УДК 681.142.33:681.14

С.А. Агеев

МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИЩЕННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Агеев Сергей Александрович, *кандидат технических наук, доцент, окончил радиотехнический факультет Ульяновского политехнического института. Начальник научно-технического центра ОАО «НИИ «Нептун», г. Санкт-Петербург. Специализируется в области проектирования телекоммуникационных систем. Имеет статьи, патенты в области систем передачи данных. [e-mail: serg123_61@ mail.ru]*.

Аннотация

В статье предложены методы интеллектуального анализа данных, используемые для управления рисками информационных угроз элементам защищенных мультисервисных сетей специального назначения (ЗМС СН). Обосновывается, что скоротечность процессов в ЗМС СН, их многообразие, неточность и неполнота, а также большая размерность априорных данных о сетевых элементах приводят к необходимости применения интеллектуальных методов обработки данных и управления. Проведен анализ факторов, влияющих на время цикла управления информационной безопасностью (ИБ) ЗМС СН, предложена единая метрика оценки угроз информационной безопасности элементов ЗМС СН. Разработана единая математическая модель процедур кластеризации, классификации и ранжирования угроз ИБ, определены критерии качества их функционирования. Представлены результаты исследования этой математической модели. Сформулированы правила оценки степени угроз ЗМС СН. Приведен анализ полученных результатов математического моделирования, и приведены рекомендации их практического применения. Показывается, что применение подобных методов и алгоритмов совместно с технологией интеллектуальных агентов позволяет существенно повысить оперативность управления ИБ ЗМС СН. Определены направления дальнейших исследований в данной предметной области.

Ключевые слова: защищенная мультисервисная сеть, оперативность управления, модель TMN, математическая модель, интеллектуальное управление, нечеткий логический вывод, база знаний, функция принадлежности, нечеткие данные, лингвистическая переменная.

DATA MINING METHODS FOR INFORMATION SECURITY RISKS MANAGEMENT OF THE SPECIAL PURPOSE PROTECTED MULTISERVICE NETWORKS

Sergei Aleksandrovich Ageev, *Candidate of Engineering, Associate Professor; graduated from the Faculty of Radioengineering at Ulyanovsk Polytechnic Institute; Head of the Scientific and Technical Centre OJSC 'Research Institute 'Neptun', St. Petersburg; specializes in the field of telecommunications system design; an author of articles and patents in the field of data-transfer system. e-mail: serg123_61@ mail.ru.*

Abstract

The data mining methods using for information threat risks management of the special-purpose protected multiservice networks (SPMN) elements are proposed. The fact that the process speed in SPMN, its variety, inaccuracy, and imperfection as well as a high aprior network element data dimension necessitates the application of intelligent techniques for data processing and management is explained. The factors effected on the SPMN information security management cycle time are analyzed, a unified metric for the threat assessment of SPMN elements information security is proposed. A unified mathematical model for the procedure of information security threat clustering, ranking, and classification is developed, its performance criteria are evaluated. The research results of this mathematical model are presented. Threat estimation rules for the special-purpose protected multiservice networks are formulated. The achieved results of mathematical modeling are analyzed, the recommendations of practical application are provided. The similar methods and algorithms application in combination with intelligent agent technology allow to increase the efficiency of SPMN information security management. Directions for future research in this subject domain are defined.

Keywords: protected multiservice network, efficiency of the management, TMN-Model, mathematical model, intelligent control, fuzzy inference, knowledge base, membership function, fuzzy data, linguistic variable.

Введение

В настоящее время системообразующей основой ведомственных инфокоммуникационных сетей связи является защищенная мультисервисная сеть специального назначения, которая создается на основе единой сетевой инфраструктуры и представляет собой цифровую телекоммуникационную сеть интегрального обслуживания с набором служб, обеспечивающих перенос разнородного трафика с заданными количественными и качественными характеристиками предоставления пользователям инфокоммуникационных услуг.

Важнейшей проблемой при создании и эксплуатации ЗМС СН является проблема обеспечения ее безопасного функционирования и безопасности циркулирующей в ней информации. Для решения данной проблемы необходимо применение методов, которые позволяют оперативно оценивать риски информационных угроз с заданной степенью достоверности[1, 2].

В работах [6–7] рассматривается интеллектуальное иерархическое управление рисками информационной безопасности в ЗМС СН как один из важнейших компонентов реализации политики ИБ функционирования ЗМС СН. Показано, что иерархия представляет собой как вертикальные связи, так и горизонтальные связи в рамках как одного уровня, так и между уровнями управления пирамиды TMN (Telecommunications Management Network – сеть управления электросвязью) [5]. Показано также, что оперативное оптимальное управление затруднено вследствие больших размерностей совокупности решаемых оптимизационных задач, которые обеспечивают решение управленческих задач. Обосновывается, что многообразие, разнородность, неполнота, неточность и нечеткость исходных данных, учитываемых в задачах управления ЗМС СН, включая управление ИБ, предопределяют необходимость использования средств и методов искусственного интеллекта при их решении. Для обеспечения оперативности и достоверности принимаемых управленческих решений в работах [6, 7] показана целесообразность применения технологии интеллектуальных мультиагентов.

Под оперативностью управления понимают [3, 4]:

$$P_{оу} = P\left\{t_y \le T_{зу}\right\}, \quad (1)$$

где $P_{оу}$ - вероятность события, заключающегося в том, что время цикла управления не превысит заданное время $T_{зу}$. В свою очередь, время цикла управления t_y складывается из времени сбора информации о состоянии сетевых элементов $t_{сб}$, поступающей от подсистемы сетевого мониторинга, времени анализа информации t_a, времени выработки решений t_p, времени доведения управляющей информации до соответствующих сетевых элементов $t_д$, времени реализации сетевыми элементами управленческих решений t_u и времени подтверждения сетевыми элементами выполнения управленческих решений t_n. Таким образом, можно записать соотношение:

$$t_y = t_{сб} + t_a + t_p + t_д + t_u + t_n. \quad (2)$$

Откуда следует, что повышение оперативности цикла управления заключается в снижении значений слагаемых в выражении (2).

Учитывая разноплановость, многокритериальность, большую размерность решаемых задач по управлению ЗМС СН, часть процедур управления предлагается реализовывать с помощью технологии интеллектуальных агентов, основой которых является технология «агент-менеджер» [7, 8].

Данная работа посвящена решению проблемы оперативной обработки и представления исходных данных для подсистемы поддержки принятия решений при управлении информационной безопасностью в ЗМС СН.

Постановка задачи исследования

Цикл управления, как известно, содержит следующие фазы: сбор исходных данных о процессе или объекте, их анализ, выработка и принятие управленческих решений, доведение решений до объекта управления, контроль выполнения решений. Основными способами повышения оперативности управления в данной работе предлагаются способы уменьшения времени анализа исходных данных

и способы уменьшения времени выработки и принятия управленческих решений. При этом качество управления, а именно значения целевых функций, которые подлежат оптимизации, должны оставаться в области Парето-оптимальных значений.

Пусть с выходов сенсоров систем обнаружения и предупреждения вторжений (СОВ, СПВ), расположенных в составе встроенных в сетевые элементы (СЭ) интеллектуальных агентов [2, 7], за некоторое время поступают данные в виде совокупности обнаруженных признаков текущего состояния ИБ $X_i = \{x_{i1}, x_{i2}, \ldots, x_{ij}, \ldots, xi_n\}$, где $i = \overline{1, M}$. Элементы множества $\{X_i\}$ могут иметь различную физическую природу, различную размерность, а также могут иметь различные системы измерений и шкалирования. Подготовка данных для функционирования подсистемы принятия решений об уровне риска угроз ИБ заключается в выполнении следующих процедур:

- производится кластеризация входных данных;
- производится классификация полученных кластеров в соответствии с известными классами и видами деструктивных воздействий на сетевые элементы ЗМС СН;
- производится ранжирование по степени риска ИБ полученных данных.

Выполнение вышеперечисленных трех процедур предполагается осуществлять за время меньшее, чем интервал ΔT_i. Данный подход иллюстрирует рисунок 1. На нем представлены X – признаки состояния ИБ СЭ, Y – кластеры известных угроз ИБ СЭ, Z – кластеры неизвестных угроз ИБ СЭ. Очевидно, что выполняются следующие отношения:

$$Y \subseteq X,\ Z \subseteq X. \tag{3}$$

$W = Y \bigcup Z$ – множество угроз ИБ СЭ ЗМС СН.

Таким образом, необходимо построить ранжированный ряд угроз ИБ $r_1 \prec r_2 \prec \ldots \prec r_n$.

Угрозы данного класса:

$$r_k = \frac{N_k \times w_k}{\Delta T_i}, \tag{4}$$

где r_k – ранжированное значение угрозы, k – класс угрозы, N_k – количество угроз данного класса, w_k – весовой коэффициент угрозы, ΔT_i – период времени, за который появились угрозы данного класса.

Применение методов нечеткой кластеризации и нечеткой классификации для обработки первичной информации мониторинга аномального поведения элементов ЗМС СН

Для решения сформулированной выше задачи предлагается использовать методы нечеткой кластеризации и нечеткой классификации [7, 9, 10]. Применение данного подхода обуславливается необходимостью повышения оперативности цикла управления рисками ИБ ЗМС СН.

Процедура кластеризации заключается в разбиении всего множества признаков состояния ИБ на группы по некоторым признакам. Полученные группы называют кластерами.Таким образом, формальная постановка задачи кластеризации имеет следующий вид.

Дано: конечное множество объектов $X_i = \{x_{k1}, x_{k2}, \ldots, x_{kj}, \ldots, x_{kn}\}$, где $k = \overline{1, M}$. Каждый из объектов характеризуется m-компонентным признаковым описанием $(p_1, p_2, \ldots, p_k, p_m)$, $p_k \in P_{k'}$, где P_k– допустимое множество значений признака. Требуется: построить множество кластеров (разбиение множества X) $\{C_i\}$, где $i = \overline{1, c}$ и отображение $f: X \to C$, со следующими свойствами:

$$\bigcup_{i=\overline{1,c}} C_i = X,\ C_i \bigcap C_j = \varnothing,\ i, j = \overline{1,c},\ i \neq j,$$
$$\varnothing \subset C_i \subset X,\ i = \overline{1,c}. \tag{5}$$

При этом для процедур субтрактивной кластеризации количество кластеров c подлежит определению. Для оценки качества разбиения применяется критерий разброса, показывающий сумму расстояний в выбранной метрике от координат признаков до координат центра своего кластера. Например, для евклидовой метрики получаем следующий критерий разбиения:

$$\sum_{i=\overline{1,c}} \sum_{X_k \in C_i} \left\| V_i - X_i \right\|^2 \to \min, \tag{6}$$

где $C_i = \left\{ x_p : \varphi_{k_i} = 1, k = \overline{1, M} \right\}$– i–й кластер;

$V_i = \dfrac{1}{|C_i|} \sum_{x_k \in C_i} x_k$ – центр i–го кластера;

$|C_i|$ – мощность множества признаков кластера C_i.

Формальная постановка задачи нечеткой кластери-

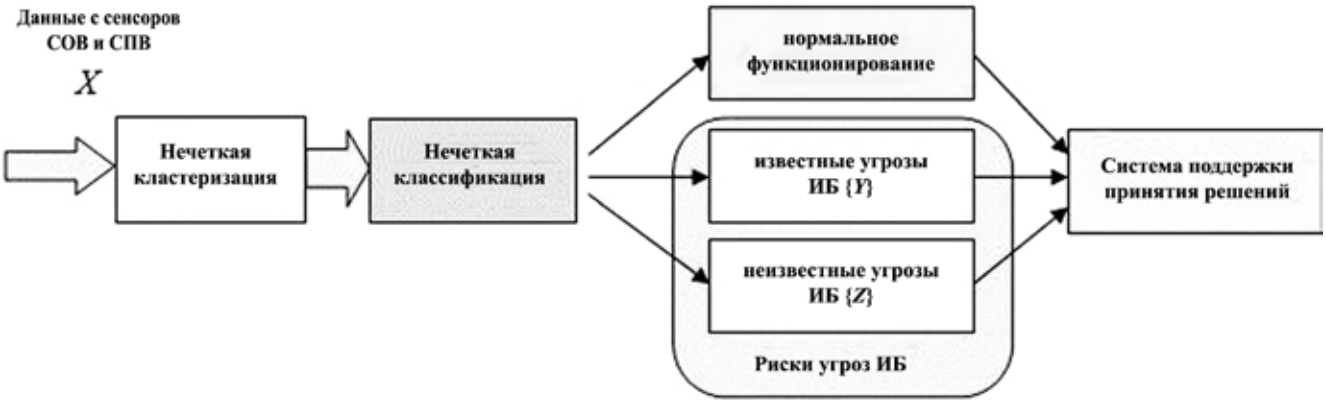

Рис. 1. Обобщенная структура процедур кластеризации, классификации и ранжирования

зации имеет следующие особенности. Нечеткие кластеры определяются матрицей нечеткого разбиения:

$$F(X)=[\mu_{ki}],\ \mu_{ki}\in[0,1]: k=\overline{1,M},\quad i=\overline{1,c}, \tag{7}$$

в которой k–я строка содержит степень принадлежности объекта X_k к кластерам $\{C_i\}$. При этом должны выполняться условия:

$$\sum_{i=\overline{1,c}}\mu_{ki}=1,\ k=\overline{1,M},$$

$$0<\sum_{k=\overline{1,M}}\mu_{ki}<M,\ i=\overline{1,c}. \tag{8}$$

Критерий качества нечеткой кластеризации в простейшем случае имеет вид:

$$\sum_{i=\overline{1,c}}\sum_{k=\overline{1,M}}(\mu_{ki})^m\left\|V_i-X_k\right\|^2\to\min, \tag{9}$$

где $V_i=\dfrac{\sum\limits_{k=\overline{1,M}}(\mu_{ki})^m X_k}{\sum\limits_{k=\overline{1,M}}(\mu_{ki})^m}$ – центр нечеткого кластера;

$m\in(1,\infty)$ – экспоненциальный вес.

Алгоритм нечеткой субтрактивной (горной) кластеризации представлен на рисунке 2. Алгоритм нечеткой классификации предлагается реализовывать на основе метода нечеткого логического вывода Мамдани [9, 10], имеющего вид:

$$\bigcup_{i=1}^{c}\left(\bigcap_{j=1}^{m}x_i=a_{i,j}\times w_j\right)\to y_j=d_j,\quad j=\overline{1,m}, \tag{10}$$

где x_i – набор входных признаков;

y_j – выходная переменная j-го правила;

$a_{i,j}$ – нечеткий терм, которым оценивается переменная в правиле j базы знаний;

w_j – весовой коэффициент правила j;

d_j – набор значений выходной переменной y_j.

Степени принадлежности $\mu_{dj}(X^*)$ признака классифицируемой угрозе ИБ вычисляются по методам, изложенным в [9, 10].

Признаки угроз ИБ также являются нечеткими величинами. Каждый признак характеризуется степенью наблюдаемости [9, 10], которой присваиваются лингвистические термы.

Ранжирование классифицируемых рисков угроз ИБ СЭ ЗМС СН осуществляется в соответствии с (4). При реализации процедур нечеткой классификации возможно предварительное обучение нечеткого классификатора. В процессе функционирования корректировка баз знаний возможна в соответствии с методами, изложенными в [9].

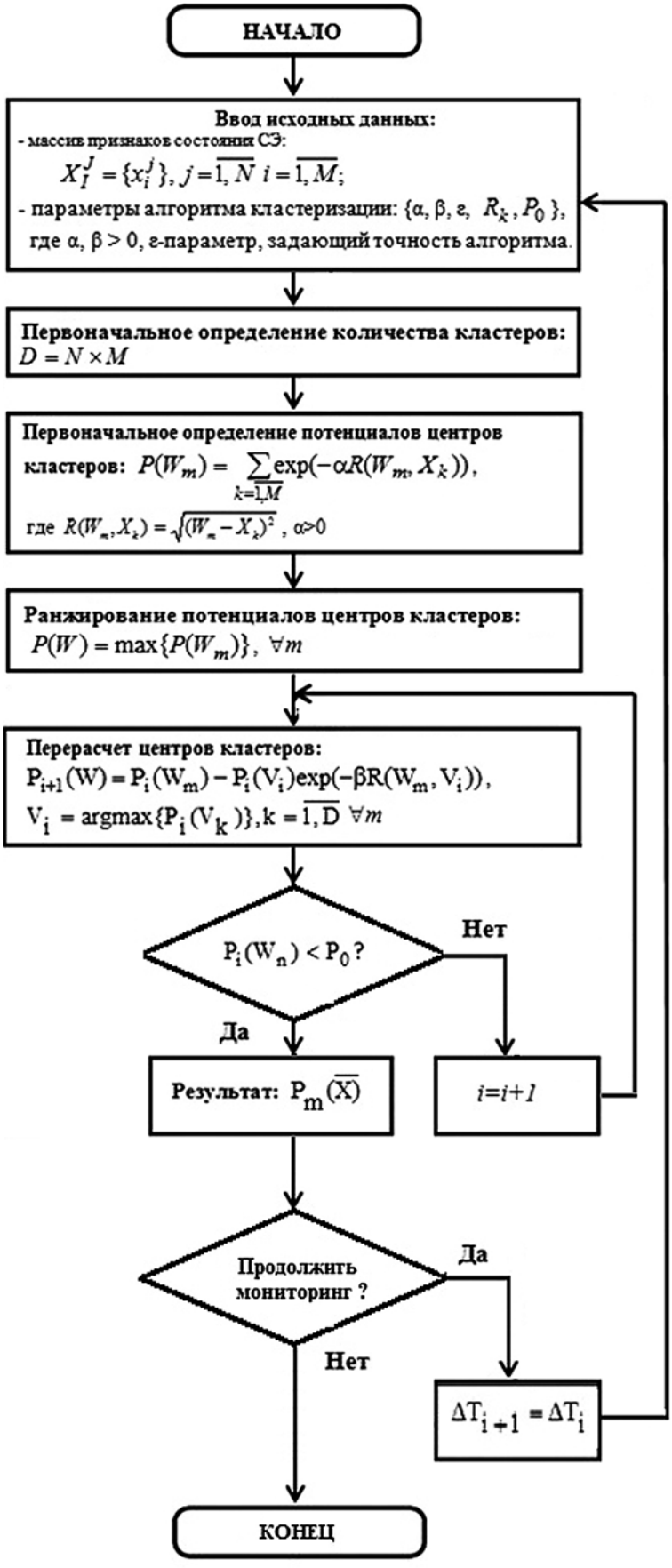

Рис. 2. Алгоритм горной кластеризации

Анализ результатов математического моделирования

Исходные данные, поступающие на вход алгоритма кластеризации, должны удовлетворять следующим условиям [10]:

- функция распределения вероятностей разброса признаков относительно центра кластера должна аппроксимироваться гауссовой функцией распределения;
- признаки состояния системы должны быть некоррелированными;
- значения признаков должны быть либо безразмерными, либо иметь одни и те же единицы измерения;
- распределение значений признаков должно быть устойчиво к влиянию случайных факторов;
- совокупности распределений значений признаков должны быть однородны и не содержать неких выбросов.

На рисунке 3 приведены некоторые результаты программной реализации предложенных методов кластеризации для двумерного случая. Признаки каждого кластера генерировались с помощью двумерного гауссова распределения, имеющего вид:

$$f(x,y)=\frac{1}{2\pi\sigma_x\sigma_y}\exp\left\{-\left(\frac{(x_i-x_ц)^2}{2\sigma_x^2}+\frac{(y_i-y_ц)^2}{2\sigma_y^2}\right)\right\}, \quad (11)$$

где σ_x – среднеквадратическое отклонение признака относительно центра по оси x;

σ_y – среднеквадратическое отклонение признака относительно центра по оси y;

$(x_ц, y_ц)$ – координаты центра кластера;

(x_i, y_i) – координаты центра i–го признака данного кластера.

В таблице 1 приведены характеристики исследуемой модели признаков.

Результаты кластеризации приведены на рисунках 4,5.

Проведенные исследования алгоритма субтрактивной кластеризации показали его высокую устойчивость к различным изменениям параметров распределения признаков. Из рисунка 3 видно, что области проекций значений признаков на координатные оси перекрываются для различных кластеров. Тем не менее, производится верное

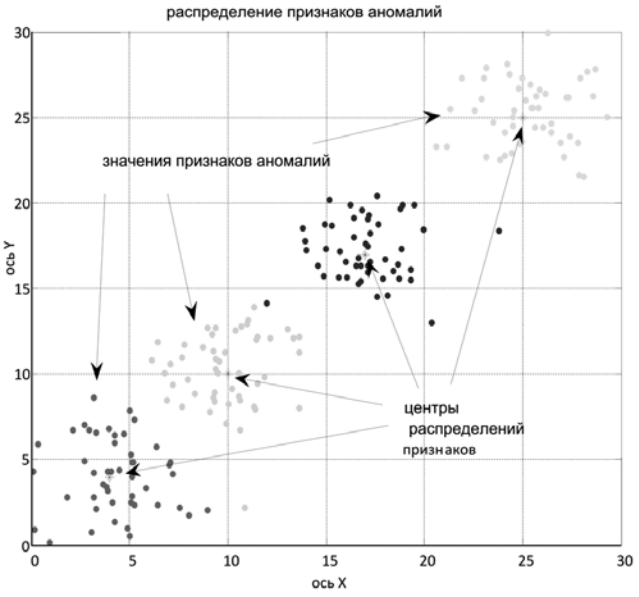

Рис. 3. Распределение признаков, центры кластеров

определение числа кластеров. Дальнейшей целью исследования применения алгоритмов кластеризации данного класса (класс алгоритмов классификации без учителя) могут быть исследования, направленные на автоматическую адаптацию параметров алгоритма в зависимости от характеристик совокупности анализируемых признаков.

Правила базы данных процедуры классификации (10) предлагается реализовывать в следующем виде:

$$\textbf{\textit{ЕСЛИ}} < (C_j \in R_j) \textbf{\textit{ И }} (R_j \in (L))> \\ \textbf{\textit{ТО}} <\textbf{\textit{УГРОЗА J – ИЗВЕСТНА}}>, \quad (12)$$

где L – соответствующая область пространства признаков. То есть, если центр кластера находится в достаточной близости от центра кластера известной угрозы, то считается, что риск идентифицирован с определенным значением коэффициента ранжирования. Если центр кластера находится на большом расстоянии от центров известных угроз, то независимо от того, в какой области он находится, риск считается максимальным, так как характеристики угрозы не определены. Далее, полученные данные поступают на вход системы поддержки принятия решений [7].

Таблица 1

Характеристики модели признаков угроз ИБ

Параметры	Первый кластер	Второй кластер	Третий кластер	Четвертый кластер
Координаты центров распределения признаков в кластерах	(4, 4)	(10, 10)	(17, 17)	(25, 25)
Среднеквадратические отклонения по осям x и y	(2, 2)	(2, 2)	(2, 2)	(2, 2)
Координаты центров кластеров	(1.8; 2.8)	(8.4; 8.9)	(17.2; 18.3)	(25.8; 25.6)
Значение потенциала кластера	0.4	1	0.82	0.64
Количество признаков в кластере	50	50	50	50
Расстояние от центра распределения до центра кластера	2.51	1.94	1.32	1.0

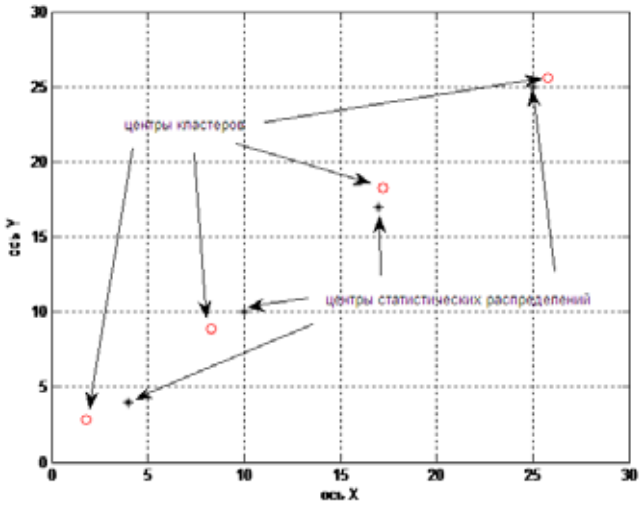

Рис. 4. Результаты кластеризации

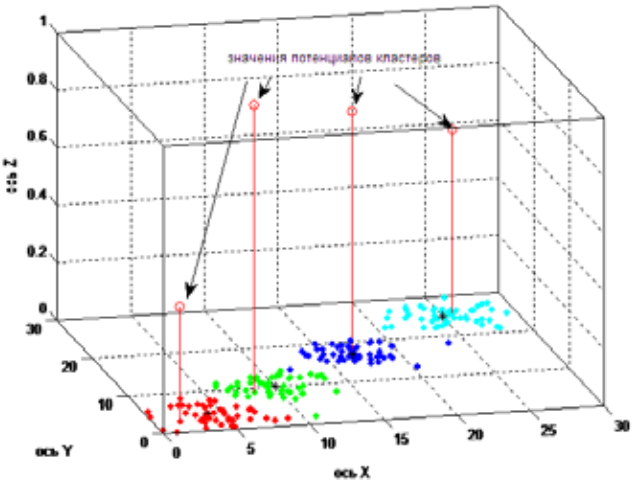

Рис. 5. Признаки кластеров, их центры, значение потенциалов кластеров

На рисунках 6-11 приведен пример функционирования предложенных методов.

На рисунке 6 представлены совокупности признаков возможных аномалий. Рисунок 7 иллюстрирует результат функционирования алгоритма субтрактивной кластеризации. Видно, что модельные и полученные центры кластеров находятся достаточно близко друг от друга. Этот факт более детально представлен на рисунке 8. На рисунке 9 представлены модельные центры кластеров. Двумерная функция принадлежности нечеткого классификатора представлена на рисунке 10. Рисунок 11 иллюстрирует функционирование процедур классификации и ранжирования. На этом рисунке R_1 – радиус максимальной достоверности принадлежности кластера к известной угрозе. Если центр кластера попадет в интервал $R_1 < C(x, y) < R_2$, то риск угрозы повышается. Если же $R_2 < C(x, y)$, то риск максимальный, так как определено наличие аномалии, но сама анамалия не идентифицирована. Таким образом, на рисунке 11 первая угроза идентифицируется как известный кластер $C(10, 15)$, степень принадлежности кластера $C(10, 20)$ известной угрозе меньше $(R_2 > R_1)$, и, следовательно, риск ИБ от ее реализации выше. Максимальный риск представляет в данном эксперименте реализация угроз, определяемых кластерами $C(20, 25)$ и $C(25, 25)$.

Признаки состояния для каждого класса угроз в данном численном эксперименте представлялись лингвистическими термами с соответствующими функциями принадлежности.

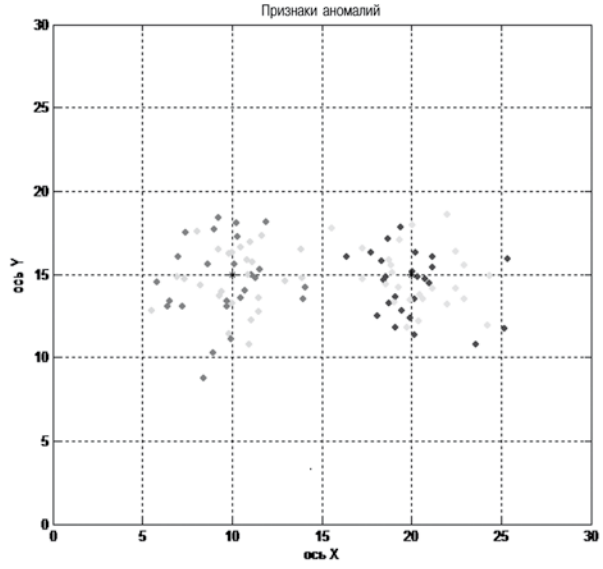

Рис. 6. Признаки аномалий

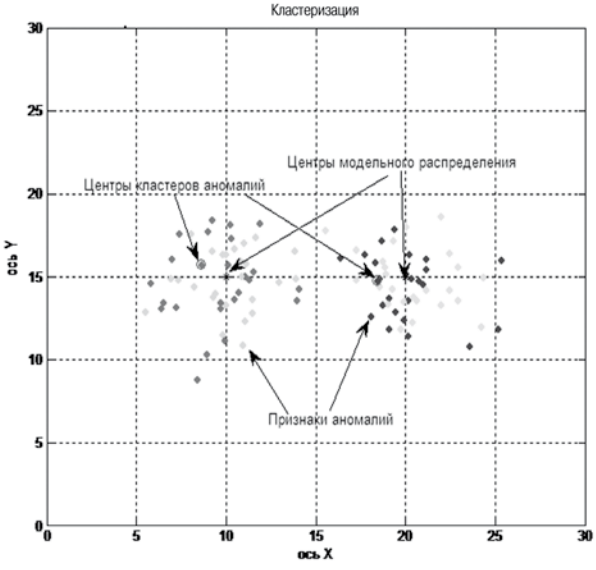

Рис. 7. Процедура субтрактивной кластеризации

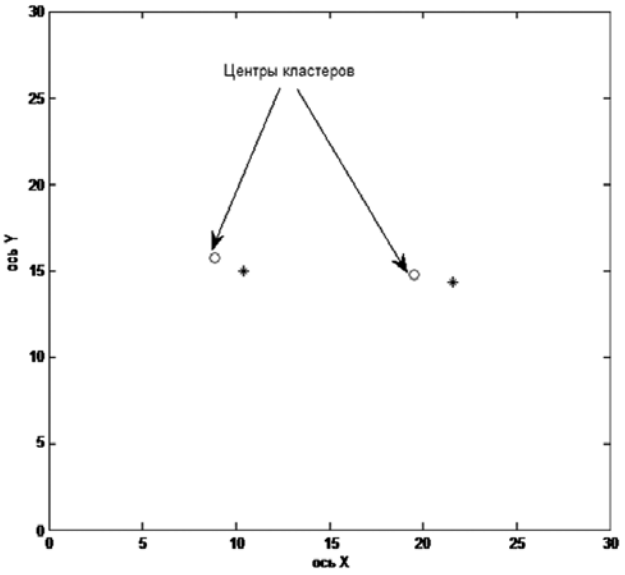

Рис. 8. Результат кластеризации

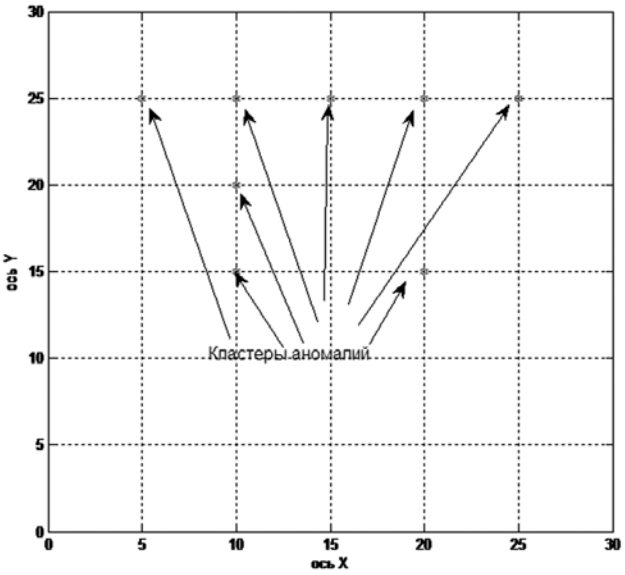

Рис. 9. Модельные кластеры аномалий

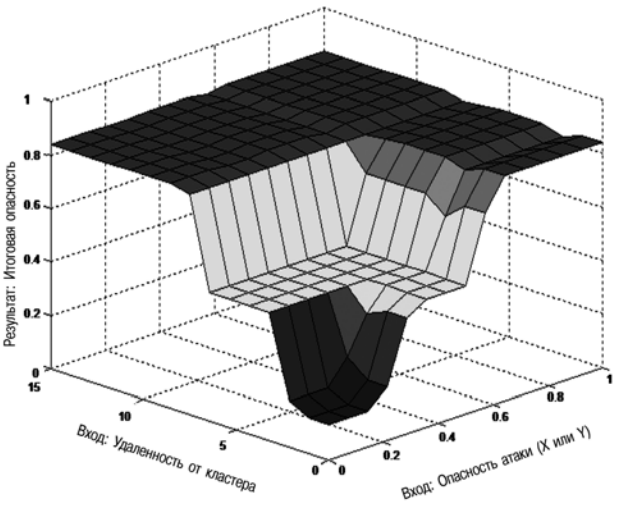

Рис. 10. Двумерная функция принадлежности нечеткого классификатора

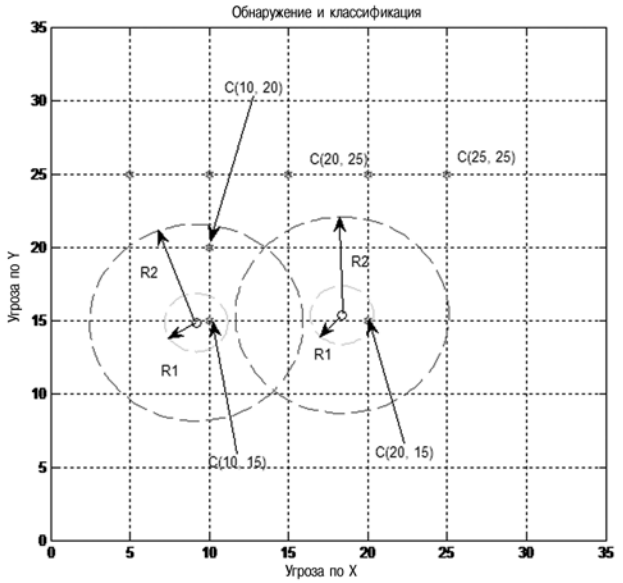

Рис. 11. Результат классификации кластеров аномалий

Анализ алгоритмов классификации и ранжирования показал их высокую устойчивость и эффективность для различных групп кластеров, для различного количества кластеров и различных их пространственных положений.

Заключение

В статье рассмотрены методы нечеткого логического вывода и нечеткой кластеризации, классификации и ранжирования, предназначенные для управления рисками информационной безопасности в ЗМС СН. Рассмотренный в статье подход позволяет поддерживать основные целевые функции сетевого и прикладного уровней ЗМС СН в части оценки и управления рисками информационной безопасности в области Парето-оптимальных значений. В ситуации динамично изменяющихся внешних обстоятельств и воздействий на ЗМС СН возможных деструктивных факторов применение данного подхода является достаточным условием успешного ее функционирования.

Предложенная математическая модель оценки рисков информационной безопасности элементов ЗМС СН достаточно просто реализуется в виде встраиваемого программного средства как на языке высокого уровня, так на средствах программирования микроконтроллеров, сигнальных процессоров или программируемых логических интегральных схем. Большинство решений по оценке рисков информационной безопасности элементов ЗМС СН подобное программное средство может принимать самостоятельно, что позволяет повысить оперативность вы-

работки управленческих решений, а также снизить объём передаваемого технологического трафика в сети.

Проведённые в работе исследования предложенных методов показали их высокую эффективность, высокие точностные характеристики, простоту программной реализации, принципиальную возможность их функционирования в режиме, близком к режиму реального времени. Оперативность выработки управленческих решений при применении данных методов может быть улучшена по сравнению с использованием статистических методов приблизительно на 8-13%, так как уменьшается время получения оценок значений признаков.

Дальнейшим направлением исследования применения алгоритмов кластеризации (класс алгоритмов классификации без учителя) могут быть исследования, ориентированные на автоматическую адаптацию параметров данных алгоритмов в зависимости от характеристик совокупности анализируемых признаков, а также разработка процедур автоматического извлечения знаний для настройки параметров этих алгоритмов, корректировки их баз знаний, исследование влияния различных метрик сопоставления признаков на качество их работы. Кроме этого, дальнейшие исследования связаны с совершенствованием методов принятия решений по обеспечению безопасности ЗМС СН на основе рассмотренных методов нечеткой оценки рисков информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. – 2011 – №1. – С. 50–57.

2. Платонов В.В. Программно-аппаратные средства защиты информации. – М. : Издательский центр «Академия», 2013. – 336 с. : ил.

3. Автоматизация управления и связь в ВМФ. // под общей редакцией Ю.М. Кононова. – 2-е изд. – СПб. : «Элмор», 2001. – 512 с.

4. Азаров Г.И. Теоретические основы анализа оперативности передачи информации в системах управления и связи. – М. : Академия ГПС МЧС России, 2012. – 62 с.

5. ITU-T Recommendation M.3400. TMN management functions. – 2000.

6. Саенко И.Б., Агеев С.А., Шерстюк Ю.М., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. – 2011. – № 3. – С. 30–39.

7. Агеев С.А., Саенко И.Б., Егоров Ю.П., Гладких А.А., Богданов А. В. Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения. // Автоматизация процессов управления. – 2014. – № 3 (37). – С. 78–88.

8. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью // Труды ИСА РАН 2009. – Т. 41. – С. 74–103.

9. Белов В.В., Смирнов А.Е., Чистякова В.И. Распознавание нечетко определяемых состояний технических систем. – М. : Горячая линия – Телеком, 2012. – 138 с.

10. Штовба С. Д. Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия – Телеком, 2007. – 288 с. : ил.

REFERENCES

1. Ageev S.A., Bushuev A.S., Egorov Yu.P., Saenko I.B. Kontseptsiia avtomatizatsii upravleniia informatsionnoi bezopasnostiu v zashchishchennykh multiservisnykh setiakh spetcialnogo naznacheniia [Concept of Automation of Information-Security Control in Protected Special-Purpose Multi-Service Networks]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2011, no. 1 (23), pp.50–57.

2. Platonov V.V. *Programmno-apparatnye sredstva zashchity informatsii* [Information Security Software and Hardware]. Moscow, Izdatelskii tsentr 'Akademiia', 2013. 336 p.

3. *Avtomatizatsiia upravleniia i sviaz v VMF*. Pod obsh. red. Yu.M. Kononova. Izd. 2-e [Automating the Navy's Management and Communications. 2nd Edition, edited by Yu.M. Kononov]. Elmor Publ., 2001. 512 p.

4. Azarov G.I. *Teoreticheskie osnovy analiza operativnosti peredachi informatsii v sistemakh upravleniia i sviazi* [Analysis Fundamentals for the Latency of Data Transmission in Control and Communications Systems]. Moscow, Akademiia GPS MChS Rossii Publ., 2012. 62 p.

5. *ITU-T Recommendation M.3400*. TMN management functions. 2000.

6. Saenko I.B., Ageev S.A., Sherstyuk Yu.M., Polubelova O.V. Kontceptualnye osnovy avtomatizatsii upravleniia zashchishchennymi multiservisnymi setiami [Conceptual Basis of Automation Control of Protected Multiservice Networks]. *Problemy informatsionnoi bezopasnosti. Kompiuternye sistemy* [Information Security Problems. Computer Systems], 2011, no. 3, pp. 30–39.

7. Ageev S.A., Saenko I.B., Egorov Yu.P., Gladkikh A.A., Bogdanov A. V. Intellektualnoe ierarkhicheskoe upravlenie riskami informatsionnoi bezopasnosti v zashchishchennykh multiservisnykh setiakh spetsialnogo naznacheniia [Intelligent Hierarchical Information Security Risk Management in Protected Special-Purpose Multiservice Networks]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2014, no. 3 (37), pp. 78–88.

8. Kotenko I.V. Intellektualnye mekhanizmy upravleniia kiberbezopasnostiu [Intelligent Mechanisms for Cyber Security Management]. *Trudy ISA RAN* [Proc. of Institute for Systems Analysis of RAS], 2009, vol. 41, pp. 74–103.

9. Belov V.V., Smirnov A.E., Chistyakova V.I. *Raspoznavanie nechetko opredeliaemykh sostoianii tekhnicheskikh system* [Detecting Engineering Systems Fuzzy States]. Moscow, Goriachaia liniia – Telekom Publ., 2012. 138 p.

10. Shtovba S. D. *Proektirovanie nechetkikh sistem sredstvami MATLAB* [Fuzzy Systems Design with MATLAB-Tools]. Moscow, Goriachaia liniia–Telekom Publ., 2007. 288 p.