

характер поведінки агента, рівень його автономності та інтелектуальності.

Процесор забезпечує об'єднання і перероблення різнорідних даних, вироблення відповідних реакцій на інформацію про стан середовища, прийняття рішень про виконання тих чи інших дій. Вибір відповідних дій за заданих обмежень – одна із ключових здібностей агентів.

Використання штучного інтелекту дозволяє дронам працювати автономно та координовано, зменшуючи залежність від людського керівництва та підвищуючи ефективність виконання завдань.

Перелік посилань. 1 Negnevitsky. A Guide to Intelligent Systems Second Edition. Addison Wesley. 2005. 415pp.

2. Russell and P. Norvig. (2010). Artificial Intelligence Modern Approach. (3rd edition). [online]. Available: www.pearsonhighered.com [Oct., 2015]. 1131 pp.

УДК 621.391

КРОЩЕНКО Д.О., аспірант (УкрДУЗТ)

Аналіз принципів представлення та декодування завадостійких кодів Лабі

У теперішній час для побудови телекомунікаційних систем та мереж різних видів потрібно використовувати сучасні телекомунікаційні технології, стандарти та протоколи, які реалізуються за допомогою цифрового обладнання. При цьому телекомунікаційна інфраструктура має задовольняти низку вимог, серед яких важливе значення має забезпечення заданої достовірності передачі інформації [1,2].

Важливим інструментом в телекомунікаційних системах, особливо для передачі даних через ненадійні канали зв'язку є застосування завадостійких кодів на основі перетворення Лабі. Коди Лабі широко застосовуються в телекомунікаціях завдяки своїм універсальним властивостям, які дозволяють забезпечити надійну передачу даних із зниженням впливу помилок і змінних умов мережі [2,3].

Проаналізовано ефективність використання завадостійких кодів Лабі. Розглянуто процеси кодування та декодування даних кодів та можливості використання кодів Лабі для забезпечення

надійності та ефективності різних мережевих протоколів.

Література

1. Ільченко М.Ю. Сучасні телекомунікаційні системи / М.Ю. Ільченко, С.О. Кравчук. – К.: НВП Видавництво «Наукова думка» НАН України. – 328 с

2. Штомпель Н. А. Тенденции развития методов помехоустойчивого кодирования информации в телекоммуникациях. Зв'язок, радіотехніка, радіолокація, акустика та навігація. 2017. 1(50). С. 35-37

3. Joe Louis Paul I, Radha S., Raja J. Throughput and Bit Error Rate Analysis of Luby Transform Codes with Low and Medium Nodal Degree Distributions. American Journal of Applied Sciences 11 (9): 1584-1593, 2014

УДК 004.89:004.383.8

д-р техн. наук, проф. А.О. Каргін, асп. Р.С. Кузьменко, УкрДУЗТ, м. Харків

МОДЕЛЬ ВИКОНАВЧОГО МЕХАНІЗМУ В М'ЯКОМУ ПРОГРАМНОМУ УПРАВЛІННІ В АВТОНОМНИХ БЕЗЛЮДНИХ СИСТЕМАХ

В сучасному світі поширені автономні безлюдні системи. Вони знайшли широке застосування у сферах військового, промислового, побутового, аграрного [1] та освітнього застосування.

Однією з важливих компонент в складі автономних безлюдних систем є управляюча програма (УП). На даний момент відомі такі моделі управління [2]: жорстке та гнучке програмне управління, ситуаційне управління та цілеспрямоване управління. Дані підходи мають свої переваги та недоліки в залежності від сфери та умов їх застосування.

В доповіді наведена інформація, щодо необхідності моделі м'якого програмного управління. Розглянемо завдання переміщення колісного робота на певному маршруті у якості прикладу такого завдання. У випадку жорсткого програмного управління, команди виконуються у певному порядку і мають фіксовані характеристики та вони при цьому будуть попередньо розрахованими у часі виконання. У разі застосування гнучкого програмного управління, команди будуть доповнені даними з сенсорів та будуть опиратися на ці дані з сенсорів для контролю моменту завершення. Обидва підходи мають певні недоліки. Наприклад, у випадку коли колісний робот наближається до

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 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 перестав 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