Запропоновані моделі, методи та засоби побудови нейроімітатора для прогнозування показника надійності системи захисту інформації, автоматизації процесів аналізу та прийняття рішень експертів з інформаційної безпеки щодо вибору системи безпеки. Перевагою запропонованої інформаційної технології є використання декількох варіантів функції активації та методів навчання мережі, що дозволяє підвищити показник об'єктивності прийняття рішень

Ключові слова: прогнозування, захист, інформація, нейрон, мережа, нейроімітатор, класифікація, алгоритм, навчання

Предложены модели, методы и средства построения нейроимитатора для прогнозирования показателя надёжности систем защиты информации, автоматизации процессов анализа и принятия решений экспертов по информационной безопасности в вопросах выбора систем безопасности. Преимуществом предложенной информационной технологии является использование нескольких вариантов активационной функции и методов обучения сети, что позволяет повысить показатель объективности принятия решения

Ключевые слова: прогнозирование, защита, информация, нейрон, сеть, нейроимитатор, классификация, алгоритм, обучение

УДК 004.891.2:519.816

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПОСТРОЕНИЯ НЕЙРОИМИТАТОРА ОЦЕНКИ СИСТЕМ БЕЗОПАСНОСТИ

И. А. Пилькевич
Доктор технических наук, профессор,
заведующий кафедры*
E-mail: igor.pilkevich@mail.ru
Н. Н. Лобанчикова
Кандидат технических наук, доцент
Кафедра компьютеризированных систем управления и автоматики
Житомирский государственный технологический университет
ул. Черняховского, 103, г. Житомир, Украина, 10005
E-mail: lobanchikovanm@rambler.ru
В. И. Котков
Кандидат технических наук, доцент*
E-mail: eko_univer@i.ua
*Кафедра мониторинга окружающей природной среды**
Т. Н. Коткова
Кандидат сельскохозяйственных наук, доцент
Кафедра общей экологии**
E-mail: eko_univer@i.ua
**Житомирский национальный агроэкологический университет
бульвар Старый, 7, г. Житомир, Украина, 10008

1. Введение

Развитие информационных технологий и информатизация общества делают необходимым совершенствование методов, средств и технологий построения систем защиты информации. Выбор эффективных систем защиты информации является комплексной задачей, решение которой требует использования системного подхода и громоздких процедур анализа показателей от экспертов по информационной безопасности.

Использование современных информационных технологий способно облегчить процесс обработки информации и автоматизировать процессы принятия решений экспертов по информационной безопасности.

Создание новых информационных технологий для автоматизации процессов анализа и принятия решений является весьма актуальной научной задачей.

2. Анализ исследований и публикаций

Анализ работ [1, 2] по созданию современных информационных технологий анализа и поддержки принятия решений экспертов в области защиты информации базируется на использовании интеллектуальных информационных систем. Экспертные системы сегодня получили широкое использование и подтвердили свою эффективность. Весомый вклад в создание экспертных систем и развитие методов и средств их построения внесли работы таких отечественных и зарубежных авторов как Глушкова В. М. [3], Палагина А. В. [4], Корченка А. Г. [5], Субботина С. А. [6], Гладуна В. П. [7], Оссовского С. [8], Грибулина В. Г. [9], Рутковской Д. [10] и др.

В данных работах представлены методы, средства и информационные технологии построения экспертных систем, в том числе с использованием нейронных сетей и искусственного интеллекта. Предлагаемые решения направлены на решение определенных прикладных

задач, однако не содержат описания создания информационной технологии для автоматизации работы экспертов по выбору систем безопасности и прогнозирования надежности их срабатывания. Исходя из этого, необходимым является разработка новой информационной технологии, которая сочетала бы процессы прогнозирования надежности срабатывания систем защиты информации и автоматизировала бы работу экспертов с использованием нейронных сетей.

3. Формирование целей и задач

Целью работы является разработка информационной технологии прогнозирования надежности срабатывания системы защиты информации для автоматизации работы экспертов по информационной безопасности.

Для достижения поставленной цели необходимо определить архитектуру нейронной сети, выбрать активационную функцию, метод обучения, создать учебную выборку, структурную модель программного комплекса, провести моделирование нейроимитатора, выбрать средство для реализации.

Объектом исследования выступают процессы построения интеллектуальных систем анализа и поддержки принятия решений. Предметом исследования являются модели, методы и средства построения интеллектуальных систем анализа и поддержки принятия решений с целью прогнозирования надежности срабатывания систем безопасности, автоматизации процессов обработки информации экспертами.

4. Построение нейроимитатора оценки системы безопасности

В задачах выбора системы защиты информации необходимо спрогнозировать надёжность системы для принятия адекватного решения по её использованию. Автоматизировать экспертные процедуры анализа позволяет применение интеллектуальных систем [6]. Особенного внимания заслуживают искусственные нейронные сети.

Важнейшей особенностью нейронных сетей является возможность параллельной обработки данных при аппаратной реализации. Ещё одной отличительной способностью нейронных сетей является их способность к обучению. При обучении сети на ограниченном множестве данных сеть способна обобщать полученную информацию и показывать хорошие результаты на данных, которые не использовались в обучающей выборке. Кроме того, следует отметить, что архитектура нейронной сети позволяет реализовать её с применением технологий сверхвысокой степени интеграции, а это даёт, в свою очередь, возможность перерабатывать разнообразную информацию [8].

4. 1. Структурная схема нейроимитатора

Нейроимитатор представляет собой компьютерную программу, которая выполняет следующие функции:

– формирование архитектуры нейронной сети;

– сбор данных для обучающей выборки;

– обучение выбранной нейросети на обучающей выборке;

– тестирование обученной нейросети;

– решение задач обученной сетью;

– запись результатов обучения.

Обобщённая структурная схема нейроимитатора прогнозирования надёжности системы защиты информации представлена на рис. 1.

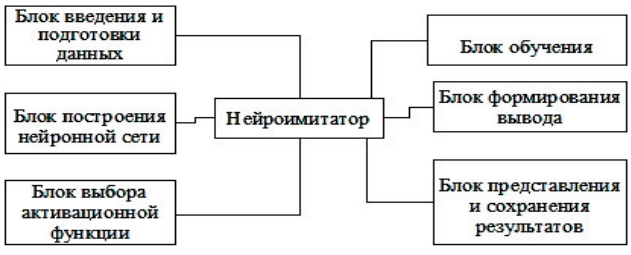

Рис. 1. Обобщённая структурная схема нейроимитатора

Блок введения и подготовки данных предназначен для взаимодействия эксперта и нейронной сети. Этот блок предусматривает считывание введённых экспертом данных и их подготовку к дальнейшему использованию.

Блок построения нейронной сети предусматривает построение нейронной сети по указанной экспертом архитектуре.

Блок выбора активационной функции предусматривает выбор способов активации функции нейронной сети, задание параметров функции активации.

Блок обучения предназначен для проведения обучения нейронной сети по выбранному методу и введенными параметрами итерации, инерциальности и скорости спуска.

Блок формирования вывода предназначен для обработки полученных результатов обучения, тестирования, формирования выхода нейронной сети.

Блок представления и сохранения результатов предназначен для вывода результатов работы нейронной сети на экран и сохранения полученных результатов на жёсткий диск компьютера.

4. 2. Схема искусственного нейрона и функции активации

При построении нейроимитатора будем использовать схему искусственного нейрона, представленную на рис. 2. Формальный нейрон состоит из адаптивного сумматора и нелинейного преобразователя. Веса синапсов принадлежат диапазону [0,1].

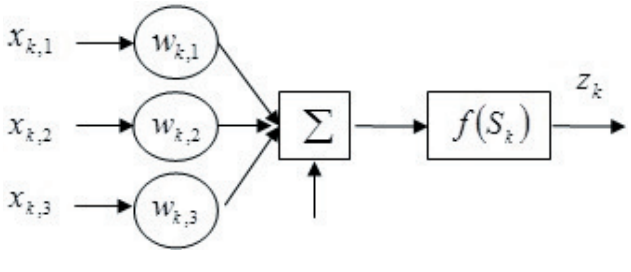

Рис. 2. Схема искусственного нейрона: $x_{k,1}$, $x_{k,2}$, $x_{k,3}$ – входные сигналы k-го нейрона; $w_{k,1}$, w_{k2}, $w_{k,3}$ – веса синапса k-го нейрона; $f(S_k)$ – функция активации (activation function) -го нейрона; S_k – сумма скалярных произведений входных сигналов и весов синапса k-го нейрона; z_k – выходной сигнал k-го нейрона

Математическую модель нейрона можно представить следующим образом:

$$S=\sum_{i=1}^{n} x_i \cdot w_i + b\,; \quad (1)$$

$$z=f(S)\,, \quad (2)$$

где x_i – входные сигналы нейрона, $i=1,...,n$;

w_i – веса (weight) синапса нейрона, $i=1,...,n$;

b – значение смещение (bias) нейрона;

S – сумма (sum) скалярных произведений входных сигналов и весов синапса нейрона;

$f(S)$ – функция активации (activation function) нейрона;

z – выходной сигнал нейрона;

n – число входов нейрона.

В качестве функции активации используем сигмоидальные функции, так как они получили наиболее широкое применение и являются строго монотонно возрастающими, непрерывными и дифференцируемыми. На выбор эксперта предоставляются следующие функции активации:

– рациональная сигмоида (рис. 3, а), функция которой имеет вид:

$$f(S)=\frac{S}{|S|+\alpha}\,; \quad (3)$$

– экспоненциальная сигмоида (рис. 3, б), функция которой имеет вид:

$$f(S)=\frac{1}{1+e^{-2\alpha S}}\,; \quad (4)$$

– гиперболический тангенс (рис. 3, в), функция которого имеет вид:

$$f(S)=\text{th}\frac{S}{\alpha}=\frac{e^{\frac{S}{\alpha}}-e^{-\frac{S}{\alpha}}}{e^{\frac{S}{\alpha}}+e^{-\frac{S}{\alpha}}}\,, \quad (5)$$

где S – сумма (sum) скалярных произведений входных сигналов и весов синапса нейрона;

α – параметр наклона сигмоидальной функции активации.

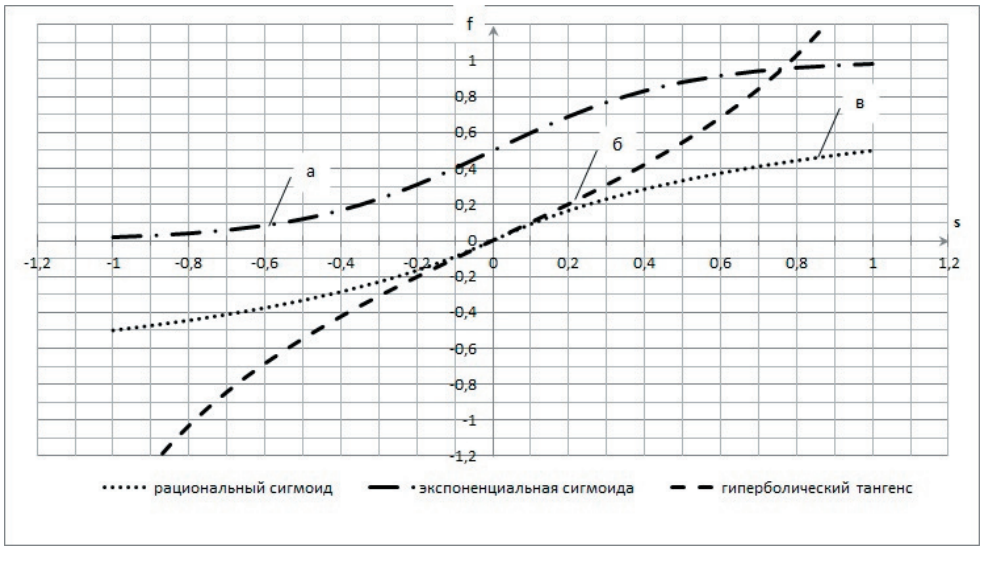

Рис. 3. Функции активации искусственного нейрона: а – рациональный сигмоид; б – экспоненциальная сигмоида; в – гиперболический тангенс

Как уже отмечалось, особенностью нейронных сетей является параллельная обработка сигналов. Это достигается многослойностью сети. Исходя из теорем Колмогорова-Арнольда и Хехт-Нильсена, трёх слоёв достаточно для получения эффективного решения с помощью нейронных сетей прямого распространения – многослойный персептрон. Структурная схема многослойной нейронной сети представлена на рис. 4.

Анализ рис. 4 показывает, что сеть состоит из слоёв (layer). Входной (input) слой используется для распределения данных по сети и не производит вычислений. Выходной (autput) слой обычно содержит один нейрон ($N_{3,1}$, рис. 4), который выдаёт результаты расчётов всей нейронной сети. Скрытые (hidden) слои передают сигналы от входа к выходу. Их входом служит выход предыдущего слоя, а выходом – вход следующего слоя.

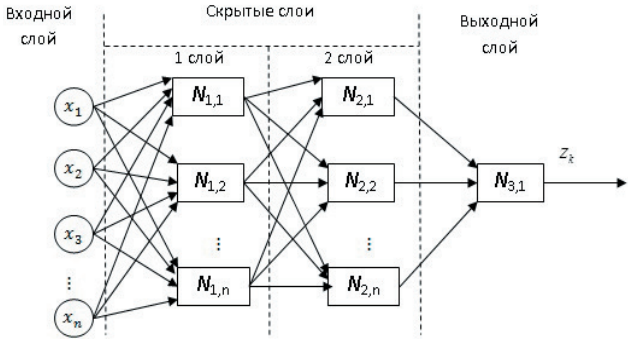

Рис. 4. Структурная схема многослойной нейронной сети

Перед подачей в сеть производится нормирование входных сигналов в диапазоне значений [-1;1] или [0;1]. Нормирование на диапазоне [-1;1] проводим с помощью функции

$$x_i'=\frac{x_i-(\max x_i+\min x_i)/2}{(\max x_i-\min x_i)/2}\,, \quad (6)$$

а нормирование на диапазоне [0;1] – функции

$$x_i'=\frac{x_i-\min x_i}{\max x_i-\min x_i}\,, \quad (7)$$

где $\max x_i$, $\min x_i$ – соответственно, максимальное и минимальное значения для данной компоненты, вычисленные по всей обучающей выборке;

x_i – i -я компонента входного вектора данных.

С помощью (6), (7) пересчитываются и компоненты векторов ответов.

4. 3. Обучение нейронной сети

Как известно [10], обучение нейронной

сети представляет собой автоматический поиск закономерности между совокупностью обучающих данных и заранее известным результатом. Обучающий пример состоит из вектора входных данных размерностью, равной числу входов нейросети, и вектора выходных данных, соответствующего выходам нейросети. Задача обучения состоит в том, чтобы нейросеть в ответ на вектор входных данных выдавала такой вектор выходных данных, который был бы наиболее близок к выходным данным. Для сравнения используем следующую норму:

$$H = \sqrt{\sum_{i=1}^{n} \left(\tilde{z}_i - z_i\right)^2}, \qquad (8)$$

где n – размерность вектора с выходными данными;

$\tilde{z}_i$ – значение i-го выхода;

z_i – значение i-го выхода, возвращаемое нейросетью.

Для обучения выбираем метод обратного распространения ошибки (error backpropagation):

1) сигнальный метод Хебба

$$w_{ij}(t) = w_{ij} \cdot (t-1) + \alpha \cdot z_i^{(k-1)} \cdot z_j^{(k)}, \qquad (9)$$

где $z_i^{(k-1)}$ – выходное значение нейрона i-го слоя $k-1$;

$z_j^{(k)}$ – выходное значение нейрона j-го слоя k;

$w_{ij}(t)$ и $w_{ij}(t-1)$ – весовые коэффициенты синапса, соединяющего эти нейроны, на итерациях t и $t-1$, соответственно;

α – коэффициент скорости обучения;

2) дифференциальный метод Хебба

$$w_{ij}(t) = w_{ij} \cdot (t-1) + \\ + \alpha \cdot \left[z_i^{(k-1)}(t) - z_i^{(k-1)}(t-1)\right] \cdot \left[z_j^{(k)}(t) - z_j^{(k)}(t-1)\right], \qquad (10)$$

где $z_i^{(k-1)}(t)$ и $z_i^{(k-1)}(t-1)$ выходное значение нейрона i-го слоя $k-1$, соответственно, на итерациях t и $t-1$;

$z_j^{(k)}(t)$ и $z_j^{(k)}(t-1)$ тоже самое для нейрона j-го слоя k.

4. 4. Интерфейс программного продукта

Данный программный продукт реализован с помощью программного обеспечения Microsoft Visual Studio на языке программирования C#. Главная форма интерфейса программного продукта представлена на рис. 5. Эта форма имеет стандартные windows-ориентированной системы закладки: „Файл”, „Данные”, „Обучение”.

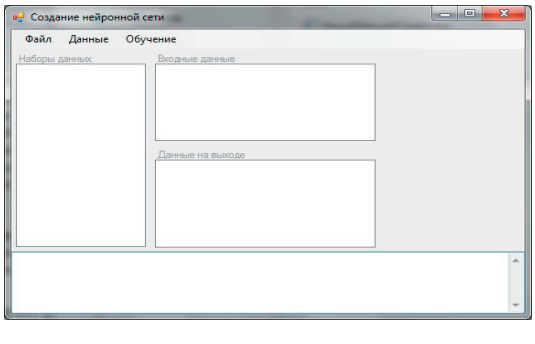

Рис. 5. Главная интерфейсная форма

Меню закладки „Файл” представлено набором следующих функций: „Создать” для создания структуры нейронной сети; „Открыть” и „Сохранить” служат для открытия и сохранения архитектур нейронных сетей, соответственно (рис. 6).

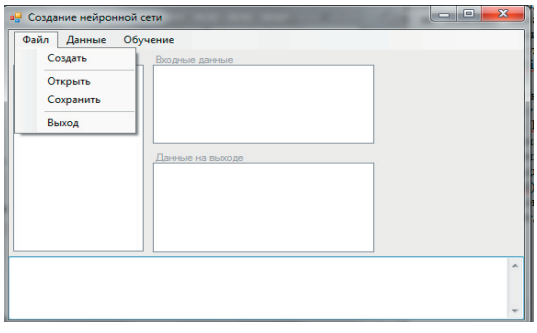

Рис. 6. Меню „Файл”

Меню закладки „Данные” позволяет открыть набор обучающей выборки и сохранить наборы в удобное пользователю место, а также очистить набор при необходимости (рис. 7).

Меню закладки „Обучение” запускает процедуру обучения нейронной сети. При создании нейронной сети пользователю необходимо заполнить следующие поля формы „Создание сети” (рис. 8).

В данной форме необходимо задать структуру нейронной сети, выбрать активационную функцию, задать параметры функции и разброс весов. Далее программный продукт создает нейронную сеть по указанным параметрам. После этого пользователю предоставляется возможность создания набора данных, задавать входные и выходные параметры (рис. 9).

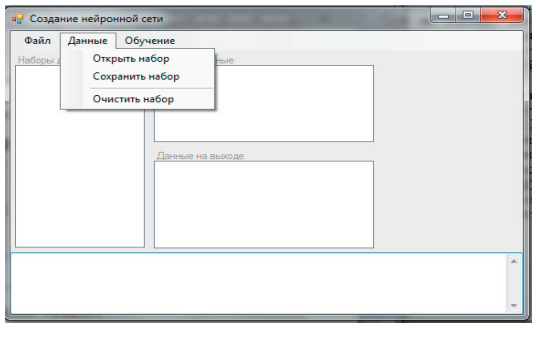

Рис. 7. Меню „Данные”

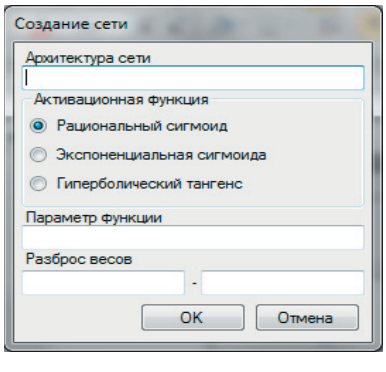

Рис. 8. Форма „Создание сети”

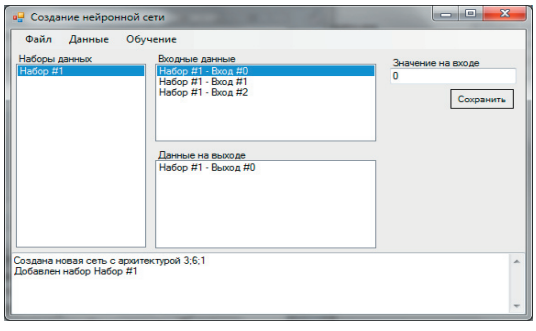

Рис. 9. Форма заполнения данных

После заполнения формы можно сохранить данные и начать обучение.

При выборе функции „начать обучение" в меню закладки „Обучение", пользователю предоставляется возможность выбора метода обучения и задание параметров (рис. 10).

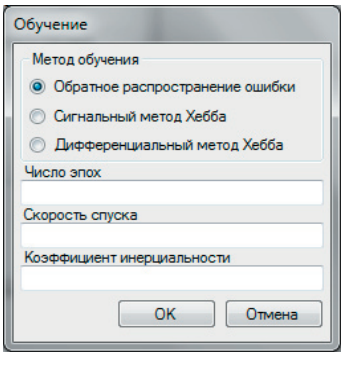

Рис. 10. Форма задания метода обучения

После заполнения формы начинается обучение сети и выдается ответ сети и её ошибка. Далее эксперт проводит анализ полученных результатов и принимает решения.

Можно провести обучение сети по трём методам обучения и обобщить полученные результаты.

4. 5. Тестирование программного продукта

Проведём тестирования программного продукта.

Для обучения сети будем использовать набор данных, которые представлены в табл. 1.

Таблица 1

Выборка для обучения

Эффективность	Функциональность	Цена	Надёжность
0,5	0,5	0,5	0,5
1	0,2	0,6	0,7
0,7	0,8	0,8	0,8
0,9	0,9	1	0,9

Создаем нейронную сеть и выбираем активационную функцию (рис. 11).

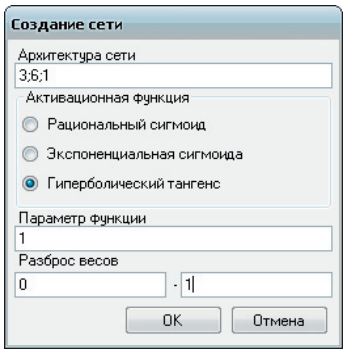

Рис. 11. Создание нейронной сети

Вводим входные данные и заполняем форму „Обучение" (рис. 12).

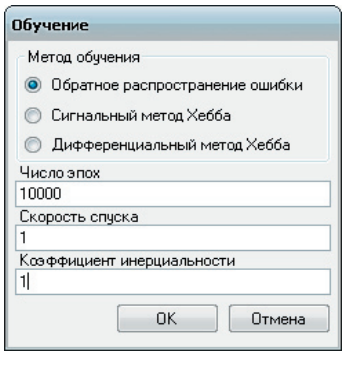

Рис. 12. Выбор метода обучения

Проверяем результат обучения (рис. 13).

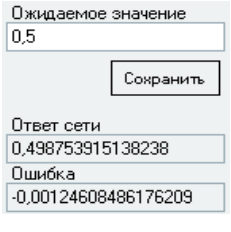

Рис. 13. Окно результата после обучения

Введём дополнительные данные, которые не входили в учебную выборку, (табл. 2).

Таблица 2

Дополнительные данные

Эффективность	Функциональность	Цена	Надёжность
0,5	0,5	0,5	0,5
1	0,2	0,6	0,7
0,7	0,8	0,8	0,8
0,9	0,9	1	0,9
0,2	0,3	0,4	?
1	1	1	?

Прогнозируемый результат надёжности системы для первого набора входных данных представлен на рис. 14.

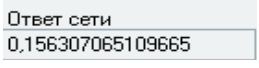

Рис. 14. Окно ответа сети для первого введённого набора

Прогнозируемый результат надёжности системы для второго набора входных данных представлен на рис. 15.

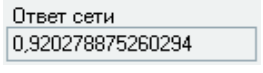

Рис. 15. Окно ответа сети для второго введённого набора

Таким образом, программный продукт создаёт нейронную сеть за указанной экспертом архитектурой и выбранными параметрами, проводит считывание введённых данных, проводит обучение нейронной сети, и прогнозирует результат надёжности системы безопасности, что позволяет автоматизировать процессы обработки информации экспертом и ускорить процесс принятие решения.

5. Вывод

В работе описана информационная технология создания и реализации нейроимитатора для прогнозирования оценки надёжности систем безопасности и автоматизации работы эксперта по информационной безопасности с целью минимизации времени обработки информации и времени, необходимого на принятия решения.

Данная информационная технология может применяться для прогнозирования широкого класса задач. Преимуществом предложенной технологии является использование нескольких вариантов активационной функции и методов обучения сети, что позволяет получить набор данных для тщательного анализа и повысить показатель объективности принятия решения.

Література

1. Chen, P. P. The Entity-Relationship Model: Toward a Unified View of Data / P. P. Chen // ACM Trans. On Database Syst. – 1976. – V.1, №1. – P. 9–36.
2. Codd, E. F. A relational model of data large shared data banks / E. F. Codd // Comm. ACM. – 1970. – V.13, №6. – P. 377–387.
3. Глушков, В. М. Строение локально бикомпактных групп и пятая проблема Гильберта [Текст] / В. М. Глушков // Успехи математических наук. – 1957. №12, 2(74). – С. 3–41.
4. Палагин, А. В. Онтологические методы и средства обработки предметных знаний : монография [Текст] / А. В. Палагин, С. Л. Крывый, Н. Г. Петренко. – Луганск : изд-во ВНУ им. В. Даля, 2012. – 323 с.
5. Корченко, О. Г. Системи захисту інформації : монографія [Текст] / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.
6. Субботін, С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навч. посібник [Текст] / С. О. Субботин. – Запоріжжя : ЗНТУ, 2008. – 341 с.
7. Гладун, В. П. Инструментальный комплекс поддержки принятия решений на основе сетевой модели предметной области : зб. допов. наук.-практ. конф. з міжнародною участю „Системи підтримки прийняття рішень. Теорія і практика” [Текст] / В. П. Гладун, В. Ю. Величко. – К. : ІПММС НАНУ, 2012. – С. 126–128.
8. Оссовский, С. Нейронные сети для обработки информации [Текст] / С. Оссовский; пер. с польск. И. Д. Рудинского. – М. : Финансы и статистика, 2002. – 344 с.
9. Грибунин, В. Г. Комплексная система зашиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений [Текст] / В. Г. Грибунин, В. В. Чудовский. – М. : Изд. центр „Академия”, 2009. – 416 с.
10. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы [Текст] / Д. Рутковская, М. Пилинский, Л. Рутковский; пер. с польск. И. Д. Рудинского. – М. : Горячая линия–Телеком, 2007. – 452 с.