TECHNICAL SCIENCES

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРЕДАЧІ ІНФОРМАЦІЇ СИСТЕМ ДИСТАНЦІЙНОГО КОНТРОЛЮ ТА ДІАГНОСТИКИ ОБРОБНИХ ЦЕНТРІВ

Лисенко Олександр Володимирович
Кандидат технічних наук, доцент
(Центральноукраїнський національний технічний університет)
Лисенко Ірина Анатоліївна
Кандидат технічних наук, старший викладач
(Центральноукраїнський національний технічний університет)

На початок 2010-х років здавалося, що можливості використання інформаційно-комунікаційних технологій у виробництві майже вичерпались, коли в 2011 році урядом Німеччини була анонсована концепція «Industry 4.0» [1], що пропонувала новий підхід до організації виробничих процесів, заснований на активному впровадженні мережевих технологій та використанні штучного інтелекту. Пізніше подібні програми були прийняті і в інших країнах: Великобританії, Франції, Італії, Нідерландах, США (Промисловий Інтернет), Японії (Ініціатива промислового ланцюга створення вартості), КНР (Зроблено в Китаї 2025), Румунії, Україні (Стратегія розвитку промислового комплексу) та ін.

Розглянемо ідеальний випадок роботи сервісного центру компанії виробника промислового обладнання, що встановлене на деяке підприємство без використання інструментів «Industry 4.0», у випадку коли воно вийшло з ладу. Першим днем будемо вважати день зупинки функціонування. Після звернення до сервісного центру компанії виробника, на другий день прибуває спеціаліст, який діагностує причину виходу з ладу устаткування, ступінь необхідного ремонту та потребу в заміні деталей, вузлів та систем, після чого передає всю отриману інформацію у свою компанію. На третій день прибуває команда спеціалістів разом з усім необхідним для ремонту обладнанням. В залежності від складності процес діагностики та ремонту може зайняти від одного до кількох днів.

Тобто в ідеальному випадку компанії виробнику знадобиться як мінімум від трьох до п’яти днів на ремонт, налагодження та повернення у роботу обробного центру. Якщо ж виникають певні форс-мажори, наприклад не можливість оперативно відреагувати сервісного центру, відсутність на складі необхідних запасних частин та вузлів, зайнятість спеціалістів для ремонту та ін. то час відновлення працездатності може розтягтись й до двох-трьох тижнів та навіть місяців, у випадку, якщо обладнання, що ремонтується унікальне та потребує виготовлення деталей та вузлів необхідних для його ремонту.

Дистанційне обслуговування обробних центрів за допомогою підключення через мережу Інтернет в межах концепції «Industry 4.0» для оптимізації процесу роботи, обслуговування, попередньої діагностики, завчасного виявлення та запобігання можливих несправностей та ремонту у випадку їх виникнення

дозволяє або взагалі запобігти поломкам обробного центру, або зменшити час його ремонту до кількох годин. Оскільки вся необхідна інформація по діагностуванню стану устаткування в режимі реального часу передається у сервісний центр виробника, команда спеціалістів прибуває завчасно та з повним розумінням необхідної для обслуговування обробного центру номенклатури робіт.

Прикладами систем «Industry 4.0» дистанційного моніторингу, контролю та діагностики обробних центрів безпосередньо у процесі роботі слугують система управління TX8i-s V8 Німецької компанії Index group [2], що під брендами INDEX та TRAUB виготовляє металообробні центри та KDT RemoteServices компанії по виготовленню деревообробних центрів KDT WoodworkingMachinery [3].

Однак практика впровадження подібних систем у реальне виробництво, показує що багато підприємств, особливо з чутливих до втрати інформації секторів, відмовляються від подібних сервісів компаній виробників обробного обладнання. Як правило, це високотехнологічні компанії, зокрема авіаційно-космічної галузі, це компанії оборонних комплексів країн та науково-дослідні центри.

Це відбувається через відсутність гарантованого захисту інформації при передачі через мережу Інтернет, тому компанії, що остерігаються витоку критично важливої інформації вимушені відмовлятись від підключення їхнього обладнання до систем дистанційного моніторингу та нести суттєві втрати при виході їх з ладу.

В цих умовах перспективним є застосування захищених каналів зв'язку передачі даних або підсилення і удосконалення існуючих методів шифрування даних. Серед перспективних напрямків розвитку систем захисту інформації на перше місце виходять методи наскрізного шифрування, а коли цінність інформації складає більше часу ніж потрібно для шифрування онлайн то, знехтувавши часом на передачу інформації можна звернути увагу на більш складні способи шифрування, які за рахунок складності мають набагато більший рівень криптостійкості.

Серед сучасних способів шифрування існує цілий ряд стандартів, прийнятих у різних країнах. Криптостійкість цих шифрів перевірена і повністю підтверджена рядом тестів та практики їх використання. Серед найбільш розповсюджених алгоритмів це RSA та ECC [4].

Для кожного з існуючих методів шифрування важливою складовою процесу є генерація ключів шифрування і їх відповідна криптостійкість, що підвищує захищеність алгоритму в цілому. Для генерації ключів шифрування використовують генератори випадкових та псевдовипадкових чисел. Під час створення числового потоку використовують різні фізичні процеси та математичні методи. Серед математичних методів це алгебраїчні, геометричні, функціональні послідовності. Звернемо увагу на метод генерації псевдовипадкових чисел, заснований на отриманні числової послідовності, як координат точок на уявній площині під час руху точки хаотично, спираючись на

початкове її положення – більярд Колмогорова-Сіная [5]. Як показують дослідження, цей процес є достатньо хаотичним, згенеровані послідовності показують гарні результати під час їх тестування на зациклювання і періодичність. Процес не потребує великих обчислювальних потужностей, при виборі для використання із стандартним методом шифрування, дасть надійний спосіб захисту технічної інформації, що передається навіть по відкритих каналах зв'язку.

Література:

1. Lüber, K. Розумні фабрики в німецькій промисловості URL: https://www.deutschland.de/ru/topic/ekonomika/iskusstvennyy-intellekt-industriya-40-umnaya-fabrika

2. TRAUB TX8i-s V8 URL:https://www.index-group.com/ru/produkcija/programmnoe-obespechenie-i-upravlenie/upravlenie/traub-tx8i-s-v8

3. KDT Woodworking Machinery URL:https://kdtmac.com.ua/uk/

4. Гнатюк С.О., Кінзерявий В.М., Поліщук Ю.Я., Нечипорук О.П., Горбаха Б.М. Аналіз методів забезпечення конфіденційності даних, які передаються з БПЛА https://csecurity.kubg.edu.ua/index.php/journal/article/view/393/326

5. Лисенко І.А. Дослідження використання більярду Сіная для генерації псевдовипадкових послідовностей / І.А. Лисенко, О.Г. Собінов // Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей III Міжнародної науково-практичної конференції, 19-20 квітня 2018 року, м. Кропивницький: ЦНТУ, 2018. – С. 91-93.