УДК 004.056.5
https://doi.org/10.47533/2020.1606-146X.135

А. С. АМИРОВА*, А. Т. ТОХМЕТОВ

Евразийский национальный университет, Нур-Султан, Казахстан
whitesilk@mail.ru, attohmetov@mail.ru

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С быстрым развитием промышленного Интернета вещей (IIoT) возникла необходимость быстро реагировать, обнаруживать и предотвращать вторжения. Эти проблемы особенно актуальны в связи с прогнозируемым ростом пользователей IIoT. Оценка рисков - важная часть процесса создания систем защиты информации, в том числе промышленных комплексов. Целью данной работы является разработка практической модели оценки рисков информационной безопасности в сетях промышленного интернета вещей. Предлагаемая модель основана на простом методе аддитивного взвешивания и нечеткой логике. Нечеткая логика является подходящей для оценки рисков и представляет практические результаты. Произведена реализация процесса нечеткого моделирования базы правил посредством применения специализированного пакета Fuzzy Logic Toolbox программного средства MATLAB.

***Ключевые слова**: промышленный Интернет вещей (IIoT), простой метод аддитивного взвешивания (SAW), безопасность, угрозы.*

Введение. Термин «Интернет вещей» впервые был использован Массачусетским технологическим институтом Массачусетского технологического института в 1999 году. Тогда он означал сетевую систему самоорганизующихся процессов и объектов, которые взаимодействуют автономно, спроектированные таким образом, чтобы вызвать сближение цифровой интернет-мир с физическими вещами. Термин «промышленный Интернет вещей» относится к применению технологий IIoT в промышленных условиях. Его также называют «Индустрия 4.0» – термин, появившийся на немецком языке из-за возможности интеграции цифровой и физической индустрии. Промышленность IIoT или 4.0 включает в себя облако, большие данные, киберфизические межсоединения [1].

Существует несколько стандартов и методологий оценки рисков, таких как NIST и ISO27001, но, хотя они и объясняют общие принципы и рекомендации, они не содержат каких-либо деталей реализации [2]. Агентство Европейского Союза по сетевой

* E-mail корреспондирующего автора: whitesilk@mail.ru

и информационной безопасности (ENISA) – это экспертный центр, который разрабатывает советы и рекомендации по передовой практике в области информационной безопасности. С 2015 года ENISA предоставляет заинтересованным сторонам новейшие документы, охватывающие вопросы безопасности в области Интернета вещей и промышленного Интернета вещей (IIoT), связанные с проблемами интеллектуального производства и Индустрии 4.0. Стандартов оценки рисков, разработанных специально для промышленных систем, практически нет [3].

Системы IIoT обладают собственной динамикой и уникальностью, что требует новых подходов к оценке рисков. Оценка рисков предоставляет промышленным системам точную оценку рисков для их активов. Это может помочь им расставить приоритеты и разработать комплексную стратегию снижения рисков.

Учитывая ограниченность количественных подходов, разработанная модель рекомендует качественный метод, основанный на экспертных заключениях, и нечеткие методы оценки рисков информационной безопасности.

Предлагаемая модель. Принятие решений по нескольким критериям – это метод, основанный на таблицах принятия решений, где ценность каждой альтернативы в принятии решений определяется экспертами. Целью многокритериальных методов принятия решений является оценка и определение приоритета среди различных альтернатив. MCDM использует различные методы, самые известные и широко используемые: AHP, TOPSIS и SAW.

Как уже упоминалось, метод AHP [4] основан на парных сравнениях и очень точен, но не может быть легко принят экспертами. Кроме того, в энтропийном методе, если все альтернативы в критерии имеют «очень высокое» значение, это приводит к значительному снижению веса этого критерия. В этой работе мы ищем реальную ценность альтернатив, и относительную ценность для случая «очень высокой» следует использовать для определения ценности этой альтернативы.

В TOPSIS [5] выбранная альтернатива должна быть как можно ближе к положительному идеалу и как можно дальше от отрицательного идеального решения. Поэтому, если мы применяем метод TOPSIS для оценки риска, он расставляет приоритеты и ранжирует риски, но это не наша цель. Таким образом, метод TOPSIS не может быть использован непосредственно в нашей модели.

Метод простого аддитивного взвешивания (SAW) [6] является наиболее популярным подходом для принятия решений по нескольким критериям. В методике SAW определение веса критериев в таблицах принятия решений производится по мнению респондентов. Как правило, эта задача выполняется либо в соответствии со значениями таблиц принятия решений, как для методов энтропии Шенона и LINMAP, либо определяется непосредственно респондентами, например, попарными сравнениями или присвоением весов непосредственно экспертами.

Поскольку наша цель – практическая модель для любой организации, для реализации была выбрана методология SAW. Кроме того, поскольку оценка риска относится к неоднозначным темам, нечеткая логика подходит для оценки неопределенных

предметов, и с ее помощью эксперты могут выражать свое мнение в виде лингвистических переменных, таких как «очень высокий», «низкий» и т.д.

Алгоритм реализации данной модели состоит из 9 этапов (Рисунок 1) [7]:

1. Получение экспертных заключений в виде лингвистических переменных о важности каждой области. Это должно быть сделано на основе таблицы решений, в которой указывается вес каждого критерия.

2. Получение экспертных заключений каждой области о проявлении нанесенного ущерба и вероятности возникновения каждой угрозы, связанной с каждой областью, в виде лингвистических переменных.

3. Замена лингвистических переменных нечеткими переменными. Объединение всех мнений экспертов в каждой области и создание матрицы решений.

$$x_{ij} = (a_{ij}, b_{ij}, c_{ij},) \tag{1}$$

$$w_j = (w_{ij}, w_{ij}, w_{ij},) \tag{2}$$

$$x_{ij} = \frac{1}{n}\left[x_{ij}^1(+)x_{ij}^2(+) \ \ldots x_{ij}^n(+)\right] \tag{3}$$

$$w_{ij} = \frac{1}{n}\left[w_{ij}^1(+)w_{ij}^2(+) \ \ldots w_{ij}^n(+)\right] \tag{4}$$

где x_{ij} и w_j – треугольные нечеткие числа, n – количество человек, из которых состоит группа принятия решений.

4. Этап фаззификации заключается в применении решающих правил к входным данным (экспертные оценки вероятности и ущерба от угрозы) и служит для преобразования четких входных данных в нечеткий формат. Линейная нормализация консолидированной матрицы.

5. Деффазификация комбинированных весов с использованием метода расстояния со знаком и нормализации:

$$w_j = \frac{w_j}{\sum jwj} \tag{5}$$

6. Расчет матрицы весов.

7. Расчет вероятности возникновения угрозы в каждой области.

8. Деффазификация нечетких значений методом простого аддитивного взвешивания (SAW) для каждой угрозы и расчет уровня риска для каждого домена.

9. Рассчитайте общий уровень риска организации, умножив уровень риска угрозы на коэффициент важности каждой области.

Различные категории и типы активов информационных технологий (ИТ) определены на основе документа ENISA «Кибербезопасность Индустрии 4.0: проблемы и рекомендации (2019)» [12]. В таблице 1 определены категории и типы активов в системах IIoT с учетом необходимых цифровых и физических элементов.

Таблица 1 – Категории и типы активов в системах IIoT

Категория	Тип
Аппаратное обеспечение	Здание, местоположение, устройство, шлюз, оконечные устройства периферийного IIoT (датчики, исполнительные механизмы)
Программное обеспечение	Приложение, платформа, система, промежуточное ПО, операционная система, прошивка
Коммуникация	Облако, коммуникационные сети и компоненты АСУ ТП (коммутаторы, точки беспроводного доступа, источники питания)
Информация	Данные в состоянии покоя (DAR), используемые данные (DIU), данные в движении (DIM)
Серверы и системы	Серверы приложений, серверы баз данных, корпоративные операционные системы, производственные операционные системы
Безопасность	Антивирус, межсетевой экран, SIEM IDS / IPS
Человек	Человек, знания и навыки персонала

Результаты экспериментов. Алгоритм оценивания риска, основанный на положениях нечеткой логики и теории нечетких множеств, предлагается реализовать с помощью пакета Fuzzy Logic Toolbox системы MATLAB [8]. Учитывая четыре входных переменных (Таблица 2), воспроизводится механизм вывода при помощи продукционных правил нечеткой логики. Структура нечеткой модели представлена на рисунке 1.

Таблица 2 – Входные и выходная переменные

Входные характеристики	Терм-множества
1	2
Финансовые затраты (Financial cost)	Низкие
	Средние
	Высокие
Уязвимость (Vulnerability)	Низкие
	Средние
	Высокие
Ценность актива (Attraction of the asset)	Очень низкая
	Низкая
	Средняя
	Высокая
	Критически высокая
Существующий контроль (Existing control)	Удовлетворительный
	Достаточный
	Полностью удовлетворяющий
Выходная характеристика	

Окончание таблицы 2

1	2
Уровень риска	Очень низкий
	Низкий
	Средний
	Высокий
	Критически высокий

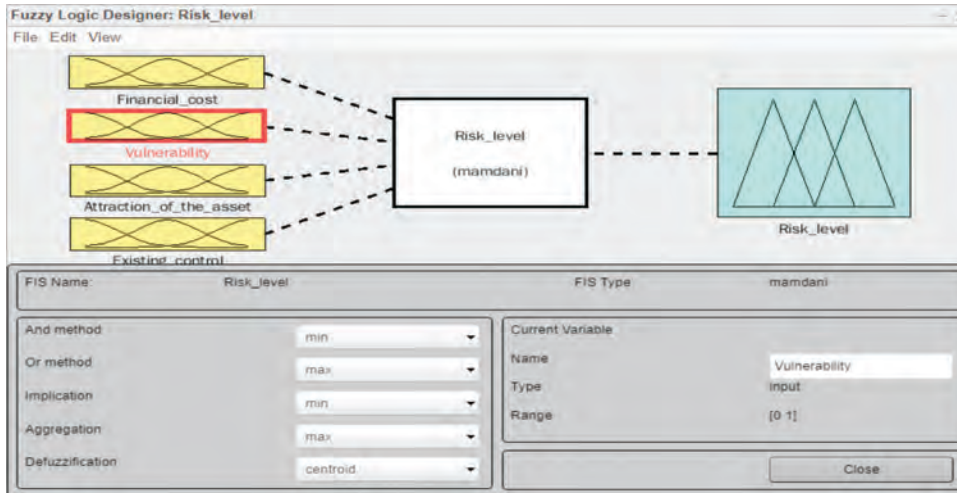

Рисунок 1 – Структура нечеткой модели

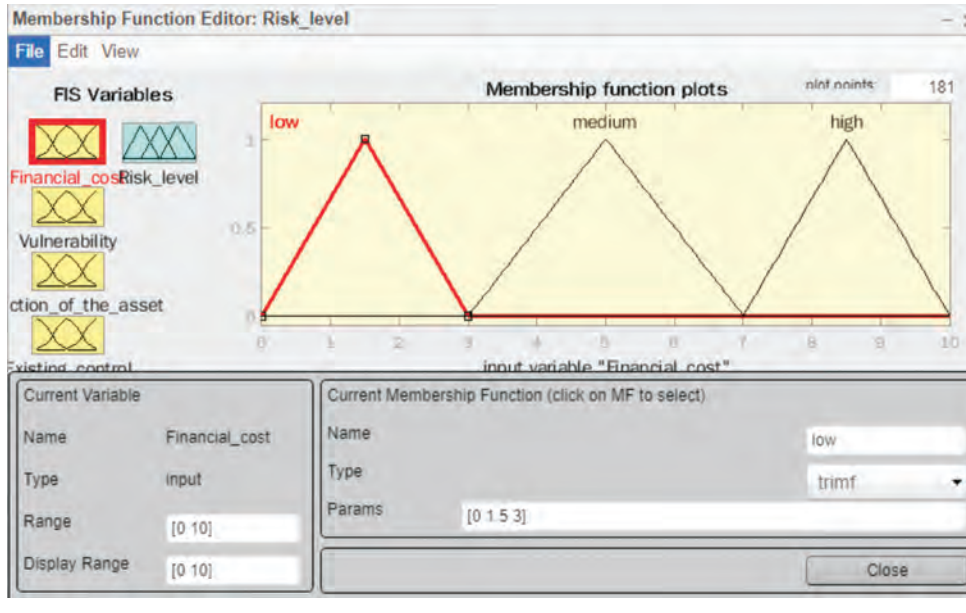

Рисунок 2 – Функции принадлежности для входной характеристики «Финансовые затраты»

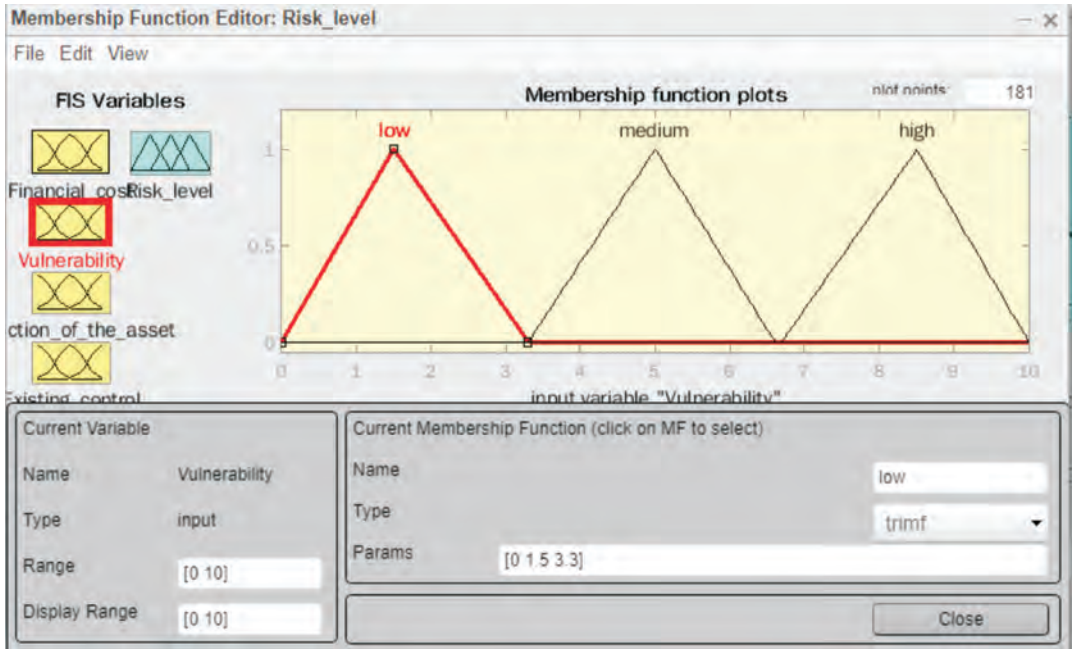

Рисунок 3 – Функции принадлежности для входной характеристики «Уязвимость»

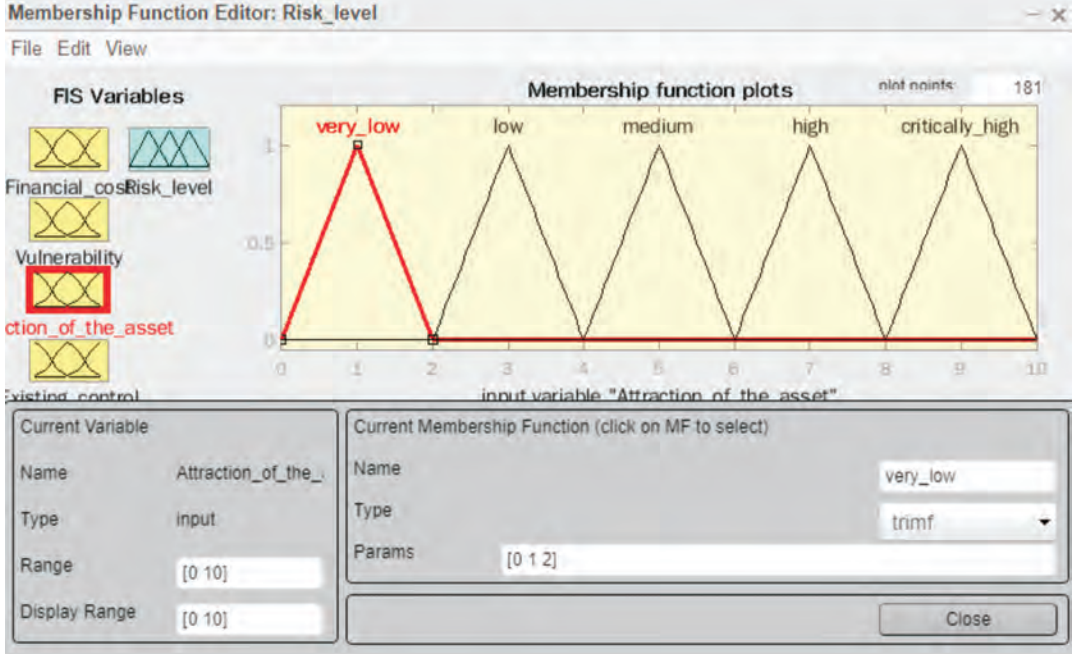

Рисунок 4 – Функции принадлежности для входной характеристики «Ценность актива»

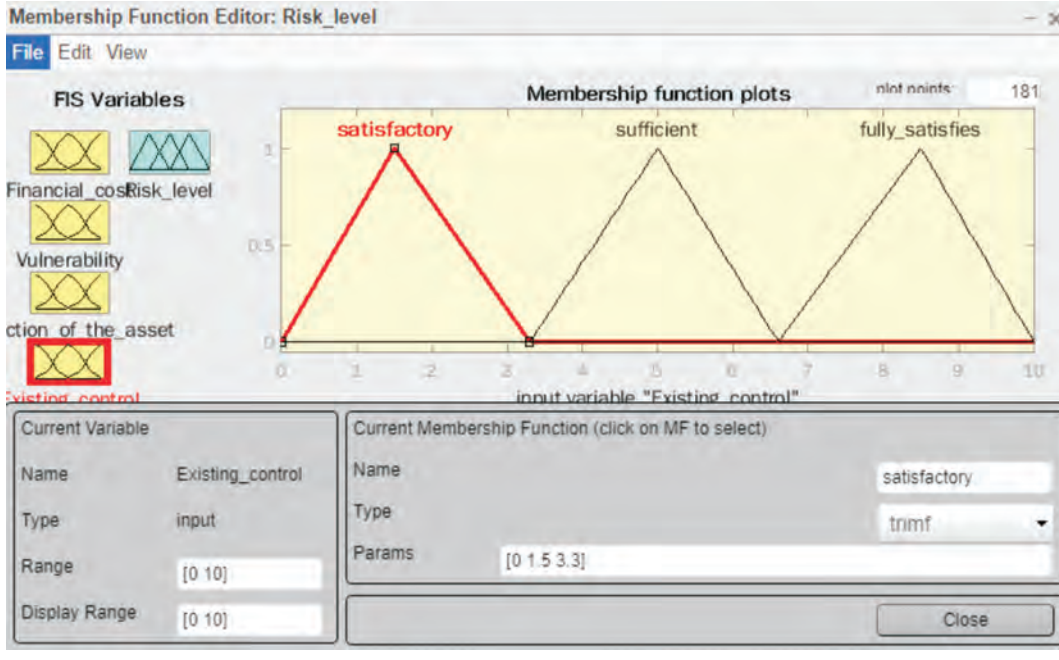

Рисунок 5 – Функции принадлежности для входной характеристики «Существующий контроль»

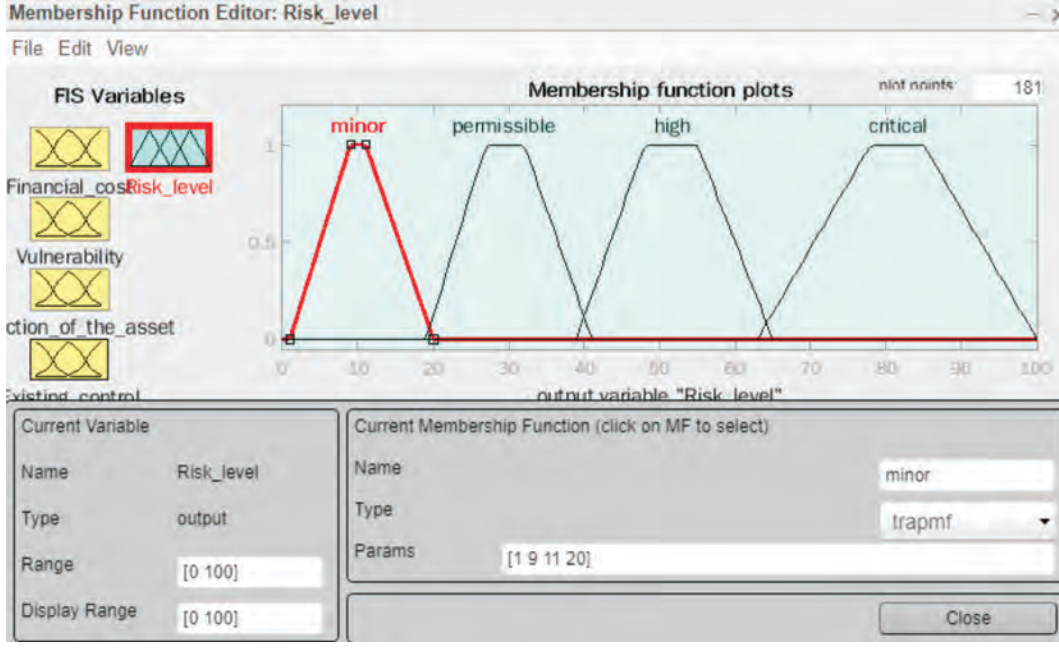

Рисунок 6 – Функции принадлежности для выходной характеристики «Уровень риска»

На рисунке 7 представлены продукционные правила, вводимые с использованием нечеткой базы знаний.

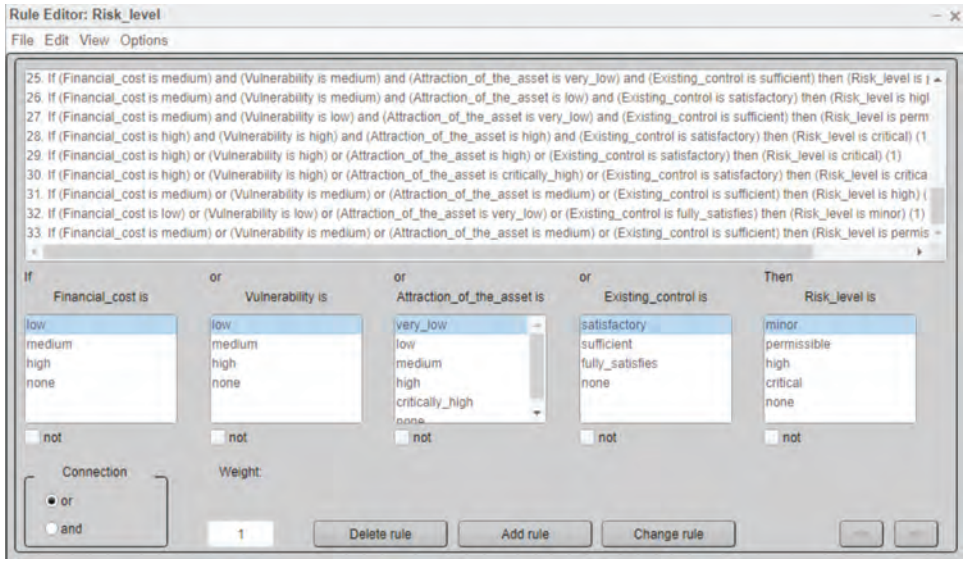

Рисунок 7 – Продукционные правила

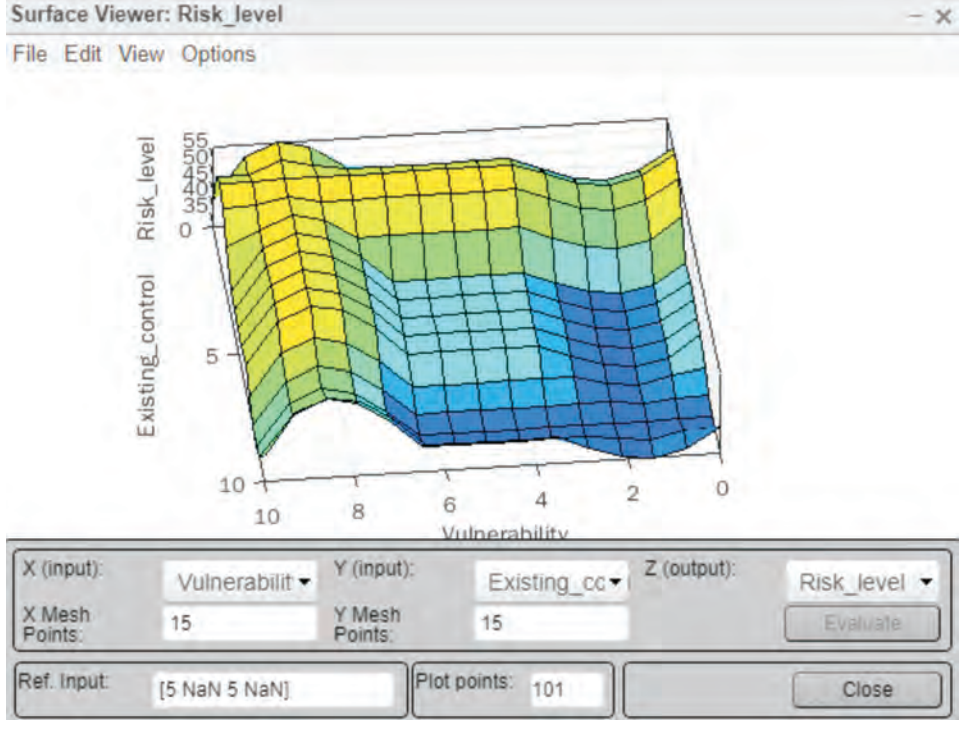

Рисунок 8 – Визуализация зависимости риска от уровня существующего контроля и уязвимости

Зная зависимость риска от значений входных параметров и используя данный алгоритм, можно определить предельный объем и структуру данных при использовании IIoT.

Заключение. Внедрение промышленных интернет-систем требует мощного инструмента для оценки рисков промышленных систем. В предложенной модели использовался нечеткий метод для связи мнений экспертов с лингвистическими переменными. Эти лингвистические переменные более точно отражают мнения экспертов. Эксперты представляют свое мнение по конкретным критериям, что позволяет нам повысить точность и надежность результатов. В результате, используя этот процесс, мы можем рассчитать уровень риска всех угроз, связанных с другими доменами. Модель, рекомендованная в этом исследовании, является многообещающей идеей для правильного анализа безопасности промышленных систем.

ЛИТЕРАТУРА

1 Амирова А., Тохметов А., Жанасбаева А. Исследование требований для построения модели обеспечения безопасности промышленного интернета вещей // Известия научно-технического общества «Кахак». – 2020. – №.3 (72). – С. 8–16

2 Амирова А., Тохметов А., Жанасбаева А. Основные проблемы безопасности в промышленном интернете вещей// Вестник Восточно-Казахстанского технического университета им. Д.Серикбаева. – 2021. – №.1. – С.82-90

3 Управление рисками информационной безопасности // Международная организация по стандартизации, ISO / IEC 27005. – 2008

4 Накамура Э. Т., Рибейро С. Л. Методология оценки рисков, сфокусированных на конфиденциальности, безопасности, устойчивости и надежности для систем IIoT. Шаги по созданию и использованию безопасных систем IIoT// Глобальный саммит Интернета вещей (GIoTS), 2018. – С. 1-6. DOI: 10.1109 / GIOTS.2018.8534521.

5 Фигероа-Лоренцо С. Обзор протоколов Интернета вещей: мера анализа рисков уязвимости на основе CVSS // ACM Comput. Surv. – 2020. – №. 2. С. 53–60. DOI: https: //doi.org/10.1145/3381038

6 Чжоу Ю. Нечеткая простая аддитивная система взвешивания при групповом принятии решений для выбора места расположения объекта с объективными/субъективными признаками// Опер.Рес. – 2018. – №. 189. – С. 132–145

7 Амирова А., Тохметов А. Модель анализа рисков в промышленном Интернете вещей // Журнал теоретических и прикладных информационных технологий. – 2021. – №14 (99). – С. 3449-3459

8 Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005

REFERENCES

1 Amirova A., Tohmetov A., ZHanasbaeva A. Issledovanie trebovanij dlya postroeniya modeli obespecheniya bezopasnosti promyshlennogo interneta veshchej // Izvestiya nauchno-tekhnicheskogo obshchestva «Kahak». – 2020. – №.3 (72). – S. 8–16

2 Amirova A., Tohmetov A., ZHanasbaeva A. Osnovnye problemy bezopasnosti v promyshlennom internete veshchej// Vestnik Vostochno-Kazahstanskogo tekhnicheskogo universiteta im. D.Serikbaeva. – 2021. – №.1. – S.82-90

3 Upravlenie riskami informacionnoj bezopasnosti // Mezhdunarodnaya organizaciya po standartizacii, ISO / IEC 27005. – 2008

4 Nakamura E. T., Ribejro S. L. Metodologiya ocenki riskov, sfokusirovannyh na konfidencial'nosti, bezopasnosti, ustojchivosti i nadezhnosti dlya sistem IIoT. SHagi po sozdaniyu i ispol'zovaniyu bezopasnyh sistem IIoT// Global'nyj sammit Interneta veshchej (GIoTS), 2018. – S. 1-6. DOI: 10.1109 / GIOTS.2018.8534521.

5 Figeroa-Lorenco S. Obzor protokolov Interneta veshchej: mera analiza riskov uyazvimosti na osnove CVSS // ACM Comput. Surv. – 2020. – №. 2. S. 53–60. DOI: https: //doi.org/10.1145/3381038

6 CHzhou YU. Nechetkaya prostaya additivnaya sistema vzveshivaniya pri gruppovom prinyatii reshenij dlya vybora mesta raspolozheniya ob»ekta s ob»ektivnymi/sub»ektivnymi priznakami// Oper.Res. – 2018. – №. 189. – S. 132–145

7 Amirova A., Tohmetov A. Model' analiza riskov v promyshlennom Internete veshchej // ZHurnal teoreticheskih i prikladnyh informacionnyh tekhnologij. – 2021. – №14 (99). – S. 3449-3459

8 Leonenkov A.V. Nechetkoe modelirovanie v srede MATLAB i fuzzyTECH. – SPb.: BHV-Peterburg, 2005

А. С. АМИРОВА, А. Т. ТОХМЕТОВ

Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан
whitesilk@mail.ru, attohmetov@mail.ru

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН ӨНЕРКӘСІПТІК ЗАТТАР ИНТЕРНЕТ ЖЕЛІЛЕРІНДЕ ТАЛДАУ

Өнеркәсіптік заттар интернетінің (IIoT) қарқынды дамуымен жылдам әрекет ету, басып кіруді анықтау және болдырмау қажеттілігі туындады. Бұл мәселелер әсіресе IIoT пайдаланушыларының болжамды өсуіне байланысты өзекті болып табылады. Тәуекелдерді бағалау ақпараттық қауіпсіздік жүйелерін, оның ішінде өндірістік кешендерді құру процесінің маңызды бөлігі болып табылады. Бұл жұмыстың мақсаты өнеркәсіптік Интернет желісінде ақпараттық қауіпсіздік тәуекелдерін бағалаудың практикалық моделін әзірлеу болып табылады. Ұсынылған модель қарапайым аддитивті салмақтау әдісіне және анық емес логикаға негізделген. Бұлыңғыр логика тәуекелді бағалауға сәйкес келеді және практикалық нәтижелерді көрсетеді. Ережелер базасын анық емес модельдеу процесін жүзеге асыру MATLAB бағдарламалық құралының Fuzzy Logic Toolbox арнайы пакетін қолдану арқылы жүзеге асырылады.

Түйін сөздер*: заттардың өнеркәсіптік Интернеті (IIoT), қарапайым өлшеу әдісі (SAW), қауіпсіздік, қауіптер.*

A. S. AMIROVA, A. T. TOKHMETOV

Eurasian National University, Nur-Sultan Kazakhstan
whitesilk@mail.ru, attohmetov@mail.ru

INFORMATION SECURITY RISK ANALYSIS IN THE NETWORKS OF THE INDUSTRIAL INTERNET OF THINGS

With the rapid development of the Industrial Internet of Things (IIoT), there has been a need to respond quickly, detect and prevent intrusions. These problems are especially relevant due to the projected

growth in IIoT users. Risk assessment is an important part of the process of creating information security systems, including industrial complexes. The aim of this work is to develop a practical model for assessing information security risks in industrial Internet of Things networks. The proposed model is based on a simple additive weighting method and fuzzy logic. Fuzzy logic is appropriate for risk assessment and represents practical results. The implementation of the process of fuzzy modeling of the rule base is carried out by using the specialized package Fuzzy Logic Toolbox of the MATLAB software tool.

***Keywords**: Industrial Internet of Things (IIoT), Simple Additive Weighting Method (SAW), Security, Threats.*