та концентраторів даних відносно зосереджених кібер-ударів. Далі представлено основні загальні проблеми вразливості WAMS. Залежність від зовнішнього джерела синхронізації. При вимірюванні з прив'язкою до GPS, тимчасове або тривале, локальне або загальне порушення синхронізації може призвести до втрати даних і подальшої спостережності засобами WAMS. Керування налаштуваннями. Всі компоненти корпоративної мережі, включаючи цифрові реєстратори повинні підтримувати аутентифікацію для конфігурування та налаштування, що в свою чергу вимагає унікальної ідентифікації користувача. Кібер-захист. Захищеність PMUs та пристроїв концентрації від зосереджених кібератак та здатність до пост-відновлення. Обмежена область ситуаційного інформування. Для відповідного оперативного керування електроенергетичних систем (ЕС) необхідним є повне уявлення про параметри режимів. При цьому, розміщення PMUs повинні забезпечувати повне і точне охоплення контрольованих ділянок електропостачання, що в свою чергу вимагає обміну значними обсягами даних в реальному часі. Довіра по замовчуванню. Сучасні стандарти WAMS (C37.118, IEEE 1334) [3] не підтримують метод аутентифікацію при використанні трафіку. Без аутентифікації, механізми інформаційного обміну WAMS схильні до впливу із сторони додаткових диспетчерських вузлів доступу до даних, естіматорів стану (моделей ЕС), та інших каналів доступу до оперативної інформації. Вразливості в частині протоколу обміну даними. Існуючі WAMS використовують кілька загальних комунікаційних інфраструктур – телефонні лінії, або радіочастотний зв'язок, синхронні оптичні мережі, а також віртуальні приватні мережі (VPN). Кожен з цих методів комунікацій має вразливості, які можуть бути використані для переривання зв'язку або інших зловмисних впливів на WAMS. Безперервність операцій. Для боротьби з наслідками відмов баз даних локальних концентраторів даних, необхідним є забезпечення резервного копіювання інформації в спеціалізовані сховища. Це вимагає надлишкових інформаційних зв'язків віддаленого архіву із диспетчерськими центрами. Однак, для безперервності операцій необхідними також є надлишкові зв'язки із окремими реєстраторами. Надійність обладнання. Загальна працездатність WAMS повинна бути забезпечена при виході з ладу окремих компонентів корпоративної мережі. Цілісність даних. При отриманні даних, від певного об'єкту енергосистеми, повинні спрацьовувати механізми валідації та верифікації. Людський фактор. Необхідність забезпечення функціонування WAMS у випадку вчинення умисних або неумисних дій, що порушують штатну роботу корпоративної комп'ютерної системи, цілісність чи повноту отримуваних даних. Захисні механізми та особливості цифрових реєстраторів. Більшість сучасних PMUs забезпечують лише односторонню передачу даних до мережевого концентратора (сервера) і не підтримують двонаправленої комунікації. Крім того більшість реєстраторів не підтримують функції конфігурування засобами мережевих інтерфейсів. Хоча мають місце тенденції розширення функціональності PMUs в представлених напрямках, слід відмітити, що на сьогоднішній час, відсутність цих можливостей зменшує рівень вразливості із сторони реєстраторів. В корпоративних мережах можуть застосовуватись інструменти, які контролюватимуть трафік реєстраторів, виявляючи несправності в режимі близькому до реального часу, забезпечуючи тим самим аналіз працездатності системи моніторингу. З допомогою інструментів спостереження за трафіком, можна встановити також випадки перезавантаження реєстратора, які можуть свідчити про несправності або несанкціоновану зміну налаштувань.

Таким чином на сьогоднішній день переважна більшість вразливостей інформаційної безпеки корпоративних комп'ютерних систем моніторингу та діагностики властива компонентам та технологіям верхніх рівнів ієрархії. При цьому інтегральна надійність нижнього вимірювального рівня, представленого пристроями реєстрації в основному визначається здатністю PMUs забезпечувати повну функціональність згідно специфікації, та рівнем їх ремонтопридатності для оперативного виявлення та усунення несправностей в процесі експлуатації.

Список використаних джерел

1. Phadke A. G. The Wide World of Wide-area Measurement / A. G. Phadke, R. M. de Moraes // IEEE Power and Energy Magazine. – 2008. – Vol. 6, No. 5. – P. 52-65.
2. Harmonic Monitoring System via GPS-Synchronized Measurements – Update and New Developments / Shalom Zelingher, Bruce Fardanesh, Edvina Uzunovic [at al.] // Power Engineering Society General Meeting, IEEE. – 2006. – No.1. – P. 1-7.
3. Synchrophasor Measurements for Power Systems: IEEE Std. C37.118.1-2011 (Revision of IEEE Std. C37.118-2005) / IEEE Standard. – New York, 2011. – 61 p.

Каргін А. О., д.т.н., професор,
Лученцов Є. О.
(УкрДУЗТ)

МОНІТОРИНГ НЕБЕЗПЕЧНИХ СИТУАЦІЙ ЗА ДОПОМОГОЮ РОБОТУ, ЩО НАДАЄ ІНТЕЛЕКТУАЛЬНЕ ОБСЛУГОВУВАННЯ

З появою глобальної хвилі застосування роботів інтелектуальне обслуговування, що надається роботами стає все більш важливим. Інтелектуальний сервіс спрямований на те, щоб задовольнити особисті

потреби користувача. Інтелектуальне обслуговування означає надання диференційованих послуг для персоналізованих вимог на відміну від надання типового сервісу для всіх замовників. [1] Так, робот що патрулює приміщення з метою моніторингу небезпечних ситуацій може визначити ситуацію пожежонебезпечною на основі ознак загоряння не залежно від особливостей приміщення. Якщо такими ознаками є задимленість приміщення, то можливо помилкове рішення, коли робот виконує моніторинг кімнати для паління де підвищена задимленість є нормою для цього приміщення. Коли робот надає інтелектуальне обслуговування він повинен знати різницю від, на перший погляд, однаковими кімнатами та застосовувати знання про специфічність приміщень з точки зору надання сервісу. Виходячи з цього, для надання інтелектуальних послуг робот повинен мати достатньо як апріорних знань, що стосуються типових послуг, так й оперативної інформації про навколишнє середовище. Додатково, для інтелектуального обслуговування робот повинен мати можливість враховувати особливості об'єкта, якому надається сервіс.

У даній роботі розглядається проблема інтелектуального обслуговування роботом, що виконує функцію моніторингу небезпечних ситуацій при патрулюванні приміщень. Виділено наступні ситуації що контролюються. Це:

пожежонебезпечність;
несанкціоновані дії;
аварійні події;
порушення регламенту.

Для кожного з перелічених типів ситуацій розглядається декілька стандартних ситуації. Наприклад, пожежонебезпечна ситуація й виявлення початкових стадій виникнення пожежі в приміщенні. Типові ситуації не враховують особливостей приміщення та інші специфічні фактори.

Так, наприклад, ситуація загоряння урни без паління на початковій стадії характеризується наступними параметрами: температура - 300 °С (датчик температури), жовте полум'я (датчик освітленості), дим – білувато-сірий (датчик диму), об'єм диму - 4,21 м3 /кг (датчик диму), токсичні продукти горіння – чадный газ, водяний пар, двоокис вуглецю та окис вуглецю (газоаналізатор).

Урна з палінням: 750 °С, помаранчеве полум'я, дим – білувато-сірий, об'єм диму - 4,40 м3 /кг, токсичні продукти горіння – сірчистий газ, шлак з порами, схожий на скло.

Прикладом другого типу небезпечних ситуацій - несанкціоновані дії – є несанкціоноване проникнення в приміщення через вікно. Ситуація цього типу характеризується зміною тиску в інфразвуковому спектрі 0,001 - 0,01 Гц (датчик тиску), наявністю рухомих об'єктів (датчик руху), порушення світлових потоків (датчик освітленості).

Аварійні події, наприклад, прорив системи опалення характеризуються підвищеною температурою, - 100 °С, вологістю – 100% та появою білого диму.

Прикладом порушення регламенту може бути відчинене вікно й паління багаття за вікном. Це призводить до збільшення температури від 1 до 5 °С на відстані 10 м від палання багаття, дим – білувато-сірий, об'єм диму - 4,90 м3 /кг, токсичні продукти горіння – пил, окис азоту, чадний газ, важкі метали.

Реалізація інтелектуального обслуговування роботом можлива на основі моделей, котрі об'єднують моделі управління роботом, моделі обробки даних від сенсорів та моделі представлення та обробки знань щодо небезпечних ситуацій.

В роботі розглядається модель представлення знань інтелектуального обслуговування у вигляді нечітких характеристик гранул.

В [2] моделі оцінки ситуації представлена у вигляді багаторівневої структури на різних рівнях абстракції. На різних рівнях, ситуація представлена концепціями різних рівнів абстракції. В моделі формалізовано три типи абстрагування даних: кількісне, визначальне та узагальнене абстрагування. Кількісна та визначальна абстракція діє як місток між описом природної мови та числовими даними від датчиків.

На кафедрі інформаційних технологій УкрДУЗТ на базі навчально-дослідницького полігону інтернету речей та розумних машин апробуються технології створення різноманітних додатків у тому числі роботів що надають інтелектуальний сервіс. У якості мобільного роботу розглядається колісний робот, виконуючий функцію моніторингу небезпечних ситуацій у приміщені. Робот реалізований на чотирьох колісному шасі з моторами редукторами, обладнаний одноплатним комп'ютером Raspberri Pi 3B, контролером Arduino Motor Shield та мікроконтролером ESP 8266. Збір даних від датчиків температури та вологості DHT11, задимленості BH1750, полум'я й освітленості MQ - 2 та КіВА реалізується на мікроконтролері ESP 8266.

Список використаних джерел

1. Wu Hao, Jiao Menglin, Tian Guohui, Ma Qing and Liu Guoliang "R-KG: A Novel Method for Implementing a Robot Intelligent Service", School of Control Science and Engineering, Shandong University, China, p. 117-140
2. A. Kargin., Y. Luchentsov. "Situation Representation Model Implemented by Granule Fuzzy Characteristics in Mobile Autonomous System", Fourth International Scientific and Technical Conference "Computer, information systems and technology», Kharkiv National University of Radio Electronics, Ukraine