класу зображень навпаки, збільшує об'єм стискуваного файлу [2], що і було досліджено і сформувано класифікацію алгоритмів зрозумілу для застосування.

Метою роботи є дослідження алгоритмів стиснення зображення, щоб виявити, який з них ефективніший для стиснення, та має кращі характеристики в роботі, і відповідає вимогам в швидкодії процесу стиснення зображень, та зменшення обчислювальної складності й збільшення стиснення за їх основним характеристикам, таким як: точність відновлення, симетричність основного перетворення і тип використовуваного перетворення [3], та забезпечує отримання зображення належної якості після стиснення.

Підсумовуючи роботу можна сказати, що розгляд і порівняння та дослідження різних алгоритмів стиснення зображення показує доречність використання потрібного алгоритму до відповідного класу зображень, відповідно до потребуючих на даний момент часу вимог, що полегшує вибір потрібного алгоритму стиснення при застосуванні стиснення зображень.

Таблиця 1

Параметри різних алгоритмів стиснення зображень

Алгоритм	Коефіцієнти стиснення	Симетричність за часом	На що орієнтований	Втрати	Розмірність
RLE	32, 2, 0.5	1	3,4-х бітні	Немає	1D
LZW	1000, 4, 5 / 7	1.2-3	1-8 бітні	Немає	1D
Хаффмана	8, 1.5, 1	1-1.5	8 бітними	Немає	1D
CCITT-3	213 (3), 5, 0.25	~ 1	1-бітні	Немає	1D
JBIG	2-30 разів	~ 1	1-бітні	Немає	2D
Lossless JPEG	2 рази	~ 1	24-бітові, сірі	Немає	2D
JPEG	2-20 разів	~ 1	24-бітові, сірі	Є	2D
Рекурсивний стиск	2-200 разів	1.5	24-бітові, сірі	Є	2D
Фрактальний	2-2000 разів	1000-10000	24-бітові, сірі	Є	2.5D

Література

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. / пер. с англ. Москва. Техносфера. 2006. 1072 с.
2. Тропченко А. Ю., Тропченко А. А. Методы сжатия изображений, аудиосигналов и видео: Учебное пособие. СПб: СПбГУ ИТМО, 2009. 108 с.
3. Сэломон Д. Сжатие данных, изображений и звука. М. Техносфера. 2004. 368 с.

УДК 004.056.5:625.748.54

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АЗС

В. І. Кацюк

На сьогоднішній день захист інформації стає більш складнішою проблемою, оскільки відбувається масове розповсюдження засобів електронної обчислювальної техніки, розповсюдження інформації про шифрувальні технології, використання неперевіреного програмного забезпечення (наприклад, що містить віруси), хакерські атаки, отриманням спаму, халатністю співробітників, що виникає доволі часто. Рідше втрата даних викликана такими причинами, як збій в роботі апаратно-програмного забезпечення або крадіжка обладнання. В результаті компанії зазнають значних втрат. Для визначення наявності у складі інформації видів, що потребують обмеження доступу, створюють КСЗІ (Комплексну систему захисту інформації) – взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, – яка згідно з НД ТЗІ 3.7-003-2005 регламентується 6 етапами [1]:

1) формулювання загальних вимог до створення КСЗІ;
2) створення чи розробка політики безпеки;

3) розробка технічного завдання на створення КСЗІ;

4) створення КСЗІ;

5) впровадження КСЗІ (оцінка ефективності функціонування КСЗІ);

6) супроводження системи.

Щоб захистити свою інформацію від зовнішніх та внутрішніх чинників, потрібно дотримуватися плану захисту, який розробляється на підставі проведеного аналізу технології, аналізу ризиків, політики безпеки, документів, які створюються на етапі створення і супроводу КСЗІ. Створення КСЗІ передбачає виконання вищенаведених шести етапів незалежно від того, чи створюється система ІТС вперше, чи створюється ІТС та КСЗІ паралельно, чи ІТ модифікується, але в деяких випадках передбачається виконання іншої послідовності створення КСЗІ [1]. Необхідність побудови КСЗІ визначається вимогами нормативних документів у сфері технічного та криптографічного захисту інформації або бажанням власника інформаційних ресурсів.

Метою роботи є розробка КСЗІ для підвищення рівня захисту автоматизованої системи обробки інформації класу «1» АЗС. Для досягнення мети потрібно визначити такі завдання:

1) аналіз об'єкта (структура організації, матриця доступу до даних, визначення автоматизації об'єкта, модель порушника, модель загроз);

2) ідентифікація внутрішніх та зовнішніх загроз об'єкту захисту;

3) створення математичної моделі оцінювання рівня захищеності та ранжування негативних факторів, що впливають на критичні інформаційні потоки та інформаційні ресурси;

4) створення політики безпеки та технічного завдання;

5) синтез оптимальної КСЗІ, що включає розробку цільової функції та комбінацію механізмів.

До аналізу об'єкта відносяться: визначення структури АЗС (автоматизований тип передачі інформації та за допомогою персоналу); матриця доступу до даних, в яку входять носії інформації та дії працівників над цими носіями; розробка моделі порушника, де визначаються зовнішні та внутрішні групи порушників [4]; створення моделі загроз – формалізованого опису методів та засобів здійснення загроз для інформації [4].

Щоб розпочати розробку математичної моделі оцінювання захищеності, необхідно ідентифікувати загрози – внутрішні та зовнішні. Це можна зробити двома способами: статистичним та методом експертних оцінок (фазифікація та дефазифікація). На практиці статистичних даних у більшості випадків недостатньо або статистика взагалі відсутня, тому у таких випадках використовують другий вищенаведений підхід. Метод експертних оцінок дозволяє формалізувати будь-які дані, які представлені у нечіткій або якісній формі, наприклад метод центру ваги.

Існує кілька видів математичних моделей, але серед них найчастіше виділяють наступні: логіко-імовірнісні, імовірнісні, нейромережеві моделі [5]. Для свого об'єкта ми обрали логіко-імовірнісне моделювання, яке дозволяє побудувати причинно-наслідкові зв'язки. Це, в свою чергу, дозволяє локалізувати так звані первинні причини виникнення (порушення) базових критеріїв (цілісності, доступності, конфіденційності). Модель може бути представлена у вигляді дерева подій або у вигляді системи логічних рівнянь [5]. Будемо застосовувати методи логіко-ймовірнісного моделювання (метод дерев ризику-відмов).

Розробка політики безпеки, тобто трьохрівневої політики безпеки, передбачає використання нормативних документів, зокрема НД ТЗІ 1.1 та НД ТЗІ 1.4, і методологій. Також вона створюється на базі отриманих результатів аналізу об'єкта захисту і обов'язково включає в себе так звану функціональну та каральну частини. Реальна політика безпеки має гарантувати заданий рівень захисту [2, 3].

У технічному завданні визначаються всі вимоги до розроблювальної КСЗІ. Технічне завдання є вихідним документом для проектування споруди чи промислового комплексу, конструювання технічного пристрою (приладу, машини, системи керування тощо), розробки автоматизованої системи, створення програмного продукту або проведення науково-дослідних

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