робіт (НДР), відповідно до якого проводиться виготовлення, приймання при введенні в дію та експлуатація відповідного об'єкта. Згідно з ГОСТ 34.602-89 ТЗ є основним документом, що визначає вимоги і порядок створення (розвитку або модернізації) інформаційної системи, відповідно до якого проводиться її розробка і приймання при введенні в дію [6].

Останнім завданням розробки являється синтез оптимальної КСЗІ, після чого відбувається її впровадження та супровід. Оптимальною системою називають систему, яка має один або декілька екстремальних значень при обмеженнях на інших значеннях (наприклад, рівень захисту, швидкодія, вартість, надійність). Далі створюються цільові функції та здійснюється вибір механізмів захисту. При прийнятті рішення про вибір найкращого варіанту КСЗІ відповідно до обраного критерію виникає завдання визначення вимог, що пред'являється до параметрів системи при заданій її структурній схемі. При побудові оптимально варіанту КСЗІ використовують основні кваліметрії (якісне вимірювання показників).

Таким чином, кожен етап являється важливим і доповнює наступний, і це дає нам можливість створити надійну систему захисту для підвищення рівня захищеності автоматизованої системи обробки інформації, яка зможе витримати потужну атаку, але, як відомо з філософії безпеки: «Система безпеки надійна настільки, наскільки надійна її найслабша ланка». Тому не існує ідеального захисту – існує удосконалений з часом захист.

Література

1. НД ТЗІ 3.7-003-05. 2005. URL : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835.

2. НД ТЗІ 1.1-002-99. 2012. URL : www.dsszzi.gov.ua/dsszzi/doccatalog/ document?id=106340.

3. НД ТЗІ 1.4-001-2000. 2012. URL : www.dsszzi.gov.ua/dsszzi/doccatalog/ document?id=106341.

4. НД ТЗІ 2.7-001-99. 2012. URL : www.dsszzi.gov.ua/dsszzi/doccatalog/ document?id=106346.

5. Дудатьєв А. В. Моделі для організації протидії інформаційним атакам. 2015. URL : jrnl.nau.edu.ua/index.php/ZI/article/download/8790/10817.

6. ГОСТ 34.602-89. 1990. URL : ingraf.su/wp-content/uploads/2015/11/gost_34_602_89.pdf.

УДК 004.032.26:621.311.1

КЛАСИФІКАЦІЯ І АЛГОРИТМИ НАВЧАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

О. А. Коротких

Актуальність теми. З кожним роком зростає зацікавленість вирішення більш складних задач розпізнавання об'єктів, що обумовлена автоматизацією, необхідністю образних процесів комунікації в інтелектуальних системах. Тому удосконалення реалізації розпізнавання комп'ютерними системами образів є актуальною. Один з перспективних напрямків вирішення даної проблеми ґрунтується на застосуванні штучних нейронних мереж і нейрокомп'ютерів, як найбільш прогресивних по відношенню проблем класифікації задач розпізнавання образів. У наш час запропоновано велику кількість архітектур нейромереж для застосування у розпізнаванні об'єктів. Аналіз запропонованих рішень показує, що й досі не існує такої моделі, яка б була кращою серед усіх результуючих показників роботи.

Одним з провідних напрямків досліджень у галузі штучного інтелекту є машинне навчання, синтез та моделювання штучних нейронних елементів (НЕ) та нейромереж, розроблення методів їх навчання та оптимізації, вдосконалення нейромережних технологій обробки та аналізу даних, створення прикладних систем на основі нейронних мереж. Штучні нейронні мережі (ШНМ) знаходять застосування у наступних сферах: класифікація та

розпізнавання образів, системи асоціативної пам'яті, компресія даних, оптимізаційні задачі, теорія керування, розробка нейрокомп'ютерів, наближення функцій з високою точністю, екстраполяція та прогнозування.

Розвиток теорії штучних нейронних мереж багато у чому пов'язаний із іменами У. Маккалока, Ф. Розенблатта, Б. Уідроу, М. Мінскі, Т. Кохонена, С. Мууроги, В. Вапніка, Д. Хопфілда, Дж. Хінтона та інших. Значний внесок був зроблений українськими вченими М. Амосовим, О. Івахненком, Є. Бодянським, Н. Айзенбергом, І. Айзенбергом Р. Ткаченком, Л. Тимченком, О. Михальовим, В. Литвиненком, Ф. Гече, П. Тимощуком, Ю. Романишином.

Однак, незважаючи на значні успіхи, досягнуті останнім часом у застосуванні нейромережних технологій, при використанні прикладних систем на основі штучних нейронних мереж необхідно вирішувати такі завдання, які існуючими системами на основі традиційних нейропарадигм розв'язуються з недостатньою точністю або швидкістю. Саме тому актуальним є вирішення задачі розробки і дослідження моделей узагальнених штучних нейронних елементів, які мають більш високі функціональні можливості, ніж звичайні нейронні елементи. Важливою науковою задачею є розроблення та обґрунтування ефективних методів навчання ШНМ, побудованих на основі узагальнених нейронних елементах.

Література

1. Хайкин С. Нейронные сети, полный курс. 2-е изд., перед. М. : Вильямс, 2008. 1103 с. ISBN 5-8459-0890-6

2. Whitely D., Starkweather T., Bogart C. Genetic Algorithms and Neural Networks: Optimizing Connections and Connectivity. *Parallel Computing.* 1990. Vol. 14.

3. Tang C., He Y., Yuan L. A Fault Diagnosis Method of Switch Current Based on Genetic Algorithm to Optimize the BP Neural Network : International Conference on Electric and Electronics. 2011. Vol. 99.

4. Jinru L., Yibing L., Keguo Y. Fault diagnosis of piston compressor based on Wavelet Neural Network and Genetic Algorithm : Proceedings of the 7th World Congress on Intelligent Control and Automation. 2008.

5. Wu W., Guozhi W., Yuanmin Z., Hongling W.Genetic Algorithm Optimizing Neural Network for Short-Term Load Forecasting : International Forum on Information Technology and Applications. 2009.

УДК 544.421.43:544.421.032.76:544.431.122.2:547.541:547.636.3

СТВОРЕННЯ ДОДАТКУ З ГРАФІЧНИМ ІНТЕРФЕЙСОМ «РЕАЛІЗАЦІЯ АЛГОРИТМУ ШИФРУВАННЯ RC5»

В. Г. Крижановський, А. І. Шевченко

Блочний шифр RC5 - алгоритм прямого шифрування, при якому береться блок даних заданого розміру (2w бітів) і з нього за допомогою залежного від ключа перетворення генерується блок шифрованого тексту такого самого розміру. Цей режим часто називають режимом ECB (режим електронної шифрувальної книги).

У класичному алгоритмі використовуються три примітивних операції їх інверсії:

- складання по модулю;
- побітовое виключення АБО (XOR);
- операції циклічного зсуву на змінне число біт.

Основним нововведенням є використання операції зсуву на змінне число біт, що не використалися в більш ранніх алгоритмах шифрування. Ці операції однаково швидко виконуються на більшості процесорів, але в той же час значно ускладнюють диференційний і лінійний криптоаналіз алгоритму.