УДК 338.2 DOI: 10.14451/1.177.77

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЗАЩИЩЕННЫХ ЭКОНОМИЧЕСКИХ СИСТЕМАХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

© 2019 **Скляров Алексей Викторович**
кандидат технических наук, доцент
Ростовский государственный экономический университет (РИНХ), Россия, Ростов-на-Дону
E-mail: SAV0701@mail.ru

© 2019 **Тищенко Евгений Николаевич**
доктор экономических наук, профессор
Ростовский государственный экономический университет (РИНХ), Россия, Ростов-на-Дону

© 2019 **Ефимова Елена Владимировна**
кандидат экономических наук, доцент
Ростовский государственный экономический университет (РИНХ), Россия, Ростов-на-Дону

© 2019 **Жилина Елена Викторовна**
кандидат экономических наук, доцент
Ростовский государственный экономический университет (РИНХ), Россия, Ростов-на-Дону

Предложен подход к решению задачи оценки эффективности мероприятий информационной безопасности на защищенных экономических системах, в котором для обработки экспертных оценок применена искусственная нейронная сеть, что позволяет существенно повысить объективность и точность оценивания и, как следствие, его качество.

Ключевые слова: информационная безопасность, эффективность, искусственные нейронные сети.

В современных условиях обеспечение информационной безопасности защищенных экономических систем происходит при воздействии на них множества факторов, имеющих, как правило, стохастический характер способных существенно снизить эффективность и даже полностью скомпрометировать защитные мероприятия. При этом, в ходе организации защиты критически важных для собственников информационных ресурсов, компании руководствуются требованиями российских и международных стандартов, регламентирующих деятельность в этой области. Однако, указанные нормативные документы практически не содержат конкретных методик и носят скорей декларативный или рекомендательный характер. По мнению авторов, такому положению дел есть ряд причин:

• при разработке защитных мероприятий не учитывается экономическое содержание и вероятностный характер событий и явлений, возникающих в процессе реализации этих мероприятий;

• отставание нормативной базы от потребностей практики вследствие исключительно высоких темпов развития информационных технологий. При этом, в сфере информационной безопасности подобное отставание оказывается особенно критичным;

• несовершенство нормативного обеспечения защиты информации, которое проявляется в фактическом отсутствии системы показателей защищенности и критериев безопасности объектов информатизации.

В результате отсутствует возможность оценки эффективности планируемых и уже реализованные защитных мер, под которой понимают степень соответствия результатов защиты информации поставленной цели [1].

Объективным видом оценки эффективности систем защиты информации (СЗИ) является функциональное тестирование, предназначенное для проверки фактической работоспособности реализованных механизмов безопасности и их соответствия предъявленным требованиям, а также обеспечивающее получение статистических данных. В методическом плане опреде-

ление эффективности СЗИ заключается в выработке суждения относительно пригодности способа действий персонала или приспособленности технических средств к достижению цели защиты информации на основе измерения соответствующих показателей, например, при функциональном тестировании. Такие данные, получаются экспериментально, посредством математического моделирования или путем экспертных оценок. При этом в соответствии с современной теорией оценки эффективности систем, качество объекта, в том числе СЗИ, проявляется лишь в процессе его использования по назначению, поэтому наиболее объективным является оценивание по эффективности применения. Причем, чем более конкретно сформулирована цель защиты информации, детально уяснены имеющиеся для этого ресурсы и определен комплекс ограничений, тем в большей степени можно ожидать получение желаемого результата. В этой связи содержание целевого назначения системы на формализованном уровне приобретает многомерный, векторный, нечеткий, субъективный характер, что при синтезе системы защищенных мероприятий приводит к необходимости решать задачи с многокритериальными показателями. В результате достаточно сложно, а зачастую и невозможно, оценить качество мероприятий информационной безопасности, а, соответственно, и определить, чем один вариант защищенных мероприятий лучше другого.

По мнению авторов, для решения задачи оценки эффективности мероприятий информационной безопасности на защищенных экономических системах в указанных условиях целесообразно применять аппарата искусственных нейронных сетей (ИНС).

В нейросетевом подходе задача оценки сводится к восстановлению нелинейной функции по набору вариантов реализации защитных мероприятий и их возможных результатов, имеющей вид:

$$y = f_y(x_1, x_2, \ldots x_n) \qquad (1)$$

для которого связь <входы(x_i)-выход(y)> представлена в виде матрицы экспертных оценок [2].

Указанную матрицу экспертных оценок можно представить в виде нечеткой базы знаний:

ЕСЛИ $\left[\left(x_1 = a_1^{j1}\right)\ \text{И:}\left(x_i = a_i^{j1}\right)\ \text{И:}\left(x_n = a_n^{j1}\right)\right]$

(с весовым коэффициентом w_{j1}):

: ИЛИ $\left[\left(x_1 = a_1^{jk_j}\right)\text{И:}\left(x_i = a_i^{jk_j}\right)\text{И:}\left(x_n = a_n^{jk_n}\right)\right]$

(с весовым коэффициентом w_{jk_j})

$$\text{ТО}\quad y = f_j \qquad j = \overline{1,m}. \qquad (2)$$

где a_j^p — лингвистический терм, описывающий входной параметр x_i в строке $p = k_j$;

k_j — число строк, соответствующих классу d_j выходного параметра y;

w_{jp} — значение функции принадлежности, описывающей степень уверенности эксперта относительно высказывания $p = k_j$.

Классы d_j, $j = \overline{1,m}$, результат дискретизации диапазона $[\underline{y}, \overline{y}]$ выходного параметра на m поддиапазонов:

$$[\underline{y}, \overline{y}] = [y, y_1) \cup \ldots \cup [y_{j-1}, y_j) \cup \ldots \cup [y_{m-1}, \overline{y}] \qquad (3)$$

Исходя из описания (2), функция (1) представляется в следующем виде:

$$y = \frac{\underline{y}\,\mu^{d_1}(y) + y_1\,\mu^{d_2}(y) + \ldots + y_{m-1}\,\mu^{d_m}(y)}{\mu^{d_1}(y) + \mu^{d_2}(y) + \ldots \mu^{d_m}(y)} \qquad (4)$$

$$\mu^{d_j}(y) = \max_{p=1,k_j}\{w_{jp}\min_{i=1,n}[\mu^{jp}\left(x_i\right)]\} \qquad (5)$$

$$\mu^{jp}\left(x_i\right) = \frac{1}{1 - \left(\frac{x_i - b_i^{jp}}{c_i^{jp}}\right)^2},\ i=\overline{1,n},\ j=\overline{1,n},\ p=k_j, \qquad (6)$$

где $\mu^{d_j}(y)$ — функция принадлежности выходного параметра y к классу $d_j \in [y_{j-1}, y_j]$;

$\mu^{jp}(x_i)$ — функция принадлежности входного параметра x_i к терму a_i^p;

b_i^{jp}, c_i^{jp} — коэффициенты, корректирующие значения соответствующих функций принадлежности.

Представим лингвистическую информацию (1) в искусственной нейронной сети (2), структура которой изображена на рисунке 1 [3].

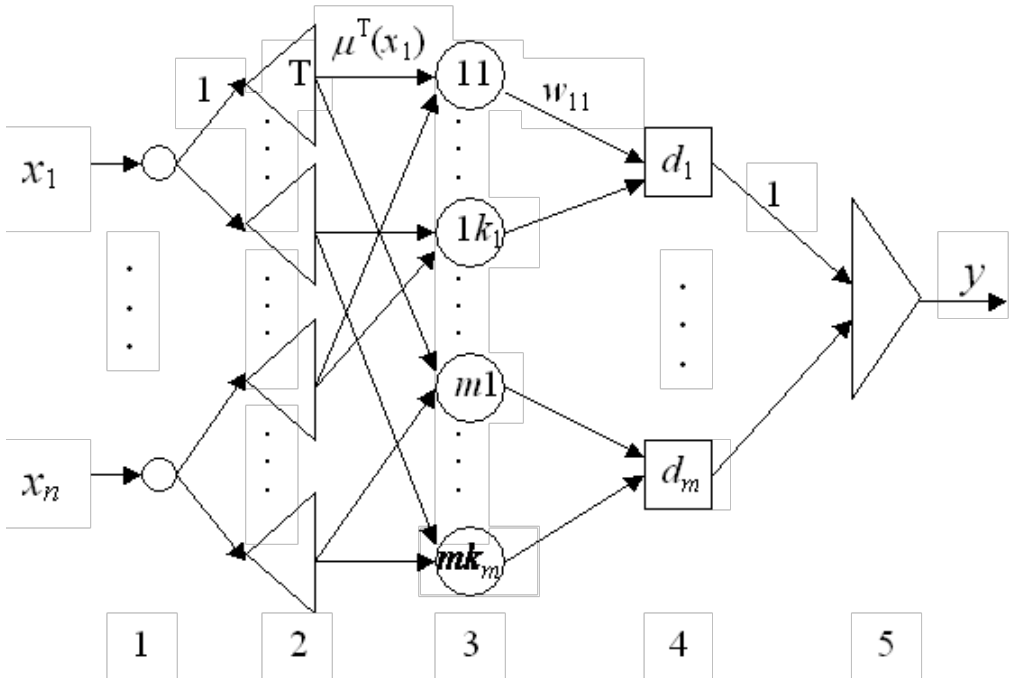

Рис. 1. **Структура искусственной нейронной сети**

где: $\mu^T(u)$ — функция принадлежности переменной u к терму T;

$\bar{d}j$ — центр класса $d_j \in \left[\underline{y}, \bar{y}\right]$.

Представленная искусственная нейронная сеть пятислойная. Назначение слоев представлено ниже:

1 — входные параметры объекта;

2 — нечеткие термы, описывающие входные параметры;

3 — строки матрицы экспертных оценок (2);

4 — правила формирования d_j, $j = \overline{1,m}$;

5 — операция преобразования нечёткого множества в чёткое число (4).

При этом послойное число узлов в ИНС определяется следующим образом:

в первом — по количеству входных параметров объекта анализа;

во втором — по количеству нечетких термов в матрице экспертных оценок (2);

в третьем — по количеству строк матрицы экспертных оценок;

в четвертом — по количеству классов выходного параметра.

При этом весовые коэффициенты дуг определяются следующим образом:

равным единице для дуг между 1-м и 2-м слоями;

равным значениям функциями принадлежности $\mu^T(u)$ для дуг между 2-м и 3-м слоями;

равным весам правила формирования d_j для дуг между 3-м и 4-м слоями;

равным единице для дуг между 4-м и 5-м слоями.

Обучение нейронной сети осуществляется подбором весов минимизирующих невязку между оценкой и фактическим состоянием объекта анализа. Обучение ИНС осуществляется посредством реализации итерационной системы:

$$w_{jp}(t+1) = w_{jp}(t) - \eta \frac{\partial E_t}{\partial w_{jp}(t)} \tag{7}$$

$$c_i^{jp}(t+1) = c_i^{jp}(t) - \eta \frac{\partial E\ t}{\partial c_i^{jp}(t)} \tag{8}$$

$$b_i^{jp}(t+1) = b_i^{jp}(t) - \eta \frac{\partial E\ t}{\partial b_i^{jp}(t)} \tag{9}$$

$j = \overline{1,m}$, $j = \overline{1,n}$, $p = k_j$,

Критерием остановки итерационных вычислений является минимум функционала:

$$E_t = \frac{1}{2}(\hat{y}_t - y_t)^2 \quad (10)$$

где:

$\hat{y}_t$ и y_t — фактический и эмпирический выходные параметры объекта (1) на t-м шаге обучения;

$w_{jp}(t)$, $c_i^{jp}(t)$, $b_i^{jp}(t)$ — весовые коэффициенты w и параметры функций принадлежности b и c на t-м шаге обучения;

m — параметр обучения.

Частные производные, в (7)-(9), описывают уровень невязки параметров ИНС, и определяются следующими выражениями:

$$\frac{\partial E_t}{\partial w_{jp}} = \varepsilon_1 \varepsilon_2 \varepsilon_3 \frac{\partial \mu^{d_j}(y)}{\partial w_{jp}} \quad (11)$$

$$\frac{\partial E_t}{\partial c_i^{jp}} = \varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon_4 \frac{\partial \mu^{jp}(x_i)}{\partial c_i^{jp}} \quad (12)$$

$$\frac{\partial E_t}{\partial b_i^{jp}} = \varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon_4 \frac{\partial \mu^{jp}(x_i)}{\partial b_i^{jp}} \quad (13)$$

где

$$\varepsilon_1 = \frac{\partial E_t}{\partial y} = y_t - \hat{y}_t \quad (14)$$

$$\varepsilon_2 = \frac{\partial y}{\mu^{d_j}(y)} = \frac{\bar{d}_j \sum_{j=1}^{m} \mu^{d_j}(y) - \sum_{j=1}^{m} d_j \mu^{d_j}(y)}{\left(\sum_{j=1}^{m} \mu^{d_j}(y)\right)^2} \quad (15)$$

$$\varepsilon_3 = \frac{\delta \mu^{d_j}(y)}{\delta\left(\prod_{i=1}^{n} \mu^{jp}(x_i)\right)} = w_{jp} \quad (16)$$

$$\varepsilon_4 = \frac{\partial\left(\prod_{i=1}^{n} \mu^{jp}(x_i)\right)}{\partial \mu^{jp}(x_i)} = \frac{1}{\mu^{jp}(x_i)} \prod_{i=1}^{n} \mu^{jp}(x_i) \quad (17)$$

$$\frac{\mu^{d_j}(y)}{\delta w^{jp}(x_i)} = \prod_{i=1}^{n} \mu^{jp}(x_i) \quad (18)$$

$$\frac{\partial \mu^{jp}(x_i)}{\partial c_i^{jp}} = \frac{2c_i^{jp}\left(x_i - b_i^{jp}\right)^2}{\left(\left(c_i^{jp}\right)^2 \left(x_i - b_i^{jp}\right)^2\right)^2} \quad (19)$$

$$\frac{\partial \mu^{jp}(x_i)}{\partial b_i^{jp}} = \frac{2\left(c_i^{jp}\right)^2 \left(x_i - b_i^{jp}\right)}{\left(\left(c_i^{jp}\right)^2 \left(x_i - b_i^{jp}\right)^2\right)^2} \quad (20)$$

Итак, алгоритм обучения ИНС реализуется в два этапа. На первом — осуществляется расчет значения выходного параметра (y), соответствующее архитектуре ИНС. На втором — значение невязки (E_t) и по формулам (11)-(20) пересчитываются весовые коэффициенты связей межу нейронами.

Таким образом, предложенный подход к решению задачи оценки эффективности мероприятий информационной безопасности на защищенных экономических системах реализован в виде ИНС, объединяющей возможности обработки гетерогенной информации об оцениваемой СЗИ, представленной в виде количественных данных и сложных качественных лингвистических описаний, полученных на основе экспертных оценок, и обучения ИНС в реальном масштабе времени. При этом привлечение возможностей ИНС для получения адекватной модели, анализируемой СЗИ, позволяет существенно повысить объективность и точность оценивания и, как следствие, его качество.

Библиографический список

1. ГОСТ Р 50922–96. Защита информации. Основные термины и определения.
2. *Скляров А.В., Тищенко Е.Н., Стрюков М.Б., Шарыпова Т.Н.* Управление информационными рисками защищенных экономических систем на основе анализа нечетких временных рядов// Вопросы экономики и права № 8 2016 с.58
3. *Ротштейн А.П.* Интеллектуальные технологии идентификации. Универсум. Винница 1999