параметрів в процесі експлуатації, вплив зношеності пристроїв на швидкість дрейфу параметрів, що однозначно визначають конкретну ситуацію, тобто прецедент.

Розширення можливостей аналізу зв'язків виміряних параметрів, несправностей та причин їх виникнення, отримані в результаті розпізнавання станів досліджуваного об'єкту у гібридній нейро-нечіткій системі, дозволяють своєчасно виявляти характерні відмови в роботі приладів, приймати заходи з підвищення безпеки, забезпечуючи своєчасний ремонт і технічне обслуговування. Крім того, встановлення причин несправності дозволяє усувати допущені при експлуатації порушення, виявляти дефекти в обладнанні та виробляти подальшу тактику дій у подібних ситуаціях.

Список використаних джерел

1. Ahmad Taher Azar, Sundarapandian Vaidyanathan. Handbook of Research on Advanced Intelligent Control Engineering and Automation. USA: Hershey, Pennsylvania. – IGI Global. – 2015. – 794c. DOI: 10.4018/978-1-4666-7248-2.

Лазарєва Н. М., інженер (УкрДУЗТ)

УДК 656.25

ВИКОРИСТАННЯ ЧИСЛОВИХ ДАНИХ ДЛЯ ІДЕНТИФІКАЦІЇ НЕЧІТКОЇ МОДЕЛІ КЕРУВАННЯ ОБ'ЄКТОМ

Для формування структури модулів нейро-нечіткого керування зазвичай застосовують відому базу правил, яка реалізується у вигляді зв'язків елементів нейронної мережі. При навчанні мережі відбувається оптимальна адаптація функцій приналежності для мінімізації похибки. При цьому верифікація заданих нечітких правил не представляється можливою і вихідний керуючий сигнал може вміщувати похибку, обумовлену не зовсім коректними правилами. Тому при проектування модулів нечіткого керування важливою є задача побудови адекватних функцій приналежності та визначення на їх основі коректних нечітких правил.

Вирішити цю задачу дозволяє підхід table look-up scheme генерації нечітких правил з навчаючих числових даних. Алгоритм розділений на 2 фази: навчання на основі самоорганізації та навчання з вчителем.

Фаза самоорганізації структури усуває необхідність гарного початкового розміщення функцій приналежності і повного апріорного знання всіх нечітких правил. При наявності навчаючих даних для розділення простору вхідних і вихідних змінних використовується метод статистичного групування чи конкурентного навчання, аби початкові функції приналежності охоплювали області, у яких знаходяться дані. Для визначення ширини функцій приналежності застосовується метод «N найближчих сусідів».

Перед тим, як почати побудову правил, формується попередня структура мережі модуля нечіткого керування. Кількість елементів у шарі L1 дорівнює кількості функцій приналежності для кожного входу. Функції одиничного вузла виконують нейронні мережі, які після навчання здатні відображати функції приналежності будь-якої складності. Елементи шару L2 виконують нечітку операцію AND, формуючи на виходах значення степенів активності правил, як мінімальне зі значень ступенів приналежності. Елементи шару L3 реалізують функції приналежності нечітких множин, відповідних висновкам конкретних правил. Після завершення навчання ваги зв'язків третього шару визначають існування висновків і лишаються лише ті зв'язки, що створюють базу правил. Таким чином формується фінальна структура модуля нечіткого керування.

Фаза навчання з вчителем базується на алгоритмі зворотного розповсюдження помилки з метою адаптації модуля нечіткого керування до рішення конкретної задачі керування. В результаті виробляються остаточні значення параметрів функцій приналежності нечітких множин, що містяться в умовах і висновках правил.

Список використаних джерел

1. Chen Wei, Li-Xin Wang. Analysis of table look-up and clustering methods for designing fuzzy systems from input-output data . 14th Triennial World Congress of IFAC, Beijing, P.R. China, 1999. ISBN: 0 08 043248 4.

Ляшенко О. С., к.т.н., доцент,
Комарець К. А. , студент (ХНУРЕ)

РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ УПРАВЛІННЯ ЗАЛІЗНИЧНИМИ ВУЗЛАМИ

Захист критичної інфраструктури включає в себе програми і діяльність власників інфраструктури, операторів і регулюючих органів, які спрямовані на те, щоб підтримувати критично важливі об'єкти інфраструктури в разі збоїв, атак або аварій.

Проблеми безпеки в критичних інфраструктурах пов'язані з особливостями їх реалізації. Критичні інфраструктури засновані на гібридної архітектурі, що поєднує в собі інформаційні комп'ютерні системи та промислові системи, які управляють компонентами, що взаємодіють з фізичними об'єктами. [1]. Така архітектура знижує витрати і підвищує ефективність

системи, але робить критичну інфраструктуру більш вразливою. Тенденція до взаємодії всіх типів інфраструктур збільшує кількість різних атак [2]. Система захисту інформації у рамках розподіленої системи критичної інфраструктури має кілька блоків, які підключаються до різних компонентів системи. Виділено блоки захисту сервера, бази даних, комп'ютера адміністратора та пристроїв. Схема підключення блоків в системі управління залізничними вузлами і шляхами представлена на рис. 1.

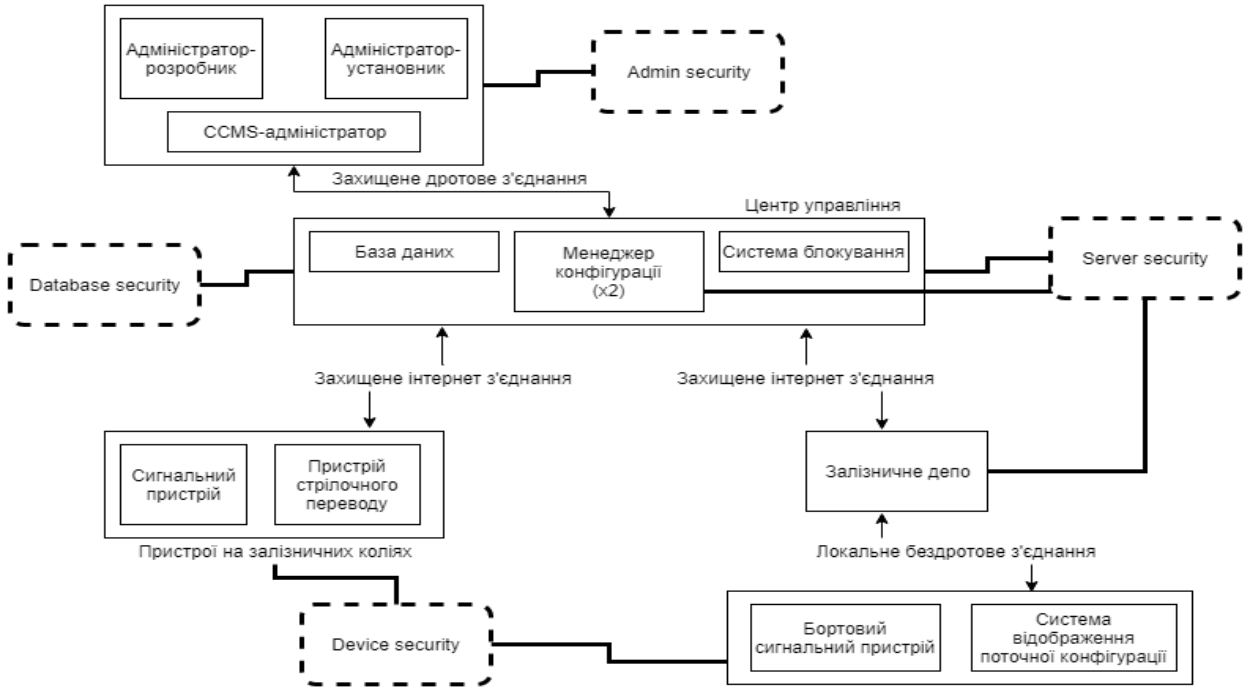

Рис. 1. Архітектура системи захисту інформації

Блок захисту комп'ютерів адміністраторів містить в собі механізм двофакторної автентифікації з паролем і одноразовим кодом, реалізацію протоколу Kerberos, симетричного шифрування AES, електронного цифрового підпису ECDSA, механізм здійснення аудиту. Також на комп'ютерах встановлюється антивірусне програмне забезпечення. Блок захисту бази даних включає в себе симетричне шифрування AES, механізм управління доступом, двухфакторную автентифікацію.

Блок системи захисту інформації сервера складається з реалізації шифрування AES, підписи ECDSA, протоколу Kerberos, підсистеми моніторингу та аудиту, механізм автентифікації за допомогою сертифікатів, управління доступом до сервера, механізми підключення і відключення пристроїв в систему.

Блок захисту інформації на пристрої включає в себе шифрування AES, підпис ECDSA, механізм автентифікації за допомогою сертифікатів, автентифікацію повідомлень, підтримку безпечної передачі даних за допомогою BitTorrent. Для організації роботи кожного блоку був розроблений модуль, відповідальний за безпеку. Його архітектура представлена на рис. 2.

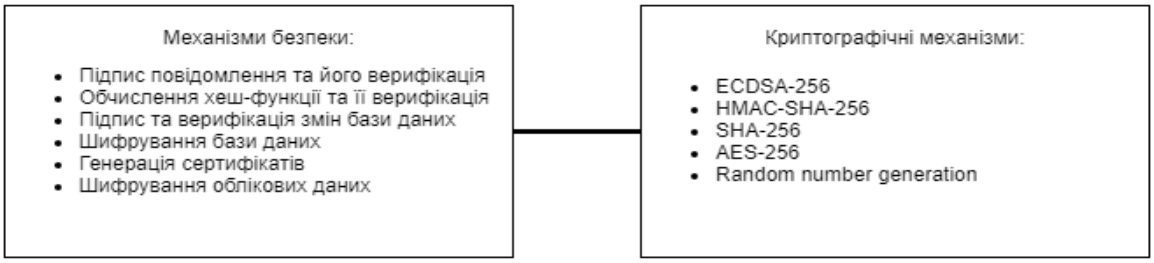

Рис.2. Модуль системи захисту інформації

В результаті злагодженої роботи всіх блоків забезпечується комплексний захист інформації в критичній інфраструктурі. Механізми безпеки, використані в системі захисту інформації повинні відповідати вимогам пристроїв по продуктивності, щоб не забирати все процесорний час. Щоб довести доступність методів для використання на пристроях з обмеженою пам'яттю і продуктивністю, використовувані методи були протестовані. Тестування механізмів безпеки проводилося на емуляторі Raspberry Pi 3.

Для тестування були обрані алгоритми HMAC, хешування SHA-256, електронного підпису ECDSA. Також були поставлені експерименти з різною довжиною переданого повідомлення M на Raspberry Pi 3. Їх результати наведені в таблиці 1. На їх основі довжина в 100 байт обрана як стандартна довжина повідомлення, а довжина 1000 байт як довжина блоку поновлення.

Таблиця

Швидкість обраних алгоритмів в залежності від розміру блоку

Processor model	ECDSA-256 signatures/min	ECDSA-256 verifications/min	HMAC operations/min	SHA-256 operations/min
M=100b	220 000	131 000	3 000 000	25 850 000
M=1000b	200 000	130 000	1 500 000	5 000 000
M=10000b	108 000	122 000	255 000	822 000

На основі цих спостережень можна зробити висновок, що всі ці операції не займуть багато процесорного часу пристрою Raspberry Pi 3, дозволивши йому виконувати основну роботу по виконанню команд і посилці сигналів. З цього випливає, що перераховані вище механізми можна безболісно застосовувати для пристроїв в даній залізничній критичної інфраструктури і в багатьох інших.

Список використаних джерел

1. Merabti M. Critical Infrastructure Protection: A 21st Century Challenge / M. Kennedy, W. Hurst // Conference paper May 2011 - 7 p.
2. Ateniese G. Critical Infrastructure Protection: Threats, Attacks and Countermeasures / R. Baldoni, D. Bloisi, A. Bondavalli, F. Buccafurri, etc. // Tenace March 2014. - 169 p.

Сєвєрінов О. В., к.т.н. доцент,
Овчаренко М. Ю., бакалавр (ХНУРЕ)

АНАЛІЗ СИСТЕМ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Управління інцидентами інформаційної безпеки грає важливу роль в рішенні питань інформаційної безпеки систем критичної інфраструктури. Інцидент інформаційної безпеки це одиночна подію або ряд небажаних та непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці [1].

При забезпеченні інформаційної безпеки систем критичної інфраструктури одним з найважливіших видів діяльності є виявлення інцидентів інформаційної безпеки. При цьому актуальною є задача автоматизації процесу управління інцидентами. На сьогоднішній день відомо багато різноманітних систем управління інцидентами, серед яких найбільш поширені DLP (Data Leack Prevention), EDR (Endpoint Detection and Response), UEBA (User and Entity Behavior Analytics) та SIEM (Security Information and Event Management) системи .

User and Entity Behavior Analytics (UEBA) – клас систем, що збирають інформацію не лише про користувачів та їх ролі у системі, а також про системне оточення (робочі станції, сервери, програмне забезпечення, мережевий трафік), що дає можливість ідентифікувати більш широкий клас загроз, та формує відповідно них моделі нормальної поведінки користувача та його взаємодії з корпоративними системами [2]. Якщо дії користувача виходять за рамки побудованої моделі, UEBA-система визначає цю поведінку як аномальну та створює відповідне попередження для адміністратора безпеки. Також система надає інформацію про те, до яких систем та з якими правами певний користувач здійснював доступ, що в свою чергу дозволяє редагувати права доступу користувачів до певних цільових систем.

SIEM (Security information and event management) - програмні продукти, які об'єднують управління інформаційною безпекою SIM (Security Information Management) та управління подіями безпеки SEM (Security Event Management) та забезпечують аналіз в реальному часі подій, отриманих від мережевих пристроїв та додатків, а також журналювання даних і генерацію звітів для подальшого їх аналізу [2].

DLP (Data Leak Prevention) - технології запобігання витоку конфіденційної інформації з інформаційної