РЕАЛИЗАЦИЯ МЕТОДИКИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СРЕДЕ MATLAB

***Булдакова Татьяна Ивановна**, доктор технических наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва*
E-mail buldakova@bmstu.ru
***Миков Дмитрий Александрович**, ассистент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана., г. Москва*
E -mail mikovda@yandex.ru

В работе рассмотрена задача анализа рисков информационной безопасности. Представлен алгоритм анализа информационных рисков в виде вложенных процедур. Приведены особенности реализации этапа оценки информационных рисков в общем процессе анализа. Предложена методика на основе нейронечёткой сети, обеспечивающая адекватность оценки и адаптированная к нечисловым входным данным. Рассмотрен пример реализации нейронечёткой сети в среде MATLAB. Даны общие рекомендации по применению методики.

***Ключевые слова**: управление информационной безопасностью, анализ информационных рисков, методы оценки, нейронечёткая сеть, MATLAB*

IMPLEMENT OF INFORMATION SECURITY RISK ASSESSMENT TECHNIQUE IN MATLAB

***Tatyana Buldakova**, Doctor of Sciences (Tech.), Professor of department "Information security" in Bauman Moscow State Technical University, Moscow*
E-mail: buldakova@bmstu.ru
***Dmitry Mikov**, Assistant of the department «Information Security» in Bauman Moscow State Technical University, Moscow*
E-mail: mikovda@yandex.ru

This paper considers the problem of information security risk analysis. The algorithm of information security risk analysis has been designed in the form of embedded procedures. Peculiarities of assessment phase realization in the overall analysis process have been formulated. The assessment technique based on neuro–fuzzy network has been developed. It provides adequate assessment and adapt to non–numeric input data. An example of neuro–fuzzy network implementation in MATLAB application has been considered. General recommendations for using this technique have been given.

***Keywords**: information security management, information security risk analysis, assessment methods, neuro–fuzzy network, MATLAB*

Введение

Управление информационной безопасностью занимает всё более значимое место в функционировании любой организации, применяющей современные технологии сбора, хранения и обработки информации. Данный процесс основывается на периодическом проведении анализа информационных рисков, который позволяет своевременно выявлять угрозы информационной безопасности, уязвимости информационной системы, внедрять соответствующие мероприятия по их нейтрализации и, как следствие, постоянно отслеживать состояние информационной безопасности в организации, учитывая предыдущий опыт и новые угрозы и уязвимости.

В настоящее время используется множество разнообразных методик анализа информационных рисков, основное отличие которых заключается в применяемых шкалах оценки уровня риска: количественных или качественных [1-4].

В количественных методиках риск оценивается через числовое значение. В качестве входных данных для оценки обычно используют накопленную статистическую информацию об инцидентах [1, 2].

Однако частое отсутствие достаточного количества статистических данных приводит к снижению адекватности результатов оценки.

Качественные методики более распространены [3-5], однако в них используются слишком упрощённые шкалы, обычно содержащие три уровня оценки риска (высокий, средний, низкий). Оценка проводится на основе экспертных опросов, а перспективные интеллектуальные методы пока применяются недостаточно [4, 5].

Цель данного исследования – разработка методики оценки информационных рисков с учётом реальных условий функционирования системы, обоснование выбора используемых в ней методов и повышение адекватности экспертных оценок для настройки нейронечёткой сети.

1. Особенности оценки информационных рисков

Риск информационной безопасности R – это комплексная величина, определяемая как функция (или функционал) ряда факторов, таких как угрозы информационной безопасности (X1), потенциально возможный ущерб (X2) и уязвимости информационной системы (X3).

Анализ информационных рисков, несмотря на имеющиеся специфические для него нюансы в различных сферах деятельности, представляет собой упорядоченный алгоритм, состоящий из одинаковых этапов, на каждом из которых могут быть применены свои методы (рис. 1).

Анализ потоков данных эффективно реализуется с помощью современных структурных методов [6, 7]. Например, в работах [8, 9] для разработки функциональной модели, описывающей информационные процессы в виртуальном центре охраны здоровья, была использована методология IDEF0. Подобные модели позволяют выявить факторы риска, подлежащие оценке [10, 11].

Основные же сложности анализа связаны с оценкой риска информационной безопасности и его факторов (угроз, возможного ущерба, уязвимостей). Это вызвано следующими проблемами:

1) неполнота информации о составляющих риска и их неоднозначные свойства;

2) сложность создания модели информационной системы и оценки её уязвимости;

3) длительность процесса оценки и быстрая потеря актуальности её результатов;

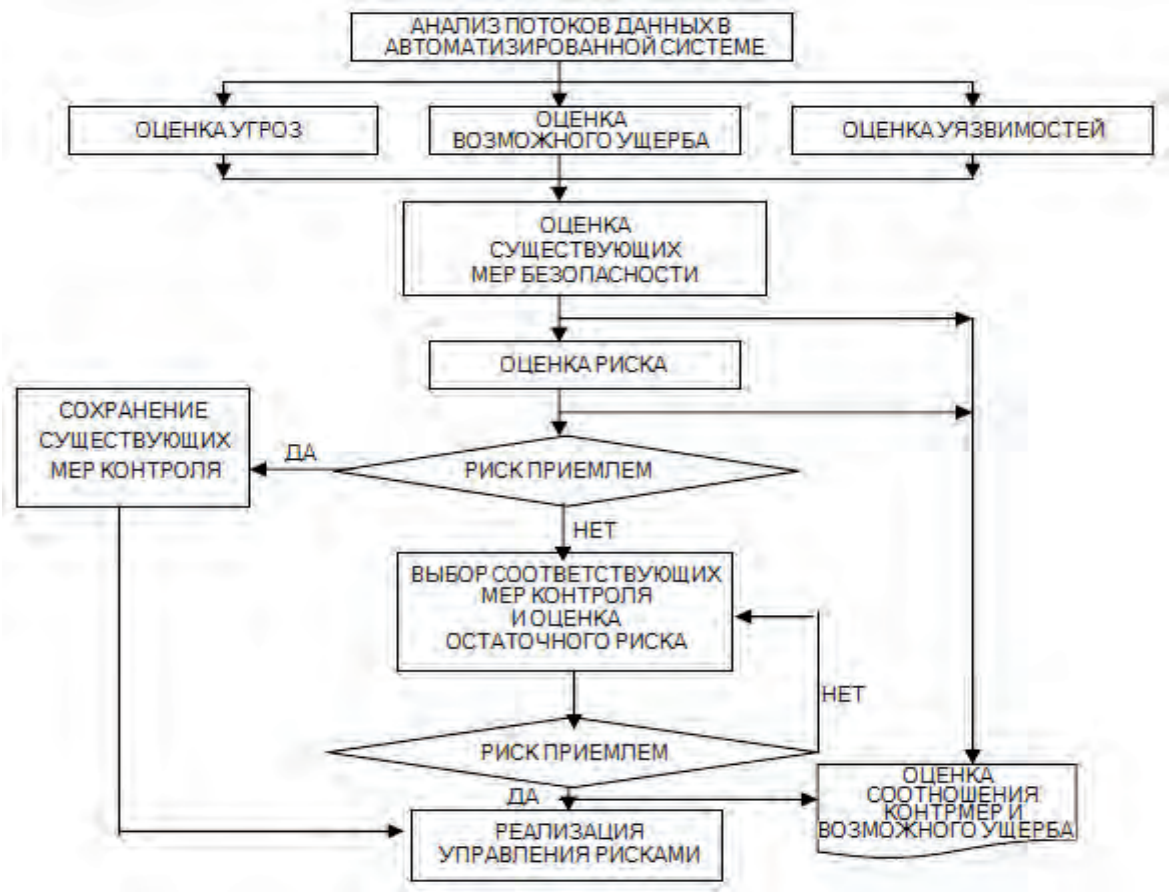

***Рис. 1**. Процесс анализа информационных рисков*

4) сложность агрегации данных из различных источников, в том числе статистической информации и экспертных оценок;

5) необходимость привлечения нескольких специалистов по анализу рисков для повышения адекватности оценок.

Поэтому задача заключается в выборе из множества Y методов оценки риска информационной безопасности такого метода y^*, который обеспечивал бы максимальную вероятность адекватной оценки с учётом адаптивности к качественным данным о факторах риска X_1, X_2 и X_3:

$$y^* \in Y \Leftrightarrow p_1^* = \max p_1(X, p_2(y)),$$

где X – множество факторов риска; $_1$ – вероятность адекватной оценки риска; $_2$ – показатель адаптивности метода к качественным данным.

Однако решение поставленной задачи связано с рядом проблем:

1) оценить показатель $_1$, для чего нужно знать X;

2) сформировать X с учётом тех факторов риска, которые могут проявиться в реальных условиях функционирования системы;

3) обеспечить достаточное значение показателя $_2$;

4) рассмотреть и проанализировать множество для оценки эффективности методов.

Таким образом, следует поставить задачу шире: необходима методика оценки информационных рисков, учитывающая указанные ограничения и сложности и отвечающая заданным требованиям.

Чтобы оценить эффективность методов, необходимо рассмотреть их множество , в соответствии с которым методы можно разделить на три основные группы:

1) статистические методы;

2) методы экспертных оценок;

3) методы моделирования.

Из результатов работ [4, 6, 10] следует, что наибольшими показателями эффективности обладают методы моделирования, среди которых выделяются нейронечёткие сети (ННС), которые способны выявлять и адекватно оценивать риск информационной безопасности за счёт нейросетевого компонента (показатель $_1$), а также за счёт использования нечёткой логики они адаптивны к нечисловым данным (показатель $_2$).

2. Разработка нейронечёткой сети в среде MATLAB

Чтобы разработать и использовать ННС для анализа рисков информационной безопасности, необходимо определить структуру сети [12, 13].

Входными переменными будут служить значения трех факторов риска на отрезке [0, 1], описанные лингвистическим терм-множеством (очень низкий, низкий, средний, высокий, очень высокий) (табл. 1).

Таблица 1. *Уровни шкалы при оценке факторов риска*

Уровни шкалы	Угрозы	Ущерб	Уязвимости
Очень низкий (от 0 до 0,2)	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов, которые быстро восполняются, или незначительное влияние на репутацию	Уязвимость, которой можно пренебречь
Низкий (от 0,2 до 0,4)	Событие случается редко	Более заметные потери материальных активов, более существенное влияние на репутацию или ущемление интересов	Незначительная уязвимость, которую легко устранить
Средний (от 0,4 до 0,6)	Событие вполне возможно при определённом стечении обстоятельств	Достаточные потери материальных активов или ресурсов или достаточный урон репутации и интересам	Умеренная уязвимость
Высокий (от 0,6 до 0,8)	Скорее всего, событие произойдёт при организации атаки	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьёзная уязвимость, ликвидация которой возможна, но связана со значительными затратами
Очень высокий (от 0,8 до 1)	Событие, вероятнее всего, произойдёт при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая уязвимость, которая ставит под сомнение возможность её устранения

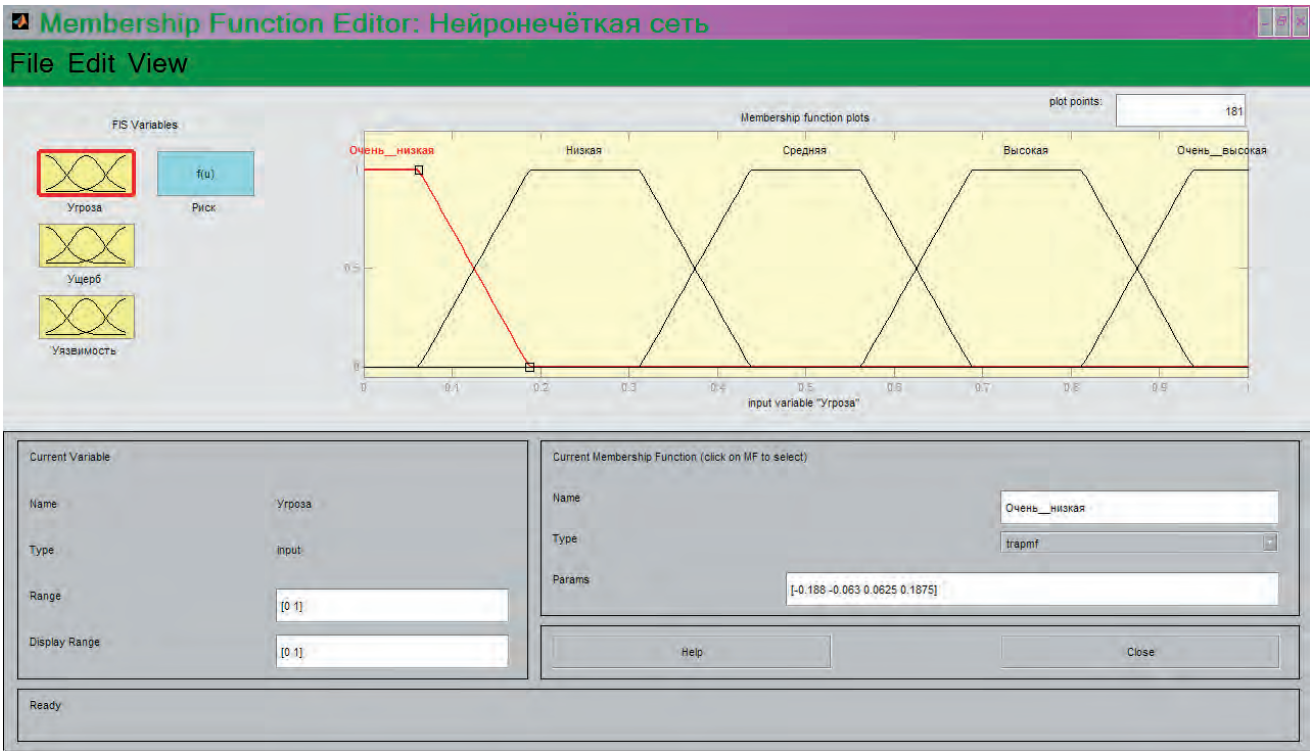

***Рис. 2**. Редактор функций принадлежности*

Для их оценки следует использовать данные датчиков о потенциально опасной активности, общем уровне сетевой активности и нагрузки на тот или иной участок автоматизированной системы и т.д., а также экспертные оценки количественных показателей функционирования системы информационной безопасности.

В итоге на выходе системы по входным данным будет получена оценка уровня риска информационной безопасности на отрезке [0, 1], описанная расширенным лингвистическим термножеством (пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический).

Шкала измерения уровня информационных рисков будет выглядеть следующим образом:

1) пренебрежимо низкий (0) – риском можно пренебречь;

2) очень низкий (0,125) – если сведения расцениваются как очень низкий риск, необходимо определить, существует ли необходимость в корректирующих действиях, или есть возможность принять этот риск;

3) низкий (0,25) – уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы;

4) ниже среднего (0,375) – необходимо разработать и применить план корректирующих действий в течение приемлемого периода времени;

5) умеренный (0,5) – уровень риска не позволяет стабильно работать, имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы в сторону уменьшения риска;

6) выше среднего (0,625) – система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее;

7) высокий (0,75) – уровень риска такой, что бизнес-процессы находятся в неустойчивом состоянии;

8) очень высокий (0,875) – необходимо незамедлительно принять меры по уменьшению риска;

9) критический (1) – уровень риска очень большой и является недопустимым для организации, что требует прекращения эксплуатации системы и принятия радикальных мер по уменьшению риска.

После определения структуры ННС следует задать функции принадлежности входных переменных, что предполагает определение их вида для каждой из входных лингвистических переменных на оси возможных значений риска. Кроме этого, необходимо задать параметры выбранных функций принадлежности. Для выполнения этих процедур разработаны специализированные программы, графический интерфейс которых существенно облегчает работу на этом этапе.

Наиболее эффективным инструментом разработки является редактор FIS программного ком-

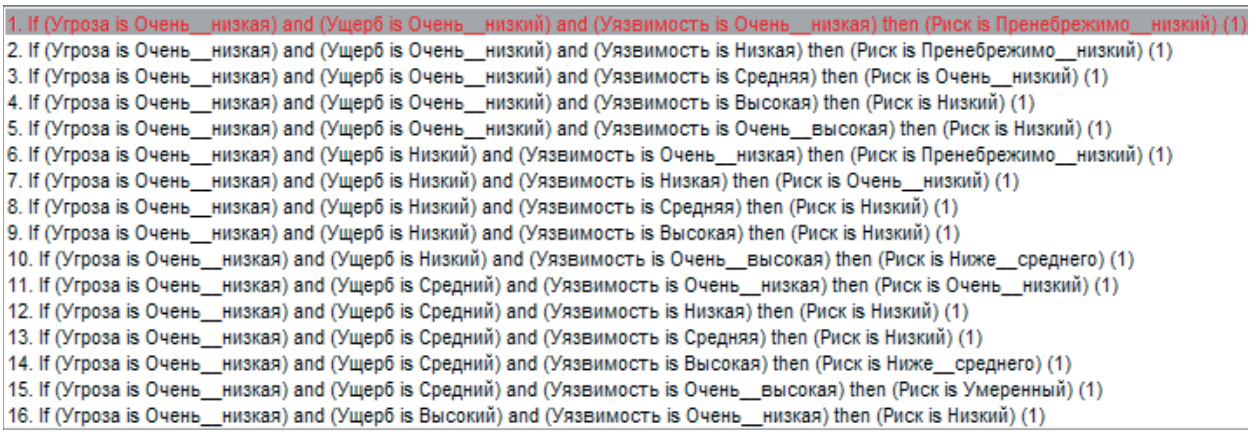

***Рис. 3**. Правила системы нечёткого вывода*

плекса MATLAB, который обладает графическим интерфейсом и позволяет вызывать все другие редакторы и программы просмотра систем нечёткого вывода. Графический интерфейс этого редактора обладает максимальным удобством и гибкостью [14]. Для создаваемой нечёткой модели выбраны следующие параметры:

1) 3 входные (угроза, ущерб, уязвимость) и 1 выходная (риск) переменные;

2) тип системы нечёткого вывода – Сугено;

3) And method (Метод логической конъюнкции) – prod (метод алгебраического произведения);

4) Or method (Метод логической дизъюнкции) – probor (метод алгебраической суммы);

5) Implication (Метод вывода заключения) – min (метод минимального значения);

6) Aggregation (Метод агрегирования) – max (метод максимального значения);

7) Defuzzification (Метод дефаззификации) – wtaver (метод взвешенного среднего).

Для 3 входных переменных (угроза, ущерб, уязвимость) выбрано 5 нечётких классов (очень низкий, низкий, средний, высокий, очень высокий) и трапецеидальная функция принадлежности (рис. 2).

Для выходной переменной (риск) выбрано 9 нечётких классов (пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический), которые в нечёткой системе типа Сугено принимают упомянутые выше фиксированные значения на отрезке [0, 1], поэтому функция принадлежности для выходной переменной отсутствует.

Нечёткая модель анализа информационных рисков должна содержать 125 правил нечёткого вывода для всех возможных сочетаний нечётких классов входных переменных. Часть правил представлена на рис. 3.

Итак, система нечёткого вывода содержит 3 входные переменные с 5 термами, 125 правил нечётких продукций и 1 выходную переменную с 9 термами (рис. 4).

Для создания ННС необходимо создать файл с обучающими данными (файл с расширением .dat), который представляет собой обычный текстовый файл. При этом обучающие данные представляют собой числовую матрицу размерности $m \times (n+1)$, в которой количество строк m соответствует объёму выборки, первые n столбцов – значениям входных переменных модели, а последний столбец – значению выходной переменной. Согласно правилам системы MATLAB, отдельные значения матрицы отделяются пробелами, а каждая строка матрицы завершается символом «перевод каретки».

Хотя по количеству строк матрицы обучающих данных не существует формальных рекомендаций, принято считать, что качество обучения гибридной сети, а, следовательно, и точность получаемых результатов пропорционально зависит от объёма обучающей выборки. Что касается количества столбцов, то в случае с ННС для анализа информационных рисков оно равно 4. После загрузки обучающих данных из файла их структура отображается в рабочем окне редактора ANFIS (рис. 5).

Для создаваемой ННС выбран гибридный (hybrid) метод обучения, представляющий собой комбинацию метода наименьших квадратов и метода убывания обратного градиента. Количество циклов обучения (Epochs) – 1000.

Получение оценок входных переменных является той процедурой, которая обеспечивает механизм вывода текущей информацией, отражающей фактическое состояние защищённости исследуемой системы на данный момент времени. Для это-

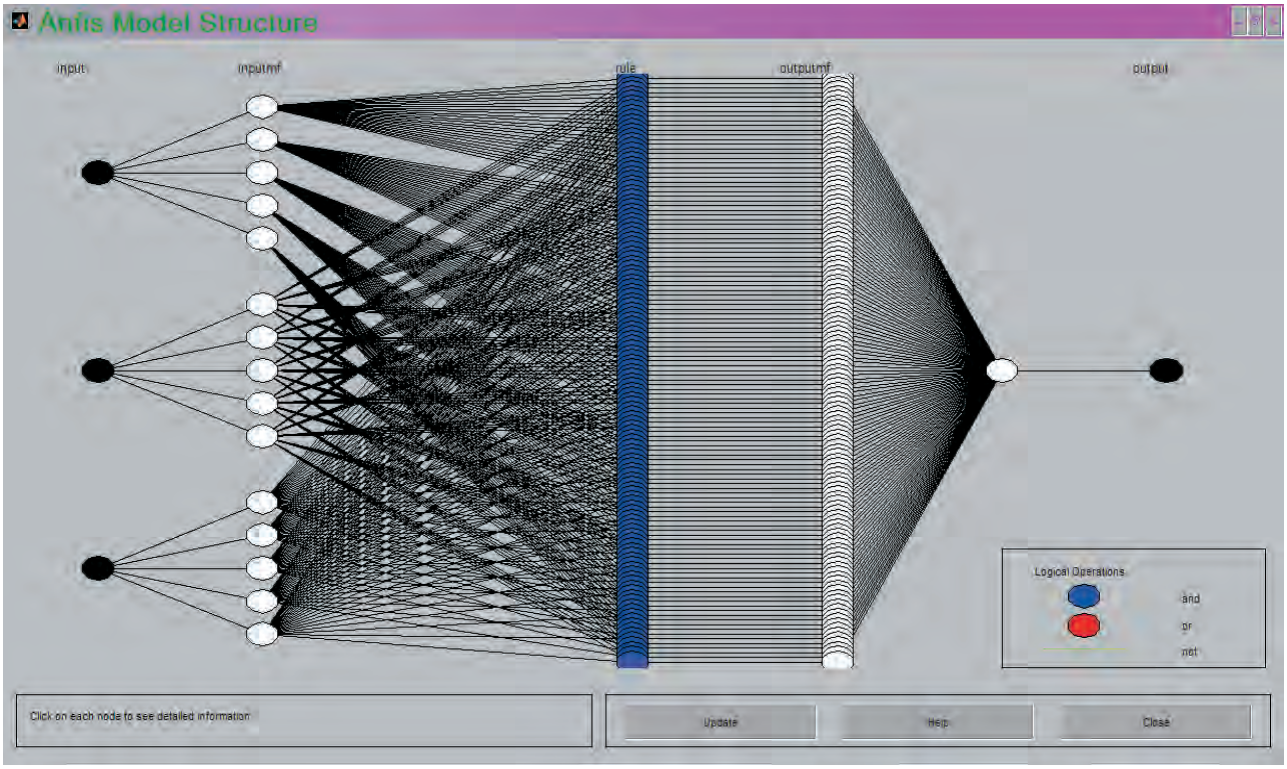

***Рис. 4**. Структура сгенерированной системы нечёткого вывода*

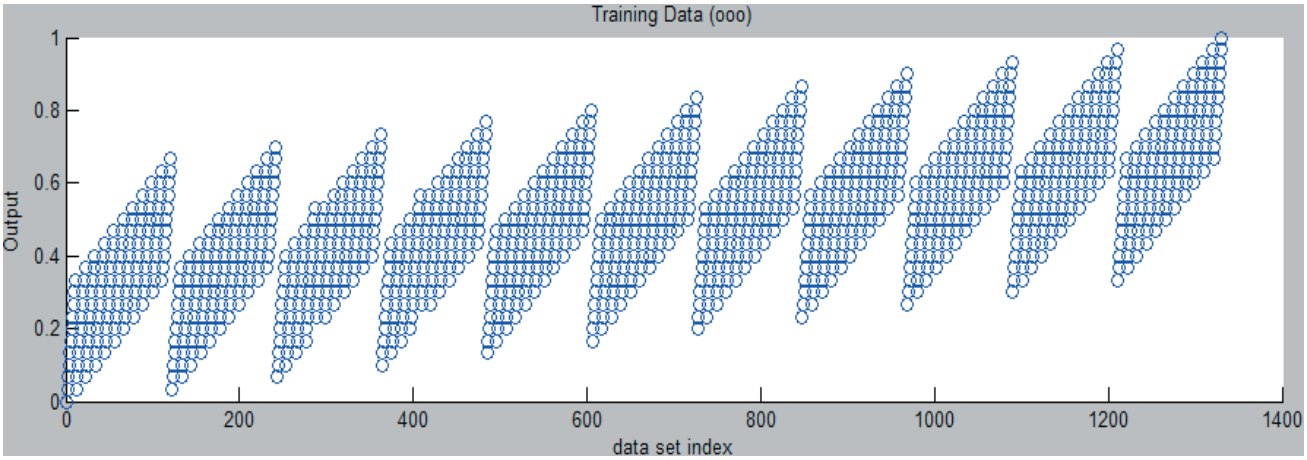

***Рис. 5**. Обучение нейронечёткой сети*

го могут быть использованы экспертные опросы. Оценки могут быть получены на основе заранее разработанных диагностических тестов, охватывающих различные аспекты проявления оцениваемых величин.

В качестве иллюстрации можно взять одну из типовых характеристик, например, проблему отслеживания действий каждого клиента в произвольный момент времени в целях выявления потенциального нарушителя.

Для определённости необходимо предположить, что на основе предварительного обследования получены некоторые оценки вероятности реализации угрозы (нарушение клиентом политики безопасности), величины потенциально возможного ущерба (урон, который понесёт организация в результате совершённого нарушения) и степени уязвимости (отсутствие протокола взаимодействия «клиент-сервер», не позволяющее своевременно отследить и выявить нарушителя). Например, угроза – 0,68, ущерб – 0,74, уязвимость – 0,72. Тогда риск равен 0,745, что соответствует значению «высокий» по шкале уровней риска (рис. 6).

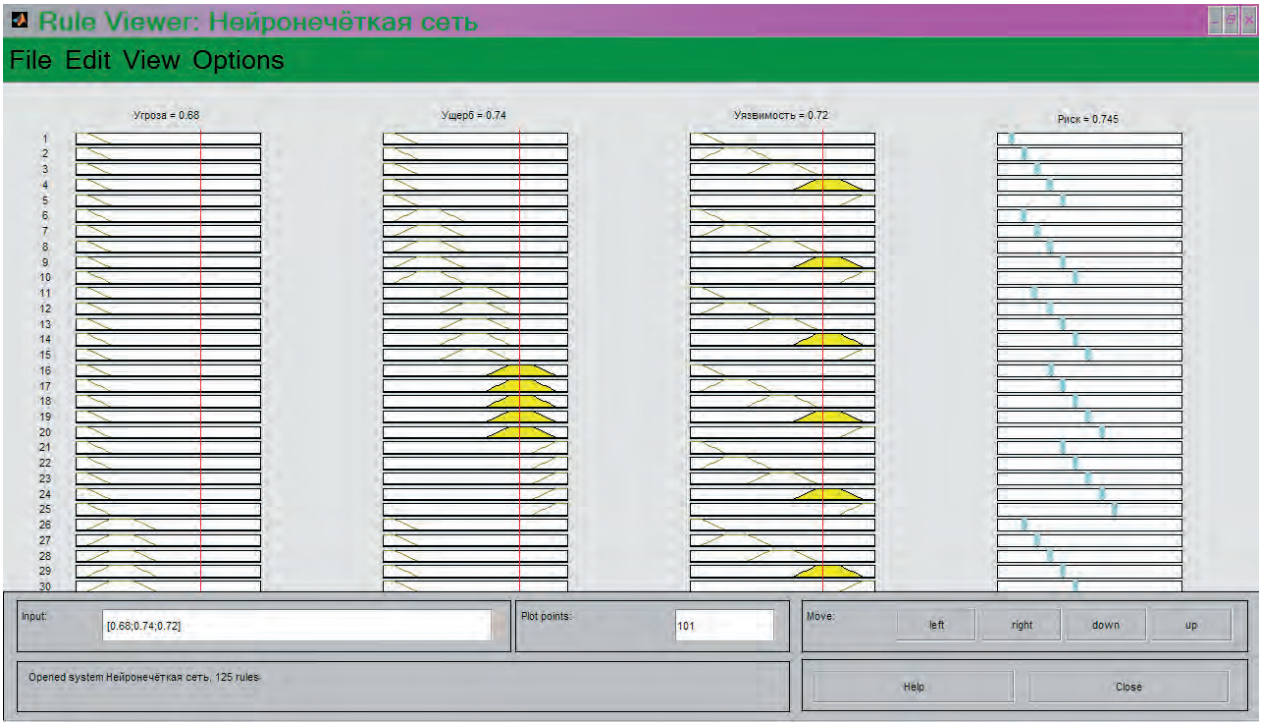

***Рис. 6**. Тестирование построенной и обученной ННС*

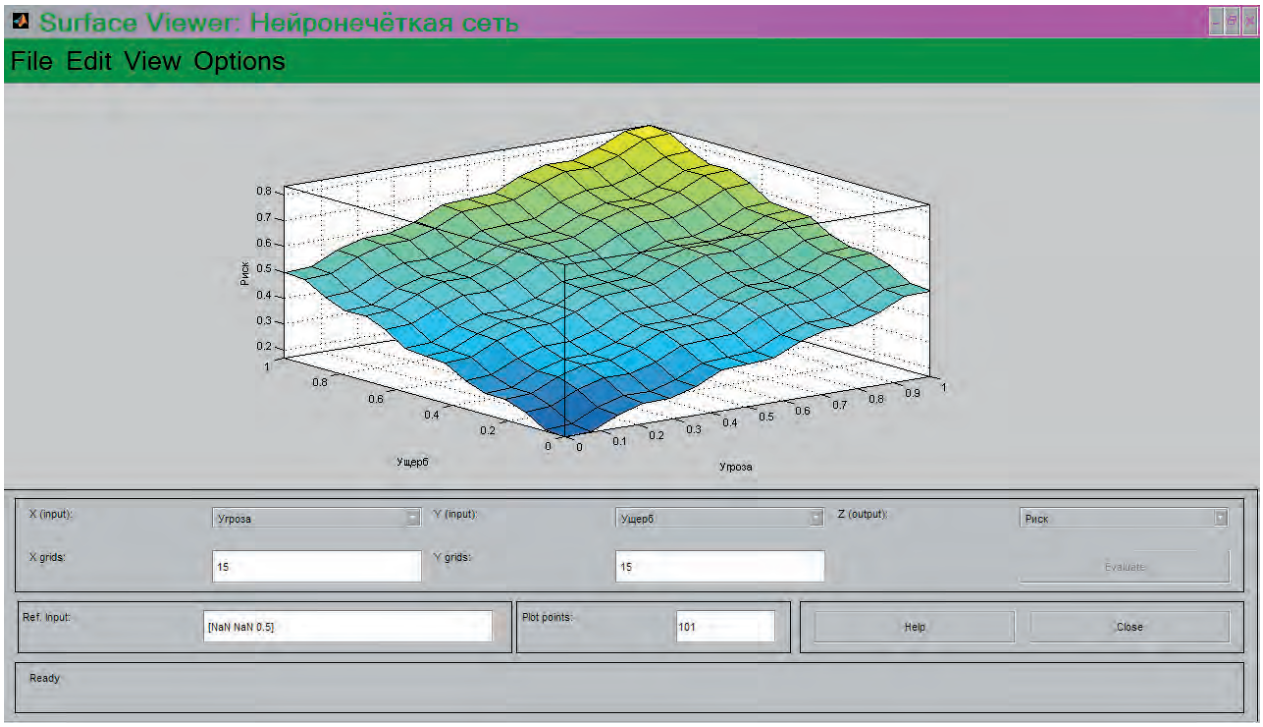

***Рис. 7**. Программа просмотра поверхности вывода*

Программа просмотра поверхности системы нечёткого вывода позволяет просматривать поверхность системы нечёткого вывода и визуализировать графики зависимости выходных переменных от отдельных входных переменных. Пример вида поверхности вывода от переменных угрозы и ущерба показан на рис. 7.

Построенная ННС имеет гибкие настройки, удобна и проста в применении, а также точно и наглядно отображает зависимость уровня информационного риска от значений угроз информационной безопасности, потенциально возможного ущерба и уязвимостей информационной системы.

3. Оценка информационных рисков на основе разработанной нейронечёткой сети

Алгоритм оценки информационных рисков на основе применения разработанной ННС состоит из следующих этапов:

1. Проведение экспертного опроса для получения оценок мощности угрозы (a_1), величины ущерба (a_2) и степени уязвимости (a_3) в интервале [0, 10];

2. Обеспечение адекватности экспертных оценок через вычисление коэффициента конкордации:

$$W = \frac{12S}{n^2 \times \left(m^3 - m\right)}.$$

Здесь W – коэффициент конкордации, S – сумма квадратов отклонений сумм оценок (ответов, данных всеми экспертами на каждый вопрос) от среднего арифметического сумм оценок, n – число экспертов (число ответов на один вопрос), m – число вопросов. Коэффициент конкордации W лежит в границах [0, 1]. Чем ближе значение коэффициента к единице, тем выше уровень согласованности мнений экспертов. Обычно минимально допустимое значение коэффициента конкордации составляет 0,4. Поэтому при согласованном результате $W \geq 0{,}4$ [15, 16];

3. По оставшимся оценкам вычисление входных переменных ННС – максимальных значений вероятности реализации угрозы информационной безопасности (x_1), нанесения наивысшего возможного ущерба (x_2) и использования уязвимости информационной системы (x_3). Так как под переменными x1, x2, x3 понимаются вероятности, то их значения должны быть в интервале [0, 1]:

$$\begin{cases} 0 \leq x_1 \leq 1, \\ 0 \leq x_2 \leq 1, \\ 0 \leq x_3 \leq 1. \end{cases}$$

Итоговая система уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \leq b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \leq b_2, \\ \cdots \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 \leq b_n, \end{cases}$$

$$a_{ij} \in [0,10]; b_i \in [0,30]; i \in 1,2,\ldots,n;\ j \in 1,2,3,$$

решается симплекс-методом. Здесь a_{i1} – экспертные оценки мощности угрозы; a_{i2} – экспертные оценки величины ущерба; a_{i3} – экспертные оценки степени уязвимости; b_i – оценки риска; n – число экспертов;

4. Подача полученных значений переменных x_1, x_2, x_3 на вход разработанной ННС;

5. Получение значения уровня риска информационной безопасности, сопоставление с качественной шкалой, анализ результатов и выработка контрмер на основе проведённого анализа.

Таким образом, алгоритм оценки информационных рисков включает проведение экспертного опроса для получения предварительных оценок, обеспечение адекватности экспертных оценок через вычисление коэффициента конкордации и отсеивание крайних значений, вычисление входных переменных нейро-нечёткой сети на основе оставшихся экспертных оценок, подачу полученных значений на вход нейро-нечёткой сети и выработку контрмер на основе анализа полученной выходной переменной.

Выводы

Рассмотренная методика оценки информационных рисков разработана для практического применения в среде MATLAB. Представленный прототип ННС позволяет не только решить поставленные задачи, но и существенно расширить возможности методов моделирования, адекватно использовать качественные и количественные оценки входных параметров, полученные от экспертов.

Методика позволяет учитывать качество входной информации и надёжность (степень доверия) источников информации. Она обладает широкими возможностями, позволяющими адаптировать её к разнообразным профилям прикладных систем и встраивать в состав собственных разработок систем управления рисками.

Таким образом, разработанная ННС полностью удовлетворяет критериям адекватности оценки информационных рисков и может быть использована для решения практических задач.

Литература:

1. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.
2. Велигура А.Н. О выборе методики оценки рисков информационной безопасности // Information Security / Информационная безопасность. 2008. №4. С. 16-17.

3. Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science. 2008. Pp. 1073-1078.
4. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method / Ming-Chang Lee // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6. No1. Pp. 29-45.
5. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности. 2014. №1 (2). С. 33-39.
6. Миков Д.А. Основные этапы оценки информационных рисков и способы их реализации // Теоретические и прикладные аспекты современной науки. 2014. №5-3. С. 103-106.
7. Миков Д.А. Анализ методов изучения потоков данных для оценки рисков информационной безопасности // Научное обозрение физико-математических и технических наук в XXI веке: сборник научных трудов XII Международной научно-практической конференции. – Москва, 2014. №7. С. 28-33.
8. Концептуальная модель виртуального центра охраны здоровья населения / В.С. Анищенко, Т.И. Булдакова, П.Я. Довгалевский и др. // Информационные технологии. 2009. №12. С. 59-64.
9. Булдакова Т.И., Миков Д.А. Анализ информационных процессов виртуального центра охраны здоровья // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. №2. С. 10-20.11.
10. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. 2014. №4 (7). С. 49-54.
11. Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т.И. Булдакова, С.И. Суятинов, Д.А. Миков // Информационное общество. 2013. №4. С. 6.
12. Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечёткой сети // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2015. №4. С. 13-17.
13. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели // Наука и образование: электронное научно-техническое издание. 2013. №11. С. 295-310.
14. Леоненков А.В. Нечёткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. 736 с.
15. Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков // Инженерный журнал: наука и инновации. 2012. №3 (3). С. 36.
16. Миков Д.А. Управление информационными рисками с использованием экспертного опроса. Германия, Саарбрюккен: LAP LAMBERT Academic Publishing, 2013. 83 с.

References:

1. Astakhov A.M. Iskusstvo upravleniya informatsionnymi riskami. M.: DMK Press, 2010. 312 s.
2. Veligura A.N. O vybore metodiki otsenki riskov informatsionnoy bezopasnosti // Information security / Informatsionnaya bezopasnost'. 2008. №4. S. 16-17.
3. Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science. 2008. Pp. 1073-1078.
4. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method / Ming-Chang Lee // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6. No1. Pp. 29-45.
5. Belfer R.A., Kalyuzhny D.A., Tarasova D.V. Analiz zavisimosti urovnya riska informatsionnoy bezopasnosti setey svyazi ot ekspertnykh dannykh pri raschetakh s ispol'zovaniem modeli netchyotkikh mnojestv // Voprosy kiberbezopasnosti. 2014. №1 (2). S. 33-39.
6. Mikov D.A. Osnovnye etapy otsenki informatsionnykh riskov i sposoby ikh realizatsii // Teoretitcheskie i prikladnye aspekty sovremennoy nauki. 2014. №5-3. S. 103-106.
7. Mikov D.A. Analiz metodov izutcheniya potokov dannykh dlya otsenki riskov informatsionnoy bezopasnosti // Nautchnoe obozrenie fiziko-matematitcheskikh i tekhnitcheskikh nauk v XXI veke: sbornik nautchnykh trudov XII Mezhdunarodnoy nautchno-praktitcheskoy konferentsii. – Moskva, 2014. №7. S. 28-33.
8. Kontseptual'naya model' virtual'nogo tsentra okhrany zdorov'ya / V.S. Anishchenko, T.I. Buldakova, P.Y. Dovgalevskiy i dr.// Informatsionnye tekhnologii. 2009. №12. S. 59-64.
9. Buldakova T.I., Mikov D.A. Analiz informatsionnykh protsessov virtual'nogo tsentra okhrany zdorov'ya / Nautchno-tekhnitcheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2014. №2. S. 10-20.
10. Mikov D.A. Analiz metodov i sredstv, ispol'zuemykh na razlitchnykh etapakh otsenki riskov informatsionnoy bezopasnosti // Voprosy kiberbezopasnosti. 2014. №4 (7). S. 49-54.
11. Analiz informatsionnykh riskov virtual'nykh infrastruktur zdravookhraneniya / T.I. Buldakova, S.I. Suyatinov, D.A. Mikov // Informatsionnoe obshchestvo. 2013. №4. S. 6.
12. Buldakova T.I., Mikov D.A. Metodika analiza informatsionnykh riskov s primeneniem neyro-netchyotkoy seti // Nautchno-tekhnitcheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2015. №4. S. 13-17.
13. Buldakova T.I., Mikov D.A. Otsenka informatsionnykh riskov v avtomatizirovannykh sistemakh s pomoshch'yu neyro-netchyotkoy modeli // Nauka i obrazovanie: elektronnoe nautchno-tekhnitcheskoe izdanie. 2013. №11. S. 295-310.
14. Leonenkov A.V. Netchyotkoe modelirovanie v srede MATLAB i fuzzyTECH. SPb.: BKHV-Peterburg, 2005. 736 s.
15. Buldakova T.I., Mikov D.A. Metod povysheniya adekvatnosti otsenok informatsionnykh riskov // Inzhenernyy zhurnal: nauka i innovatsii. 2012. №3 (3). S. 36.
16. Mikov D.A. Upravlenie informatsionnymi riskami s ispol'zovaniem ekspertnogo oprosa. Germaniya, Saarbryukken: LAP LAMBERT Academic Publishing, 2013. 83 s.