повороту, було б краще щоб він спочатку знизив швидкість і плавно повернув колеса для виконання повороту. При цьому важливо, щоб в управляючій програмі не завершувалася поточна команда і вже починалася інша, та обидві команди деякий час виконувалися одночасно. Нова модель припускає виконання наступної команди з послідовності УП без завершення попередньої. Тобто контролер підтримує режим паралельного й одночасного виконання різних команд.

Для застосування методу м'якого програмного управління, необхідно створювати спеціальну модель виконуючого механізму. Головна ідея виконуючого механізму запозичена у живій природі та сформульована у вигляді концептуальної моделі. Модель біологічного виконавчого механізму (м'язове волокно) з дослідженою біологами динамікою поведінки, формалізована у математичну модель елементарного виконавчого механізму та створюється комп'ютерна модель. Це дасть можливість створити нечіткий контролер, який буде виконувати кооперацію множини елементарних виконавчих механізмів з урахуванням особливостей методу м'якого програмного управління.

Список літератури:

1. *Siciliano B., Khatib O.* (eds.) Springer Handbook of Robotics (2nd ed.) / *B. Siciliano, O. Khatib.* – Berlin, Heidelberg: Springer-Verlag, 2016. – 2227 P. – ISBN: 978-3-319-32550-7. – e-ISBN: 978-3-319-32552-1. **2.** *Anatolii Kargin, Tetyana Petrenko.* Knowledge Distillation for Autonomous Intelligent Unmanned System / In: *Witold Pedrycz, Shyi-Ming Chen*. Advancements in Knowledge Distillation: Towards New Horizons of Intelligent Systems. Studies in Computational Intelligence, vol. 1100. Springer International Publishing, 2023, Pages 193-230. https://doi.org/10.1007/978-3-031-32095-8_7

УДК 330.131.7

Кандидат технічних наук В. В. Лагута
Український державний університет науки і технологій, м. Дніпро
О.В. Лагута
Луганський науково-дослідний експертно-криміналістичний центр МВС України, м. Дніпро.

КОМПОНЕНТИ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Інформація, що має має цінність для організації, повинна бути захищеною. В багатьох випадках загрози, що приносять незначну для організації шкоду, не враховуються. У разі реалізації кількох таких загроз разом організація може відчутно «постраждати». Нові загрози та вразливості знижують ефективність впроваджених засобів захисту за відсутності змін. Реалізація контрзаходів перестає бути останнім етапом захисту інформації об'єкта. Розуміння необхідності впровадження заходів щодо забезпечення інформаційної безпеки організації як безперервного процесу зумовлює потребу в управлінні цією діяльністю.

Важливими компонентами системи інформаційної безпеки (ІБ) є її рівні управління. При проектуванні інформаційних систем питання безпеки не завжди беруться до уваги [1]. Питання управління інформаційною безпекою включають не лише технічну складову. Без підтримки керівництва та виділення необхідних ресурсів неможливо забезпечити ефективний захист від інформаційних загроз.

Процес управління ІБ носить циклічний характер і полягає в наступному:

– опис активів, що захищаються;

– виявлення та формалізація можливих загроз інформаційній безпеці;

– аналіз ризиків інформаційної безпеки;

– розробка контрзаходів;

Управління ІБ включає 3 рівні.

Стратегічний рівень характеризує забезпечення інтересів організації у сфері безпеки. На цьому рівні визначаються стратегія та основні заходи щодо забезпечення інформаційної безпеки.

На *тактичному* рівні здійснюється планування та забезпечення виконання Політики інформаційної безпеки. Розробляються необхідні регламенти, правила та інструкції. Проводяться розслідування та аналіз інцидентів інформаційної безпеки.

Оперативний рівень управління включає реалізацію конкретних контрзаходів, що нейтралізують інформаційні загрози.

Іншим важливим компонентом управління інформаційною безпекою є моніторинг впроваджених контрзаходів. Комплекс заходів щодо забезпечення інформаційної безпеки повинен оцінюватися з постійним інтервалом шляхом внутрішнього та незалежного аудиту [2].

Внутрішній аудит проводиться для визначення ефективності впроваджених контрзаходів. Такі перевірки передусім мають бути спрямовані на усунення недоліків. Вони повинні ретельно готуватися для забезпечення якомога ефективнішого досягнення їх цілей, водночас не викликаючи порушення штатної роботи організації. За результатами дій з моніторингу керівництву має бути поданий звіт. Цей документ має містити перелік рекомендованих дій з чітко визначеними

пріоритетами разом із реальною оцінкою передбачуваних витрат виконання кожного з цих дій.

Вибір аудиторів для внутрішнього аудиту може виявитися складним для невеликих компаній. Для проведення перевірочних заходів важливо призначити працівників, які не брали участь у плануванні та розробці заходів щодо забезпечення інформаційної безпеки через необ'єктивність такої перевірки. Необхідно також враховувати суб'єктивність прийняття рішень щодо оцінки діяльності своїх колег по роботі. Щодо цього, якщо керівництво готове виділити кошти, можна залучити зовнішніх аудиторів. Погляд із боку завжди дозволяє виявити певні аспекти, які можуть бути втрачені під час проведення перевірок власними силами. Зовнішні аудитори компетентні у своїй галузі, однак, можуть врахувати не всі особливості організаційного середовища компанії, що перевіряється. Безумовно, власні співробітники краще знають тонкощі процесів, що протікають в організації. Тому для ефективного моніторингу захищеності об'єкта від інформаційних загроз корисно чергувати періодичні перевірки, які проводяться власними силами, з перевірками, що здійснюються зовнішніми аудиторами.

Важливо наголосити на необхідності розгляду заходів щодо забезпечення інформаційної безпеки як безперервного процесу, яким необхідно керувати, реалізації певних заходів щодо забезпечення інформаційної безпеки за допомогою розробки економічного обґрунтування. Економічне обґрунтування є основним засобом для того, щоб переконати керівництво у фінансуванні запропонованих заходів. Необхідно приділяти особливу увагу моніторингу запроваджених контрзаходів. З метою підвищення ефективності управління інформаційною безпекою важливо періодично залучати зовнішніх аудиторів до внутрішніх перевірок.

Перелік посилань

5. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection – Guidance on managing information security risks [Электронный ресурс] // – URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en (Дата звернення: 01.09.2022)
6. ISO/IEC 27004, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. [Электронный ресурс] // – URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27004:ed-2:v1:en (Дата звернення: 01.09.2022)

УДК 004.05

к.т.н. В.В. Лагута, Л.С. Тимошенко
Український державний університет науки і технологій, Дніпро

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ ЕФЕКТИВНОСТІ КОМПОНЕНТІВ СИСТЕМИ ЗАЛІЗНИЧНОЇ АВТОМАТИКИ З УРАХУВАННЯМ ЇХ ПОТОЧНОГО СТАНУ

Ефективність системи залізничної автоматики та телемеханіки (СЗАТ) є головним чинником у виконанні перевізного процесу та забезпечення безпеки руху поїздів. Завдання, що базуються на кількісній оцінці ефективності СЗАТ [1, с. 25], передбачають визначення кількісного показника, який виражає ймовірність виконання певним засобом поставленого завдання. Метою дослідження є визначення ключових принципів, дотримання яких дозволить системі ефективно виконувати свої функції:

– система повинна бути постійно готовою до експлуатації та зберігати працездатність;

– справна система повинна володіти набором характеристик, які забезпечують успішне виконання поставленого завдання.

Для оцінки надійності можуть використовуватись технічні та організаційні показники, що відображають:

– співвідношення між часом роботи та простоєм елементів СЗАТ (коефіцієнти готовності, вимушеного простою, профілактичних робіт);

– частоту проведення профілактичних заходів для запобігання відмовам;

– вплив надійності елементів СЗАТ на загальні експлуатаційні показники системи управління рухом поїздів.

Пристрої СЗАТ належать до систем, що потребують обслуговування. З одного боку, проведення профілактичних оглядів сприяє підвищенню готовності пристроїв до їх експлуатації, але з іншого боку, це може негативно вплинути на деякі показники, які визначають ефективність системи. Це обумовлено тим, що профілактика вимагає залучення кваліфікованого персоналу та використання спеціалізованої контрольно-вимірювальної апаратури, що збільшує витрати на експлуатацію. Крім того, технічний ресурс обладнання використовується не за прямим призначенням. Також відомо, що під час профілактичних робіт може зрости інтенсивність відмов через втручання обслуговуючого персоналу в діючі пристрої. Відновлення працездатності системи потребує певного часу, який включає: