УДК 621.3

Л. М. Куперштейн, к. т. н.

ДО ПРОБЛЕМИ ВИЯВЛЕННЯ ШАХРАЙСТВА У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА БАЗІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

Розглянуто основні методи та засоби реалізації систем виявлення шахрайства в телекомунікаціях. Запропоновано їх реалізацію на базі нейронечітких мереж. Запропоновано реалізацію апаратної частини нейронечіткої системи виявлення шахрайства у вигляді нейрообчислювача на базі програмованих логічних інтегральних схем, а також описана методика такої реалізації.

Актуальність теми

У всіх галузях людської діяльності періоди процвітання економіки характеризуються, з одного боку, значними обсягами інвестицій в неї, а з іншого боку — стійким інтересом потенційних споживачів до її продукції і послуг. На хвилі успіху і росту бізнесу компанії інколи ігнорують непередбачені втрати, очікуючи, що майбутні прибутки сповна покриють їх. Телекомунікаційний бізнес є цьому яскравим прикладом. Так за оцінкою Асоціації з контролю за шахрайством в телекомунікаціях (Communications Fraud Control Association), втрати від шахрайства на теперішній час складають до 100 млрд. доларів і щорічно збільшуються приблизно на 7 % [1].

Найефективнішим і перспективним напрямком зменшення та ліквідації такого роду втрат є інтелектуальні системи для боротьби з шахрайством (Fraud Management System (FMS)), які широко представлені на ринку [1, 2]. За допомогою цих інструментів оператори можуть виявляти випадки шахрайства й успішно боротися з ним. Встановлення такої системи може окупитися менше, ніж за рік, однак далеко не кожний оператор може дозволити собі її придбання. Вартість подібних систем досить висока, часто вона співставна з вартістю білінгових систем [3]. Тому, впровадження спеціалізованих рішень для боротьби із шахрайством можуть дозволити собі, зазвичай, тільки оператори з великою кількістю абонентів і високим обсягом сукупного доходу, тобто там, де збитки від шахрайства співставні з вартістю цих систем.

Основними важливими характеристиками спеціалізованих FMS, у порівнянні з стандартними (білінговими), є [2, 3]:

— режим роботи у реальному часі (або близькому до реального);

— здійснення аналітичного контролю апаратно-програмним комплексом;

— низький відсоток використання людського ресурсу.

Отже, актуальною є задача розробки і впровадження вітчизняної відносно недорогої та ефективної спеціалізованої FMS (як для стаціонарного, так і для мобільного зв'язку) з відповідною конкурентоспроможністю у порівнянні з закордонними аналогами (Compaq Fraud Management System компанії HP; Lightbridge Fraud Sentinel, компанії Lightbridge; Centurion; WatchDog, PhoneLoc компанії Basset та ін.).

Методи реалізації системи виявлення шахрайства

Всі FMS функціонують у відповідності з алгоритмами, які використовують [2]:

1) адаптивний метод (на базі самоадаптивних нейронних мереж (НМ));

2) інструктивний метод (на базі керувальних нейронних мереж);

3) аналітичний метод (або метод розслідування порушень).

З аналізу вищенаведених методів випливає, що найефективнішим для реалізації FMS є адаптивний метод, оскільки він базується на використанні некерованих НМ — непрограмованих адаптивних систем для обробки інформації. Такі системи здатні змінювати свою поведінку в залежності від зміни зовнішніх умов (впливів), коли FMS розпізнає очікувану (нормальну) поведінку кожного користувача. Цей метод придатний для виявлення змін в режимі використання мережі зв’язку.

Використовуючи адаптивний метод, FMS сама вчиться розпізнавати звичайний режим роботи (дії у мережі) абонента й сигналізувати, коли цей режим починає різко відрізнятися від звичайного [2]. При цьому, якщо поведінка користувача з часом змінюється, адаптивна система вносить зміни

в картину звичайного режиму роботи.

Однак цей метод має низку недоліків. Адаптивну систему неможливо навчити, що саме варто виявляти, і якщо параметри ймовірних змін не визначені правильно, то розумний шахрай може довго залишатися невиявленим.

Проте, ці недоліки відсутні у інструктивному методі, який базується на керованих НМ або на, так званих, вирішальних правилах (rule-based). У такі системи вводяться дані про те, якою може бути найімовірніша поведінка шахрая, і потім вони намагаються виявити подібний тип поведінки.

Використовуючи інструктивний метод, аналізуються реальні приклади шахрайства для того, щоб навчити систему, що саме варто шукати [2]. У системах на базі вирішальних правил також виробляється аналіз конкретних випадків для виявлення характерних рис шахрайства. Отримані дані потім перетворяться у вирішальні правила з використанням граничних значень або відносних критеріїв. Для навчання систем, що працюють із використанням інструктивного методу, використовуються приклади шахрайства разом зі зразками нормального режиму роботи, щоб система могла розпізнати нормальний режим роботи від шахрайства [2].

Однак ці системи мають недолік: вони не можуть виявити нових видів шахрайства, які можуть бути викриті за допомогою адаптивних методів.

Тому, для уникнення недоліків адаптивного та інструктивного методів пропонується для проектування FMS використання гібридного методу, який базується на двох інтелектуальних технологіях: нейронні мережі, нечітка логіка.

Тобто, всі розрахунки виконуються нейромережею, а логічний висновок щодо дій абонента мережі — на базі нечіткої логіки.

Основна перевага систем з нечіткою логікою — це здатність використовувати умови й методи розв'язання задач, описані мовою, близькою до природної [4—6]. Однак класичним системам з нечіткою логікою, не здатним автоматично навчатися, властивий і певний недолік: набір нечітких правил, вигляд і параметри функцій належності, що описують вхідні й вихідні змінні системи, а також вигляд алгоритму нечіткого виводу вибираються суб'єктивно експертом — людиною, і вони можуть виявитися не цілком адекватними дійсності [7].

Тому для усунення зазначеного недоліку пропонується використовувати апарат нечітких нейронних мереж (Fuzzy Neural Networks), системи на базі якого відомі також як адаптивні нейро-нечіткі системи виводу (Adaptive Neuro-Fuzzy Inference System, ANFIS) [6].

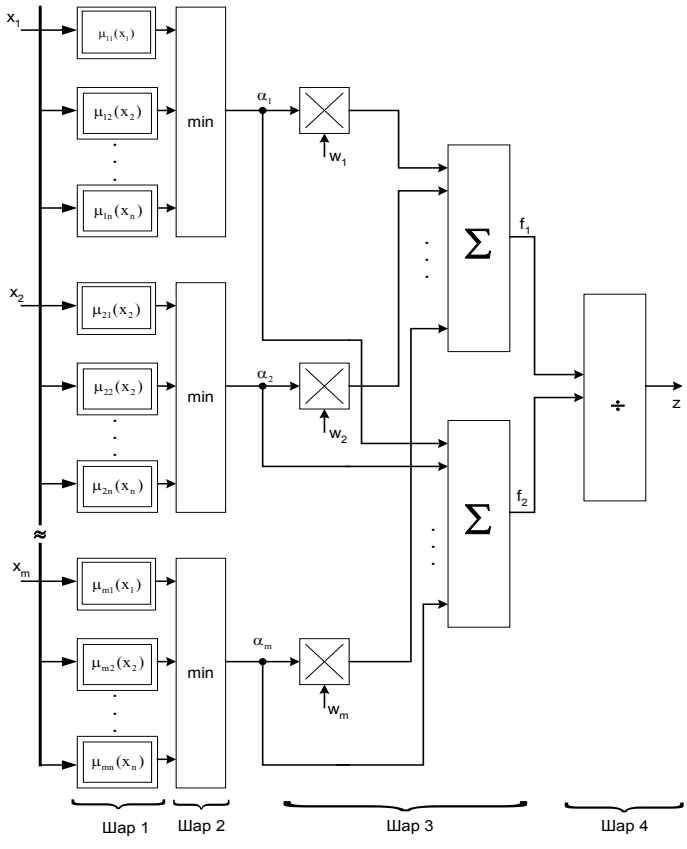

Рис. 1. Нечітка НМ на базі логічного виводу алгоритму Сугено 0-го порядку

Нечітка НМ — це багатошарова НМ, у якій шари виконують функції елементів системи нечіткого виводу. Нейрони даної мережі характеризуються набором параметрів, налаштування яких здійснюється в процесі навчання, як у звичайних НМ [6]. Таким чином, симбіоз нейро- та і фазісистем може дати бажаний результат при розробці FMS, оскільки вони є універсальними апроксиматорами для моделювання нелінійних задач.

На рис. 1 показана нечітка НМ на базі логічного виводу алгоритму Сугено 0-го порядку, яку пропонується використовувати в розробці системи виявлення й шахрайства в телекомунікаціях [7].

Шар 1 здійснює газифікацію. В шарі 1 $\mu_{rj}(x_j)$ — нелінійні функції, де r — номер продукційного правила, j — номер компонента вхідного вектора x відповідає функціям належності передумов правил. Налаштовувані параметри даного шару — параметри використовуваних функцій належності. Шар 2 мережі здійснює роз-

рахунки підсумкових функцій належності передумов нечітких правил. У цьому випадку цей шар не має параметрів, що налаштовуються.

Шар 3, що складається із двох нейронів, здійснює підсумовування й зважене підсумовування вихідних сигналів шару 2. Параметрами даного шару є вагові коефіцієнти w_r. Шар 4 реалізує операцію ділення $z = f_1 / f_2$ і не містить параметрів, що налаштовуються [7].

У класичних алгоритмах навчання нечітких НМ кількість продукційних правил, вигляд функцій належності, тип алгоритму нечіткого виведення тощо задаються апріорі й не піддаються змінам в процесі навчання мережі. У випадку неправильного вибору даних параметрів нечіткі НМ можуть виявитися малоефективними. Тому, для запобігання зазначеній ситуації в проектованій FMS пропонується застосовувати алгоритм адаптації (самоорганізації) нечіткої НМ, що буде налаштовувати в процесі навчання не тільки параметри, але й структуру мережі [6].

Засоби реалізації системи виявлення шахрайства

Фізична реалізація нейронечткої FMS виконується у вигляді програмно-апаратного комплексу. Доведено, що найперспективнішою та ефективною елементною базою для реалізації апаратного забезпечення НМ є цифрові нейрочіпи на базі програмованих логічних інтегральних схем (ПЛІС), у порівнянні з іншими кристалами (надвеликі інтегральні схеми, процесори цифрової обробки сигналів, процесори загального призначення, мікроконтролери та ін.) [8]. В такому ж виконанні пропонується реалізація апаратної частини FMS, а саме у вигляді спецобчислювача на базі ПЛИС фірми Xilinx із стандартним інтерфейсом, наприклад, типу PCI/PCI-Express.

Наведемо основні особливості високопродуктивних серій ПЛИС Xilinx, що забезпечують можливість апаратної реалізації нейромережевих алгоритмів [9, 10]:

– високі системні частоти обробки — до 400 Мгц;
– ступінь інтеграції — до 10 млн еквівалентних логічних вентилів на кристалі;
– наявність для кожного кристала широкого спектра корпусів з великою кількістю зовнішніх користувальницьких виводів (до 514);
– наявність на кристалі двох типів синхронного високошвидкісного ОЗП (до 5 нс);
– можливість часткової реконфігурації в процесі роботи;
– внутрішнє тестування й налаштування через JTAG 1149.1;
– розвинені засоби проектування;
– незначний термін проектування системи;
– низька вартість кристалів.

Побудову апаратної частини нейронечіткої системи виявлення шахрайства в телекомунікаціях на базі ПЛИС Xilinx слід виконувати за методикою декількома послідовними етапами, які показані на рис. 2 [11]. Дамо їм коротку характеристику.

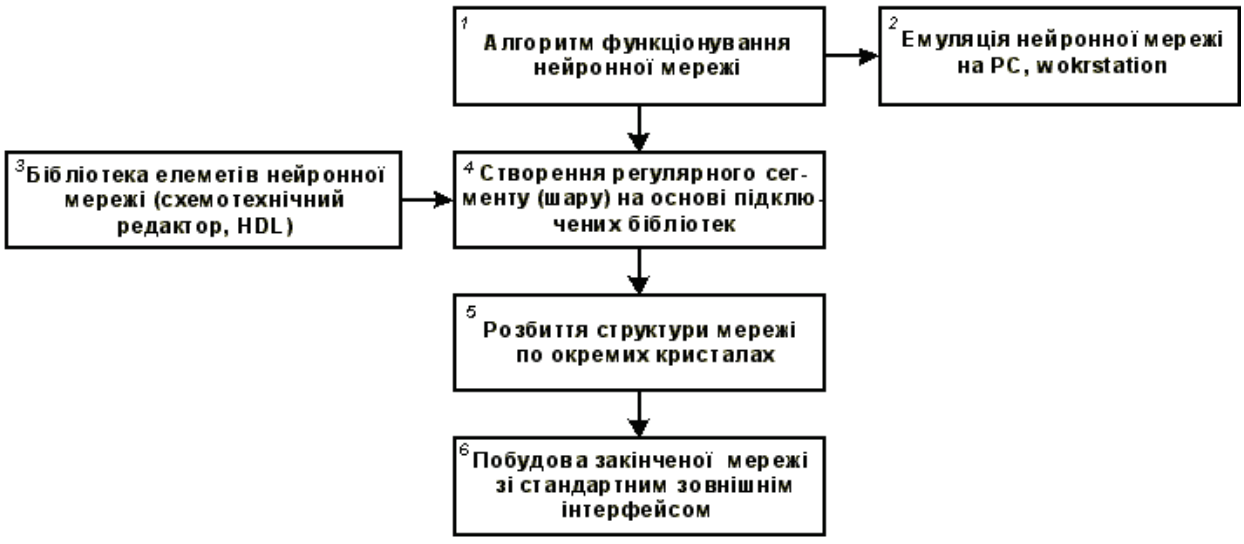

Рис. 2. Послідовні етапи створення НМ на ПЛІС Xilinx

Eman 1. Цей етап є одним з основних. Необхідно вибрати тип архітектури нейро-нечткої мережі та алгоритм. У більшості випадків використовується багатошарова архітектура мережі прямого розповсюдження. Кількість нейронів у вхідному шарі залежить від розмірності та зображення вхідних даних.

Eman 2. Емуляція нейронної мережі на персональному комп'ютері або робочій станції. На даному етапі здійснюється комп'ютерне моделювання роботи нейро-нечіткої мережі за допомогою програми, яку пишуть на одній з мов програмування високого рівня, або краще пакета прикладних програм (нейроімітатора). Це необхідно для того, щоб з'ясувати наскільки ефективно та чи інша архітектура мережі розв'язує поставлену задачу. Виконання даного етапу рекомендується за допомогою інструментарію Neural Networks Toolbox та Fuzzy Logic Toolbox пакету прикладних програм MatLAB 7.

Eman 3. Створення бібліотеки елементів нейронної мережі за допомогою схемотехнічного редактора або HDL-редактора. На даному етапі безпосередньо у системі автоматизованого проектування здійснюється розробка основних компонентів системи для подальшого їх використання у проектуванні. Якщо компоненти не складні, то рекомендується використати схемотехнічний редактор САПР Xilinx Foundation Series 4.0 (Xilinx WEB-pack ISE 6.0). Якщо ж передбачається особливе налаштування архітектури мережі, то необхідним є використання саме HDL-редактора, який є досить гнучким та професійним інструментом.

Eman 4. Створення регулярного сегмента (шару) на основі підключених бібліотек. Тут виконується формування логічної структури нейро-нечіткої системи на базі елементів, створених на попередньому етапі. Передбачається, що дана структура є базовою для складнішої структури, яка будується дублюванням простішої на ієрархічному рівні. Для нейронної мережі це може бути нейрон (фазі-нерон), декілька нейронів або навіть шар нейромережі.

Eman 5. Розбиття структури мережі по окремих кристалах. На даному етапі здійснюється вибір типу ПЛІС та імплементація для того, щоб визначити наявні помилки у проекті, а також процент ємності кристалу, який займає нейрон чи декілька нейронів. За такими результатами можна зробити висновок про можливість дублювання фрагмента шару нейромережі та необхідні апаратні ресурси для побудови усієї мережі. Для більшої швидкодії рекомендується використовувати ПЛІС типу FPGA, але це компенсується неповним завантаженням ємності кристалу. Якщо ж ємність кристалу є пріоритетнішим показником, то слід використовувати ПЛІС типу CPLD.

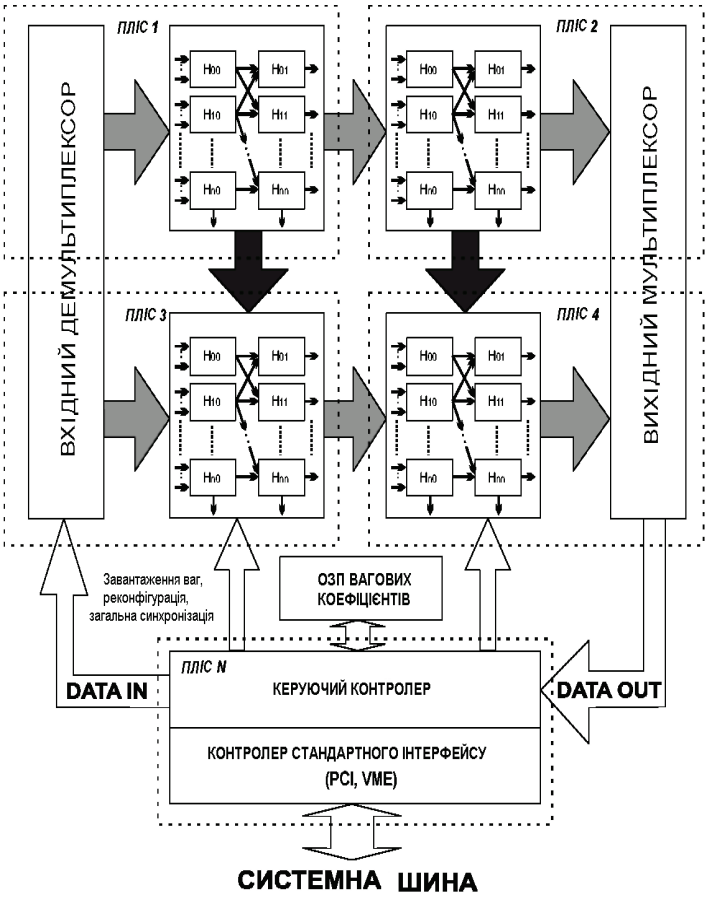

Рис. 3. Узагальнена структурна схема нейронної (нейро-нечіткої) мережі на програмованій логіці Xilinx

Eman 6. Побудова завершеної мережі зі стандартним інтерфейсом. На даному етапі здійснюється програмування ПЛІС, тобто завантаження проекту (нейро-нечітка мережа чи фрагмент її шару зі стандартним інтерфейсом) у ПЛІС і отримання готового повнофункціонального нейромодуля.

Структура нейро-нечіткої мережі на ПЛІС Xilinx, яка є типовою для систем такого класу, зображена на рис. 3 [12].

Ядро мережі являє собою матрицю з 4-х ПЛІС, зв'язаних максимально можливою кількістю взаємозв'язків. У загальному випадку розмірність матриці практично необмежена. У кожному стовпці ПЛІС розміщаються від одного

до декількох шарів мережі, у той же час, нарощуючи число рядків матриці ПЛІС, можна збільшувати розмірність вхідного простору ознак.

Вхідний демультиплексор і вихідний мультиплексор розміщуються безпосередньо в ПЛІС крайніх стовпців і призначені для введення-виведення даних на стандартний інтерфейс (системну шину).

Керуючий контролер, служить для загальної синхронізації роботи мережі, організації процесу навчання й завантаження вагових коефіцієнтів. Даний контролер безпосередньо пов'язаний з контролером стандартного інтерфейсу (PCI, VME) і має специфічний набір команд, які є необхідними і задаються розробником.

Через стандартний інтерфейс здійснюється зв'язок мережі з досить повільними (у порівнянні з можливостями взаємозв'язків ПЛІС) периферійними пристроями, наприклад, персональний комп'ютер, де здійснюється необхідна візуалізація й часткова обробка переданої і прийнятої з мережі інформації програмною частиною нейро-нечіткої FMS.

Принцип роботи FMS у системі керування та моніторингу телекомунікаційної мережі

Основною задачею, яка ставиться перед проектованою FMS, є ідентифікація (розпізнавання) дій шахрая за нестандартною поведінкою профілю абонента, який характеризують комплексом ознак, а саме: тривалість, напрям, відстань дзвінків, ідентифікаційні дані та ін. Отже, ця задача є не що інше як розпізнавання образу за вхідним набором сигналів, які знімаються безпосередньо з комутатора сканером CDR (Call Detail Record — службова інформація та відомості про здійснені дзвінки [1]). На рис. 4 показана схема системи керування та моніторингу телекомунікаційної мережі та місце у ній нейро-нечіткої FMS. Пунктиром позначені інші можливі шляхи проходження інформації.

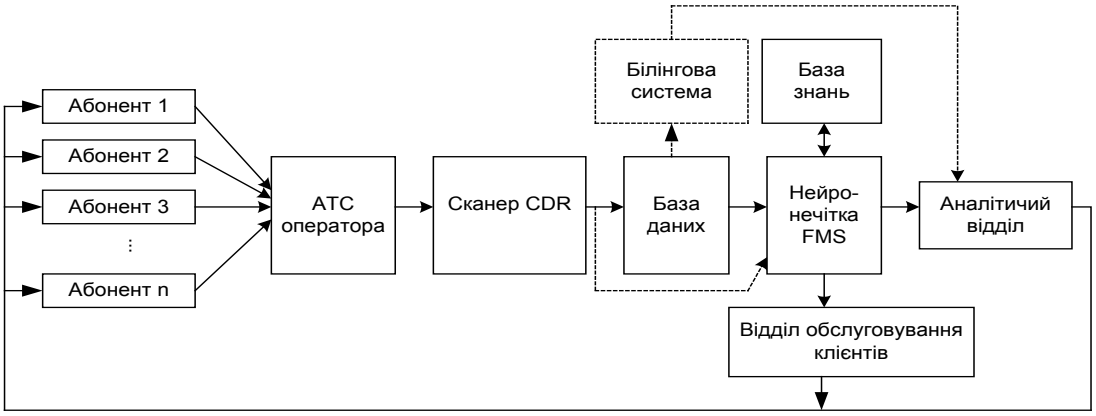

Рис. 4. Пропонована узагальнена схема організації системи керування та моніторингу телекомунікаційної мережі

Узагальнений принцип роботи FMS у системі керування та моніторингу телекомунікаційної мережі такий. Первісна інформація (CDR), що знаходиться на АТС оператора телефонного зв'язку, заноситься в базу даних або/і надходить на вхід нейро-нечіткої FMS. Вона, в свою чергу, виконує в реальному масштабі часу моніторинг і аналіз закономірностей та поведінку абонентів щодо всіх здійснених та нездійснених викликів, а саме зміни в базі даних (тривалість дзвінків, напрямок і відстань дзвінків, регулярність дзвінків тощо). У випадку виявлення підозрілої інформації, що ідентифікується за допомогою накопиченої бази знань, FMS подає сигнал тривоги в аналітичний відділ. Крім того, система може також автоматично запускати процедури реагування (наприклад, давати системі запобіжних заходів команду про припинення міжнародного доступу або повідомляти підрозділ обслуговування клієнтів про необхідність негайно зв'язатися з абонентом) на основі правил, які визначає постачальник послуг відповідно до принципів компанії й політики відносно шахрайства. Після чого, уповноважені співробітники компанії приймають рішення як вплинути на того чи іншого абонента-порушника. Типи шахрайства, на які буде реагувати така нейронечітка FMS: абонентське, технічне, процедурне, хакерське, а також виявляти приховані частини тарифікаційної інформації на комутаторі.

Висновки

Кількість випадків несанкціонованого доступу до послуг зв'язку з появою 3G-мереж неухильно зростає. Бар'єром на шляху шахраїв можуть стати спеціалізовані FMS-системи. При цьому хочеться сподіватися, що гідне місце серед засобів забезпечення безпеки телекомунікаційних систем займуть саме вітчизняні комплекси. І хоча найчастіше виявлені факти шахрайства не можуть служити юридичною підставою для відмови від надання послуг зв'язку й тим більше для звернення до суду, і нехай навіть накопичена інформація свідчить про незаконну діяльність абонента, але оператор завжди може знайти формальний привід, щоб розірвати контракт із клієнтом.

СПИСОК ЛІТЕРАТУРИ

1. Лезин В., Перминов К. Мошенничество в сетях операторов фиксированной связи и как с ним бороться // Информкурьерсвязь. — 2004. — № 3. — Режим доступа: http://www. miks. ru/ magazine/ magazine_look. php? id=192.

2. Русеев Д. Мошенничество в мобильных сетях и средства борьбы с ним // Мобильные телекомуникации. — 2003. — № 3. Режим доступа: http://www. mobilecomm. ru /view. php? id=423.

3. Мазняк А., Лихванцев Н, Генне О. FMS-системы: барьер на пути мошенников // Connect! — 2005. — № 1 Режим доступа: http://www. connect. ru/article. asp? id=5356.

4. Архангельский В. И., Богаенко И. Н., Грабовский Г. Г., Рюмшин Н. А. Нейронные сети в системах автоматизации. — К.: Техника, 1999. — 364 с.

5. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. — Винница: УНІВЕРСУМ–Вінниця, 1999. — 320 с.

6. Усков А. А., Кузьмин А. В. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. — М.: Горячая Линия — Телеком, 2004. — 143 с.

7. Омату С., Халид. М. Нейроуправление и его приприложения / Пер. с. англ. — М.: ИПРЖР, 2000. — 272 с.

8. Куперштейн Л. М. Методи та засоби нейроподібної обробки даних для систем керування: Автореф. дис… канд. техн. наук / Вінницький національний технічний університет. — Вінниця: ВНТУ, 2007. — 20 с.

9. Соловьев В. В. Проектирование цифровых систем на основе программируемых логических интегральных схем. — М.: Горячая линия-Телеком, 2001. — 636 с.

10. Логовский А. Технология ПЛИС и ее применение для создания нейрочипов // Открытые системы. — 2000. — № 10. — С. 20—25. — Режим доступа: http://www. osp. ru/os/2000 /10/019_print. htm.

11. Капитанов В. Д., Мистюков В. Г. Построение на ПЛИС фирмы Xilinx высокопроизводительных нейронных сетей // Scan Engineering Telecom. — 1999. Режим доступа: http://www. scan. com/art_neur. pdf.

12. Галушкин А. И. Нейрокомпьютеры Кн. 3. Нейрокомпьютеры и их применение: Учеб. пособие для вузов / Общая ред. А. И. Галушкина — М.: ИПРЖР, 2000. — 258 с.

Матеріали статті рекомендовані до опублікування оргкомітетом III Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2007)» (31.05—2.06.2007 р.)

Надійшла до редакції 30.09.07
Рекомендована до друку 04.10.07

Куперштейн Леонід Михайлович — старший викладач кафедри економічної кібернетики.

Вінницький фінансово-економічний університет