При цьому логічно вважати, що найгіршим, або інакше – катастрофічним випадком є відмова, внаслідок якої атака на стегосистему може бути проведена випадковим порушником.

Вочевидь з (1) слідує, що множини E,D,C,B та A не перетинаються, тому для ймовірності $p_{від}$ виникнення в ЗРСП відмови маємо: $p_{від}=p_e+p_d+p_c+p_b+p_a$, де складові правої частини рівняння є ймовірностями належності відмови до однієї з п'яти визначених множин.

У визначених умовах у разі $n \cdot p_{від} \to \lambda_{від}=\lambda_e+\lambda_d+\lambda_c+\lambda_b+\lambda_a$ при $n \to \infty$ для оцінки розподілу відмов, що мають наслідком погіршення стеганографічних властивостей, можливо скористатися апроксимацією у вигляді розподілу Пуассона:

$$e^{-(\lambda_d+\lambda_c+\lambda_b+\lambda_a)} \cdot \frac{\lambda_d^j \cdot \lambda_c^k \cdot \lambda_b^l \cdot \lambda_a^m}{j!\cdot k!\cdot l!\cdot m!}$$

Зокрема, для ймовірності надійної роботи з точки зору інформаційної безпеки $p_{ніб}$ маємо:

$$p_{ніб} = e^{-(\lambda_d+\lambda_c+\lambda_b+\lambda_a)}$$

З урахуванням викладеного, у підсумку проведення інженерного аналізу ЗРСП мають бути оцінені відповідні параметри та розрахована ймовірність небезпечних ситуацій у випадку виникнення відмов.

Список літератури.

1. *Липаев В.В.,* Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств, Информационный бюллетень "Jet Info 08(135)/2004", www.jetinfo.ru

2. *Гулак Г.М.* Оцінка ризиків у ході проведення інженерного аналізу безпеки стеганографічних систем/ Защита информации: сборник научных трудов.– Киев, НАУ, 2008. С.259-264

3. *ГОСТ 27.002-89.* Надежность в технике. Основные понятия. Термины и определения. - М.: Издательство стандартов, 1989. –37с.

4. *ДСТУ 3524-97 (ГОСТ 27.205-97).* Надійність техніки. Проектна оцінка надійності систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. - К.: Держстандарт України, 1999. –21с.

5. *Иванов М.А.* Криптографические методы защиты информации в системах и сетях. - М.: КУДИЦ-ОБРАЗ, 2001. -368с.

6. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: СОЛОН-Пресс, 2002, -272с.

7. Основы компьютерной стеганографии: Учеб. Пособие для вузов/ Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. – М.: Радио и связь, 2003. – 152с.: ил.

8. *Методы и средства защиты информации,* В 2-х томах/ Ленков С.В., Перегудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. –344с., ил.

УДК 681.3.06

Терейковський І.А.
Державний університет
інформаційно-комунікаційних технологій

МЕТОДИ КОННЕКТЕВІЗМУ ТА ЗАХИСТ В НИХ

Сучасний стан розвитку комп'ютерних систем і мереж характеризується підвищенням вимог до рівня захисту інформації, який вже практично не можливо забезпечити за допомогою комплексних систем захисту інформації, контури контролю та управління яких використ-

товують класичні методи розпізнавання атак/загроз та формування управлінських рішень. Разом з тим, в різних галузях науки, техніки, економіки та медицини збільшився інтерес до використання коннектевістського напрямку розвитку штучного інтелекту, який включає в себе методи та моделі основані на зв'язках. Багато в чому популярність коннектевістського підходу можна пояснити доведеністю ефективного застосування в задачах класифікації та кластеризації образів, апроксимації функцій, прогнозування, оптимізації, управління, створення інформаційно-обчислювальних систем з асоціативною пам'яттю, які частково або в комплексі, доводиться вирішувати при розробці методів і засобів захисту інформації (ЗІ). На сьогодні, відомі спроби використання методів коннектевізму на основі ланцюгів Маркова (ЛМ) та нейронних мереж (НМ), при розробці систем виявлення атак (СВА), систем виявлення вразливостей (СВВ), систем балансування навантаженням комп'ютерних систем, тощо. Загальноприйняті алгоритми застосування вказаних моделей в засобах ЗІ, показані на рис. 1 та рис.2. Однак високий рівень помилкових тривог, складність підбору оптимальних граничних параметрів, складність введення в систему нового суб'єкта/об'єкту контролю, недостатня адаптація до багатьох особливостей сучасного стану галузі інформаційних технологій, обмежують практичну цінність таких засобів захисту.

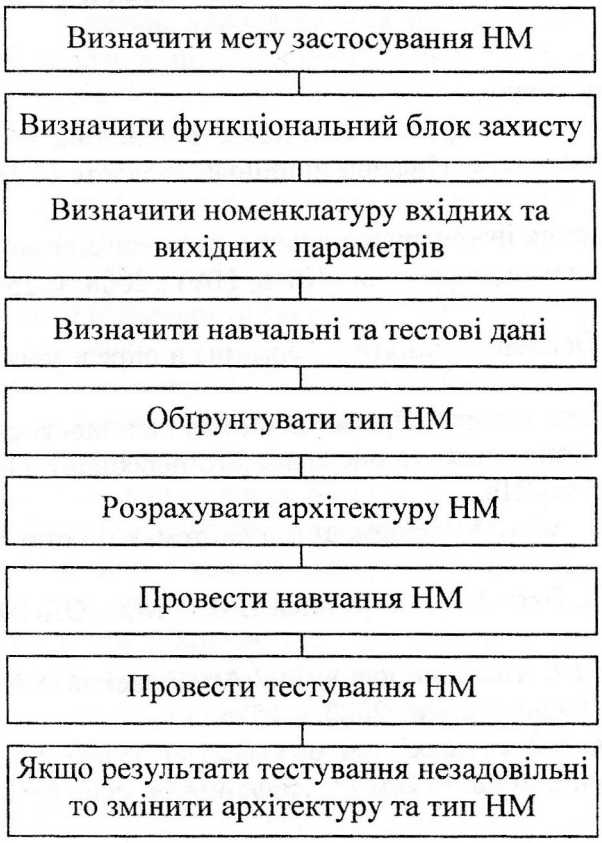

Рис. 1 Алгоритм застосування НМ в засобах ЗІ

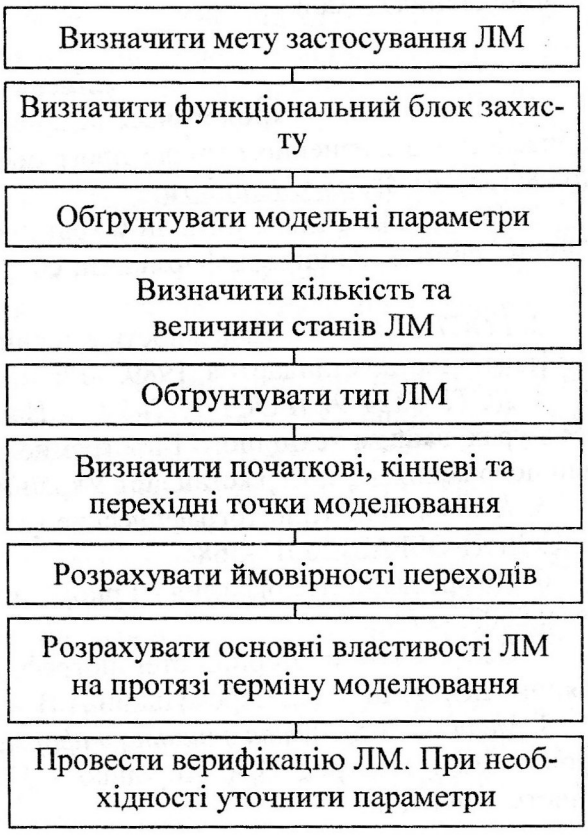

Рис. 2 Алгоритм застосування ЛМ в засобах ЗІ

Більшість означених недоліків пов'язані з недосконалістю методології застосування коннектевістських моделей та методів в галузі захисту інформації. В першу чергу слід вказати на невизначеність перспектив застосування НМ та ЛМ в сучасних засобах ЗІ. Крім того, для НМ практично відсутня методика вибору типу мережі, а також розрахунку параметрів її архітектури. Якщо ж навіть обґрунтування методики вибору частково і є, то в ньому недостатньо висвітлені питання обмежень обчислювальних можливостей того чи іншого типу

мереж. Стосовно марківських моделей, основні недоліки полягають в неякісній методиці обробки статистичних даних при розрахунку перехідних точок та ймовірностей переходів по станам ЛМ. В той же час ефективність розв'язання практичних задач захисту інформації в значній мірі залежить і від типу і від параметрів НМ та ЛМ, а сучасна теорія дозволяє знайти достатньо точні відповіді на подібні питання. При цьому формулювання відповідей повинно починатись з чіткого окреслення перспектив застосування методів коннектевізму в задачах ЗІ.

Оцінка перспектив застосування коннектевістських моделей

В роботах [1-5] сформульовано висновок про те, що основними напрямками застосування НМ та ЛМ в галузі комп'ютерного забезпечення технічних та економічних систем є розпізнавання образів, визначення оптимальних управляючих рішень та створення асоціативної пам'яті. До першого напрямку віднесемо задачі класифікації образів, кластеризації образів та апроксимації функцій. Зазначимо, що до групи задач апроксимації функції слід віднести розрахунок параметрів процесів, що відбуваються в технічних системах. Адже по своїй суті оцінка регресивних або прогнозованих значень параметрів деякого процесу є апроксимацією функції, що описує цей процес. До другого напрямку віднесемо власне задачі оптимального управління та задачі управління з еталонною моделлю. До третього напрямку входять задачі створення інформаційно-обчислювальних систем з пам'яттю, що адресується за змістом. Перші два напрямки є спільними для НМ та ЛМ, третій – специфічним для НМ. Зрозуміло, що використання методів коннектевізму для вирішення конкретної задачі галузі ЗІ комп'ютерних систем повинно починатись із визначення до якого із вказаних напрямків відноситься задача.

На практиці найбільш актуальними та важливими задачами ЗІ є створення: СВВ, СВА, антивірусів, антикейлогерів, систем протидії спаму та фішінгу, систем управління функціональними параметрами та параметрами безпеки, систем резервування та відновлення даних. З метою визначення місця застосування методів коннектевізму розглянемо типовий алгоритму функціонування СВВ, СВА, антивірусів, антикейлогерів, систем протидії спаму та фішінгу. Алгоритм складається із наступних етапів:

– Проводиться початкова настройка параметрів системи захисту. Як правило, в початкових настройках відображається режим контролю, підконтрольні параметри та деякі параметри захисних заходів. Наприклад в антивірусних системах може настроюватись період контролю об'єктів файлової системи, режим функціонування постійного захисту, номенклатура заходів проти заражених файлів (блокування, лікування та знищення).

– З визначеною періодичністю реєструються певні параметри комп'ютерної системи. Наприклад, в СВВ реєструються відкриті порти операційної системи, імена користувачів, версія операційної системи, права користувачів та ін. В СВА можуть реєструватись параметри мережених запитів, обсяг мережевого трафіку, кількість мережевих запитів за певний проміжок часу.

– Проводиться первинна обробка зареєстрованих параметрів. Наприклад, в СВА підраховується частота мережевих запитів за одиницю часу. При необхідності первинна обробка проводиться до реєстрації або паралельно з нею.

– Спрацьовує блок розпізнавання в якому на основі зареєстрованих даних приймається рішення про безпеку комп'ютерних систем. Наприклад, для СВВ це рішення про потенційні вразливості, а для СВА – про наявність атаки. Зазначимо, що для СВА в основу алгоритму покладено аналіз шаблонів нормальної поведінки (ШНП) та/або шаблонів атак (ША) на комп'ютерну систему. Вказані шаблони будуються на основі експлуатаційних та/або експериментальних статистичних даних. Рішення про атаку приймається в тому випадку, коли параметри функціонування комп'ютерних систем значно відхиляються від ШНП та/або ряд параметрів відповідають ША.

– Адміністратор системи інформується про виявлену загрозу або вразливість.

– Спрацьовує захисний модуль системи. Спочатку приймається рішення про захисний захід, а потім цей захід реалізується. В простих випадках рішення про захисний захід приймається на основі тільки початкових настройок системи, а в складних випадках – за допомогою набору спеціальних правил. Наприклад, заражений вірусом файл необхідно спробувати вилікувати. Якщо ж спроба не вдалась, то файл необхідно знищити.

– Якщо в розглянутій системі модуль реакції на загрозу відсутній, то висновок про небезпеку може бути переданий іншій системі, що управляє параметрами захисту.

Як свідчить практичний досвід та висновки [1-5], вдосконалення вказаних систем захисту відбувається за рахунок:

– Підвищення ефективності блоку розпізнавання стану безпеки комп'ютерних систем.

– Оптимізації управляючих рішень, включаючи режим контролю захищеності та проведення захисних заходів.

З точки зору теорії НМ задачі, які вирішується за допомогою блоку розпізнавання для всіх перерахованих систем захисту, відносяться до найбільш дослідженого напрямку розпізнавання образів. Це вказує на беззаперечні перспективи використання НМ для розпізнавання вірусів, кейлогерів, спаму, мережевих атак на комп'ютерних систем та вразливостей комп'ютерних систем. В той же час, для СВА обробку статистичного матеріалу з метою формування ШНП та ША доцільно вести з використанням ЛМ. Передумовою такого твердження є доведена ефективність застосування ЛМ в подібних задачах моделювання динаміки параметрів технічних систем на основі статистичних даних. В якості прикладу можна навести класичну задачу прогнозу завантаженості телефонної станції, яка багато в чому подібна визначенню ШНП та ША на мережеву комп'ютерну систему. Також можливо висловити припущення, що ЛМ знайдуть застосування при формуванні множини навчальних прикладів НМ. Однак справедливість такого припущення не є очевидною, а тому потребує подальших досліджень.

Вирішення оптимізаційних задач є традиційною сферою застосування ЛМ. Крім задач оптимізації захисних заходів в СВВ, СВА, антивірусах, антикейлогерах, системах протидії спаму та фішінгу до цієї сфери можна віднести задачі визначення оптимальних функціональних параметрів та параметрів політики безпеки конкретної еомп'ютерної системи. Наприклад, за допомогою ЛМ можливо визначити розподіл навантаження декількох комп'ютерів–серверів, необхідність та тривалість блокування ресурсу, захищеного паролем, або оптимальний період контролю антивірусом локальної мережі. Відносно НМ відомі лише окремі вдалі спроби вирішення оптимізаційних задач за допомогою мереж Хопфілда та Кохонена. Тому оцінка ефективності їх застосування для оптимізації управління параметрами захисту не може бути вище середньої.

Напрямок створення систем з асоціативною пам'яттю (специфічний для НМ) може знайти своє відтворення в системах резервного збереження даних та системах відновлення пошкодженої інформації. Однак, відповідно висновків [1, 5], створення ефективних комп'ютерних систем з асоціативною пам'яттю багато в чому є проблемою розробки оригінального, а значить і достатньо дорогого апаратного забезпечення. Крім того, практичному використанню НМ в цьому напрямку заважає недостатня теоретична база. В підсумку, оцінки перспектив застосування НМ та ЛМ при вирішенні актуальних задач ЗІ наведено в табл. 1, 2.

Вказані оцінки виставлені в числовому вигляді по трьохбальній системі (-1 – мінімальна, 0 – середня, 1 – максимальна).

Таблиця 1

Оцінка перспектив використання НМ в розповсюджених системах захисту

Система захисту	Мета застосування НМ	Оцінка	Функціональний блок	Вид задачі
Антивірус	Розпізнавання вірусів	1	Розпізнавання атак (загроз)	Розпізнавання образів
Антикейлогер	Розпізнавання кейлогерів	1		
СВА	Розпізнавання мережевих та локальних атак	1		
Антиспамова система	Класифікація електронних листів	1		
СВВ	Розпізнавання неправильних настройок та параметрів	1	Розпізнавання вразливостей	
Антивірус	Визначення параметрів протидії розпізнаним вірусам	0	Прийняття рішення про захисні заходи	Визначення оптимальних управляючих рішень
Антикейлогер	Визначення параметрів протидії розпізнаним кейлогерам	0		
СВВ	Визначення величини корекції параметрів	0		
СВА	Визначення параметрів протидії атаці	0		
Антиспамова система	Визначення параметрів протидії спаму та підозрілим листам	0		
Захисту від НСД	Визначення прав користувачів, визначення параметрів протидії спробі НСД	0		
Балансування навантаження серверів	Визначення серверу, який буде виконувати черговий запит	0		
Резервування даних	Підвищення живучості даних	-1	Зберігання даних	Система з асоціативної пам'яттю

Таблиця 2

Оцінка перспектив використання ЛМ в розповсюджених системах захисту

Система захисту	Мета застосування ЛМ	Оцінка	Функціональний блок	Вид задачі
1	2	3	4	5
Антивірус	Шаблон функціонування вірусу	-1	Розпізнавання атак (загроз)	Формування шаблонів поведінки
	Шаблон функціонування не зараженої комп'ютерної системи	-1		
Антикейлогер	Шаблон функціонування кейлогеру	-1		
	Шаблон функціонування не зараженої комп'ютерної системи	-1		

1	2	3	4	5
СВА, включаючи спроби НСД	ШНП мережевих комп'ютерних систем	1		
	ША на мережевих комп'ютерних систем	1		
Захисту від НСД	ШНП легального користувача	0		
Парольного захисту	Шаблон вводу паролю легального користувача	0		
	Шаблон підбору паролю	0		
СВВ	Розпізнавання неправильних настройок за допомогою шаблонів вірних параметрів	0	Розпізнавання вразливостей	
Антивірус	Визначення періодичності розпізнавання вірусів	0	Контролю та прийняття рішення про ЗЗ	Визначення оптимальних управляючих рішень
Антикейлогер	Визначення періодичності розпізнавання кейлогерів	0		
СВВ	Визначення оптимальної періодичності контролю вразливостей та величин корекції параметрів	1		
СВА (в комплексі з системою протидії)	Визначення оптимальної періодичності контролю діагностичних параметрів та параметрів протидії атаці	1		
Антиспамова система	Визначення періодичності контролю електронних листів	0		
Парольного захисту	Визначення оптимальної кількості неправильних спроб вводу парольних даних	0		
Захисту від НСД	Визначення оптимальних прав користувачів	0		
Балансування навантаження серверів	Визначення серверу, який буде виконувати черговий запит	1		
	Визначення оптимальної потужності та кількості серверів	1		
Резервування даних	Визначення розкладу резервування даних	0	Зберігання даних	

Таким чином, комп'ютерних систем, а також балансуванні навантаження мережевих серверів найбільш високі перспективи НМ пов'язані з розпізнаванням шкідливого програмного забезпечення, спаму, атак та вразливостей комп'ютерної системи. Перспективи використання ЛМ стосуються формування шаблонів поведінки (ШНП та ША) об'єктів мережевих. Зазначимо, що розв'язання останньої задачі багато в чому залежить від досконалості прогнозу навантаження серверів, тобто від досконалості шаблону його поведінки. Відповідно, основною метою використання ЛМ є створення ШНП та ША.

Методика визначення доцільності застосування типу нейронної мережі

Аналіз сучасного стану найромережевих технологій дозволяє сформулювати висновок про те, що доцільність застосування конкретного типу НМ слід визначати на основі співста-

влення характеристик мережі з умовами прикладної задачі. До вказаних характеристик НМ відносяться:

1. Параметри навчальних даних.
2. Загальні обмеження процесу навчання НМ.
3. Вимоги до обчислювальних потужностей НМ.
4. Вимоги до вихідної інформації НМ.
5. Обмеження технічної реалізації НМ.
6. Сфера застосування.

Розглянемо вказані характеристики в ракурсі ЗІ комп'ютерних систем.

1. До основних параметрів навчальних даних відносяться: кількість параметрів, що характеризують навчальний приклад, вид параметрів, дискретний (символьний) чи безперервний (числовий), загальна кількість навчальних прикладів, наявність помилок (шуму) в навчальних прикладах, наявність кореляції навчальних прикладів, можливість та необхідність попередньої обробки вхідних даних з метою їх нормалізації та видалення шуму, можливість відображення в навчальній виборці всіх аспектів модельного процесу, пропорційність навчальних прикладів, що відповідають різним аспектам процесу, який моделюється. В якості прикладу в табл. 4 наведено перелік можливих параметрів для деяких засобів ЗІ.

Таблиця 3

Можливі вхідні параметри НМ в засобах ЗІ

Засоби захисту	Вхідні параметри
СВА	Параметри мережевих запитів та явищ в комп'ютерній системі: вхід/вихід користувачів, кількість процесів, доступ до файлів, часові інтервали запитів до об'єктів комп'ютерної системи.
СВВ	Параметри настройок комп'ютерної системи: кількість користувачів, привілеї користувачів, параметри доступу до об'єктів комп'ютерної системи, кількість і номенклатура відкритих портів, запущені мережеві служби, параметри адміністративних настройок служб DCOM/COM+.
Антивіруси, антикейлогери	Параметри явищ в комп'ютерній системі: кількість і номенклатура запущених програм та процесів, доступ процесів до файлів, спроби доступу до мережевих служб, спроби модифікації програмних (.exe, .com, .bat) файлів, доступ до API-функцій операційної системи. Фрагменти програмного коду, що відповідають потенційно небезпечним функціям: встановлення мережевих з'єднань, відкриття, запис, знищення, створення, модифікація об'єктів файлової системи, запуск додаткових процесів та потоків.

Безпосередньо на вхід НМ вказані параметри повинні подаватись в числовому (кодованому) вигляді. Методика кодування може проводитись або по принципу наявність/відсутність явища, або по принципу оцінки величини параметру. Наприклад, вхідний параметр який відповідає наявності в програмному коді функції відкриття файлу може приймати два значення: -1 – функція відсутня, 1 – функція є. Вхідний параметр який відповідає кількості запущених процесів може приймати значення від 0 і вище з кроком 1. Зазначимо, що вхідні параметр НМ, можуть бути як дискретні, так і безперервні.

2. Загальні обмеження процесу навчання обумовлюються: максимальним терміном навчання, необхідністю представлення в навчальних даних очікуваного вихідного сигналу, можливістю автоматизації процесу навчання, можливістю донавчання в процесі експлуатації, вимогами до якості навчання, можливістю навчання в лабораторних умовах.

3. На практиці вимоги до обчислювальних потужностей визначаються максимальною кількістю прикладів (обсяг пам'яті), яку може запам'ятати мережа для досягнення необхідної достовірності прийняття рішення. В свою чергу достовірність прийняття рішення характери-

зується допустимими величинами максимальної та середньої помилки мережі на реальних даних які в загальному випадку можуть виходити за межі множини навчальних даних. Відповідно виникає задача екстраполяції результатів навчання НМ за межі навчальних прикладів. Ще однією вимогою може бути незмінність виходу мережі для різних прикладів з однаковими параметрами.

4. Вимоги до вихідної інформації НМ вказують на те в якому вигляді має бути представлена ця інформація. Наприклад, при розпізнавані вірусів може виникнути необхідність не тільки визначення ситуації "вірус А присутній", але й розрахунку ймовірності цієї ситуації. Стосовно класифікації електронних листів вихідною інформацією НМ може бути відображення листів на площину, яке дозволить провести остаточну класифікацію користувачеві. Ще однією вимогою може бути необхідність визначення вербальних залежностей між вхідною та вихідною інформацією.

5. Обмеження технічної реалізації НМ стосуються швидкості прийняття рішення, інтеграції в існуючі засоби захисту та обсягу програмної реалізації. Для зменшення обсягу можливо відділити програмний код для навчання від функціонального коду.

6. Сфера застосування визначає засоби захисту в яких буде використовуватись НМ. На сьогодні достатньо дослідженим є використання НМ для розпізнавання образів та при проведенні оптимізаційних розрахунків. Відзначимо, що системи розпізнавання образів принципово відрізняються від систем аналізу тексту тим, що в них кількість вихідних та кількість комбінацій вхідних параметрів принципово обмежена. В системах аналізу тексту ця кількість принципово необмежена. Відповідно в СВА та СВВ слід використовувати НМ призначені для розпізнавання образів. В системах захисту від спаму можливо використати НМ призначені для аналізу тексту. В системах керування параметрами засобів захисту слід застосувати НМ призначені для проведення оптимізаційних розрахунків. В перспективі доцільно застосувати НМ з метою реалізації паралельних розрахунків в комп'ютерних системах, що дозволить значно підвищити їх стійкість від багатьох типів атак з метою відмови в обслуговуванні. Крім того, сфера застосування визначається пристосованістю мережі до автономного функціонування. Для цього в архітектурі НМ повинно бути передбачено можливість повної автоматизації процесу донавчання на експлуатації.

Якісні оцінки відповідності основних характеристик НМ умовам задач захисту для перспективних типів мереж наведені в табл. 4. В табл. 4 відсутні характеристики, які хоча і застосовуються при побудові мережі, але не впливають на вибір типу НМ. Як і в табл. 1, та табл. 2 оцінки виставлені по трьохбальній системі. Їх величини розраховані в результаті порівняльного аналізу розглянутих типів НМ, проведеного в [1, 5]. Відсутність оцінки означає, що для її визначення потрібні додаткові дослідження. При виставленні оцінок увага була зосереджена на адаптації НМ з найбільш перспективною базовою архітектурою до проблем ЗІ. Для розгляду було вибрано багатошаровий перспетрон (БШП), мережа радіальної базисної функції (РБФ), мережа адаптивної резонансної теорії (АРТ), ймовірністні НМ типу PNN та GRNN, мережі Хеммінга, Хопфілда, Коско та Кохонена. та синаптичну НМ (СНМ), яка є однією із найбільш досконалих мереж в галузі обробки текстової інформації. Відзначимо, що внаслідок заданого обсягу публікації остаються без уваги деякі інші, можливо і перспективні, але не достатньо апробовані та теоретично вивчені архітектури.

Таблиця 4

Якісні оцінки відповідності НМ умовам задач захисту

Умова	БШП	РБФ	Кохонена	АРТ	СНМ	PNN/ GRNN	Асоціативні
1	2	3	4	5	6	7	8
Навчальні дані							
Допустимість шуму	1	0	1	-1	1	0	-1

1	2	3	4	5	6	7	8
Допустимість кореляції	1	1	1	1	1	1	-1
Необхідність відображення всіх аспектів процесу	-1	1	1	-1	-1	1	0
Необхідність пропорційного представлення прикладів	1	-1	-1	-1	-1	-1	0
Загальні обмеження процесу навчання							
Короткий термін навчання	-1	0	1	1	0	1	1
Необхідність представлення в навчальних прикладах очікуваного виходу	1	1	-1	-1	-1	1	1
Автоматизація навчання	1	-1	0	1	1	1	0
Можливість донавчання	0	1	1	1	1	1	0
Якість навчання	1	0	0	1	1	1	1
Обчислювальні потужності							
Обсяг пам'яті	1	-1	-1	-1		-1	0
Екстраполяції результатів навчання	1	-1	-1	-1		-1	1
Незмінність результатів	1	1	0	1	1	1	0
Вихідна інформація							
Можливість інтерпретація виходу у вигляді ймовірності	0	0	-1	-1	-1	1	0
Можливість інтерпретації виходу у графічному вигляді	-1	-1	1	-1	-1	-1	-1
Можливість вербалізації	1	0	-1	-1	-1	0	-1
Обмеження технічної реалізації НМ							
Швидкості прийняття рішення	1	1	1	1	0	1	-1
Обсяг програмної реалізації	-1	1	-1	0	-1	-1	0
Сфера застосування							
Системи розпізнавання образів	1	1	1	1	0	1	1
Системи аналізу тексту	-1	-1	1	0	1	0	-1
Системи управління	-1	-1	1	-1	-1	-1	1
Пристосованість до автономного функціонування	-1	-1	-1	1	1	-1	-1

Слід відзначити, що в задачах які зводяться до розпізнавання образів при відсутності обмежень на використання методу навчання "з вчителем", термін навчання, донавчання, автономність функціонування, представлення результатів розпізнавання, обсяг програмної реалізації, кількість та якість навчальних даних найбільш ефективним є використання БШП. Його ефективність пояснюється найбільшою обчислювальною потужністю, можливістю автоматизації процесу навчання та вербалізації результатів. При цьому інші типи НМ доцільно застосувати для оперативного попереднього аналізу або в специфічних випадках, що характеризуються певними обмеженнями.

Методика обробки статистичних даних при формуванні ЛМ

Очевидно, що формування означених шаблонів поведінки повинно базуватись на оцінці параметрів мережевого трафіку. Практичний досвід свідчить, що динаміка обсягу мережевого трафіку, а відповідно і динаміка більшості параметрів, носить циклічно-нерівномірний ("не пуассонівський") характер. Відповідно для моделювання зміни парамет-

рів слід застосовувати негомогенні ЛМ. Негомогенність полягає в тому, що інтенсивності переходу ЛМ будуть залежати від часу. Ключовим моментом створення таких ЛМ є розрахунок перехідних (нестаціонарних) точок процесу, тобто моментів часу в яких відбувається зміна інтенсивностей переходу. Проведені автором дослідження дозволяють твердити, що для ШНП та ША, визначити ці нестаціонарні точки можливо за допомогою спектрального аналізу статистики параметрів мережевого трафіку. По причині апробованості в аналогічних задачах, спектральний аналіз доцільно реалізувати методом Фур'є. Результатом аналізу є представлення статистичних даних у вигляді *K*-періодичного ряду динаміки. При цьому, пропонується моделювати кожну із визначених гармонік (періодів) ряду окремим, негомогенним ЛМ. Відповідно, для моделювання *K*-періодичного ряду даних слід застосовувати *K* ЛМ. Блок-схема алгоритму розрахунку інтенсивностей переходів ЛМ в випадку представлення статистики у вигляді *K*-періодичного ряду даних показана на рис. 2.

Зазначимо, що в представленому алгоритмі на часовому інтервалі *AB* функція $f'(t)$ зростає, а на часовому інтервалі *BA* спадає. Таким чином точка *A* відповідає максимуму, а точка *B* мінімуму статистичної функції зміни параметру $f'(t)$ на протязі одного лагу. Тому *A* і *B* є нестаціонарними точкам процесу. Очевидно, що в цих точках відбувається зміна інтенсивностей переходів ЛМ.

Проведена автором верифікація запропонованої методики обробки статистичних даних показала достатню для інженерних розрахунків точність та ефективність. В якості прикладу було використано статистику мережевих запитів до Web-серверів, що обслуговували вітчизняні Web-сайти інформаційного напрямку. При цьому відносна похибка моделювання становила 2-3%.

Висновки

1. Результати дослідження систем захисту комп'ютерної інформації вказують на наявність основних недоліків пов'язаних з недосконалістю функціонування підсистеми управління параметрами захисту та діагностики атак в умовах функціональної невизначеності параметрів, а дослідження таких напрямків теорії коннектевізму, як НМ та ЛМ показали їх позитивні можливості щодо обробки неформалізованої інформації та побудови на цій основі моделей та засобів ЗІ.

2. На основі аналізу актуальних задач ЗІ встановлено, що сучасні типи НМ слід використовувати в контурах контролю та управління антивірусів, СВА, антиспамових систем, антикейлогерів та СВВ, завдяки чому підвищиться достовірність розпізнавання атак (вразливостей) сигнатури яких не представлені в базах даних ЗЗІ.

3. Вперше розроблена методика визначення доцільності застосування та адаптації параметрів конкретного типу НМ для розв'язання задачі ЗІ, яка базується на результатах співставлення таких характеристик мережі як параметри навчальних даних, загальні обмеження процесу навчання, вимоги до обчислювальних потужностей, вимоги до вихідної інформації, обмеження технічної реалізації та традиційна сфера застосування, з умовами прикладної задачі. Розраховані якісні оцінки відповідності основних характеристик НМ умовам типових задач захисту. Методика дозволяє формалізувати та спростити процес визначення архітектури НМ адекватної умовам задачі ЗІ.

4. Вперше створена методологія проектування негомогенної ергодичної марківської моделі шаблону поведінки об'єктів захисту комп'ютерних систем, адаптована до використання статистичних даних у вигляді багатоперіодичних рядів динаміки, яким відповідають типові статистичні залежності параметрів безпеки. Завдяки цьому стало можливим виявити та прогнозувати сезонні та добові періодичні зміни величин параметрів, що визначають стан захищеності вказаних об'єктів.

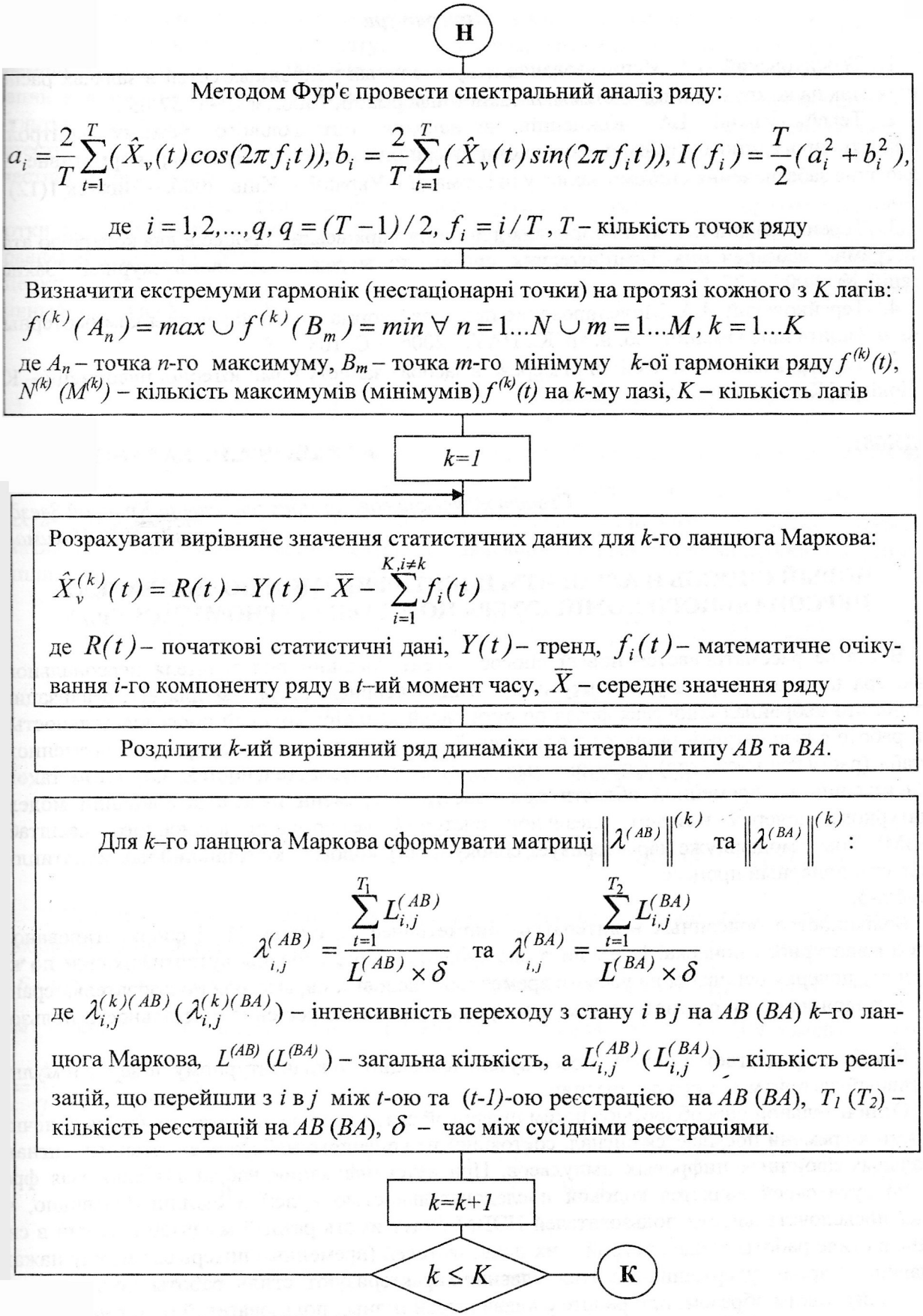

Рис. 2 Блок-схема розрахунку інтенсивностей ЛМ

Література

1. Терейковский И.А. Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы. // Захист інформації, 2006, №3. – С.57-65 .
2. Терейковський І.А. Концепція визначення оптимального режиму контролю захищеності програмного забезпечення комп'ютерних систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2006. – Випуск 1(12) – С.88-96
3. Терейковський І.А. Концепція використання марківських процесів для контролю атак на програмне забезпечення комп'ютерних систем та мереж. Науковоий журнал "Захист інфорації" №3 2005, с.37-49.
4. Терейковский И.А. Моделирование профилей нормального поведения компьютерных систем. // Защита информации, Сб. н. тр. К.: НАУ. –2006. – С. 103-108.
5. Терейковський І.А. Нейронні мережі в засобах захисту комп'ютерної інформації.– К.: ТОВ ПоліграфКонсалтинг, 2007. – 209 с.

УДК681.3

БАРАНОВ А.Н., БАРАНОВ Н.А.

Севастопольський военно морской ордена Красной Звезды институт им. П.С. Нахимова

НОВЫЙ СПОСОБ И АЛГОРИТМ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

В статье рассматривается новый способ аутентификации пользователя персонального компьютера по клавиатурному почерку и мультипликативный алгоритм для его реализации. Показано, что набранная ключевая фраза по сути своей является кодовой последовательностью и при работе с клавиатурой разных пользователей будут наблюдаться деформации временного масштаба (растяжение-сжатие) формируемых кодовых последовательностей. С учётом такого типа искажений во временной области при известном времени начала комбинации модель клавиатурного почерка назовём идеальной системой деформации временного масштаба (ИСДВМ). Новая модель уже характеризует совокупность кодовых комбинаций как мультипликативно стационарный процесс.

Библ.-5.

Большинство описанных в литературе биометрических систем [1-3] сориентировано на анализ клавиатурного почерка. Все известные существующие способы аутентификации по клавиатурному почерку основаны на расчете временных числовых параметров пользователя, сравнении их с эталонными по статистическим критериям и принятии решения о легальности пользователя.

В работе предлагается новый способ аутентификации по клавиатурному почерку и мультипликативный алгоритм для его реализации.

Отличительной способностью систем цифровой связи вообще является то, что за конечный промежуток времени посылается сигнал, состоящий из конечного набора элементарных сигналов – идеальных двоичных цифровых импульсов. При аутентификации набранная ключевая фраза также по сути своей является кодовой последовательностью нулей и единиц. Очевидно, что кодовые последовательности пользователей ПЭВМ будут иметь разный масштаб времени в силу разницы в стиле работы с клавиатурой этих пользователей (временные интервалы между нажатием клавиш и время удержания-нажатия клавиш характеризуют стиль работы пользователя с клавиатурой). Таким образом, при работе с клавиатурой разных пользователей будут наблюдаться деформации временного масштаба (растяжение-сжатие) формируемых кодовых последовательно-