ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-2-15 -24 Оригинальная статья/Original Paper

Оценка рисков информационной безопасности автоматизированной системы с помощью нейро-нечеткой логики

А.Р. Айдинян, О.Л. Цветкова
Донской государственный технический университет,
344000, г. Ростов-на-Дону, площадь Гагарина,1, Россия

Резюме. Цель. Автоматизированные системы широко применяются на производстве и, важным критерием их надежности является информационная безопасность. Целью исследования является обеспечение баланса между возможными потерями в результате реализации угроз и стоимостью средств защиты, обеспечивающих снижение рисков с помощью нейро-нечеткой логики. **Метод.** Разработка модели основана на использовании методов нечеткой логики. **Результат.** Получена модель интегрированной оценки рисков информационной безопасности, которая может быть практически применена для комплексного анализа эффективности организации системы защиты автоматизированных систем, функционирующих в различных областях деятельности. Выявлены показатели риска информационной безопасности автоматизированной системы, описанные с помощью лингвистических переменных. На основе этих показателей получены оценки рисков информационной безопасности от состояния: программного обеспечения; технического обеспечения; информационного обеспечения; организационно-методического обеспечения; уровня подготовки и мотивации работников. Сформулированы нечеткие продукционные правила модели для определения интегрированной оценки информационной безопасности автоматизированной системы, обеспечивая полный учет всех факторов, оказывающих существенное влияние на уровень защищенности автоматизированной системы. **Вывод.** Особенностью предложенного подхода является формализация процесса оценки, уменьшение уровня субъективизма при формировании оценок риска.

Ключевые слова: автоматизированная система, информационная безопасность, оценка уровня информационной безопасности, защита информации

Для цитирования: А.Р. Айдинян, О.Л. Цветкова. Оценка рисков информационной безопасности автоматизированной системы с помощью нейро-нечеткой логики. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):15-24. DOI:10.21822/2073-6185-2023-50-2-15-24

Assessment of information security risks of automated system using neuro-fuzzy logic

A.R. Aydinyan, O.L. Tsvetkova
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344000, Russia

Abstract. Objective. Automated systems are widely used in production, and an important criterion for their reliability is information security. The aim of the study is to provide a balance between possible losses as a result of the implementation of threats and the cost of protection tools that reduce risks using neuro-fuzzy logic. **Method.** The developed model is based on the use of fuzzy logic. **Result.** A model of integrated information security risk assessment has been obtained, which can be practically applied for a comprehensive analysis of the effectiveness of organizing a protection system for automated systems operating in various fields of activity. The risk indicators of information security of an automated system, described with the help of linguistic variables, are revealed. Based on these indicators, information security risk assessments were obtained from the state of: software; technical support; information support; organizational and methodological support; the level of training and motivation of employees. The

fuzzy production rules of the model are formulated to determine the integrated assessment of the information security of an automated system, providing a full account of all factors that have a significant impact on the level of security of an automated system. **Conclusions.** A feature of the proposed approach is the formalization of the assessment process, reducing the level of subjectivity in the formation of risk assessments.

Keywords: automated system, information security, assessment of the level of information security, information protection

For citation: A.R. Aydinyan, O.L. Tsvetkova. Assessment of information security risks of automated system using neuro-fuzzy logic. Herald of Daghestan State Technical University. Technical Science. 2023; 50 (2): 15-24. DOI: 10.21822 /2073-6185-2023-50-2-15-24

Введение. Под риском информационной безопасности понимается возможность злоумышленника использовать уязвимость инфраструктуры предприятия для совершения атаки и реализации угроз информационной безопасности. Результатом будет снижение уровня защищенности информации и причинение ущерба предприятию. В процессе проведения анализа (оценки) рисков специалисты решают следующие задачи: проводят идентификацию и оценку ценности активов предприятия, идентификацию угроз информационной безопасности и уязвимостей системы защиты, расчет вероятности успешной реализации угроз и их влияние на бизнес.

Постановка задачи. Целью процесса анализа рисков является обеспечение баланса между возможными потерями в результате реализации угроз и стоимостью средств защиты, обеспечивающих снижение рисков.

Методы исследования. Особенность процесса анализа защищенности автоматизированных систем заключается в том, что при оценке информационных рисков в качестве исходных данных часто используются нечеткие значения в виде экспертных оценок. Одним из перспективных направлений исследований в этой области является использование нейро-нечеткой логики.

Автоматизированная система обеспечивает формирование решений в различных областях деятельности на основе автоматизации определенных информационных процессов, и, по сути, является организационно-технической системой, состоящей из средств автоматизации и видов деятельности персонала [1].

Автоматизированные системы делятся на системы управления процессами, системы поддержки проектирования, системы управления производством и т.д. [2].

На рис. 1 приведена классификация автоматизированных систем.

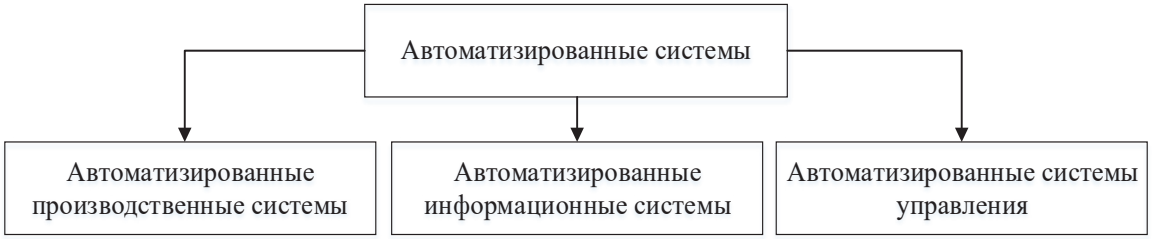

Рис. 1. Классификация автоматизированных систем
Fig. 1. Classification of automated systems

Автоматизированная система производственного назначения выполняет сбор и обработку информации от объекта управления, формирование на основе этой информации и передачу управляющих воздействий на объект.

Таким образом, автоматизированная производственная система реализует функции, поддающиеся автоматизации. Функции человека заключатся в определении и корректировке цели, критериев управления, программы управления. Автоматизированная информационная система предназначена для выполнения информационной технологии реализации определенных функций [3]. В целом автоматизированная система - это система, состоящая из персонала и комплекса

средств автоматизации его деятельности, и реализует информационную технологию выполнения установленных функций [4].

Автоматизированная система управления - комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия.

На рис. 2 приведена обобщенная структура автоматизированной системы.

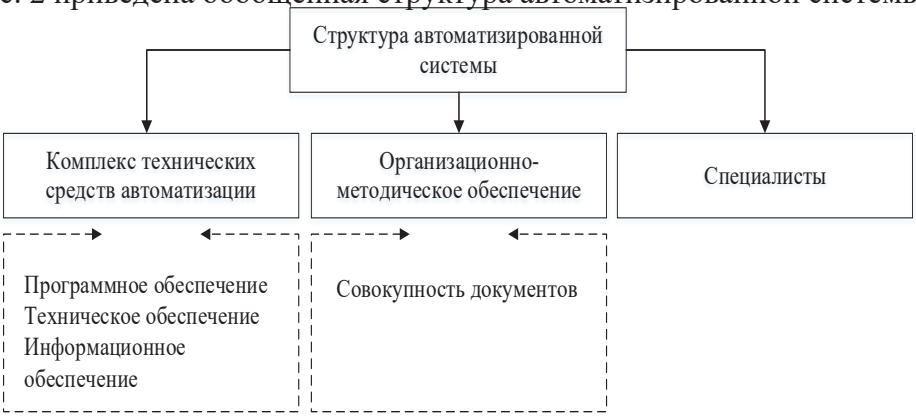

Рис. 2. Обобщенная структура автоматизированной системы
Fig. 2. Generalized structure of the automated system

Автоматизированная система представляет собой совокупность компонент:
−технические средства автоматизации — программное обеспечение автоматизированной системы, техническое обеспечение, информационное обеспечение;
−организационно-методическое обеспечение — совокупность документов, определяющих организационную структуру объекта и системы автоматизации, описание процессов деятельности, формы представления результатов деятельности;
−персонал, который применяет автоматизированную систему в процессе своей профессиональной деятельности.

Для анализа рисков информационной безопасности автоматизированной системы предлагается использовать нейро-нечеткий подход, основанный на искусственных нейронных сетях и моделях нечеткой логики [5-7].

Обсуждение результатов. Анализ показателей риска информационной безопасности автоматизированной системы. Эффективность функционирования системы защиты при возникновении угрозы несанкционированного доступа зависит от многих факторов, которые измеряются с помощью экспертных оценок и посредством математического моделирования [8]. Существуют подходы к количественной оценке рисков реализации угрозы несанкционированного доступа к информации, позволяющие оценивать уровень защищенности информации [9].

В табл. 1 представлены показатели риска информационной безопасности автоматизированной системы, описанные с помощью лингвистических переменных с указанием их возможных значений.

Оценка риска информационной безопасности автоматизированной системы от состояния программного обеспечения. Для оценки влияния на риск информационной безопасности программного обеспечения, которым оснащена автоматизированная система, необходимо учитывать ее составляющие: системное и прикладное программное обеспечение. Системное программное обеспечение предназначено для обеспечения функционирования компьютера, сетей и прикладных программ.

В качестве системного программного обеспечения используются операционная система, сервисные пакеты, программные средства для сетевой коммуникации. Операционная система компьютера является основной системной программой, и обеспечивает синхронизацию работы всех частей и устройств, управляет запуском программ, создает папки, организует файловую систему и сервисные функции.

Таблица 1. Показатели риска информационной безопасности автоматизированной системы
Table 1. Information security risk indicators of an automated system

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X1	Риск информационной безопасности от состояния программного обеспечения/Information security risk from software state	X1.Н – низкий/ low level X1.С – средний/ average X1.В –высокий/ high level
X2	Риск информационной безопасности от состояния технического обеспечения/ Information security risk from the state of technical support	X2.Н – низкий/ low level X2.С – средний / average X2.В – высокий/ high level
X3	Риск информационной безопасности от состояния информационного обеспечения/ Information security risk from the state of information support	X3.Н – низкий/ low level X3.В – высокий/ high level
X4	Риск информационной безопасности от состояния организационно-методического обеспечения/Information security risk from the state of organizational and methodological support	X4.Н – низкий/ low level X4.В – высокий/ high level
X5	Риск информационной безопасности от уровня подготовки и мотиваций работников/Information security risk from the level of training and motivation of employees	X5.Н – низкий/ low level X5.С – средний/ average X5.В – высокий/ high level

Сервисные пакеты обеспечивают поддержку пользователя при работе с системой:

- программы обслуживания дисков (форматирования, дефрагментации, проверки, очистки), драйверы, расширяющие возможности операционной системы;
- антивирусные программы, выполняющие проверку дисков на наличие вирусов и их уничтожение;
- программы защиты от несанкционированного доступа.

Антивирусные программы и программы защиты от несанкционированного доступа необходимо оценивать отдельно, поскольку они уменьшают риск при их использовании, и предлагается ввести отрицательный риск от их использования.

Поскольку они хорошо изучены и могут оцениваться достаточно точно предлагаются следующие возможные значения лингвистической переменной: очень низкая защита ОНЗ, низкая защита НЗ, средняя защита СЗ, высокая ВЗ, очень высокая защита ОВЗ.

Системы поддержки сетевых коммуникаций предназначены для создания и функционирования компьютерных сетей. К системам поддержки сетевых коммуникаций относятся сетевые операционные системы и другие программы.

Определяющую роль для обеспечения информационной безопасности автоматизированной системы играет операционная система.

Оценку безопасности использования драйверов можно отнести к информационной безопасности операционной системы, поскольку операционная система может содержать средства сертификации драйверов и т.д. К тому же оценить безопасность драйверов эксперту невозможно в связи с отсутствием подробной информации.

Вследствие этого предлагается оценку информационной безопасности автоматизированной системы от состояния программного обеспечения проводить исходя из факторов, представленных в табл. 2.

В случае использования нескольких сервисных пакетов в одной автоматизированной системе риск возрастает. Так при использовании двух пакетов с рисками, соответственно, p_1 и p_2 интегрированный риск может быть вычислен по формуле сложения двух вероятностей $p=p_1+p_2-p_1*p_2$.

Оценка риска информационной безопасности автоматизированной системы от используемого прикладного программного обеспечения может быть оценена экспертами на основе имеющихся данных о программном обеспечении, как разработанном сторонними организациями, так и собственными разработчиками.

Таблица 2. Факторы, влияющие на информационную безопасность автоматизированной системы от состояния программного обеспечения
Table 2. Factors affecting the information security of an automated system from the state of the software

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X1.1	Риск информационной безопасности от используемой операционной системы и драйверов/ Information security risk from the operating system and drivers used	X1.1.H – низкий/ low level X1.1.C – средний/ average X1.1.B – высокий/ high level
X1.2	Риск информационной безопасности от используемых сервисных пакетов/ Information security risk from the used service packages	X1.2.H – низкий/ low level X1.2.C – средний/ average X1.2.B – высокий/ high level
X1.3	Риск информационной безопасности от использования антивирусных пакетов/Information security risk from the use of anti-virus packages	X1.3.H – низкий/ low level X1.3.C – средний/ average X1.3.B – высокий/ high level
X1.4	Риск информационной безопасности от использования защиты от несанкционированного доступа/Information security risk from the use of protection against unauthorized access	X1.4.H – низкий/ low level X1.4.C–средний/average X1.4.B – высокий/ high level
X1.5	Риск информационной безопасности от используемого прикладного программного обеспечения/ Information security risk from the application software used	X1.5.H – низкий/ low level X1.5.C – средний/ average X1.5.B – высокий/ high level

В случае использования различного программного обеспечения необходимо также вычислять интегрированную оценку риска.

Риски информационной безопасности программного обеспечения делятся на две группы:

- риск постоянен во времени, например, риск информационной безопасности базы данных;
- риск возникает только в интервалы времени, когда программное обеспечение запущено, например, только в этот момент возникает канал взлома или утечки.

  Однако при этом необходимо учитывать долю времени, т.е. риск необходимо умножить на долю времени, когда программа запущена.

Для системного программного обеспечения, поскольку оно всегда запущено, доля времени не актуальна.

В табл. 3 представлены нечеткие продукционные модели для определения лингвистической переменной X_1.

Таблица 3. Нечеткие продукционные правила модели для определения лингвистической переменной X_1
Table 3. Fuzzy production rules of the model for determining the linguistic variable X_1

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П1.1	X1.1=X.1.1.H И X1.2= X.1.2.H И X1.3= X.1.3.H И X1.4= X.1.4.H И X1.5= X.1.5.H	Y1=H
П1.2	(X1.1= X.1.1.C ИЛИ X1.2= X.1.2.C ИЛИ X1.3= X.1.3.C ИЛИ X1.4= X.1.4.C ИЛИ X1.5= X.1.5.C) И (X1.1<> X.1.1.B И X1.2<> X.1.1.B И X1.3<> X.1.3.B И X1.4<> X.1.4.B И X1.5<> X.1.5.B)	Y1=C
П1.3	X1.1=B ИЛИ X1.2=B ИЛИ X1.3=B ИЛИ X1.4=B ИЛИ X1.5=B	Y1=B

Оценка риска информационной безопасности автоматизированной системы от состояния технического обеспечения. Техническое обеспечение автоматизированной системы состоит из следующих элементов:

- комплекс средств передачи информации — это GPS связь; компьютерные сети (локальные, региональные, глобальные);
- средства телеграфной связи; радиосвязь; спутниковая связь и др;
- средства хранения данных — это оптические диски (CD, DVD);
- USB-накопители (flash, HDD); жесткие диски (2,5»,3,5»).

В табл. 4 представлены факторы, оказывающие влияние на информационную безопасность автоматизированной системы от состояния технического обеспечения.

Таблица 4. Факторы, влияющие на информационную безопасность автоматизированной системы от состояния технического обеспечения

Table 4. Factors affecting the information security of an automated system from the state of technical support

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X2.1	Риск информационной безопасности от используемых хранилищ данных/Information security risk from used data stores	X2.1.H – низкий риск/low level X2.1.C – средний/ average X2.1.B – высокий/ high level
X2.2	Риск информационной безопасности от используемых системных модулей/ Information security risk from used system modules	X2.2.H – низкий риск/low level X2.2.B – высокий/ high level
X2.3	Риск информационной безопасности от используемых средств передачи информации/ Information security risk from the means of information transmission used	X2.3.H – низкий риск/low level X2.3.B – высокий/ high level
X2.4	Риск информационной безопасности от используемых аппаратных средств защиты/ Information security risk from the hardware protections used	X2.4.H – низкий риск/low level X2.4.C – средний/ average X2.4.B – высокий/ high level

В табл. 5 представлены нечеткие продукционные модели для определения лингвистической переменной X2.

Таблица 5. Нечеткие продукционные правила модели для определения лингвистической переменной X_2

Table 5. Fuzzy production rules of the model for determining the linguistic variable X_2

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П2.1	X2.1=H И X2.2=H И X2.3=H И X2.4=H	Y2=H
П2.2	(X2.1=C ИЛИ X2.4=C) И (X2.1<>B И X2.2<>B И X2.3<>B И X2.4<>B)	Y2=C
П2.3	X2.1=B ИЛИ X2.2=B ИЛИ X2.3=B ИЛИ X2.4=B	Y2=B

Оценка риска информационной безопасности автоматизированной системы от состояния информационного обеспечения автоматизированной системы.

В качестве факторов, возникающих в зависимости от состояния информационного обеспечения автоматизированной системы, которые могут оказывать влияние на информационную безопасность, необходимо рассмотреть (табл. 6):

- форматы информационного обеспечения;
- методы шифрования баз данных;
- процедуры резервного копирования информационного обеспечения;
- средства обмена информацией и электронного документооборота.

Таблица 6. Факторы, влияющие на информационную безопасность автоматизированной системы от состояния информационного обеспечения автоматизированной системы
Table 6. Factors affecting the information security of an automated system from the state of information support of an automated system

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X3.1	Риск информационной безопасности от используемых форматов информационного обеспечения/Information security risk from the used information support formats	X3.1.Н – низкий риск/low level X3.1.В – высокий/ high level
X3.2	Риск информационной безопасности от используемого метода шифрования баз данных/ Information security risk from the database encryption method used	X3.2.Н – низкий риск/low level X3.2.В – высокий/ high level
X3.3	Риск информационной безопасности от процедуры резервного копирования информационного обеспечения/ Information security risk from information security backup procedure	X3.3.Н – низкий риск/low level X3.3.В – высокий/ high level
X3.4	Риск информационной безопасности от используемых средств обмена информацией и реализованной процедуры электронного документооборота/ Information security risk from the means of information exchange used and the implemented electronic document management procedure	X3.4.Н – низкий риск/low level X3.4.В – высокий/ high level

В табл. 7 представлены нечеткие продукционные модели для определения лингвистической переменной X3.

Таблица 7. Нечеткие продукционные правила модели для определения лингвистической переменной X_3
Table 7. Fuzzy production rules of the model for determining the linguistic variable X_3

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П3.1	X3.1=Н И X3.2=Н И X3.3=Н И X3.4=Н	Y3=Н
П3.2	X3.1=В ИЛИ X3.2=В ИЛИ X3.3=В ИЛИ X3.4=В	Y3=В

Оценка риска информационной безопасности автоматизированной системы от состояния организационно-методического обеспечения автоматизированной системы.

В качестве факторов, возникающих в зависимости от состояния организационно-методического обеспечения автоматизированной системы, необходимо рассмотреть (табл. 8): наличие инструкций по эксплуатации автоматизированной системы; соблюдение правил обеспечения информационной безопасности автоматизированной системы.

Таблица 8. Факторы, влияющие на информационную безопасность автоматизированной системы от состояния организационно-методического обеспечения автоматизированной системы
Table 8. Factors affecting the information security of an automated system from the state of organizational and methodological support of an automated system

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X4.1	Наличие инструкций по эксплуатации АС/Availability of operating instructions	X4.1.Н – низкий риск/low level X4.1.В – высокий/ high level
X4.2	Соблюдение правил обеспечения ИБ АС/ Compliance with the rules for ensuring IS IS	X4.2.Н – низкий риск/low level X4.2.В – высокий/ high level

В табл. 9 представлены нечеткие продукционные модели для определения лингвистической переменной X_4.

Таблица 9. Нечеткие продукционные правила модели для определения лингвистической переменной X_4

Table 9. Fuzzy production rules of the model for determining the linguistic variable X_4

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П4.1	X4.1=Н И X4.2=Н	Y1=Н
П4.2	X4.1=В ИЛИ X4.2=В	Y1=В

Оценка риска информационной безопасности автоматизированной системы от уровня подготовки и мотиваций работников. В качестве факторов, возникающих в зависимости от уровня подготовки и мотиваций работников, необходимо рассмотреть (табл. 10): уровень образования сотрудников; степень заинтересованности сотрудников в сохранении должности; степень лояльности сотрудников к руководству; уровень ответственности сотрудников.

Таблица 10. Факторы, влияющие на информационную безопасность автоматизированной системы от уровня подготовки и мотиваций работников

Table 10. Factors affecting the information security of an automated system depending on the level of training and motivation of employees

Обозначение Notation	Наименование лингвистической переменной Name of the linguistic variable	Возможные значения лингвистической переменной Possible values of a linguistic variable
X5.1	Уровень образования сотрудников/ The level of education of employees	X5.1.Н – низкое образование/ low education X5.1.С – средний уровень образования/ average level of education X5.1.В – высокий уровень образования/ high level of education
X5.2	Степень заинтересованности сотрудников в сохранении должности/ The degree of interest of employees in maintaining the position	X5.2.Н – низкая заинтересованность/ low interest X5.2.С – средняя заинтересованность/ average interest X5.2.В – высокая заинтересованность/ high interest
X5.3	Степень лояльности сотрудников к руководству/ The degree of employee loyalty to management	X5.3.Н – низкая степень/ low degree X5.3.В – высокая степень/ high degree
X5.4	Уровень ответственности сотрудников/ The level of responsibility of employees	X5.4.Н – низкая ответственность/ low liability X5.4.В – высокая ответственность/ high responsibility

В табл. 11 представлены нечеткие продукционные модели для определения лингвистической переменной X_5.

Таблица 11. Нечеткие продукционные правила модели для определения лингвистической переменной X_5

Таблица 11. Нечеткие продукционные правила модели для определения лингвистической переменной X_5

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П5.1	X5.1=Н И X5.2=Н И X5.3=Н И X5.4=Н	Y5=Н
П5.2	(X5.1=С ИЛИ X5.2=С) И (X5.1<>В И X5.2<>В И X5.3<>В И X5.4<>В)	Y5=С
П5.3	X5.1=В ИЛИ X5.2=В ИЛИ X5.3=В ИЛИ X5.4=В	Y5=В

Интегрированная оценка риска информационной безопасности автоматизированной системы. Для получения интегрированной оценки риска используется также нейро-нечеткая логика. Здесь необходимо объединить риски от других модулей и вычислить

итоговую оценку. Нечеткие продукционные правила модели для определения комплексной оценки приведены в табл. 12.

Таблица 12. Нечеткие продукционные правила модели для определения комплексной оценки безопасности

Table 12. Fuzzy production rules of the model for determining the integrated safety assessment

Обозначение правила Rule notation	Антецент Antecedent	Консеквент Consequent
П1	Y1=Н И Y2=Н И Y3=Н И Y4=Н И Y5=Н	Z1=Н
П2	(Y1=С ИЛИ Y2=С ИЛИ Y5=С) И (Y1<>В И Y2<>В И Y3<>В И Y4<>В И Y5<>В)	Z1=С
П3	Y1=В ИЛИ Y2=В ИЛИ Y3=В ИЛИ Y4=В ИЛИ Y5=В	Z1=В

Таким образом, были сформулированы нечеткие продукционные правила модели для определения интегрированной оценки информационной безопасности автоматизированной системы, которая складывается из оценок рисков по нескольким направлениями (состояния программного, технического, информационного и организационно-методического обеспечения, а также уровень подготовки и мотиваций работников), обеспечивая полный учет всех факторов, оказывающих существенное влияние на уровень защищенности автоматизированной системы.

Вывод. Полученная модель интегрированной оценки рисков информационной безопасности может быть практически применена для комплексного анализа эффективности организации системы защиты автоматизированных систем, функционирующих в различных областях деятельности. Особенностью предложенного подхода является формализм процесса оценки, уменьшение уровня субъективизма при формировании оценок риска.

Библиографический список:

1. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилинский, Л. Рутковский. – М.: Горячая линия – Телеком, 2007. – 452 с.
2. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия Телеком, 2007. – 284 с.
3. Abe, S. Fuzzy rule extraction directly from numerical data for function approximation / S. Abe, M.-S. Lan // IEEE Transaction Systems, Man, and Cybernetics. – 1995. – Vol. 25. – P. 119–129.
4. Abe S.A method for fuzzy rule extraction directly from numerical data and its application to pattern classification / S. Abe, M.-S. Lan // IEEE Transaction on Fuzzy Systems. – 1995. – Vol. 3, № 1. – P. 18–28.
5. Круглов В.В. Искусственные нейронные сети. Теория и практика / В.В. Круглов, В.В. Борисов. – М.: Горячая линия – Телеком, 2002. – 382 с.
6. Nelles O. Comparison of two construction algorithms for Takagi-Sugeno fuzzy models / O.Nelles, A.Fink, R.Babuska, M.Setnes // International Journal of Applied Mathematics and Computer Science. – 2000. – Vol. 4, № 10. – P. 835–855.
7. Новак В. Математические принципы нечеткой логики / В.Новак, И.Перфильева, И.Мочкорж. – М.: Физматлит, 2006. – 352 с.
8. Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах // Вестник Дагестанского государственного технического университета. Технические науки. – 2018; 45 (1): С. 147-159. DOI:10.21822/2073-6185-2018-45-1-147-159. URL: https://vestnik.dgtu.ru/jour/article/view/500/421.
9. Мещерякова Т.В., Рогозин Е.А., Ефимов А.О., Романова В.Р., Коноваленко С.А. Методический подход к количественной оценке рисков реализации угроз несанкционированного доступа к информационному ресурсу автоматизированных систем органов внутренних дел. // Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3):91-103. DOI:10.21822/2073-6185-2022-49-3-91-103. URL: https://vestnik.dgtu.ru/jour/article/view/1126/728.

References:

1. Rutkovskaya D., M. Pilinsky, L. Rutkovsky. Neural networks, genetic algorithms and fuzzy systems Moscow: Hotline . Telecom, 2007; 452. (In Russ.)
2. Borisov V.V., Kruglov V.V., Fedulov A.S. Fuzzy models and networks. Moscow: Goryachaya liniya – Telekom, 2007; 284. (In Russ.)
3. Abe, S. Fuzzy rule extraction directly from numerical data for function approximation / S. Abe, M.-S. Lan. IEEE Transaction Systems, Man, and Cybernetics. 1995; 25:119–129.
4. Abe S.A method for fuzzy rule extraction directly from numerical data and its application to pattern classification / S. Abe, M.-S. Lan. *IEEE Transaction on Fuzzy Systems*. 1995; 3(1):18–28.

5. Kruglov V.V., Borisov V.V. Artificial neural networks. Theory and practice. Moscow: *Goryachaya liniya*. Telekom, 2002; 382. (In Russ.)
6. Nelles O. Comparison of two construction algorithms for Takagi-Sugeno fuzzy models. O.Nelles, A.Fink, R.Babuska, M.Setnes. *International Journal of Applied Mathematics and Computer Science.* 2000; 4(10): 835–855.
7. Novak V. Mathematical principles of fuzzy logic. V.Novak, I. Perfil'yeva, I. Mochkorzh. Moscow: Fizmatlit, 2006; 352. (In Russ.)
8. Kachaeva G.I., Popov A.D., Rogozin E.A. Functional performance indicators during systems development to protect information from unauthorised access. *Herald of Daghestan State Technical University. Technical Sciences.* 2018; 45 (1):147-159. (In Russ.) DOI:10.21822/2073-6185-2018-45-1-147-159. URL: https://vestnik.dgtu.ru/jour/article/view/500/421.
9. Meshcheryakova T.V., Rogozin E.A., Efimov A.O., Romanova V.R., Konovalenko S.A. Methodical approach to quantitative assessment of the risks of the implementation of threats unauthorized access to an information resource automated systems of internal affairs bodies. *Herald of the Daghestan State Technical University. Technical Science.* 2022; 49(3):91-103. DOI:10.21822/2073-6185-2022-49-3-91-103. URL: https://vestnik.dgtu.ru/jour/article/view/500/421. (In Russ.)

Сведения об авторах:

Айдинян Андрей Размикович, кандидат технических наук, доцент, кафедра «Вычислительные системы и информационная безопасность», aaydinyan@donstu.ru; ORCID 0000-0001-9455-4079.

Цветкова Ольга Леонидовна, кандидат технических наук, доцент, кафедра «Вычислительные системы и информационная безопасность», olga_cvetkova@mail.ru; ORCID 0000-0003-4071-6313

Information about authors:

Andrey R. Aydinyan, Cand. Sci. (Eng.), Assoc. Prof., Department of Computing Systems and Information Security, aaydinyan@donstu.ru; ORCID 0000-0001-9455-4079.

Olga L. Tsvetkova, Cand. Sci. (Eng.), Assoc. Prof., Department of Computing Systems and Information Security, olga_cvetkova@mail.ru; ORCID 0000-0003-4071-6313

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 15.02.2023.

Одобрена после рецензирования/ Reviced 12.03.2023.

Принята в печать/Accepted for publication 12.03.2023.