між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014 № 984_011 URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 24.04.2021).

УДК 621.3::004.056.53

Одарченко Роман Сергійович,
Національний авіаційний університет,
д.т.н., доцент, завідувач кафедри
odarchenko.r.s@ukr.net

Дика Тетяна Василівна
Національний авіаційний університет,Київ,
студент
tanya_dyka@ukr.net

ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В МЕРЕЖАХ 5G ДЛЯ КОНЦЕПЦІЇ SMART GRID

Abstract: Today, in the energy sector, we are seeing an increasing number of used energy equipment and face new challenges such as network reliability, increasing network complexity and efficiency. One of the trends in the development of world energy is the creation of the concept and implementation of Smart Grid technologies. This article discusses the concept of Smart Grid as an appropriate way to address these new challenges.

Анотація: Сьогодні в енергетичній галузі ми спостерігаємо все більшу кількість використовуваного енергетичного обладнання та стикаємось із новими проблемами, такими як надійність мережі, зростаюча складність мережі та ефективність використання. Однією з тенденцій розвитку світової енергетики є створення концепції та впровадження технологій SmartGrid.В даній статті розглядається концепція SmartGrid, як відповідний спосіб вирішення цих нових викликів.

З швидким розвитком збору інформації про енергоспоживання, автоматизації розподілу, розподіленого доступу до енергії, обслуговування електромобілів та двонаправленої взаємодії з користувачем, швидко зростають вимоги до зв'язку різних пристроїв електромереж, терміналів та споживачів. Нові стабільні, надійні та ефективні комунікаційні технології та системи в режимі реального часу, придатні для електроенергетики, терміново потрібні для моніторингу стану та збору інформації про інтелектуальні пристрої та запуску нових режимів роботи та режимів енергообслуговування.

Технологія 4G змінює життя, але 5G змінює суспільство. Вертикальні галузі, представлені електромережами, закінчать цифрову трансформацію в епоху 5G.

Мережі 5G забезпечать кращий досвід пропускної здатності та забезпечать вертикальні галузі. В епоху 5G різноманітні вертикальні галузеві

додатки принесуть більше широкі вимоги до мобільних мереж. Надзвичайно висока пропускна здатність, наднизька затримка та надмірна кількість з'єднань змінять режими роботи та роботи основних служб у вертикальних галузях, покращуючи операційну ефективність та інтелектуальність прийняття рішень традиційних вертикальних галузей. Нарізання мережі виникає з цього фону. Він забезпечує гнучкі та настроюванні можливості, які дозволяють будувати спеціальні мережі для різних додатків.

SmartGrid – це модернізовані мережі електропостачання, які використовують інформаційні і комунікаційні мережі і технології для збору інформації про енерговиробництві і енергоспоживанні, що дозволяє автоматично підвищувати ефективність, надійність, економічну вигоду, а також стійкість виробництва і розподілу електроенергії. SmartGrid побудована на основі інтегрованих та високошвидкісних двонаправлених мереж зв'язку. Передові технології використовуються для побудови надійних, безпечних, економічних, ефективних та екологічно чистих електромереж. До цих технологій належать технології зондування, вимірювання, приладів та систем підтримки прийняття рішень, а також методи контролю.

Фактично - це сильно модернізовані мережі з використанням останніх IT-рішень. У мережі інтегровані комунікаційні технології, а також технології для збору інформації про виробництво, передачу та споживанні електроенергії, ефективного контролю і управління мережею. SmartGrid це основа SmartCity – розумного і безпечного міста, про життя в якому мріє кожна сучасна людина [1].

Постійний попит на електроенергію є критично важливим питанням, яке потребує значної уваги в даний час ери інтелектуальної мережі. Для досягнення більш розподіленого виробництва та накопичення енергії, нові режими технологій бездротового зв'язку повинні бути включені до мережі. Розумні мережі працюють з малими розподіленими джерелами генерації, на відміну від звичайної мережі, яка спирається на велику централізовану генерацію. Основною метою звичайної електромережі є зміна виробництва електроенергії відповідно до необхідних потреб у електроенергії. Це вимагає переходу розумних мереж до регулювання попиту відповідно до наявного покоління. Отже, необхідні високозахищені комунікації як для зондування, так і для управління у всіх засобах взаємодії між стороною передачі та розподілу.

SmartGrid – це екосистема операційних технологій, що включає пристрої зв'язку ліній електропередач, контроль, інтелектуальні електронні пристрої, системи збору даних (SCADA) та системи управління енергією. Поряд із цими специфічними технологіями є загальні проблеми для кібербезпеки, включаючи системи організаційних комунікацій та електронну інформацію, з точки зору безпеки інтелектуальна мережа має велику

поверхню атаки. Ключовим викликом для сектору кібербезпеки була відсутність стандартної довідкової архітектури, а відсутність механізмів випуску перешкоджали зростанню сектору.

Переваги SmartGrid значною мірою походять від їх підключення, що надає традиційно скрипучій енергетичній мережі значну гнучкість. Здатність інтелектуальної мережі використовувати потоки даних також сприяє їх вразливості, неетичні або зловмисні актори можуть розпочати атаку на інфраструктуру Інтернету речей, яка становить сітку, що, в свою чергу, може не врівноважувати навантаження непередбачуваним чином. Збільшення використання мікросіток робить вплив цих атак більш локальним за своєю суттю, що є вдосконаленням централізованої інфраструктури минулого, проте недостатньо лише обмежити шкоду від потенційної атаки, і технічний сектор придумує деякі інноваційні способи сприяти покращенню безпеки мережі [2].

Хоча перехід до стійкої енергетики може допомогти забезпечити краще майбутнє для планети та зменшити вуглецевий слід, SmartGrid, що підживлюється пов'язаними речами, мікромережами тощо - створює двосторонні ризиковані потоки даних, які додають складності вже застарілій енергії сітка.Нові джерела енергії та методи розподілу, включаючи сонячні панелі, генератори та мікромережі, обіцяють стримувати кліматичні зміни та допомагати споживачам контролювати споживання енергії під час пікового використання [3].

Технології розумних мереж децентралізують доставку енергії, дозволяючи людям швидко підключатися до більшої мережі та відключатися від неї, а також виробляти та доставляти електроенергію на місцевому рівні. На відміну від сучасної масивної централізованої мережі, атака або порушення мікромережі, наприклад, не впливає на всю систему. Але розумні мережі також створюють нестабільний попит на більшу мережу та представляють двосторонній трафік до цієї мережі, створюючи ризики для безпеки. І ці ризики посилюються старінням інфраструктури енергомереж.

Зростає децентралізоване виробництво енергії, компоненти якої використовуються в інтелектуальних мережах. Міжнародне енергетичне агентство очікує, що потужність відновлюваної енергії збільшиться на 50% до 2024 року, а сонячна фотоелектрика та прибережний вітер становлять левову частку цього збільшення [4].

Потенційним засобом від цих ризиків є поява машинного навчання для допомоги IT-професіоналам. Засоби машинного навчання можуть виявляти загрози серед величезної кількості сповіщень, які можуть отримати IT-професіонали. Інструменти кібербезпеки з підтримкою штучного інтелекту стають ключовими для кращої безпеки, оскільки люди просто не можуть встигати з усією інформацією.

Робочою групою CIGRE були сформульовані основні вимоги до забезпечення кібербезпеки в енергетиці:

управління доступом – для захисту від несанкціонованого доступу до пристрою або інформації;

управління використанням – для захисту від несанкціонованого оперування або використання інформації;

цілісність даних – для захисту від несанкціонованого зміни;

конфіденційність даних – для захисту від несанкціонованого доступу;

обмеження потоку даних – для захисту від публікації інформації на несанкціонованих джерелах;

своєчасний відповідь на подію, моніторинг і протоколювання пов'язаних з безпекою подій і прийняття своєчасних заходів по ліквідації наслідків в відповідальних завданнях і в критичних ситуаціях з безпеки;

доступність мережевого ресурсу – для захисту від атак «відмова в обслуговуванні [5].

Серед основних завдань забезпечення кібернетичної безпеки в SmartGrid виділяють цілісність, доступність і конфіденційність, причому головним завданням є забезпечення доступності, при одночасному забезпеченні цілісності і конфіденційності. Це означає, що суб'єкти, які мають право на доступ до інформації, повинні мати можливість реалізувати своє право безперешкодно, але в той же час система повинна бути безпечною і забезпечувати захист від кібернетичних загроз.

Кібернетична безпека може бути порушена при наступних обставинах:

Незахищеність інформаційного ресурсу на носії (відсутність якісної криптографічного захисту)

Незахищеність каналів передачі інформації

Незахищеність носія інформації або пристроїв передачі інформації (наприклад, невідповідний контроль доступу в приміщення) [5].

SmartGridє основою розумної енергетики та важлива для сприяння економічній та соціальній координації та сталому розвитку. Він забезпечує міцну підтримку кращого життя, чистішого навколишнього середовища та більш гармонійного суспільства. Це допомагає вдосконалити управління енергією та дозволяє трансформувати чисту та електричну енергію.

Очевидно, що успішна реалізація цієї концепції вимагає підвищеної уваги до проблем, як сучасних інформаційних технологій (IT), так і до проблем кібербезпеки, оскільки ускладнення сучасних інформаційно телекомунікаційних технологій збільшує вразливість створюваних систем.

SmartGrid відкриває двері для нових додатків із далекосяжним соціальним та економічним впливом. Забезпечуючи потужність для безпечної інтеграції більше відновлюваних джерел енергії, електричних транспортних засобів та розподілених генераторів в мережу, а також забезпечуючи енергію

більш ефективно та надійно завдяки реагуванню на попит та всебічним можливостям контролю та моніторингу, інтелектуальні мережі дозволяють споживачам мати більший контроль над своєю електроенергією споживання, отже, сприяючи їхній участі на ринку електроенергії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fang X., Misra S., Xue G., Yang D. Smart grid – the new and improved power grid: a survey. – IEEE Communications Surveys & Tutorials, Vol.14, №4, 2012, p. 944-980.
2. Cyber Security in Smart Grids. URL: https: //www.greenrecruitmentcompany.com/ blog/2020/09/cyber-security-in-smart-grids.
3. Smart Grids. Smart Specialization Platform. European Commission. URL: Mode of access: https://s3platform.jrc. ec.europa.eu/smart-grids.
4. Smart Grid Security Will Get Boost from AI and 5G - [Electron resource] - Mode of access: https://www.iotworldtoday.com/2020/07/14/smart-grid-security-will-get-boost-from-ai-and-5g/
5. Массель Л.В. Проблема построения интеллектуальных и программных компонентов SmartGrid и подход к ее решению на основе агентной технологии. Материалы XL Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». Гурзуф, 2012. С.22–25.

УДК 621.3+620.9

Владимирский Александр Альбертович,
ИПМЭ им. Г.Е. Пухова НАН Украины,
ведущий научный сотрудник
av1000000@ukr.net

Владимирский Игорь Альбертович,
ИПМЭ им. Г.Е. Пухова НАН Украины,
старший научный сотрудник

Криворучко Игорь Петрович,
ИПМЭ им. Г.Е. Пухова НАН Украины, аспирант
uhmi_igorkr@ukr.net

Анфимова Галина Викторовна,
ИПМЭ им. Г.Е. Пухова НАН Украины,
инженер
anfimova77@ukr.net

РАЗРАБОТКА СТЕНДА ДЛЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ ИСКРОБЕЗОПАСНЫХ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ

Анотація: Представлений стенд для випробувань іскробезпечних електричних ланцюгів відповідно до вимог ДСТУ EN 60079-11:2017 Вибухонебезпечні середовища. Частина 11. Вид вибухозахисту іскробезпечне коло “i”. Формування вибухонебезпечних сумішей здійснюється відповідно до парціального тиску газів.

Abstract: Test stand for electrical circuits in accordance with the requirements EN 60079-11:2012 Explosive atmospheres – Part 11: Equipment protection by intrinsic safety “i” presented. The formation of explosive mixtures is carried out in accordance with the partial pressures of the gases.

Возможность применения во взрывоопасных средах электрических цепей, подвергающихся воздействию взрывоопасной среды устанавливается требованиями ДСТУ ЕН 60079-11:2017 [1]. В частности, в этом стандарте определен порядок проведения испытаний на искро- и взрывобезопасность различного оборудования, состав тестовых взрывоопасных смесей газов и конструкция искроформирующего механизма.

Разработка стенда “ИСКРА” для проведения испытаний искробезопасных электрических цепей выполнена совместно с ООО “ТЕСКО” и базируется на имеющейся в лаборатории ООО “ТЕСКО” взрывной камере с искроформирующим механизмом.

Структура разработанного стенда представлена на рис.1. Основной конструктивный модуль – взрывная камера с искроформирующим механизмом.

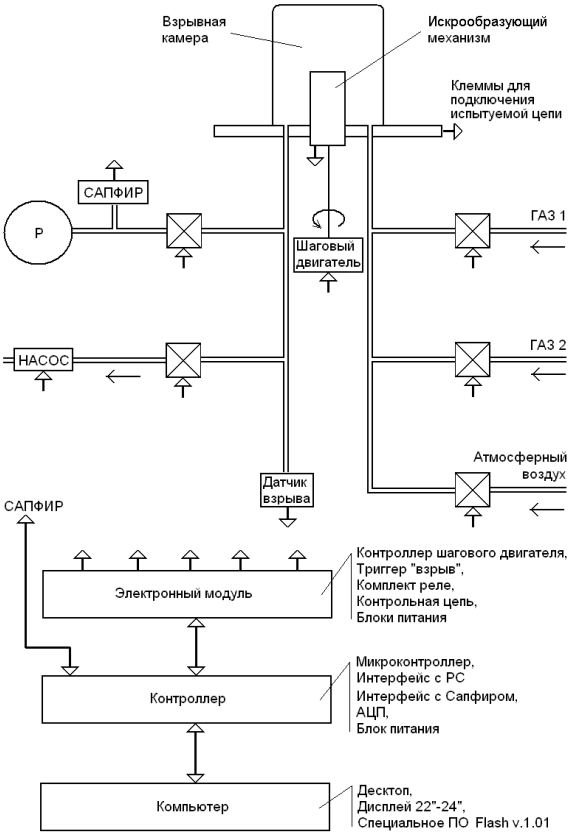

Рисунок 1 – Структура стенда

В состав стенда входят электромагнитные клапаны для управления потоками газов, вакуумный насос, датчик разряжения САПФИР электронный блок, контроллер и компьютер. Контроллер принимает команды от компьютера, передает данные о состоянии стенда в компьютер, содержит интерфейс с датчиком САПФИР и АЦП, управляет ресурсами стенда через электронный блок. Электронный блок -набор узлов, выполненных в виде плат и блоков. В его состав входят драйвер шагового двигателя

(обеспечивает его вращение с требуемой скоростью), триггер “взрыв” (устанавливается в состояние “1” сигналом с датчика взрыва, сбрасывается в состояние “0” и опрашивается программно), набор управляющих клапанами реле, контрольная цепь с реле управления (для выбора значения тока), блоки питания и пр. PC–совместимый компьютер со специальным программным обеспечением Flash v.1.01 предоставляет интерфейс взаимодействия с оператором, обеспечивает индикацию состояния стенда, набор низкоуровневых команд управления всеми ресурсами стенда (для тестирования, проверки, отладки), набор стандартных режимов работы с отображением текущих этапов.

Газы для формирования смесей подаются в стенд по шлангам (5-10 м) из герметичных резиновых подушек. Давление газов близко к атмосферному. Размещение подушек – удаленное.

Управление всеми режимами работы стенда осуществляется с клавиатуры компьютера. Состояние основных компонентов стенда отображается на дисплее в виде мнемосхемы и необходимых цифровых параметров. Оператор выбирает режим работы, указывает необходимые параметры. Далее испытания проводятся автоматически под управлением программного обеспечения, установленного на компьютере.

- Вентиляция камеры - откачка воздуха из камеры и последующее заполнение ее атмосферным воздухом.
- Автоматическая подготовка 2-х и 3-х компонентных смесей в пропорциях, предусмотренных стандартом [1] или задаваемых оператором. В качестве горючего газа в различных режимах могут применяться метан, пропан, этилен и водород (подаются на патрубок “ГАЗ 1”). В некоторых смесях применяется кислород (подается на патрубок “ГАЗ 2”). В большинстве смесей применяется атмосферный воздух. Формирование взрывоопасных смесей осуществляется в соответствии с парциальным давлением газов.
- Измерение разряжения в камере осуществляется с помощью датчика разряжения типа САПФИР, данные отображаются в цифровом виде на экране дисплея. На время включения искрообразующего механизма средства измерения разряжения отключаются от камеры для исключения их повреждения взрывной волной.
- Автоматическое испытание цепей:
  - постоянного тока – 400 оборотов вала искрообразующего механизма по 200 оборотов каждой полярности;
  - переменного тока – 1000 оборотов;
  - емкостных цепей – 400 оборотов по 200 оборотов каждой полярности (если время перезарядки 20 мс недостаточно, то

снижается скорость вращения). Если регистрируется взрыв в камере, испытания автоматически прекращаются.

- Автоматическое формирование подробного протокола испытаний, с указанием даты и времени включения установки, начала испытаний, заданных оператором параметров испытаний, всех важных событий с привязкой к системным часам – срабатывание клапанов, достигнутые уровни разряжения, включение двигателя, обороты искроформирующего механизма, регистрация взрыва и счетчики оборотов на момент взрыва и т.д. и т.п. Фрагменты этого протокола могут включаться в экспертные заключения по результатам испытаний конкретных образцов цепей в качестве фактического материала.
- Для проверки чувствительности искроформирующего механизма и соответствия газовой смеси предъявляемым требованиям предусмотрен тестовый подрыв сформированной смеси газов в камере с помощью контрольной цепи 24 В, 95 мГн и калиброванного значения тока в соответствие с выбранным типом испытаний. Взрыв должен быть зарегистрирован за 440 оборотов вала искроформирующего механизма.
- Калибровка искроформирующего механизма – 20000 оборотов, цепь 95 мГн, 24 В, 100 мА, атмосферный воздух. Калибровка необходима при обнаружении проблем с чувствительностью искроформирующего механизма или после его ремонта.
- Для отладки и для поиска возможных неисправностей стенда предусматривается возможность ручного управления всеми ресурсами из специального режима (управление двигателем, насосом, клапанами).

Задаваемые параметры испытаний.

- ток контрольной цепи, мА: 110-111; 100-101; 73-74; 66-67; 65-66; 43-44; 30-30,5; 20-21; 15-15,3.
- скорость вращения держателя электродов искроформирующего механизма, оборотов/мин - 80, 40, 20, 10. Допуск -0% +10%. Двигатель искроформирующего механизма шаговый, управление цифровое.
- смеси приготавливаются с точностью не ниже 0,25 % или с точностью, которая указана в стандарте [1].

Калибровка метрологических параметров осуществляется в соответствии с методикой [2].

В связи с тем, что предусматривается возможность работы с кислородом, применяется вакуумный насос, в котором исключен контакт газовой смеси с маслом. Дополнительных требований по взрывобезопасности, по герметичности и пр. к стенду не предъявляется. Предполагается применение стенда по предназначению в хорошо проветриваемом сухом помещении достаточного объема.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. ДСТУ ЕН 60079-11:2017 (EN 60079-11:2012, IDT; IEC 60079-11:2011, IDT). ВИБУХОНЕБЕЗПЕЧНІ СЕРЕДОВИЩА. Частина 11. Вид вибухозахисту іскробезпечне електричне коло “і”. Київ. ДП “УкрНДНЦ”. 2019. – 118с. Чинний з 2019.01.01
2. МИ 1997-89 Рекомендация. ГСИ. Преобразователи давления измерительные. Методика поверки. Москва. 1989. -19с. Дата введения 01.11.89

УДК 621.3

Владимирский Александр Альбертович,
ИПМЭ им. Г.Е. Пухова НАН Украины,
ведущий научный сотрудник,
av1000000@ukr.net

Владимирский Игорь Альбертович,
ИПМЭ им. Г.Е. Пухова НАН Украины,
старший научный сотрудник,
leakdetect@rambler.ru

Криворучко Игорь Петрович,
ИПМЭ им. Г.Е. Пухова НАН Украины,
аспирант,
uhmi_igorkr@ukr.net.

РЕГИСТРАЦИЯ СОПУТСТВУЮЩИХ СОБЫТИЙ В ИЗМЕРИТЕЛЕ ПАРАМЕТРОВ ДВИЖЕНИЯ

Анотація: Представлено апаратно-програмний комплект модернізації вимірювача кінематичних і динамічних параметрів ліфтів, який дозволяє здійснювати синхронну реєстрацію спрацьовування контактних датчиків і параметрів руху різних механізмів. Забезпечується коректне заміщення контактних датчиків, що входять в "ланцюг безпеки".

Abstract: A hardware and software kit for the modernization of the meter of the kinematic and dynamic parameters of elevators is presented. The kit allows for synchronous registration of the triggering of contact sensors and the parameters of movement of various mechanisms. The correct replacement of the contact sensors, which are included in the “safety circuit”, is ensured.

Разработанные в ИПМЭ им. Г.Е, Пухова НАН Украины измерители кинематических и динамических параметров лифтов ИКПЛ-М3 (далее – измерители) получили достаточно широкое распространение в лифтостроительной отрасли, ими оснащены большинство экспертно-технических центров Украины и ряд лифтостроительных предприятий [1, 2]. Институт осуществляет гарантийное обслуживание и пожизненное сопровождение измерителей, совершенствование их програмного обеспечения с целью расширения функциональных возможностей и периодическую калибровку метрологических характеристик [3]. Применение указанных измерителей при экспертизе технического состояния лифтов и эскалаторов позволяет в полной мере контролировать соответствие их параметров движения требованиям современных нормативних документов в области безопасности [4, 5].

В святи с расширением сферы применения измерителей возникла необходимость в дополнение к параметрам движения (путь, скорость и ускорение линейного или вращательного движения) осуществлять синхронную регистрацию сопутствующих событий. В качестве таких событий подразумевается факт срабатывания каких-либо контактних датчиков (концевые выключатели дверей, датчики положения кабины вдоль шахты лифта и пр.). При этом указанные контактные датчики в большинстве случав являются неотъемлемой частью схемы управления лифта, могут входить в, так называемую, "цепь безопасности лифта". Включение лифта с нарушенной "цепью безопасности" запрещается по правилам Техники безопасности. Величина напряжения, коммутируемого контактными датчиками различных лифтов, может находиться в диапазоне от 5 в до 380 В постоянного или переменного тока, что создает дополнительные сложности.

По заказу ТОВ "ТЕСКО" (орган по оценке соответствия ООО "ТЕСКО", испытательная лаборатория "ТЕСКО") группой технической диагностики разработан модуль КМ3 и программное обеспечение Лифт-3.05-km3, которые предназначены для доукомплектаци существующего парка измерителей ИКПЛ-М3. Дополнительные функциональные возможности заключаются в следующем:

– возможность регистрации срабатывания контактных датчиков синхронно с регистрацией параметров движения,

– для восстановления "цепи безопасности" исследуемого объекта контактный датчик заменяется контактами подменного реле.

Блок КМ3 включается в разрыв кабеля между измерительным преобразователем и ноутбуком и поддерживает обычный темп передачи данных о параметрах движения исследуемого объекта от измерительного преобразователя в ноутбук.

Схема применения КМ 3 для регистрации состояния контактного датчика, входящего в цепь безопасности, представлена на рисунке.

Контактный датчик (п. 1) отключается от цепи безопасности (п. 2) и подключается к блоку КМ 3. В цепь безопасности вместо контактного датчика (в п. 2) включаются контакты электромагнитного реле Р блока КМ3, которое срабатывает при замыкании контактного датчика. Таким образом, с помощью контактов подменного реле Р восстанавливается цепь безопасности лифта, из которой на время контрольных измерений изъяли контактный датчик. При этом обеспечиваются гальваническая развязка измерителя от цепи безопасности и совместимость со всеми возможными вариантами ее электропитания. Факт срабатывания (замыкания-размыкания) контактного датчика регистрируется для последующего контроля блоком КМ3, в поток данных между измерительным преобразователем ИКПЛ-М3 и ноутбуком встраивается соответствующий маркер контролируемых событий.

В программном обеспечении предусмотрены форматы формирования и анализа записей. Имеется возможность отслеживать значения параметров движения в различные моменты времени, исследовать последовательность событий и измерять интервалы времени.

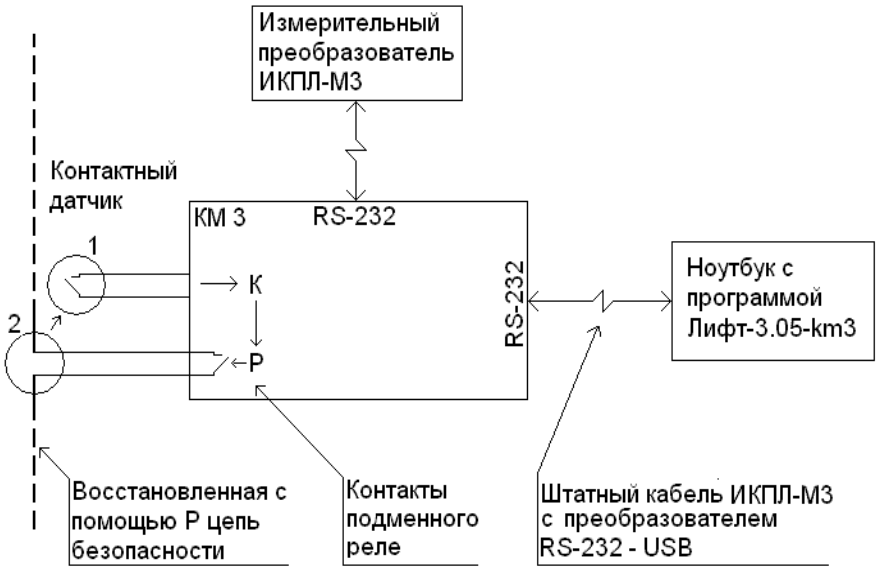

Рисунок 1 – Схема применения КМ3

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Владимирский А. А. Разработка средств контроля параметров движения подъемно-транспортного оборудования. Подъемные сооружения. Специальная техника. 2013. № 2. С. 21-24.
2. Владимирский О. А. Комп'ютерна програма “Измеритель кинематических и динамических параметров лифтов”, версия В3.05” (“Lift V3.05”). Свідоцтво про реєстрацію авторського права на твір №60780. Україна. 23.07.2015р. ІПМЕ НАН України.
3. Анфімова Г. В. Досвід створення системи метрологічного та технічного супроводу впроваджених засобів технічної діагностики енергетичного та енергоємного обладнання. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», ІПМЕ ім. Г.Е.Пухова НАН України, Київ, 20.12.2019р. С. 35-36.
4. Правила будови і безпечної експлуатації ліфтів = Правила устройства и безопасной эксплуатации лифтов: НПАОП 0.00-1.02-08: Затв.

01.09.2008 № 190 / Державний комітет України з промислової безпеки, охорони праці та гірничого нагляду. Харків : Вид-во “Індустрія”. “Основа”. 2008. 192 с.

5. ДСТУ EN 81-50:2015 Норми безпеки щодо конструкції та експлуатації ліфтів. Випробування та перевіряння. Частина 50. Норми проектування, розрахування, випробування та перевіряння компонентів ліфта (EN 81-50:2014, IDT) – [Чинний від 2018-01-01]. – Київ, 2016. 22 с.

УДК 621.3::004.056.53

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
ст. наук. співр., д-р техн. наук,
hilgurt@ipme.kiev.ua

ПІДХОДИ ДО ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ АТАК НА ПРОТОКОЛИ ЦИФРОВИХ ЕЛЕКТРИЧНИХ ПІДСТАНЦІЙ

Анотація: Засоби цифровізації, такі як стандарт МЕК-61850, надають багато переваг системам промислової автоматизації, додають нові протоколи та функціональні можливості. На жаль, нова якість зв'язків в таких системах призводить до збільшення загроз безпеці та появи нових кібератак, які можуть спричинити катастрофічні наслідки. Для їх захисту необхідно адаптувати відомі системи виявлення вторгнень. В даній роботі досліджуються особливості цифрових підстанції на основі стандарту МЕК-61850 та відповідних протоколів. Аналізуються прийнятні підходи, архітектури та методи виявлення вторгнень. Розглядаються можливості використання реконфігуровних обчислювальних засобів.

Abstract: Digitalization means, such as the IEC-61850 standard, introduce many benefits for industrial automation systems, including new protocols and functionalities. Unfortunately, the increased connectivity in such systems has exposed them to a wide range of cyberattacks and security threats that can cause catastrophic consequences. Consequently, the adapting of known IDSs is required for their protecting. In this work, digital substations based on the IEC-61850 standard and correspondent protocols are investigated. Acceptable intrusion detection approaches, architectures and methods are analyzed. Possibilities of using reconfigurable computing facilities are examined.

Застосування IT-підходів при побудові кіберфізичних систем (цифровізованих АСУ ТП і систем автоматики) разом з перевагами привносить і такі недоліки, як проблеми інформаційної безпеки.

Якщо автоматизуються об'єкти критичної інфраструктури, до якої належить енергетична галузь, наслідки від реалізації кіберзагроз можуть бути більш важкими в порівнянні з традиційними галузями застосування інформаційних технологій [1–5].

Як визнають дослідники, ситуація в області інформаційного захисту кіберфізичних систем поки що залишається на початковому етапі. Отже, питання аналізу особливостей та підвищення ефективності вирішення завдань інформаційної безпеки щодо автоматизованих і автоматичних систем управління на виробництві, зокрема, в енергетиці є актуальними та злободенними.

У даній роботі досліджені проблеми ефективного вирішення задач інформаційної безпеки систем автоматизації стосовно цифрових підстанцій (ЦПС). При цьому головну увагу приділено протоколам обміну даними, що використовуються, та особливостям їх захисту від зовнішніх атак. Також розглянуті питання застосування апаратного прискорення з використанням реконфігуровних засобів.

1. Стандарт МЕК 61850

Електричні підстанції є одними з найчисленніших об'єктів енергетики [6]. Складнощі, що виникають при переводі їх обладнання на цифрову елементну базу, пов'язані в першу чергу зі стандартизацією. Якщо життєвий цикл силового обладнання, такого як трансформатори, комутаційні апарати роз'єднувачі, тощо складає близько 40 років, то керуючі системи оновлюються в середньому кожні 15 років. В результаті змушені спільно взаємодіяти пристрої декількох поколінь, не сумісні між собою.

Для вирішення даної проблеми було створено стандарт МЕК 61850 (англ. IEC 61850) «Мережі та системи зв'язку на підстанціях» [7]. Головна ідея документа – розробити єдині специфікації, які дозволили б, з одного боку, захистити фінансові вкладення в енергетичне обладнання, з іншого – використовувати передові обчислювальні та комунікаційні технології. Документ, перша редакція якого з'явилася ще в 2003 році, містить цілу низку стандартів (див. таблицю).

У поточній версії комплекс нормативів МЕК 61850 є доволі об'ємним документом, що складається з десятка підрозділів, продовжуючи розвиватися, й на сьогоднішній день у фахівців асоціюється з такими поняттями як "цифрова підстанція" та Smart Grid, що між іншим, обумовлює використання цифрових вимірювальних приладів замість аналогових, а також використання інтелектуальних електронних пристроїв, які в англомовній літературі позначаються скороченням IED (Intelligent Electronic Devices).

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів [8]:

– станційний (Station Level) – найвищій рівень;

– рівень приєднання (Bay Level);

– рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень.

Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв [9].

Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

Станційний рівень забезпечує людино-машинний інтерфейс з персоналом, який керує підстанцією, і включає системи моніторингу, Автоматизовані робочі місця (АРМ) та SCADA-системи.

Таблиця

Секція	Назва
МЕК 61850-1	Вступ і загальний огляд
МЕК 61850-2	Глосарій
МЕК 61850-3	Основні вимоги
МЕК 61850-4	Управління системою і проектуванням
МЕК 61850-5	Вимоги зв'язку до функцій і моделей пристроїв
МЕК 61850-6	Мова опису конфігурації зв'язку між мікропроцесорними електронними пристроями підстанцій
МЕК 61850-7	Основна структура зв'язку для обладнання підстанції та лінії живлення (4 частини)
МЕК 61850-8-1	Опис передачі даних по протоколу MMS
МЕК 61850-9-1	Вибіркові значення по послідовному ненаправленого багаточочковому каналу передачі даних типу точка-точка
МЕК 61850-9-2	Вибіркові значення по ISO / IEC 8802-3
МЕК 61850-10	Перевірка на сумісність

Рівень приєднання в режимі реального часу виконує всі автоматичні функції з керування станцією, що не потребують втручання людини, включаючи функції контролю, вимірювання, синхронізації часу та захисту (аварійної автоматики). Реалізують ці функції інтелектуальні пристрої IED, які пов'язують станційний рівень з польовим, надаючи пристроям рівня станції можливість зчитувати та записувати інформацію з пристроїв IED.

Рівень процесу включає як звичайне (застаріле), так і сучасне електричне обладнання (рубильники, пускачі, вимірювальні трансформатори тощо). Сучасні кінцеві пристрої здатні передавати інформацію через Ethernet. Звичайне ж обладнання нові стандарти передачі даних не підтримує, тому для зв'язку з ним на рівні процесу використовують додаткові компоненти, такі як Merging Units (MU) та Intelligent Terminals (IT) [10].

На додаток до традиційних протоколів, таких як FTP та HTTP, стандарт IEC 61850 вводить нові протоколи, а саме:

– MMS (Manufacturing Message Specification) – для зв'язку IED зі станційним рівнем;

– GOOSE (Generic Object Oriented Substation Events) – для зв'язку IED між собою;

– SV (Sampled Values) – для зв'язку між IED та MU.

Строго кажучи, MMS є не протоколом, а специфікацією, що описує інформаційну модель пристроїв та даних рівня приєднання. Але, оскільки сервіс, що використовує MMS, використовує рівень додатків стандартного стеку OSI мережевих протоколів, його умовно можна вважати протоколом обміну. Принаймні, в технічній літературі з питань використання стандарту

МЕК 61850 та вирішення проблем захисту інформації у системах Smart Grid на його основі, цей термін в переважної більшості публікацій застосовується саме в такому сенсі.

Достатньо змістовний опис згаданих протоколів, включаючи часові діаграми, можна знайти в літературі, наприклад, в [10]. Зауважимо, що в кіберфізичних системах, побудованих на базі стандарту МЕК 61850, також можуть використовуватися інші мережеві протоколи, наприклад, поширена польова шина MODBUS, або її пропрієтарна модифікація MODBUS Plus, протокол часової синхронізації PTP (Precision Time Protocol), протокол виявлення мережевих пристроїв LLDP (Link Layer Discovery Protocol) та ін.

2. Атаки на протоколи стандарту МЕК 61850

Як свідчить аналіз вразливостей багатоадресних протоколів, до яких належать GOOSE та SV, існує дев'ять основних шляхів використання вразливостей з метою порушення роботи компонентів енергосистеми [11]:

1) компрометація інтерфейсу користувача;

2) переривання процесу синхронізації часу;

3) компрометація шини зв'язку на станційному рівні;

4) отримання доступу до пристроїв рівня приєднання;

5) зміна налаштувань захисного пристрою;

6) захоплення та модифікація повідомлень протоколу GOOSE;

7) компрометація комунікаційної шини на рівні процесу;

8) розміщення підроблених значень у повідомленнях протоколу SV;

9) компрометація міжмережевого екрану для отримання доступу до мережі підстанції.

Незалежно від перелічених способів використання вразливостей, існують певні варіації здійснення конкретної атаки. Нижче перелічені типи різновидів атак з описами, а також потрібні заходи протидії [10].

1. Дублювання (Replay) – старі повідомлення передаються повторно – перевірка узгодженості атрибутів.

2. Безпосереднє вкидання (Naive injection) – передаються сфабриковані повідомлення (команди для GOOSE або виміри для SV) – стандартна перевірка цілісності за стандартом МЕК 61850.

3. Вкидання МЕК 61850 (IEC 61850 injection) – передаються сумісні з МЕК 61850 шкідливі команди (GOOSE) або повідомлення з фальшивими вимірами (SV) – перевірка узгодженості атрибутів контексту (GOOSE) або кореляція вимірювань кількох джерел (SV).

4. Маскування (Masquerade) – передаються повідомлення, що імітують реальну поведінку – перевірка узгодженості та кореляції.

5. Псування (Poisoning) – поле *StNum* надмірно збільшене – перевірка узгодженості атрибутів.

6. Модифікація (Modification) – фальшиві атрибути – перевірка узгодженості атрибутів.

7. Flood-атака (Flooding) – багато повідомлень передаються з високою частотою – перевірка статистики повідомлень.

Оскільки протокол MMS використовує на рівні додатків стандартний стек мережевих протоколів, на нього можуть здійснюватися всі типи атак, притаманні типовим протоколам IT-галузі.

3. Системи виявлення вторгнень для цифрових електричних підстанцій

Розглянуті вище особливості організації кіберзахисту ЦПС накладають певну специфіку на для створення систем виявлення вторгнень для інтелектуальних підстанцій на базі стандарту МЕК 61850. Дослідження в цьому напрямку, як відзначають самі вчені, досі знаходяться на початковій стадії [1]. Однак, деякі відомості вже можна витягти з виконаних та опублікованих робіт.

Як відомо, за принципом розпізнавання системи виявлення вторгнень (СВВ), англомовне скорочення – IDS (Intrusion Detection System) – можна умовно розділити на такі, що використовують сигнатури (Signature-based IDS) та ті, що виявляють аномалії (Anomaly-based IDS) [12]. До недоліків сигнатурних СВВ відноситься властивість неможливості розпізнавати атаки, що недавно з'явилися та не внесені ще в базу зразків системи. Однак рішення на основі аномалій все ще демонструють неприпустимо високий рівень помилок як першого, так і другого роду. Особливості захисту кіберфізичних систем, а саме, відносно менша, порівняно з традиційними IT-системами, різнорідність та, як наслідок, значно менша кількість варіантів конфігурації та режимів функціонування, дозволяють деяким дослідникам говорити про застосування третього підходу, так званих СВВ на базі специфікацій (Specification-based IDS). Суть підходу полягає у моделюванні поведінки системи на основі її функціональності та політики безпеки [13]. При цьому, як свідчить аналіз літератури, під орієнтованими на специфікації СВВ автори інколи мають на увазі сигнатурні системи з гнучким розпізнаванням патернів [14]. В публікації [10] (у табл. 4) автори серед 11 розробок, виконаних з 2010 по 2019 роки, нарахували одну сигнатурну, три аномальні та сім систем на основі на специфікацій.

Технічно робота таких СВВ базується на складанні так званих специфікаційних правил (specification rules) окремо для всіх можливих атак кожного протоколу. Нижче наведені кілька прикладів таких правил [10].

(#R1) Повідомлення GOOSE повинні мати MAC-адресу, що починається з 01-0c-cd-01;

(#R2) Повідомлення GOOSE повинні мати поле *TPID* зі значенням0x8100;

(#R3) Повідомлення GOOSE повинні мати поле *ethertype* рівним 0x88B8;

(#R4) Повідомлення GOOSE повинні мати поле *TimeAllowedToLive* рівним подвоєному значенню *MaxTime* (наприклад, 5000 мс);

(#R5) Повідомлення GOOSE повинні мати поле *APPID*, відформатоване як шістнадцяткове а4-байтове (наприклад, 0000-3FFF);

(#R7) Повідомлення GOOSE повинні мати поле *APPID*, яке відповідає останнім двом октетам багатоадресної адреси призначення;

(#R8) Ім'я блоку управління IED має узгоджуватися зі значенням поля *goID* (тобто значення *LD* / *LN* у полі *gocoRef* повинно збігатися з полем *datSet* з GOOSE *APDU*);

(#R9) Розмір кадрів, що містять повідомлення GOOSE, повинен дорівнювати 8 байтам + *APDU size*, а *APDU size* повинен бути менше 1492 байтів;

(#R12) Кількість повідомлень, захоплених через інтервал, не повинна дорівнювати нулю;

(#R13) Мітка часу передавача не повинна бути вище мітки часу приймача;

(#R14) Мітка часу передавача з повідомлень GOOSE не повинна знаходитись на відстані більше 4 мс від мітки часу приймача;

(#R15) Метрика *Recency*, що представлена останнім повідомленням GOOSE, повинна відповідати мінімальному та максимальному пороговому значенню;

(#R16) Показник частоти, представлений середньою кількістю отриманих повідомлень GOOSE, повинен відповідати мінімальному та максимальному заздалегідь визначеному порогу;

(#R20) Повинна бути узгодженість повідомлень GOOSE *switch-in* (тобто відкриття вимикача) та значення звіту, надісланого протоколом MMS (тобто звіту про сигнал MMS);

(#R21) Кількість байтів, які проходять за секунду, не повинна перевищувати заздалегідь визначеного порогу;

(#R22) Кількість пакетів, які рухаються в секунду, не повинна перевищувати заздалегідь визначеного порогу;

(#R23) Довжина пакета (вказана в заголовку пакета) не повинна перевищувати заздалегідь визначеного порогу;

(#R24) Загальний розмір пакету не повинен перевищувати заздалегідь визначеного порогу.

4. Особливості кіберзахисту промислових систем

Як свідчать дослідження, методологія боротьби з кіберзагрозами, що традиційно використовується в IT-сфері, не в повній мірі може бути застосована для кіберфізичних систем на базі стандарту МЕК 61850 [1]. Цифрові пристрої, що використовуються як в Smart Grid, мають обмеженими обчислювальними ресурсами. У таких пристроях важко оновлювати ПЗ та

firmware, використовувати традиційні міжмережеві екрани та антивіруси [6]. СВВ, особливо їх програмні реалізації на традиційних комп'ютерах, також недостатньо ефективні стосовно промислових мереж.

Говорячи про особливості та специфіку кіберзахисту систем промислової автоматики, дослідники згадують можливість і необхідність в процесі розпізнавання шкідливої активності враховувати фізичну інфраструктуру. Якщо традиційні ІТ-комунікації є різнорідними і в широких межах варіюються за своєю природою, кіберфізичні системи мають певну сталу структуру і типові шаблони комунікації, які слід брати до уваги при виявленні підозрілої активності [1]. Тобто, можливість врахування структурної специфіки можна розглядати як перевагу промислових систем перед інформаційними об'єктами в плані захисту інформації. Дійсно, якщо, наприклад, в трафіку між двома конкретними вузлами промислової мережі відповідно до структури інформаційних обмінів повинні бути присутніми пакети лише деяких конкретних протоколів, то система виявлення вторгнень має інтерпретувати будь-які інші пакети як зловмисні та видавати попередження про вторгнення [6].

5. Застосування реконфігуровних засобів для промислових СВВ

Як зазначалося вище, одним з обмежень використання традиційних засобів кіберзахисту, що накладаються специфікою промислового застосування, є брак обчислювальної потужності. Реконфігуровні обчислювачі на базі програмованих логічних інтегральних схем (ПЛІС) [15], що застосовуються для апаратного прискорення в ІТ-сфері, орієнтовані на використання спільно з традиційною обчислювальною технікою, що ускладнює їх використання для захисту кіберфізичних систем. Але, як свідчить аналіз технічної інформації, існує можливість використання програмованої логіки в кіберфізичних системах шляхом застосування вже наявних в них реконфігуровних ресурсів. В даному дослідженні знайдено два джерела технічних засобів, що містять ПЛІС.

По-перше, існують деякі технологічні задачі енергетики, для вирішення яких вже використовуються ресурси програмованої логіки, частину яких можна задіяти для цілей кібербезпеки, зокрема, для створення систем виявлення вторгнень. Прикладами таких застосувань можуть бути системи управління, алгоритми яких засновані на використанні апаратів нейронних мереж і нечіткої логіки, інтелектуальні системи збору даних, частотні перетворювачі для керування потужними електроприводами і т.п. [16]. По-друге, інтелектуальні пристрої також мають в своєму складі ПЛІС або системи на кристалі для реалізації, зокрема, сумісних зі стандартом IEEE-1588 протоколів паралельного резервування з'єднань HSR (High-availability Seamless Redundancy) і PRP (Parallel Redundancy Protocol), а також для підтримки розглянутих вище протоколів стандарту МЕК 61850 [17].

Отже, засоби цифровізації, такі як стандарт МЕК-61850, надають багато переваг системам промислової автоматизації, впроваджують нові протоколи та функціональні можливості. Але нова якість зв'язків в таких системах, на жаль, призводить до збільшення загроз кібербезпеки, реалізація яких може привести до катастрофічних наслідків. Для їх захисту необхідно адаптувати відомі системи виявлення вторгнень.

В роботі досліджені особливості побудови цифрових підстанції на основі стандарту МЕК-61850 та відповідних протоколів. Проаналізовано атаки, які можуть здійснюватися на протоколи стандарту МЕК 61850.

Розглянуто питання створення системи виявлення вторгнень для цифрових електричних підстанцій. Наведені відомості щодо побудови таких систем з використанням підходу на базі специфікацій. Досліджені особливості кіберзахисту промислових систем в цілому. З'ясовано, що деякі особливості промислових систем надають певну перевагу в плані кіберзахисту в порівнянні з інформаційно-комунікаційними додатками.

Також досліджено можливості використання для синтезу систем виявлення вторгнень реконфігуровних обчислювальних засобів, зокрема, що присутні в пристроях промислової автоматики та входять до складу інтелектуального цифрового обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Multidimensional intrusion detection system for IEC 61850-based SCADA networks / Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer // IEEE Trans. Power Deliv. – 2017. – Vol. 32, № 2. – P. 1068-1078.
2. Styczynski J. When The Lights Went Out / Jake Styczynski, Nate Beach-Westmoreland (November 2016). – 82 p. [Електронний ресурс]. – Режим доступу: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf. – Загл. з екрану. – (Дата звернення: 15.05.2021).
3. Assante M.J. Confirmation of a Coordinated Attack on the Ukrainian Power Grid / M.J. Assante // SANS Institute, Bethesda, USA (January 6, 2016) [Електронний ресурс]. – Режим доступу: https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid. – Загл. з екрану. – (Дата звернення: 15.05.2021).
4. Sanger D.E. Cyberattack Forces a Shutdown of a Top U.S. Pipeline / D.E. Sanger, C. Krauss, N. Perlroth // The New York Times (May 8, 2021) [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. – Загл. з екрану. – (Дата звернення: 15.05.2021).
5. Radichel T. Colonial Pipeline Hack / T. Radichel // 2nd Sight Lab (May 15, 2021) [Електронний ресурс]. – Режим доступу: https://medium.com/cloud-security/colonial-pipeline-hack-4486d16f2957. – (Дата звернення: 15.05.2021).

6. Multi-attribute SCADA-specific intrusion detection system for power networks / Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E.G. Im, B. Pranggono, H.F. Wang // IEEE Trans. on Power Delivery. – 2014. – Vol. 29, P. 1092-1102.
7. Communication Networks and Systems in Substations, IEC Std. 61850, 2003.
8. Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці / Міністерство енергетики та вугільної промисловості України, ДП «НЕК «Укренерго», Науково-технічний центр електроенергетики. – К.: 2014. – 113 с.
9. Бойченко О.В. Построение информационной модели цифровой подстанции на основе стандарта МЭК 61850 / О.В. Бойченко, В.С. Дячук // Международный научно-исследовательский журнал. – № 4 (46). – Екатеринбург: 2016. – С.39-42.
10. A survey on intrusion detection and prevention systems in digital substations / S.E. Quincozes, C. Albuquerque, D. Passos, D. Mossé // Computer Networks. – 2021. – Vol. 184. – Article 107683.
11. Hong J. Detection of cyber intrusions using network-based multicast messages for substation automation / J. Hong, C. Liu, M. Govindarasu // IEEE conf. on Innovative Smart Grid Technologies (ISGT), IEEE: 2014. – P. 1-5.
12. Коростиль Ю.М. Принципы построения сетевых систем обнаружения вторжений на базе ПЛИС / Ю.М. Коростиль, С.Я. Гильгурт // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Вип. 57. – К.: 2010. – С.87-94.
13. Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values / M.E. Hariri, T.A. Youssef, H.F. Habib, O. Mohammed // IEEE conf. on Innovative Smart Grid Technologies (ISGT), IEEE: 2017. – P. 1-5.
14. Kim J. FPGA-based network intrusion detection for IEC 61850-based industrial / J. Kim, J. Park // Elesevier ICT Express. – 2018. – Vol. 4, P. 1-5.
15. Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор / С.Я. Гильгурт // Электронное моделирование. – 2013. – Т. 35, № 4. – С. 49-72.
16. Monmasson E. FPGA design methodology for industrial control systems – a review / E. Monmasson, M.N. Cirstea // IEEE Transactions on Industrial Electronics. – 2007. – Vol. 54, № 4. – P. 1824-1842.
17. Гільгурт С.Я. Апаратне рішення задач кібербезпеки в електроенергетичній галузі / С.Я. Гільгурт // Кібербезпека енергетики: Збірка праць конференції, м. Одеса, 28 травня – 1 червня 2019. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2019. – С. 11-14.

УДК 621::[004.056.53+006.3]

Герасимов Ростислав Павлович,
ІПМЕ ім. Г.Є. Пухова НАН України,
наук. співроб.
gerasimov.rostislav@gmail.com

Крук Ольга Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
мол. наук. співроб.
o.n.kruk@gmail.com

ОГЛЯД ЕТАПІВ І НАПРЯМІВ ДОСЛІДЖЕНЬ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГАЛУЗІ ЕЛЕКТРОЕНЕРГЕТИКИ

Анотація: В рамках світового досвіду розглянуті і проаналізовані етапи, систематичне виконання яких необхідне щодо оцінювання стану інформаційної безпеки ключових систем критичної інформаційної інфраструктури галузі електроенергетики в умовах прояву негативних факторів невизначеності. Також розглянуті основні напрямки та критерії оцінки програмної захищеності інформації, інформаційної надійності суб'єктів критичної інфраструктури. Окремо розглянуто значення експертів при прийнятті рішень, щодо стану інформаційної безпеки ключових систем критичної інформаційної інфраструктури галузі електроенергетики в умовах прояву негативних факторів невизначеності.

Abstract: Within the framework of world experience the stages are considered and analyzed, the systematic implementation of which is necessary to assess the state of information security of key systems of critical information infrastructure of the power industry in the face of negative uncertainties. The main directions and criteria for assessing the software security of information, information reliability of critical infrastructure entities are also considered. The importance of experts in making decisions about the situation is considered separately information security of key systems of critical information infrastructure of the electric power industry in the conditions of manifestation of negative factors of uncertainty.

УДК 621.3::[004.056.53+006.3]

Мохор Володимир Володимирович,
ІПМЕ ім. Г.Є. Пухова НАН України,
директор, чл.-кор. НАН України,
професор, д-р техн. наук
v.mokhor@gmail.com

Цуркан Оксана Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
мол. наук. співроб.
otsurkan24@gmail.com

Клименко Тетяна Михайлівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
зав. відділу
klimenko-t@ukr.net

Яшенков Вадим Петрович,
ІЕЗ ім. Є.О. Патона НАН України,
наук. співроб.
vadym.yashenkov@gmail.com

Цуркан Василь Васильович,
КПІ ім. Ігоря Сікорського,
канд. техн. наук, доц.
v.v.tsurkan@gmail.com

РІЗНОВИДИ ЕКТОРІВ ПРИ АНАЛІЗУВАННІ ВРАЗЛИВОСТЕЙ СОЦІОТЕХНІЧНИХ СИСТЕМ ДО ВПЛИВІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація: Розглянуто представлення впливу соціального інженера на користувача нечітким соціальним графом. Виокремлено його елементи, зокрема, екторів. Їх різновиди запропоновано встановлювати за направленістю вхідних і вихідних дуг. Серед них визначено таких екторів: ізольований, відправник, отримувач. Це дозволило аналізувати вразливості соціотехнічних систем з огляду на форму маніпулятивного впливу соціального інженера.

Abstract: Representations of the social engineer's influence on the user by a fuzzy social graph are considered. Its elements are highlighted, in particular, actors. Their varieties are proposed to be defined by the direction of incoming and outgoing arcs. Among them are allocate such actors: isolated, sender, the recipient. This made it possible to analyze the socio-technical system's vulnerabilities in terms of the manipulative influence form of a social engineer.

УДК 621.3::004.056.53

Гончар Сергій Феодосійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
учений секретар, д-р. техн. наук
sfgonchar@gmail.com

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

Анотація: На сьогоднішній день неможливо гарантувати повну кібербезпеку будь-якої інформаційної системи, у тому числі системи енергетичного сектора. Якщо раніше метою кібербезпеки були заходи щодо запобігання кіберпроникненням, то на сьогодні вона поступово трансформується у виявлення кібератак, адекватне та негайне реагування на них та усунення наслідків цих кібератак, тобто забезпечення кіберстійкості. Дослідження показують, що кіберстійкість охоплює більш широкий підхід, ніж забезпечення кібербезпеки, і спрямована на захист від потенційних кібератак та забезпечення функціонування об'єкту енергетики в нормальному режимі після кібератаки.

Abstract: Today it is impossible to guarantee the complete cybersecurity of any information system, including the system of the energy sector. If earlier the goal of cybersecurity was measures to prevent cyber penetration, today it is gradually transforming into detecting cyber-attacks, adequately and immediately responding to them and eliminating the consequences of these cyber-attacks, that is, ensuring cyber resilience. Research shows that cyber security encompasses a broader approach than cyber security, and is aimed at protecting against potential cyberattacks and ensuring that the energy facility operates normally after a cyber-attack.

УДК 621.3+620.9

Джигун Олена Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. співроб., канд. техн. наук
elromanenko@gmail.com

АНАЛІЗ ДИНАМІКИ ВИРОБНИЦТВА ЕЛЕКТРОЕНЕРГІЇ ТЕЦ В УМОВАХ НОВОГО РИНКУ ЕЛЕКТРОЕНЕРГІЇ В УКРАЇНІ

Анотація: Істотну частку ТЕС в Україні становлять теплоцентралі (ТЕЦ), що здійснюють комбіноване виробництво (когенерацію) теплової та електричної енергії. Більшість ТЕЦ працює по тепловому графіку в зимовий період, коли пріоритетом є опалення житлових приміщень, а по електричному — в літній період, коли міські опалювальні системи відключено. Проведено дослідження залежності погодинного виробництва електроенергії на ТЕЦ від погодинних температури повітря і тарифів за електроенергію на ринку за період з жовтня 2019 р. по березень 2021 р. Встановлено, що на виробництво електроенергії впливає не тільки сезонний фактор, але й ринкова ціна.

Abstract: A significant share of thermal power plants in Ukraine are cogeneration heat plants (CHP), which carry out combined production (cogeneration) of heat and electricity. Most CHP operate on a thermal schedule in winter, when the priority is heating of living quarters, and on the electric – in summer, when district heating systems are turned off. The study of the dependence of hourly electricity production at CHP on hourly air temperatures and electricity tariffs in the market for the period from October 2019 to March 2021 was conducted. It is established that the production of electricity is influenced not only by the seasonal factor, but also by the market price.

Спільне виробництво теплової та електричної енергії (когенерація) в Україні використовується енергетиками вже давно, оскільки дозволяє значно збільшити ефективність використання палива. Більшість ТЕЦ працює по тепловому графіку в зимовий період, коли пріоритетом є опалення житлових приміщень, а по електричному — в літній період, коли міські опалювальні системи відключено.

Прийнятий у 2010 р. Закон «Про комбіноване виробництво теплової та електричної енергії (когенерацію) та використання скидного енергопотенціалу» [1] визначає правові, економічні та організаційні засади діяльності суб'єктів відносин у сфері енергозбереження щодо використання когенераційних установок, регулює відносини, пов'язані з особливостями виробництва, передачі, розподілу і постачання електричної та теплової

енергії від когенераційних установок. Ринок когенерації в Україні знаходиться на етапі становлення.

На початку двадцять першого століття вироблення більшості енергетичних об'єктів в Україні склало 100% заявленого ресурсу, намітилися зростання ціни на енергоносії (в першу чергу на газ і нафту). І все це на тлі зростання енергоспоживання як підприємствами, так і населенням. Виходом з ситуації, що склалася в енергетиці, на першому місці стоїть когенерація як спосіб значного збільшення ККД енергогенеруючих установок [2].

Теплове навантаження, що визначається витратою тепла на виробничі процеси і побутові потреби (гаряче водопостачання), залежить від зовнішньої температури повітря. В умовах України влітку це навантаження (як і електричне) менше зимового. Промислове і побутове теплові навантаження змінюються впродовж діб, крім того, середньодобове теплове навантаження електростанції, що витрачається на побутові потреби, змінюється в робочі та вихідні дні. Добові графіки електричного навантаження змінюються в залежності від пори року, дня тижня і характеризуються зазвичай мінімальним навантаженням в нічний період і максимальним навантаженням в години пік.

За даними, отриманими з [3,4] проведено дослідження залежності погодинного виробництва електроенергії на ТЕЦ від погодинних температури повітря і тарифів за електроенергію на ринку за період з жовтня 2019 р. по березень 2021 р. Встановлено, що на виробництво електроенергії енергоблоками теплоцентралей впливає не тільки сезонний фактор, але й ринкова ціна. При цьому, з введенням Закону України «Про ринок електричної енергії» [5] відбулися зміни у поведінці компаній ТЕЦ: спостерігається зростання виробництва електроенергії вдень, а вночі — теплової енергії; середньозважені ціни купівлі-продажу електричної енергії вдень майже вдвічі більші, ніж вночі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про комбіноване виробництво теплової та електричної енергії (когенерацію) та використання скидного енергопотенціалу» від 7.10.2010 № 2592-VI. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T052509.html.
2. Панькив В. Когенерация: как это работает. Обзор рынка. Киев : Сети и бизнес, 2010, № 4 (53). URL: http://ges-ukraine.com/maininfo_14-16.html.
3. Погодинні середньозважені ціни купівлі-продажу електричної енергії на РДН по ОЕС України (грн/МВт.год). Оператор ринку. URL: https://ukrainian.wunderground.com/history/airport.
5. Закон України «Про ринок електричної енергії» від 13.04.2017 № 2019-VIII. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172019.html.

УДК 621.3::004.056.53

Заблоцький Костянтин Васильович,
Національний авіаційній університет, Київ,
студент
kzablotskiy@gmail.com

Малик Святослав Васильович,
Національний авіаційній університет, Київ,
студент
sviatmal760@gmail.com

Чумаченко Богдан Сергійович
Національний авіаційній університет, Київ,
студент
Body21033@gmail.com

Одарченко Роман Сергійович,
Національний авіаційній університет, Київ,
д-р. техн.. наук, доцент, зав. кафедри ТКРС НАУ
5295634@stud.nau.edu.ua

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОНЦЕПЦІЇ SMARTGRID

Анотація: На зміну застарілої інфраструктури електромережі приходить нова розумна екосистема Smart Grid. Але з оновленням системи та додаванням нових функцій з'являються і нові вразливості системи, що є загрозою кібербезпеки.

Abstract: The obsolete power grid infrastructure is being replaced by a new smart ecosystem Smart Grid. But as the system is upgraded and new features are added, new system vulnerabilities appear that pose a threat to cybersecurity.

Електромережа в даний час є застарілою інфраструктурою і з розвитком технологій потребує постійного оновлення для забезпечення додаткових функціональних можливостей. Але оновлення усієї системи не лише задовольнить поточні та майбутні потреби споживачів, а й надасть багато нових вразливих місць у системі безпеки.

Новою інфраструктурою електроенергетики, яка містить усі функції електромережі, що є в даний час, а також нові функціональні можливості – це SmartGrid.

SmartGrid (розумна енергосистема) – електрична мережа, що містить розумні рішення для керування станом електроенергетичної системи для забезпечення енергоефективності та підтримки стабільності середовища.

Дана система забезпечує оптимізацію споживання електроенергії, підвищує якість живлення, корегує роботу у разі переривання шляху передачі електроенергії та проводить постійну оцінку стану енергосистеми.

Система може перенаправляти та корегувати розподіл електроенергії, що в результаті зменшує частоту та тривалість основних відключень. Застаріла інфраструктура України негативно позначається на показнику SAIDI (тривалість перерв в електропостачанні), що згідно з даними моніторингу в IV кварталі 2020 року становив більше 300 хвилин [1] і навіть збільшився, порівняно з 2019 роком. В країнах ЄС показник SAIDI в 3 рази менший, а у Південній Кореї він складає близько 10 хв.

Причиною збільшення тривалості перерв у відключенні є ручне управління та низький рівень автоматизації електромережі. Для вирішення даної проблеми існує система SmartGrid.

Автоматизація забезпечує зменшення витрат електроенергії та імовірність виходу обладнання з ладу, а також зменшення втрат під час транзиту та усунення надлишкових втрат. Але усі зміни призведуть до нових ризиків, що пов’язані із забезпеченням зв’язку, технологіями та великою кількістю даних. Разом із введенням нових технологій та компонентів збільшиться кількість вразливих місць та точок входу у систему.

Оскільки система використовує розумні лічильники [2] та інші компоненти для моніторингу у реальному часі, то будь-яке втручання зловмисників, що може збільшити затримку або призвести до втрати даних. Також саме управління станом системи, що містить програмне забезпечення може піддатися злочинним діям. Таким чином, будь-яке порушення зв’язку або втручання у програмне забезпечення може призвести до травмування людей або навіть до втрати електроенергії.

Також перехід від старої системи до нової відбувається не одразу, а поступово, щоб забезпечити взаємодію усіх технологій. Як правило, там використовуються застарілі методи захисту або вони взагалі відсутні, що у свою чергу надає нові вразливі місця у системі безпеки. Зі збільшенням кількості пристроїв у системі буде збільшуватися збір даних і їх обробка, що призведе до збільшення проблем конфіденційності. Для забезпечення взаємодії усіх компонентів необхідний постійний контроль затримки, надійності та пропускної здатності, що в свою чергу реалізується через протоколи, реалізація яких потребує певної підготовки для захисту від кібератак.

Для впровадження SmartGrid необхідно провести повну модернізацію поточної електромережі та впровадити нові компоненти у систему, що в свою чергу збільшує ризики злочинного впливу та втручання в кібербезпеку системи.

Енергосистема в даний час існує з мінімальним, або відсутнім набором засобів захисту енергетики, тому для модернізації необхідно створити протоколи та політику захисту.

Також перед самим запуском системи необхідно провести різноманітні мережеві симуляції [3] виявлення усіх вразливих місць системи. Під час безпосереднього функціонування системи необхідно забезпечити постійний контроль введених та переданих даних, що можуть піддатися втручанню зі сторони злочинців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Звіт з моніторингу функціонування роздрібного ринку електричної енергії у IVкварталі 2020 [Електронний ресурс] URL: https://www.slideshare.net/NKREKP/v-2020-245961018
2. Wikipedia. Розумні лічильники. URL: https://en.wikipedia.org/wiki/ Smart_meter.
3. Мережевий симулятор. Інформація користувача. URL: http://nsnam. sourceforge.net/ wiki/index.php/User_Information

УДК 621.3

Верлань Анатолій Федорович,
ІПМЕ ім. Г.Є. Пухова НАН України,
гол. наук. спів роб.
a.f.verlan@gmail.com

Митько Лідія Олексіївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. спів роб.
lmitko@ukr.net

МЕТОД ДІАГНОСТУВАННЯ НЕЛІНІЙНИХ ДИНАМІЧНИХ ОБ'ЄКТІВ НА ОСНОВІ НЕПАРАМЕТРИЧНИХ ІНТЕГРАЛЬНИХ МОДЕЛЕЙ

Анотація: В роботі розглянуті питання обґрунтування сучасного підходу до організації процесів діагностування складних нелінійних динамічних об'єктів. Запропоновано використання інтегральних непараметричних моделей, що одночасно відображають нелінійні та динамічні властивості об'єкту діагностики.

Abstract: The paper considers the issues of substantiation of the modern approach to the organization of processes of diagnosing complex nonlinear dynamic objects. It is proposed to use integrated non-parametric models that simultaneously reflect the nonlinear and dynamic properties of the diagnostic object.

З ростом складності сучасних об'єктів та умов їх експлуатації у різних галузях промисловості, медицини, економіки посилюється роль автоматизованих систем технічного діагностування (АСТД) в задачах своєчасного і достовірного визначення виду технічного стану, пошуку місця та причин відмови об'єктів діагностування (ОД) щодо попередження аварій, оцінки якості виробів, мінімізації витрат при технічному обслуговуванні тощо.

Великий інтерес з боку практики, викликають і стають розповсюдженими прикладні задачі діагностування складних об'єктів, зокрема нелінійні інерційні об'єкти, у тому числі з неперервними характеристиками та невідомою структурою, які можна розглядати як «чорний ящик». Прикладами таких об'єктів в промисловості є електричні двигуни, інструменти в системах обробки металів, в біомедицині – об'єкти живої природи, в економіці – маркетингові заходи та ін.

В багатьох випадках такі об’єкти супроводжуються апріорною невизначеністю, серед причин виникнення якої розглядаються недостатня вивченість процесів, що протікають в ОД, а також експлуатація у широкому діапазоні зовнішніх умов, наявність великої кількості збурюючих впливів і перешкод навколишнього середовища.

Для первинного опису означених ОД, тобто побудови інформаційних моделей, доцільно використовувати інтегральні непараметричні динамічні моделі на основі багатовимірних вагових (БВФ) та багатовимірних перехідних функцій (БПФ), які визначаються за даними експерименту «вхід–вихід». Головними перевагами застосування означених моделей в задачах діагностування є здатність враховувати несправності, спричинені як зміною параметрів ОД, так і його структури, а також зручність використання при тестовому і функціональному діагностуванні.Завдяки сумісному урахуванню нелінійних та інерційних властивостей ОД інтегральні непараметричні динамічні моделі забезпечують високу достовірність діагностування, але великий обсяг первинної ідентифікаційної інформації приводить до зниження оперативності налаштування АСТД [1]. Зменшення обсягу первинної ідентифікаційної інформації шляхом використання більш компактних моделей (наприклад, інтегралів згортки) дозволяє підвищити оперативність налаштування АСТД, але приводить до зниження достовірності діагностування. Таким чином виникає протиріччя між достовірністю технічного діагностування (ТД) і оперативністю налаштування АСТД при використанні інтегральних непараметричних динамічних моделей. Це протиріччя може бути розв’язане за рахунок застосування вторинної ідентифікації – побудови діагностичних моделей з суттєво меншим розміром діагностичної інформації (редукції інформаційних моделей).

Поширені методи редукції моделей, засновані на інформаційному та компонентному аналізі, потребують великого обсягу апріорних даних, отже, орієнтовані на роботу ОД у визначених режимах функціонування та діапазонах зовнішніх умов. Розширення сфери практичних застосувань, адаптація до нових функціональних вимог, експлуатації у широкому діапазоні зовнішніх умов призводить до зростання апріорної невизначеності даних про об’єкт, а отже, до зменшення достовірності діагностування та її завадостійкості.

З урахуванням цих обставин запропоновано новий підхід до побудови діагностичних моделей на основі вторинної спектрально-статистичної ідентифікації ОД[2]. Використання такого підходу дозволяє одночасно забезпечити редукцію інформаційних моделей завдяки спектральним перетворенням БВФ при формуванні простору діагностичних ознак та високу достовірність діагностування і її завадостійкість за рахунок застосування

статистичних методів машинного навчання та процедури інформаційної оптимізації діагностичних моделей.

Наведені положення визначають актуальність розробки моделей, методів та інформаційної технології вторинної спектрально-статистичної ідентифікації нелінійних інерційних об’єктів в системах ТД на основі інтегральних непараметричних динамічних моделей, що забезпечує високу достовірність та оперативність діагностування складних об´єктів різної природи в умовах апріорної невизначеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ПавленкоВ. Д., Фомин А. А. Информационная технология диагностики нелинейных динамических объектов с использованием рядов Вольтерра. Вісник Національного технічногоу ніверситету «Харківський політехнічний інститут»: Тематичний випуск «Системний аналіз, управління та інформаційні технології». 2007. №5. С. 67–74.
2. Верлань А. Ф., Положаенко С.А. Модельно-ориентированные методы технической диагностики. Київ, НВП "Видавництво "Наукова думка" НАН України, 2019. 263 с.

УДК 621.3::004.056.53

Потенко Олександр Сергійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
наук. спів роб.
potenko@ipme.kiev.ua

ПОБУДОВА ПРОФІЛІВ ПРОТИДІЇ ЗАГРОЗАМ ЗА ДОПОМОГОЮ ПРИНЦИПУ ОПТИМУМУ Р. БЕЛМАНА В АС 1-3 КЛАСІВ

Анотація: Відповідно до НД ТЗІ 2.5-004-99, стандартним функціональним профілем захищеності являється перелік мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту інформації обчислювальної системи, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. В даній роботі, для вирішення завдання розробки методики проектування профілів, адаптивних за підкласами АС, пропонується використовувати метод динамічного програмування Р. Беллмана.

Abstract: According to НД ТЗІ 2.5-004-99, the standard functional security profile is a list of the minimum required levels of services that must implement a set of information security tools of the computer system to meet certain requirements for the security of information processed in this AS. In this paper, to solve the problem of developing a methodology for designing profiles, adaptive to the subclasses of the AS, it is proposed to use the method of dynamic programming R. Bellman.

УДК 621.3::004.056.53

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
пров. наук. співр.,
davidenkoan@gmail.com

Довбня Сергій Якович,
КНУ імені Тараса Шевченка, доцент кафедри радіотехніки та радіоелектронних систем, dovbnja.sergej@i.ua

Сулима Олександр Андрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
наук. співр.,
rfitfo@gmail.com

Кіслов Олексій Геннадійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
мол. наук. співр.,
alekskislov@i.ua

ПРОТИДІЯ ЗОВНІШНИМ АТАКАМ НА ІНФОРМАЦІЙНІ РЕСУРСИ ПІДПРИЄМСТВ ЕНЕРГЕТИКИ

Анотація: Робота спрямована на вирішення актуальної проблеми захисту веб-додатків підприємств енергетики від зловмисних дії зовнішніх порушників. Проаналізовано та досліджено існуючі засоби протидії таким атакам.

Abstract: The research is aimed at solving the urgent problem of protecting web applications of energy companies from external attackers. Existing means to prevent such attacks are analyzed and studied.

Захист веб-ресурсів від зловмисних дій зовнішніх порушників є актуальною проблемою сьогодення, особливо, якщо ці ресурси належать підприємствам критичної інфраструктури, зокрема, в енергетичній галузі.

Відсутність єдиних стандартів безпечного програмування веб-додатків призводить до помилок в їх розробці, внаслідок чого у веб-сервісах виникають вразливості, які можуть бути скомпрометовані зловмисником навіть без використання спеціальних засобів, лише за допомогою штатних можливостей браузера.

Ризики підприємств в таких умовах занадто великі, щоб ігнорувати дану проблему, оскільки вразливості в веб-додатках наражають критично важливі бізнес-операції і конфіденційні дані на небезпеку. Значні фінансові

втрати можуть виникнути в результаті непередбачених затримок в бізнес-процесах, крадіжки інтелектуальної власності та втрати довіри клієнтів, а також репутації бренду. У багатьох випадках, безпека веб-додатків також є юридичною вимогою до компанії, яка обробляє персональні дані користувачів.

Тому зростає актуальність застосування додаткових засобів захисту, що використовуються на етапі експлуатації, такі як системи виявлення / запобігання вторгнень (СВВ / СЗВ), міжмережеві екрани нового покоління – Next Generation Firewall (NGFW), а також засоби фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки – Web Application Firewall (WAF).

Системи виявлення та запобігання вторгнень на відміну від захисних екранів здатні аналізувати не тільки заголовки, а й тіла мережевих пакетів і здійснювати інспекцію на рівні додатку за певними сигнатурам. Такі засоби здатні виявляти атаки не тільки ззовні, але й всередині мережі за рахунок прослуховування SPAN-порту комутатора.

Для вдосконалення захисних механізмів в СВВ / СЗВ стали застосовуватися декодери (розбір полів TCP-пакета) і препроцесори (розбір частин протоколу рівня додатків, наприклад, HTTP). Застосування препроцесорів в IDS Snort дозволило істотно поліпшити функціональність периметрового захисту в порівнянні з пакетним фільтром, навіть якщо останній перевіряє пакети на рівні додатків (IpTables з модулем Layer7).

Але при цьому зберігається головний недолік пакетного фільтра: перевірка здійснюється попакетно, без урахування сесій, cookies та всієї іншої логіки роботи програми.

Наступним етапом еволюції систем виявлення вторгнень стала поява пристроїв класу міжмережеві екрани нового покоління NGF. Такі засоби є спробою об'єднати функції різних продуктів (антивірус, СВВ / СЗВ, пакетний фільтр, VPN-шлюз, маршрутизатор, балансувальник тощо) в одному засобі. При цьому виявлення атак в пристроях NGFW нерідко здійснюється на старій технологічній базі, за допомогою згаданих вище препроцесорів.

WAF – засіб фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки. Застосування такого засобу вважається найбільш ефективним підходом до захисту веб-ресурсів. WAF може бути реалізований як хмарний сервіс, додаток на веб-сервері або спеціалізоване залізний або віртуальний пристрій.

Порівняння основних можливостей технологій, наведено у табл., а саме:

СВВ / СЗВ;
NGFW;
WAF.

Таблиця

Порівняння функціоналу систем СВВ / СЗВ, NGFW та WAF

Засіб захисту	**СВВ / СЗВ**	**NGFW**	**WAF**
Мультіпротокольна безпека	+	+	–
IP-репутація	– /+	– /+	– /+
Сигнатури веб-атак	– /+	–	+
Сигнатури веб-вразливостей	– /+	– /+	+
Автоматичне навчання політиці	–	–	+
URL, cookie-параметри та захист форми	–	–	+
Результати сканування вразливостей	– /+	–	+

Отже, захист веб-додатків, який не вдалося здійснити шляхом усунення вразливостей програмного забезпечення веб-додатків, може бути реалізованим за рахунок використання спеціалізованих засобів захисту цих продуктів – СВВ / СЗВ, Next Generation Firewall та Web Application Firewall.

ЗМІСТ

ДЛЯ ПРИМІТОК

Науково-практична конференція
«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

ЗАПРОШЕННЯ
ПРОГРАМА ТА МАТЕРІАЛИ

28 травня 2021 року
м. Київ

Оператор конференції – ТОВ «ІНФОРМАТІО»

Формат 60×90/16. Тираж 100.
Підписано до опублікування 23.05.2021.

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua