Евразийский национальный университет имени Л.Н. Гумилева

УДК 004.413.4 На правах рукописи

**АМИРОВА АКЖИБЕК СЕЙТЖАНОВНА**

Разработка системы анализа рисков информационной безопасности в сетях промышленного интернета вещей

8D06103 – Информационные системы

Диссертация на соискание степени

доктора философии (PhD)

Научные консультанты

кандидат физико-математических наук,

доцент

А.Т. Тохметов,

доктор технических наук,

профессор

Н.И. Листопад,

(Минск)

Республика Казахстан

Астана, 2024

**СОДЕРЖАНИЕ**

|  |  |  |
| --- | --- | --- |
| **НОРМАТИВНЫЕ ССЫЛКИ**........................................................................... | | 4 |
| **ОПРЕДЕЛЕНИЯ**................................................................................................. | | 5 |
| **ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**............................................................. | | 7 |
| **ВВЕДЕНИЕ**.......................................................................................................... | | 8 |
| **1** | **СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В IIOT**......................................................................................................... | 12 |
| 1.1 | Концепция промышленного Интернета вещей....................................... | 12 |
| 1.2 | Особенности современных промышленных IoT систем с точки зрения информационной безопасности................................................... | 15 |
| 1.2.1 | Обзор исследований, посвященных проблемам информационной безопасности в IIoT................................................................................... | 15 |
| 1.2.2 | Исследование таксономии атак в IIoT..................................................... | 18 |
| 1.2.3 | Исследование классификации защищаемых активов............................ | 27 |
| 1.2.4 | Исследование уязвимостей в IIoT............................................................ | 30 |
| 1.3 | Разработка рекомендаций, направленных на совершенствование мер по обеспечению информационной безопасности в сетях IIoT……….. | 31 |
| 1.4 | Анализ основных методов оценки рисков информационной безопасности промышленных IoT-систем............................................. | 33 |
| **2** | **РАЗРАБОТКА МОДЕЛИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ НЕЧЕТКОЙ ЛОГИКИ**........................................................................... | 39 |
| 2.1 | Описание основных этапов создания нечеткой системы вывода......... | 39 |
| 2.2 | Описание нечеткой модели расчета риска ИБ промышленной IoT-системы....................................................................................................... | 42 |
| 2.2.1 | Определение нечетких переменных и функций принадлежности........ | 48 |
| 2.2.2 | Определение весов критериев.................................................................. | 64 |
| 2.2.3 | Формирование базы нечетких продукционных правил......................... | 68 |
| 2.3 | Моделирование нечеткой системы оценки риска информационной безопасности с помощью пакета Fuzzy Logic Toolbox.......................... | 85 |
| **3** | **Создание экспертно-аналитической системы оценки рисков информационной безопасности в промышленных IOT-системах**......................................... | 89 |
| 3.1 | Выбор и разработка алгоритма работы экспертно-аналитической системы оценки рисков информационной безопасности IIoT-систем | 89 |
| 3.2 | Технология разработки экспертно-аналитической системы................. | 95 |
| 3.3 | Применение экспертно-аналитической системы для оценки степени рисков для информационной безопасности IIoT-систем....................... | 97 |
| **ЗАКЛЮЧЕНИЕ**……....................................................................................…... | | 103 |
| **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**….............................… | | 104 |
| **ПРИЛОЖЕНИЕ А** - Свидетельство об авторском праве............................... | | 109 |
| **ПРИЛОЖЕНИЕ Б –** Акт внедрения................................................................. | | 110 |
| **ПРИЛОЖЕНИЕ В –** Часть кода программы................................................... | | 111 |

**НОРМАТИВНЫЕ ССЫЛКИ**

В настоящей диссертации использованы ссылки на следующие стандарты:

Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности ("Киберщит Казахстан"): утв. 30 июня 2017 года, №407.

Постановление Правительства Республики Казахстан. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности ("Киберщит Казахстана") до 2022 года: утв. 28 октября 2017 года, №676.

СТ РК ИСО/МЭК 13335-5-2008. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий.

СТ РК ИСО/МЭК 15408-2-2006. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

СТ РК ИСО/МЭК 27001-2015. Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования.

СТ РК ИСО/МЭК 27002-2009. Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации.

СТ РК 34.023-2006. Информационная технология. Методика оценки соответствия информационных систем требованиям безопасности.

NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology.

ISO/IEC 27400:2022. Cybersecurity – IoT security and privacy – Guidelines;

NIST Special Publication 800-213. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.

NIST SPECIAL PUBLICATION 1800-32. Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources.

NIST Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments.

NIST Special Publication 800-37 Revision 2 – Risk Management Framework for Information Systems and Organizations.

**ОПРЕДЕЛЕНИЯ**

В настоящей диссертации применяют следующие термины с соответствующими определениями:

**Атака на информационную систему** – это совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех свойств информации - доступности, целостности или конфиденциальности.

**Интернет Вещей (IoT, Internet of Things)** – система объединенных компьютерных сетей и подключенных физических объектов (вещей) со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

**Индустриальный (Промышленный) Интернет Вещей (Industrial Internet of Things, IIoT)** – интернет вещей для корпоративного/отраслевого применения - система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

**Индустрия 4.0 (Четвёртая промышленная революция)** – новый подход к производству, основанный на массовом внедрении информационных технологий в промышленность, автоматизации бизнес-процессов и распространении искусственного интеллекта.

**Интенсивность угрозы** – потенциальный ущерб, который может быть нанесен организации в случае реализации данной угрозы.

**Информационные активы** – информационные ресурсы, в том числе различные виды информации, циркулирующие в информационной системе на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение), или средства обработки информации.

**Информационная безопасность** – состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

**Информационные системы** – системы, предназначенные для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Киберфизическая система (CPS)** – информационно-технологическая концепция, подразумевающая интеграцию вычислительных ресурсов в физические сущности любого вида, включая биологические и рукотворные объекты.

**Лингвистическая переменная** – это переменная, значения которой определяются набором вербальных (то есть словесных) характеристик некоторого свойства.

**Метод анализа иерархий (МАИ)** – математический инструмент системного подхода к сложным проблемам принятия решений.

**Межмашинное взаимодействие (М2М)** – общее название технологий, которые позволяют машинам обмениваться информацией друг с другом, или же передавать её в одностороннем порядке.

**Риск ИБ** – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

**Терм–множество** – множество всех возможных значений лингвистической переменной.

**Терм** – любой элемент терм–множества. В теории нечетких множеств терм формализуется нечетким множеством с помощью функции принадлежности.

**Угроза** – любое действие, которое может быть направлено на нарушение информационной безопасности системы.

**Экспертные системы (ЭС)** – особые компьютерные программы, моделирующие действия эксперта-человека при решении задач в какой-либо предметной области на основе накопленных знаний, составляющих базу знаний.

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|  |  |
| --- | --- |
| ENISA | – Европейское агентство по сетевой и информационной безопасности |
| ICS | – промышленные системы управления |
| IDS | – Intrusion Detection System/система обнаружения вторжений |
| IPS | – Intrusion Prevention System/система предотвращения вторжений |
| OWASP | – Open Web Application Security Project/это открытый проект обеспечения безопасности веб-приложений |

**ВВЕДЕНИЕ**

**Общая характеристика работы**.

Промышленный интернет вещей (IIoT) быстро становится реальностью, используя интеллектуальные взаимосвязанные киберфизические системы для автоматизации всех этапов промышленных операций, от проектирования и производства до эксплуатации, цепочки поставок и сервисного обслуживания. IIoT формирует будущее производственных отраслей, используя возможности гибкого и умного производства, обеспечивает революционный рост производительности.

Среди наиболее значимых сдерживающих факторов развития цифровой составляющей промышленности является недостаточное обеспечение информационной безопасности. Четвертая промышленная революция и экспоненциальный рост количества подключенных устройств во всем мире вместе с быстрорастущим числом инцидентов кибербезопасности еще больше подчеркивают необходимость повышения киберустойчивости, особенно среди промышленных операторов, которые начинают использовать решения концепции интернета вещей~~.~~ Недавние инициативы в отношении «Индустрии 4.0» и «Умного производства» привлекают больше внимания к аспектам, связанным с безопасностью технических решений и безопасностью граждан, которые на них полагаются. Эта тема тем более важна, что потенциальное воздействие новых угроз варьируется от нарушения физической безопасности до повреждения оборудования, порчи продукции, простоев производства и вытекающих из этого финансовых и репутационных потерь.

**Актуальность работы.**

Одной из основных задач Государственной программы «Цифровой Казахстан» является цифровизация промышленности. Современные предприятия в своём стремительном развитии за прошедшее десятилетие перешагнули незримую черту, отделяющую физический мир машин и агрегатов от виртуального мира компьютерных программ, превратившись, по сути, в киберфизические системы, где объектами физического мира управляют инструкции машинного кода. Такие системы создаются при помощи современных IT-технологий и интегрируются с внешним кибермиром при помощи проводных и беспроводных каналов связи. Это многократно упрощает их эффективное использование и развитие, но одновременно делает их уязвимыми перед угрозой компьютерных атак.

С позиции бизнеса, управление информационной безопасностью (ИБ) является дочерним процессом более широкого процесса управления рисками: если компания после анализа и оценки всех своих бизнес-рисков делает вывод об актуальности рисков ИБ, то в игру вступает уже непосредственно защита информации как способ минимизации этих рисков.

Ключевым этапом внедрения систем информационной безопасности является *оценка рисков*, которым может быть подвержена работа предприятия. Этот этап может помочь ~~им~~ расставить приоритеты в создаваемой на предприятии системе кибербезопасности.

Существует несколько стандартов и методологий для оценки информационных рисков предприятий, например, NIST SP 800-39 и ISO/IEC 27005. И хотя они объясняют общие принципы оценки и предлагают некоторые рекомендации, они не содержат деталей реализации сценария в том или ином случае кибератак. Кроме того, в данных стандартах отсутствуют рекомендации для оценки рисков систем промышленного Интернета вещей.

Поэтому разработка практической модели оценки рисков информационной безопасности IIoT-систем является актуальной и востребованной задачей, решения которой ждут многие промышленные предприятия.

**Цель и задачи исследования.**

Целью диссертационного исследованияявляется создание системы поддержки принятия решения в сфере информационной безопасности промышленных IoT-систем на основе методов нечеткой логики.

В соответствии с поставленной целью, в диссертационной работе решались следующие **задачи**:

1. Определение и классификация угроз информационной безопасности для промышленных IoT-систем на основе стандартов и научных публикаций.

2. Разработка нечеткой модели оценки риска информационной безопасности для IIoT-систем.

3. Создание системы поддержки принятия решения в сфере информационной безопасности промышленных IoT-систем на основе разработанной нечеткой модели.

**Объектом исследования** являютсяриски информационной безопасности, возникающие в процессе эксплуатации промышленных IoT-систем.

**Предметом исследования** являютсямодели, методы и алгоритмы оценки и управления рисками информационной безопасности, возникающих при работе промышленных IoT-систем.

**Методы исследования.** Диссертационное исследование проведено на основе современных многокритериальных статистических методов, методов нечеткой логики, математического и компьютерного моделирования; а также законодательных и нормативных документов, направленных на обеспечение информационной безопасности промышленных систем.

**Научная новизна работы.** В настоящей работе получены следующие результаты:

1. Разработана классификация (онтология) угроз информационной безопасности для промышленных IoT-систем.
2. Разработана модель анализа рисков информационной безопасности в IIoT-систем, работающая на основе нечеткой логики.
3. Создана система поддержки принятия решения по определению уровня информационной безопасности в промышленных IoT-системах.
4. Разработаны научно-практические рекомендации, направленные на повышение информационной безопасности в сетях промышленного Интернета вещей.

**Основные положения** диссертационного исследования, выносимые на защиту:

* разработанная онтология угроз информационной безопасности в промышленных IoT-системах;
* разработанная модель анализа рисков информационной безопасности в IIoT-систем, работающая на основе нечеткой логики;
* разработанная система поддержки принятия решения по определению уровня информационной безопасности в промышленных IoT-системах.

**Теоретическая и практическая значимость исследования.** В современной реальности для корректной деятельности промышленных предприятий существенное значениеимеет реальная оценка уровня риска информационной безопасности с целью минимизации потерь различных видов.

Практическая значимость данного исследования определена тем, что результаты работы дают возможность своевременного реагирования на нештатное состояние промышленных IoT-систем и предлагают пути решения проблемы. Предложенный в работе метод был впервые применен для оценки информационной безопасности в промышленных IoT-системах.

Теоретическая значимость исследования заключается в предложенной модели решения задачи оценки уровня риска информационной безопасности. Исследованы методы и модели оценки информационной безопасности IIoT систем. Предложенные модели и методы ранее не применялись для решения аналогичной задачи при использовании выбранных критериев оценки.

Достоверность работы подтверждается апробацией результатов диссертационного исследования на международных и республиканских научно-практических конференциях, а также публикациями в изданиях, рекомендованных КОКСНВО МНВО РК и индексируемых в международной базе цитирования Scopus.

Результаты исследования могут быть использованы:

* для анализа и оценки уровня информационной безопасности промышленных систем IIoT;
* при разработке нормативной документации в области обеспечения информационной безопасности промышленных систем IIoT;
* в учебном процессе в области образования и научных исследований.

**Апробация работы.** Основные результатыдиссертационного исследования были представлены на международных конференциях:

1. Глобальная наука и инновация 2022: Центральная Азия: материалы международной научно-практической конференции». (Астана, 2022).

2. BIG DATA и анализ высокого уровня: материалы VI международной научно-практической конференции (Беларусь, 2020).

3. Наука и образование в современном мире: вызовы ХХI века: материалы V Международной научно-практической конференции (Астана, 2019).

Работа была обсуждена на расширенном заседании кафедры «Информационных систем» ЕНУ им. Л.Н. Гумилева.

**Публикации.** По материалам диссертации опубликовано 10 работ, из них 2 (две) – в журналах с ненулевым импакт–фактором (базы Scopus):

1. Symmetry, процентиль – 93 (General Mathematics).
2. Journal of Theoretical and Applied Information Technology, процентиль – 36 (General Computer Science).

5 (пять) в изданиях, рекомендованных КОКСНВО МНВО РК и 3 (три) – в трудах международных конференций.

**Структура и объем диссертации**. Диссертационная работа состоит из введения, трех взаимосвязанных разделов, которые разбиты на подразделы, заключения, списка использованных источников и приложений. Работа изложена на 122 страницах, содержит 33 рисунка и 39 таблиц. Список использованных источников содержит 75 наименований.

**1 СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В IIOT**

**1.1 Концепция промышленного Интернета вещей**

Термин «Интернет вещей» впервые был использован профессорами 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. Интернет вещей – это сложная сеть устройств и элементов, укрепленных повсеместным интеллектом, подключенных через Интернет. Он воплощает в себе универсальные услуги и сетевую инфраструктуру с переменным подключением и плотностью с возможностями самоконфигурации, основанными на стандартных и совместимых форматах и протоколах [1, 2].

Industrial Internet of Things (IIoT) относится к применению технологий IoT в промышленных условиях. Его также называют «Индустрия 4.0» – термин, появившийся на немецком языке благоларя возможности интеграции цифровой и физической индустрии. Промышленность IIoT или 4.0 включает в себя облако, большие данные, киберфизические межсоединения и т.д. Промышленная область, вероятно, больше, чем какая-либо другая, стала свидетелем новаторских методологий, которые открыли новую эру мышления. Это, конечно, помогло фирмам использовать эффект масштаба и размах, чтобы занять конкурентные позиции на рынке до сегодняшнего дня. Теперь IIoT – это сеть устройств и вещей, которые все когнитивные, предлагают массу данных, которые начинают сдвигать промышленные возможности, как это было лучше всего раньше. Речь идет не только об увеличении производства, но и о предоставлении данных в режиме 24/7 в реальном времени, которые меняют все при правильном использовании. Кроме того, IIoT позволил создать новые и гибридные бизнес-модели, которые трансформируют отрасль [3, 4].

IoT, IIoT и Индустрия 4.0 – это тесно связанные концепции, но их нельзя использовать взаимозаменяемо. Что касается Интернета вещей, существует несколько определений, каждое из которых пытается уловить одну из своих фундаментальных характеристик. Его часто считают своего рода сетью для машин, подчеркивая цель – позволить вещам обмениваться данными. Однако области применения настолько разнообразны, что некоторые требования (особенно связанные с аспектами коммуникации) могут сильно отличаться в зависимости от намеченных целей и конечных пользователей, лежащих в основе бизнес-моделей и принятых технологических решений. Потребительский IoT ориентирован на человека; «вещи» – это умные бытовые электронные устройства, соединенные друг с другом с целью повышения осведомленности людей об окружающей среде, экономии времени и денег. В целом, потребительские IoT-коммуникации можно классифицировать как межмашинные взаимодействия и в форме взаимодействий клиент-сервер. С другой стороны, в промышленном мире мы содействуем появлению цифрового и интеллектуального производства, цель которого - при интеграции операционных технологий с областями информационных технологий [5].

Одним словом, IIoT (основная опора цифрового производства) – это соединение всех промышленных активов, включая машины и системы управления, с информационными системами и бизнес-процессами. Как следствие, большой объем собранных данных может служить источником аналитических решений и вести к оптимальным производственным операциям. С другой стороны, интеллектуальное производство, очевидно, сосредоточено на производственном этапе жизненного цикла (интеллектуального) продукта с целью быстрого и динамичного реагирования на изменения спроса. Следовательно, IIoT влияет на всю производственно-сбытовую цепочку и является обязательным требованием для интеллектуального производства.

Как подчеркивается ниже, коммуникация в IIoT ориентирована на машины и может охватывать большое количество различных секторов рынка и видов деятельности. Сценарии IIoT включают устаревшие приложения для мониторинга (например, мониторинг процессов на производственных предприятиях) и инновационные подходы для самоорганизующихся систем (например, автономное промышленное предприятие, которое практически не требует вмешательства человека) [6].

Требования IoT и IIoT схожи, например, поддержка экосистемы Интернета с использованием недорогих устройств с ограниченными ресурсами и масштабируемость сети, многие требования к связи специфичны для каждого домена и могут сильно отличаться, например, качество обслуживания QoS (с точки зрения детерминизма, задержки, пропускной способности), доступности и надежности, а также безопасности и конфиденциальности. IoT больше фокусируется на разработке новых стандартов связи, которые могут гибко и удобно подключать новые устройства к экосистеме Интернета. Напротив, текущий дизайн IIoT делает упор на возможную интеграцию и взаимосвязь когда-то изолированных заводов и рабочих участков или даже оборудования, тем самым предлагая более эффективное производство и новые услуги [7]. По этой причине, по сравнению с IoT, IIoT можно считать скорее эволюцией, чем революцией.

Что касается возможности подключения и критичности, IoT более гибок, допускает специальные и мобильные сетевые структуры и не имеет жестких требований к срокам и надежности. С другой стороны, IIoT обычно использует фиксированные сетевые решения и сетевые решения на основе инфраструктуры, которые хорошо спроектированы для удовлетворения потребностей связи и сосуществования. В IIoT связь осуществляется в форме каналов M2M, которые должны удовлетворять строгим требованиям с точки зрения своевременности и надежности. В области автоматизации процессов приложения для мониторинга и управления процессами можно разделить на три подкатегории: мониторинг/надзор, управление с обратной связью и управление с блокировкой. В то время как приложения для мониторинга и контроля нечувствительны к потерям пакетов и джиттеру и могут допускать задержку передачи на втором уровне, для управления с обратной связью и взаимоблокировок, а также для управляющих приложений требуется ограниченная задержка на уровне миллисекунд (10-100 мс) и надежность передачи 99,99% [8, 9].

Если рассматривать ситуации с промышленными цифровыми системами в Казахстане, то говорить о резком скачке не приходится, потому что процесс трансформации требует времени. Тем не менее есть отрасли, которые более активны во внедрении Индустрии 4.0 на своих производствах.

Например, 13 крупных предприятий горнодобывающей промышленности планируют осуществить 58 крупных проектов с общей суммой инвестиций в 315,4 млрд тг. На текущий момент завершено уже 20 проектов на сумму 88,7 млрд тг. Можно отметить, что ГМК выступает лидером в цифровой трансформации [10].

Кроме того, Министерство реализует проект по созданию 7 модельных цифровых фабрик (АО «АК Алтыналмас», АО «Евразиан Фудс», АО «Кентауский трансформаторный завод», АО «Химфарм», ТОО «Карлскрона», ТОО «Балтекстиль», ТОО «Алматинский вентиляторный завод») с целью демонстрации цифровых технологий и эффектов от цифровизации, популяризации Индустрии 4.0 и выработки мер государственной поддержки. Компании на сегодняшний день уже реализовали 14 проектов на 7,5 млрд тг и получают выгоды в виде экономии за счет снижения простоев оборудования, снижения потерь ресурсов и т.д. В общем по регионам до 2023 года запланировано внедрение цифровых решений на 90 предприятиях (примерно 200 проектов цифровизации), из которых на 35 предприятиях проекты уже реализованы.

В настоящее время на передовой в части планов по цифровизации находятся экспортоориентированные предприятия, имеющие высокую добавленную стоимость (горно-металлургический комплекс, машиностроение, химическая промышленность, фармацевтика) [8].

Говоря о встраивании в глобальные цепочки производства, можно выделить предприятие АО «Усть-Каменогорский титано-магниевый комбинат», которое в партнерстве с южнокорейской компанией «POSCO» создало совместное предприятие ТОО «ПОСУК Титаниум» («POSUK Titanium»). На данном предприятии в настоящее время реализуется проект по автоматизации и контролю всех этапов производства, что позволит выдавать электронные сертификаты с подтвержденным паспортом производства на выпускаемую продукцию для дальнейшей реализации крупным судостроительным компаниям.

В настоящее время эффективное производство невозможно без современных информационных технологий. Внедрение "умных" продуктов имеет важное значение для развития приоритетных секторов экономики, включая горно-металлургический комплекс Казахстана. Например, в горно-металлургическом секторе реализуются следующие проекты: внедрение технологии интеллектуального решения IntelliSense на золотодобывающей фабрике Актогайского филиала АО «АК Алтыналмас» - ведущего производителя золотых слитков в Казахстане и одного из лидеров среди модельных цифровых фабрик. Эта технология позволяет построить сложную модель нейронных сетей для предиктивного анализа технологического процесса и управления большими данными. Актогайская золотодобывающая фабрика стала первым модельным производством в Казахстане, где использование технологий искусственного интеллекта позволяет прогнозировать уровень загрузки шаров и износа внутренних футеровок, а также предотвращает перегрузку мельничного комплекса, что приводит к повышению прозрачности процесса и снижению простоев мельницы.

Также, в рамках проектов по цифровизации системообразующих предприятий горнодобывающей промышленности, таких как ТОО «Казцинк», Eurasian Resources Group и АО «Усть-Каменогорский титано-магниевый комбинат», внедрены системы управления мобильным персоналом Pitram, ERP, расчета балансов, а также проект «Умный карьер» на Качарском карьере. В этих проектах используются передовые технологии, такие как ERP-датчики, бортовые компьютеры и спутниковое позиционирование, все работает в режиме реального времени [10].

Проект «Умный карьер» был запущен в 2017 году на Качарской площадке АО «Соколовско-Сарбайское горно-обогатительное производственное объединение» («ССГПО»). Этот проект предусматривает полную прозрачность и контроль за показателями эффективности, что повысит общий экономический эффект производимой предприятием продукции. Нововведение включает в себя полностью интегрированный цикл производства железной руды с внедрением нескольких элементов Индустрии 4.0.

Одним из элементов проекта является внедрение автоматизированной системы Modular, интегрированной с ГИС и ERP системой. Эта система включает в себя моделирование производственных процессов. Оперативный мониторинг ситуации на карьере, корректировка и оптимальное распределение горнотранспортного оборудования осуществляются не оператором, а компьютерами. Человек играет роль наблюдателя, следящего за бесперебойной работой «Умного карьера».

**1.2 Особенности современных промышленных IoT систем с точки зрения информационной безопасности**

1.2.1 Обзор исследований, посвященных проблемам информационной безопасности в IIoT

На текущий момент вопрос обеспечения безопасности в контексте IIoT является одним из наиболее уязвимых моментов, препятствующих масштабному внедрению этой технологии.

Безусловно, без решения данной проблемы IIoT никогда не сможет полностью реализовать свой потенциал. В свете этого, в последние годы наблюдается значительный рост научных исследований, посвященных обеспечению безопасности IIoT. Настоящий обзор литературы направлен на систематизацию и анализ ключевых проблем информационной безопасности в контексте IIoT за период с 2018 по 2023 год. Он осуществляется с целью изучения следующих аспектов: угрозы, с которыми сталкивается IIoT, защищаемые активы, предлагаемые модели и методологии, направленные на обеспечение безопасности.

Одними из наиболее масштабных исследований в области безопасности IIoT являются работы [11-13]. Если [11, р. 1-9] посвящено системной архитектуре Индустрии 4.0 в целом и отмечает, что наблюдается рост предложений по архитектуре, ориентированных на безопасность, но не обсуждает безопасность в деталях, то [12, р. 4724-4733] фокусируется в первую очередь на характеристике угроз путем изучения существующих атак. Кроме того, следует отметить, что в вышеупомянутых исследованиях авторы солидарны в том, что традиционная стратегия безопасности недостаточна и не готова к IIoT.

В [14] обращается внимание на то, что модели для определения угроз ИТ-инфраструктуры, такие как Microsoft STRIDE, OWASP, классификация ENISA всецело описывают угрозы Интернета вещей, однако не могут в полной мере выявить угрозы Промышленного Интернета вещей. В связи с этим стоит вопрос определения корректной классификации угроз промышленных систем.

Так, например, в [15] были проанализированы потенциальные угрозы безопасности для отраслей, адаптирующихся к IIoT, изучены атаки, которым могут подвергаться компоненты многоуровневой архитектуры IIoT, а также предложены некоторые превентивные мерыБыла предложена таксономия атак IIoT, которая, по мнению авторов, поможет снизить риски атак. Данная таксономия была рассмотрена в разрезе четырех измерений: вектор атаки, цель атаки, воздействие атаки и последствие атаки. Однако недостатком данной таксономии является ограниченное количество рассмотренных угроз, что не позволяет полностью охватить всю картину ситуации.

Авторы в [16] рассмотрели некоторые виды угроз такие как спуфинг, SQL-инъекции, DOS атаки в контексте компонентов пятиуровневой архитектуры IIoT. Авторы отмечают, что для более точной и полной классификации угроз в IIoT требуется дальнейшее их исследование.

При рассмотрении моделей безопасности в исследованиях, можно выделить две основные группы: превентивные модели, предназначенные для оценки рисков, и модели, разработанные для обнаружения уже совершенных атак. В процессе анализа литературы, было установлено, что существует значительное количество качественных исследований, в которых были предложены системы обнаружения аномалий и атак. Для этого были использованы различные инструменты, такие как графовые методы, технология блокчейн и алгоритмы машинного обучения [17-20].

Системы IIoT обладают собственной динамикой и уникальностью, что требует новых подходов к оценке рисков. Оценка рисков для IIoT – еще одна область, требующая особого внимания. На данный момент имеется малое количество работ по данной тематике. Рассмотрим несколько исследований, наиболее весомые из них.

Авторы в [21] предложили модель оценки рисков на основе AHP (Analytic Hierarchy Process) для облака IIoT. Недостатком данной модели является то, что она не может предоставить новое решение для принятия решений, так же не рассмотрен вопрос идентификации и классификации активов. Структура предложенной 4-уровневой модели оценки рисков на основе AHP показана на рисунке 1.



Рисунок 1 – Модель оценки рисков на основе AHP

Примечание – Составлено по источнику [21, р. 638]

Стоит уделить внимание исследованию [22], где на основе стандарта IEC 62443 была разработана модель оценки рисков безопасности в среде IIoT. Исследуемая в данной статье модель предназначена для наиболее точной оценки рисков, которым подвергается промышленная установка с учетом обнаруженных уязвимостей. Несмотря на преимущества, описанные в статье, модель оценки не рассматривает такие требования безопасности, как целостность системы, доступность ресурсов, а также данная модель не предлагает меры для устранения последствий угроз на систему IIoT.

Обзор литературы подтверждает важность и актуальность изучения проблемы обеспечения информационной безопасности промышленных IoT. В частности, такие вопросы как классификация угроз, идентификация активов, а также анализ рисков безопасности IIoT-систем. Также анализ исследований указывает на то, что значительное количество исследований посвящено обнаруживающим мерам безопасности, при этом вопрос превентивных мер, включающих в себя анализ рисков ИБ, почти не изучен.

1.2.2 Исследование таксономии угроз в IIoT

На сегодняшний день существует несколько моделей угроз для определения угроз ИТ-инфраструктуре. Многие из этих моделей также адаптируются для включения угроз Интернета вещей. К наиболее распространенным из них относятся:

1. Модель угроз Microsoft STRIDE – это систематика угроз Microsoft и связанных с ними стратегий смягчения. STRIDE означает спуфинг, фальсификацию, отказ, раскрытие информации, отказ в обслуживании и повышение привилегий. Кроме того, Microsoft также предлагает инструменты, основанные на модели STRIDE, которые собирают и анализируют архитектурные компоненты, выявляют угрозы и рекомендуют действенные меры по их устранению [23].

2. Проект IoT Vulnerabilities Project: Open Web Application Security Project (OWASP) определил уязвимости IoT, выпущенные в порядке их возникновения в определенные временные рамки. Для каждой из основных уязвимостей Интернета вещей эта модель содержит сводку и определяет связанную с ней поверхность атаки [24].

3. Классификация угроз Агентства Европейского Союза по сетевой и информационной безопасности (ENISA). Эта таксономия обеспечивает обширное и многоуровневое определение угроз. Модель угроз включает угрозы для инфраструктуры, исходящие от векторов физических атак, таких как стихийные бедствия или судебные иски [25].

Необходимо обратить внимание, что приведенное выше представляет собой небольшую выборку моделей угроз, разработанных экспертами по безопасности для анализа сред ИТ и Интернета вещей. Предприятия и организации могут разрабатывать или адаптировать те или иные модели к своим собственным средам. Таксономия ENISA предоставляет библиотеку угроз, связанных с широким спектром векторов атак, как кибер, так и физических.

Данные модели всецело описывают угрозы Интернета вещей, однако не могут в полной мере выявить угрозы Промышленного Интернета вещей. В связи с этим в данном разделе предлагается следующая классификация угроз IIoT, разработанная на основе таксономии ENISA (рисунок 2).

Классификация представлена в виде таблицы 1. Все угрозы были разделены по категориям: недобросовестная деятельность и злоупотребления, прослушивание/перехват/хакинг, физические атаки, непреднамеренные повреждения (случайные), отказы и неисправности, перебои, правовые вопросы и катастрофы. Отдельно описаны каждая угроза, относящаяся к определенной категории и область воздействия данной угрозы [26, 27].

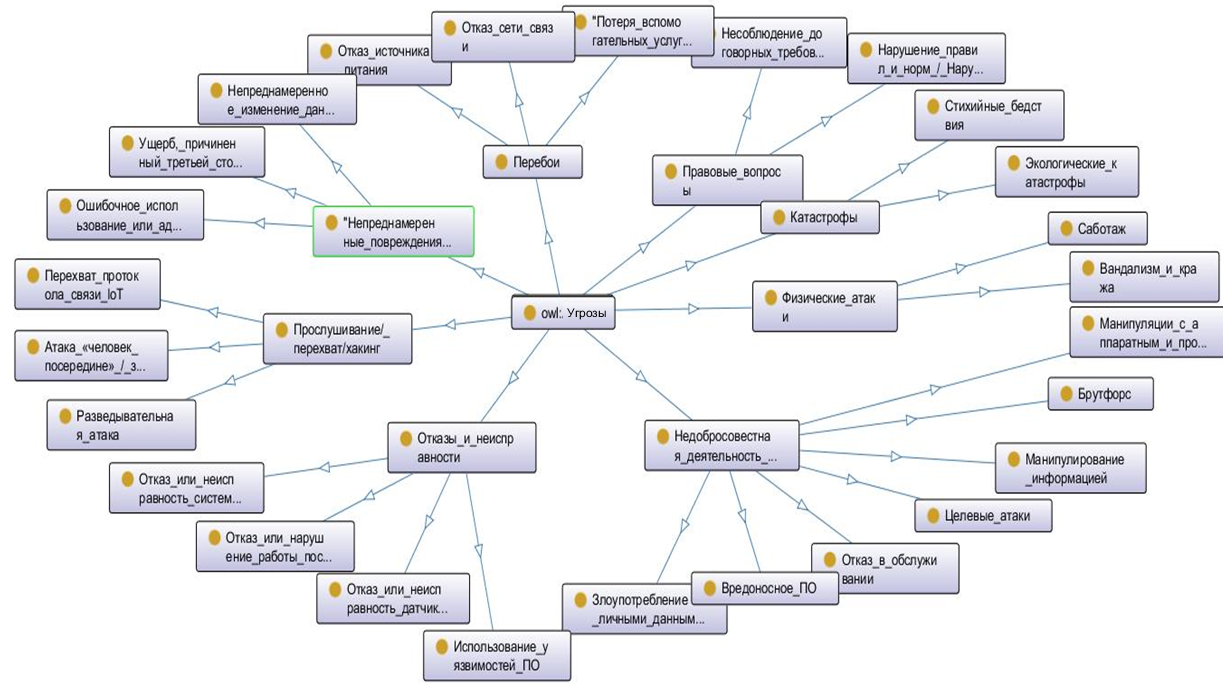


Рисунок 2 – Таксономия угроз IIoT

Примечание – Составлено автором

Таблица 1 – Классификация угроз в IIoT

|  |  |  |  |
| --- | --- | --- | --- |
| Категория | Угроза | Описание | На что влияет |
| 1 | 2 | 3 | 4 |
| Недобросовестная деятельность и злоупотребления | Отказ в обслуживании: распределённый отказ в обслуживании (DDoS), отказ в обслуживании с применением IoT/IIoT-устройств | Атака отказа в обслуживании может быть двунаправленной: она может быть нацелена на систему IIoT, что приведет к недоступности системы и сбоям в работе, вызванным огромным количеством запросов, отправленных в систему. С другой стороны, злоумышленник может воспользоваться преимуществом большого количе ства устройств IIoT в промышленной среде и создать армию ботнетов IoT в качестве платформы для атаки на какую-либо другую систему. | Оконечные устройства IIoT, ICS, сети и компоненты связи ICS, информация, услуги облачных вычислений, мобильные устройства, серверы и системы, программное обеспечение |
| Вредоносное ПО: программы-вымогатели,  вирусы,  троянкий конь,  шпионcкие программы,  эксплойт | Проникновение вредоносного программного обеспечения в IIoT с целью выполнения нежелательных и несанкционированных действий, которые могут нанести ущерб OT-системе, операционным процессам и связанным данным. Программы-вымогатели, вирусы, троянские программы и шпионское ПО являются типичными примерами этой угрозы. | Оконечные устройства IIoT, ICS, серверы и системы , инструменты для мониторинга и обеспечения безопасности в реальном времени, информация, услуги облачных вычислений, программное обеспечение |
| Манипуляции с аппаратным и программным обеспечением | Угроза несанкционированного манипулирования программным обеспечением устройств или приложениями в системе ОТ со стороны злоумышленника. Что касается промышленных систем IoT, действия злоумышленника могут включать в себя манипулирование промышленным роботом, манипулирование устройствами удаленного управления, подавляющими состояние устройства управления, и изменение его конфигурации. | Оконечные устройства IIoT, ICS, коммуникационные сети и компоненты, программное обеспечение, мониторинг в реальном времени и инструменты безопасности, передовая робототехника |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  | Манипулирование информацией | Угроза нежелательной и несанкционированной модификации данных злоумышленником. Это может относиться к компрометации OT или систем поддержки производства, таких как SCADA, MES, Historian и манипулирования данными процесса. Возможные последствия могут включать неправильные решения, основанные на фальсифицированных данных. | Оконечные устройства IIoT, ICS, информация, услуги облачных вычислений, аналитика данных, инструменты мониторинга и безопасности в реальном времени, серверы и системы, программное обеспечение и лицензии |
| Целевые атаки: APT-атака,  беспроводные атаки | Угроза кибератаки, нацеленной на конкретную организацию (или конкретного человека в этой организации). Такая атака направлена на то, чтобы нанести вред организации, чтобы получить конт роль над системой с помощью различных техниче ских средств, таких как взлом ключевых устрой ств и фальсификация телеметрии, вводящая в заб луждение неосведомленных операторов. К другим последствиям относятся нанесение ущерба репута ции или кража секретов компании. Когда целью является производственная компания, злоумыш ленник может, например, попытаться украсть фор мулы или рецепты и продать их конкурентам. Злоумышленник может использовать искусствен ный интеллект для проведения персонализирован ной атаки, ориентированной на выбранную группу или отдельных сотрудников. Эта атака отличается от более масштабных атак, цель которых – зара зить любую компанию, которая подключается к определенному веб-сайту, подготовленному злоу мышленником, или любой компанией, которая | Оконечные устройства IIoT, ICS, информация |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  |  | использует устройство или программное обеспече ние с определенной уязвимостью. |  |
|  | Злоупотребление личными данными | Угроза компрометации личной/конфиденциа льной информации, хранящейся на устройствах или в облаке. Цель злоумышленника - получить несанкционированный доступ к таким данным и использовать их незаконным образом. В произ водственных компаниях это может относиться к именам и ролям пользователей системы ОТ. Произ водственные данные не считаются конфиденциаль ными, но они также могут создавать проблемы, если их можно связать с работой отдельных сотрудников. | Оконечные устройства IIoT, информация, сервисы облачных вычислений, персонал |
| Брутфорс | Угроза получения несанкционированного доступа к ресурсам организации (т.е. данным, системам, устройствам). Через большое количество попыток угадать правильный ключ или пароль. Организации Индустрии 4.0, которые позволяют использовать несложные пароли или пароли по умолчанию для промышленных устройств и сис тем, могут быть особенно уязвимы для таких атак. | Оконечные устройства IIoT, ICS, мобильные устройства, сети и компоненты связи ICS, инструменты мониторинга и безопасности в реальном времени |
| Прослушивание/ перехват/хакинг | Атака «человек посередине»/ захват сеанса | Угроза активного подслушивания, когда злоумыш ленник ретранслирует сообщения, которыми обме ниваются не подозревающие стороны. Злоумыш ленник может просто прослушать сообщения, ко торыми обмениваются (например, чтобы украсть конфиденциальную или конфиденциальную ин формацию компании), или изменить или удалить переданную информацию, что приведет к нарушению связи. | Информация, сети связи ICS и их компоненты, Оконечные устройства IIoT, мобильные устройства |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  | Перехват протокола связи IoT | Угроза того, что злоумышленник получит контроль над существующим сеансом связи между двумя компонентами сети, что может привести к раскрытию паролей и другой конфиденциальной информации. | Информация, сети связи ICS и их компоненты, Оконечные устройства IIoT, алгоритмы принятия решений |
| Разведывательная атака | Угроза раскрытия внутренней сетевой инфор мации (например, подключенных устройств, ис пользуемых протоколов, открытых портов и ис пользуемых служб и т.д.) Злоумышленнику, кото рому удается выполнить сканирование сеть пассив но обладая этими знаниями, злоумышленник может спланировать, какие действия предпринять после компрометации работы системы. | Информация, Оконечные устройства IIoT, сети и компоненты связи ICS |
| Физические атаки | Вандализм и кража | Угроза причинения физического ущерба устрой ству диверсантом, который получает физический доступ к среде ОТ - либо посторонним, которому удалось обойти недостаточные меры физической безопасности, либо инсайдером, например, недовольный сотрудник, который по каким-то причинам хочет навредить организации. Эта угроза также включает в себя кражу. Необходимость замены поврежденного или украденного устройства может привести к незапланированным простоям производства, связанным со сроками поставки запасных частей. | Оконечные устройства IIoT, ICS, мобильные устройства, сети и компоненты связи ICS, передовая робототехника, персонал |
| Саботаж | Угроза взлома устройства со стороны диверсанта, который получает физический доступ к среде ОТ - либо постороннего, которому удается обойти недостаточные меры физической безопасности, | Оконечные устройства IIoT, ICS, мобильные устройства |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  |  | либо инсайдера, например, недовольный сотрудник, который по каким-то причинам хочет навредить организации. Злоумышленник может воспользоваться неправильной конфигурацией портов и возможностью использовать открытые порты. Злоумышленник также может использовать доступ для выполнения несанкционированных действий оператора. |  |
| Непреднамерен ные повреждения (случайные) | Непреднамеренное изменение данных или конфигурации в системе OT. | Угроза нарушения рабочего процесса из-за непреднамеренного изменения данных или конфигурации в системе OT, выполняемая недостаточно обученным сотрудником. Даже имея добрые намерения, неквалифицированный сотрудник, не подозревая о последствиях, может внести неправильные изменения в систему, особенно если он или она получает более высокие, чем необходимые привилегии. | Оконечные устройства IIoT, сети и компоненты связи ICS, передовая робототехника, информация, услуги облачных вычислений, аналитика больших данных, программное обеспечение и лицензии, серверы и системы, персонал |
| Ошибочное использование или администрирование устройств и систем | Угроза нарушения рабочего процесса или причинение физического повреждения устройству в результате непреднамеренного неправильного использования устройства IIoT/OT недостаточно подготовленным сотрудником. Даже имея добрые намерения, неквалифицированный сотрудник может непреднамеренно не использовать устройство в соответствии с инструкциями и инструкциями, тем самым нарушая работу устройства или нанося ему физический ущерб. | Оконечные устройства IIoT, ICS, мобильные устройства, сети и компоненты связи ICS, передовая робототехника, информация, персонал |
| Ущерб, причиненный третьей стороной | В Индустрии 4.0 третьи стороны могут иметь доступ к системе OT, например, для обслуживания | Оконечные устройства IIoT, ICS, передовая робототехника, услуги |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  |  | или обновления программного обеспечения. Если этот доступ не контролируется в достаточной степени, нарушения безопасности сторонней организации могут повлиять на компанию, которая получает услугу. | облачных вычислений, информация |
| Отказы и неисправности | Отказ или неисправность датчика / исполнительного механизма | Угроза выхода из строя или неисправности око нечных устройств IIoT. Это может иногда проис ходить, особенно если надлежащее обслуживание и соблюдение руководств и инструкций устройств во время эксплуатации не обеспечиваются. | *Оконечные устройства IIoT, ICS* |
| Отказ или неисправность системы управления (PLC, RTU, DCS) | Угроза выхода из строя или неисправности системы управления. Это может иногда проис ходить, особенно если надлежащее обслуживание и соблюдение руководств и инструкций устройств во время эксплуатации не обеспечиваются. | Оконечные устройства IIoT, ICS |
| Использование уязвимостей ПО | Угроза того, что злоумышленник воспользуется преимуществами встроенного ПО или программных уязвимостей оконечного устройства IIoT. Такие устройства часто уязвимы из-за отсутствия обновлений, использования слабых паролей или паролей по умолчанию и неправильной конфигурации. | Оконечные устройства IIoT, информация, программное обеспечение и лицензии |
| Отказ или нарушение работы поставщиков услуг | Угроза нарушения процессов, которые полагаются на сторонние услуги, в случае отказа или неисправности этих услуг. | Оконечные устройства IIoT, ICS, сети и компоненты связи ICS, инфор мация, услуги облачных вычислени, аналитика больших данных |
| Перебои | Отказ сети связи | Угроза недоступности каналов связи, связанная с проблемами с кабельной, беспроводной или мобильной сетью. | Коммуникационные сети и компоненты ICS |
| Продолжение таблицы 1 | | | |
| 1 | 2 | 3 | 4 |
|  | Отказ источника питания | Угроза отказа или неисправности источника питания. Если для критических систем отсутствует аварийное электроснабжение, любое нарушение электроснабжения может привести к серьезным последствиям из-за внезапного останова производственных процессов. | Оконечные устройства IIoT, ICS, передовая робототехника |
|  | Потеря вспомогательных услуг (MES, ERP, CRM) | Угроза отказа или сбоев в работе систем, поддерживающих производство или логистику, то есть MES, ERP и CRM. | Серверы и системы |
| Правовые вопросы | Нарушение правил и норм / Нарушение законодательства / Злоупотребление личными данными | Угроза юридических проблем и финансовых потерь, связанных с обработкой персональных данных, например связанных с использованием оконечных устройств IIoT без соблюдения местных законов и правил. | Оконечные устройства IIoT, информация |
| Несоблюдение договорных требований | Угроза нарушения договорных требований производителями компонентов и поставщиками программного обеспечения в случае несоблюдения необходимых мер безопасности. | Оконечные устройства IIoT, услуги облачных вычислений, информация, ПО и лицензии |
| Катастрофы | Стихийные бедствия | Угроза стихийных бедствий, таких как наводнения, удары молнии, сильный ветер, дождь и снегопад, которые могут нанести физический ущерб компонентам окружающей среды ОТ. | Оконечные устройства IIoT, ICS, сети и компоненты связи ICS, передовая робототехника, персонал |
| Экологические катастрофы | Угроза происшествий и неблагоприятных условий, таких как пожары, загрязнение, пыль, коррозия, взрывы, которые могут нанести физический ущерб компонентам окружающей среды ОТ. | Оконечные устройства IIoT, ICS, сети и компоненты связи ICS, передовая робототехника, персонал |
| Примечание – Составлено автором | | | |

1.2.3 Исследование классификации защищаемых активов

Активы IIoT – это устройства, системы и данные, используемые в промышленности для сбора, обработки, передачи и управления информацией. Классификация и идентификация активов IIoT являются важным шагом в процессе обеспечения безопасности этих систем [28].

Активы в рамках установленных границ рассмотрения должны быть идентифицированы с достаточным уровнем детальности по отношению к сфере и уровню проводимой оценки. И наоборот, любые активы, исключенные из сферы рассмотрения по любым причинам, должны быть приписаны к другому рассмотрению, чтобы гарантировать, что они не забыты или не упущены из виду. Также для целей менеджмента риска важно вести запись активов, деловых процессов, которые они поддерживают, и их соответственной значимости для организации в инвентарном списке активов.

Предлагается следующая классификация защищаемых активов.

0 Активы:

* 1. Оконечные устройства IIoT:
     1. Датчики – устройства обнаруживают и/или измеряют события в своей среде и передают информацию другим электронным системам для обработки:
        1. Датчики температуры.
        2. Датчики движения.
        3. Датчики вибраций.
        4. Датчики влажности.
        5. Датчики приближения.
     2. Автоматизированные системы безопасности (SIS) – системы состоят из датчиков, логических вычислителей и исполнительных элементов управления (исполнительных механизмов), задачей которых является приведение процесса в безопасное состояние в случае нарушения заданных условий.
     3. Исполнительные механизмы – устройства взаимодействуют с окружающей средой, перемещая или управляя механизмом или системой.
  2. Промышленные системы управления (ICS):
     1. Программируемые логические контроллеры (PLCs) –специализированные промышленные компьютеры используются для автоматизации функций управления в промышленной сети. Как правило, они оснащены дополнительными сменными модулями, такими как модули ввода/вывода для подключения датчиков и исполнительных механизмов.
     2. Удаленные терминальные блоки (RTUs) – устройства обычно используются на подстанциях или в удаленных местах. Их задача заключается в мониторинге параметров поля и отправке данных на центральную станцию.
     3. Распределенная система управления (DCS) – системы управления распределяют информацию, то есть логику управления, о контролируемом процессе.
     4. Диспетчерское управление и сбор данных (SCADA) – системы используются для сбора данных о промышленных объектах и процессах, их визуализации, наблюдения и контроля.
     5. Человеко-машинные интерфейсы (HMI) – панели управления и приборные панели позволяют операторам контролировать и контролировать PLCs, RTU и другие электронные устройства.
  3. Компоненты коммуникационной сети:
     1. Маршрутизаторы – сетевые устройства, которые пересылают пакеты данных между различными сетями в промышленных средах и экосистемах IoT.
     2. Шлюзы IIoT – сетевые узлы используются для взаимодействия с другой сетью из среды IoT с использованием разных протоколов.
     3. Коммутаторы – сетевые компоненты фильтруют и пересылают пакеты в локальной сети:
        1. Управляемые
        2. Неуправляемые
     4. Беспроводные точки доступа – компоненты позволяют беспроводным устройствам подключаться к проводной сети с использованием Wi-Fi или связанных стандартов.
     5. Межсетевые экраны – устройства или системы сетевой безопасности контролируют сетевой трафик между сетями или между хостом и сетью на основе заранее определенных правил.
  4. Информация:
     1. Эксплуатационные и производственные данные.
     2. Информация об устройстве.
     3. Информация о пользователе.
  5. Программное обеспечение и лицензии:
     1. Программы – для устройств в экосистеме IIoT для достижения конкретных технологических целей, включая логику ПЛК, приложения SCADA, приложения HMI, программы для промышленных роботов и т.д.
     2. Операционные системы – системы, которые управляют аппаратными ресурсами компьютера и предоставляет общие службы для запуска других компьютерных программ
     3. Мобильные приложения – программы работают на мобильных устройствах, таких как планшеты и смартфоны, которые используются для удаленного контроля и управления процессом (например, мобильные клиентские приложения SCADA), обслуживания оборудования и других задач (например, инвентаризация склада).
     4. Антивирусы – программное обеспечение, которое отслеживает компьютер или сеть для выявления вредоносного ПО, предотвращения заражения устройств и очистки зараженных устройств
     5. Прошивки – класс программного обеспечения, хранящегося в постоянной памяти устройства, и предоставляет инструкции о том, как устройство должно работать. Во время выполнения он не может быть динамически записан или изменен.
  6. Серверы и системы:
     1. Серверы приложений – на этих компьютерах размещаются приложения, например. приложения рабочих станций пользователей.
     2. Серверы баз данных – серверы используются в качестве репозиториев для информации о событиях, предоставляемой датчиками, агентами и серверами управления.
     3. Операционные системы предприятия (например, ERP, CRM) – системы объединяют информацию из различных частей организации (например, производство, распределение, финансы, человеческие ресурсы).
     4. Системы производственных операций (например, MES) – системы автоматизируют управление производством и процессами с помощью сетевых вычислений, устраняя разрыв между бизнесом и производственным цехом.

0.7 Человеческие ресурсы – люди являются неотъемлемыми элементами производственной среды и, следовательно, должны учитываться при определении критически важных активов с точки зрения безопасности. Все люди, имеющие доступ к среде OT, могут (преднамеренно или непреднамеренно) внедрять в систему вредоносное ПО, становиться объектами фишинга или наносить ущерб системе и подвергать риску ее безопасность различными способами.

Соответствие угроз активам.

В таблице 2 определены категории защищаемых активов в системах IIoT и угрозы, которым наиболее часто подвержены данные активы.

Таблица 2 – Атаки в IIoT, разделенные по защищаемым активам

|  |  |
| --- | --- |
| Группа активов | Атаки |
| 1 | 2 |
| Оконечные устройства IIoT | DDoS атаки,  программы-вымогатели,  вирусы,  троянкий конь,  шпионские программы |
| Промышленные системы управления (ICS) | DDoS атаки,  вредоносные программы,  манипулирование информацией, таргетированные атаки,  брутфорс атака |
| Программное обеспечение и лицензии | Управление конфигурацией устройства/  SCADA,  Эксплуатация уязвимостей программного обеспечения,  Несанкционированный доступ к программному обеспечению,  Ввод ложной информации в программное обеспечение,  Человеческая ошибка в программе |
| Продолжение таблицы 2 | |
| 1 | 2 |
| Коммуникационные сети и компоненты промышленной системы управления | Нарушение связи,  DDoS атаки,  Управление промышленным роботом,  Атаки с использованием ИИ,  Физические атаки |
| Информация | Раскрытие пароля  Активное прослушивание  Кража информации  Злоупотребление личными данными  SQL-инъекция |
| Серверы и системы | Отказ в обслуживании  Вредоносное ПО  Манипуляции с информацией  Непреднамеренное изменение данных |
| Человеческие ресурсы | Кража  Нехватка квалифицированных кадров  Человеческая ошибка |
| Примечание – Составлено автором | |

* + 1. Исследование уязвимостей в IIoT

Согласно стандарту ISO/IEC 29147 уязвимость – это недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации [29].

Раасмотрим уязвимости, которые могут быть выявлены в стандартных сетях, использующих промышленный интернет вещей (IIoT). Уязвимости разделены на группы по темам "Политика и процедуры", "Платформа" и "Сеть":

1. Уязвимости политики и процедур

Уязвимости часто появляются в ICS из-за неполной, несоответствующей или несуществующей документации по безопасности, включая политики и руководства по реализации (процедуры). Документация по безопасности, наряду с поддержкой управления, является краеугольным камнем любой программы безопасности. Корпоративная политика безопасности может уменьшить уязвимости, предписывая такие действия, как использование и обслуживание паролей или требования по подключению модемов к ICS.

2. Уязвимости платформы

Уязвимости в ICS могут возникать из-за недостатков, неправильных настроек или плохого обслуживания их платформ, включая оборудование, операционные системы и приложения ICS. Эти уязвимости можно уменьшить с помощью различных средств обеспечения безопасности, таких как установка исправлений для ОС и приложений, контроль физического доступа и программное обеспечение для обеспечения безопасности (например, антивирусное программное обеспечение):

Уязвимости конфигурации платформы.

Уязвимости оборудования платформы.

Уязвимости программного обеспечения платформы.

Уязвимости защиты платформы от вредоносных программ.

3. Сетевые уязвимости.

Уязвимости в ICS могут возникать из-за недостатков, неправильных конфигураций или плохого администрирования сетей ICS и их соединений с другими сетями. Эти уязвимости могут быть устранены или смягчены с помощью различных элементов управления безопасностью, такие как глубокая защита сети, шифрование сетевых коммуникаций, ограничение потоков сетевого трафика и обеспечение контроля физического доступа к сетевым компонентам:

Уязвимости конфигурации сети.

Уязвимости сетевого оборудования.

Уязвимости сетевого периметра.

Сетевой мониторинг и ведение журнала уязвимостей.

Коммуникационные уязвимости.

Уязвимости беспроводного соединения.

**1.3 Разработка рекомендаций, направленных на совершенствование мер по обеспечению информационной безопасности в сетях IIoT**

В таблице 3 приведены некоторые показатели из отчета “Об использовании информационно-коммуникационных технологий на предприятиях Республики Казахстан” за 2021 г., опубликованного на официальном сайте stat.gov.kz [30].

Таблица 3 – Показатели использования ИКТ-технологий за 2020-2021 гг. в РК

|  |  |  |
| --- | --- | --- |
| Показатель | 2020 год | 2021 год |
| Количество организаций, использующих цифровые технологии при производстве | 2 184 | 2 965 |
| Доля крупных и средних предприятий промышленности, использующих цифровые технологии, в % | 7,8 | 9,9 |
| Затраты на информационные и коммуникационные технологии, млн. тенге | 388 928,5 | 443 121,3 |
| Количество организаций, использующих Облачные ИТ-услуги | 11 884 | 17 708 |
| Количество крупных и средних организаций, использующих робототехнику | 799 | 180 |
| Количество организаций, проводивших анализ больших данных | 2 381 | 981 |
| Примечание – Составлено по источнику [30] | | |

Согласно приведенным данным, можно отметить рост числа промышленных предприятий, использующих цифровые технологии при производстве. В связи с этим, представляется весьма актуальным разработка рекомендаций, направленных на совершенствование мер по обеспечению информационной безопасности на промышленных предприятиях.

*Меры безопасности на этапе проектирования:*

* оборудовать, если это будет сочтено целесообразным после оценки безопасности, даже самые простые подключенные устройства, обладающие очень ограниченными возможностями обработки (например, приводы, преобразователи), функциями идентификации и аутентификации и обеспечить совместимость с решениями класса IAM;
* выполнять анализ рисков и угроз с привлечением экспертов по кибербезопасности на самых ранних этапах процесса проектирования устройства, чтобы выяснить, какие функции безопасности будут необходимы;
* в каждый проектный документ включать главу, посвященную безопасности всей информации и систем управления в промышленной среде.

*Меры безопасности, связанные с конфиденциальностью и защитой данных:*

* определить объем данных, которые будут обрабатываться устройством, а также цель этой обработки на этапе проектирования, избегая сбора или излишнего предоставления конфиденциальных данных;
* определить физическое местоположение хранилища данных и обозначить между какими организациями будут передаваться данные, ограничивая доступ к собранным личным данным только уполномоченным лицам;
* проводить анализ воздействия на конфиденциальность (PIA) для данных, которые будут обрабатываться устройством;
* строго контролировать доступ третьих лиц к уровню управления или производственному уровню, предоставляя доступ только по запросу, в указанном временном окне, для определенной цели и с наименьшими привилегиями.

*Меры безопасности, касающиеся обнаружения, администрирования, мониторинга и обслуживания активов:*

* использовать инструменты, поддерживающие управление активами, которые способны динамически обнаруживать, идентифицировать и перечислять активы, характерные для организации и промышленной среды;
* рассмотреть возможность безопасного администрирования активов с управлением инфраструктурой и устройствами безопасности через выделенную сеть управления;
* вводить новое устройство в систему только в соответствии с установленным, принятым и переданным процессом управления изменениями;
* избегать использования съемных устройств, отключающих порты USB, если нет принятых бизнес-требований.

*Меры безопасности, касающиеся рекомендованного подхода к процессу управления рисками и угрозами:*

* для критически важных инфраструктур в производственной среде установить ряд областей управления рисками, полностью согласованных с корпоративными аспектами, вопросами безопасности и окружающей среды. Оценивать и охарактеризовать угрозы, уязвимости и меры защиты от этих областей управления рисками;
* установить процесс управления рисками и угрозами в соответствии с индивидуальными потребностями и требованиями безопасности вашей компании;
* не реже одного раза в год проводить анализ рисков, который включает аспекты кибербезопасности. Оценка риска должна охватывать техническое и процедурное тестирование эффективности политик и процессов безопасности.

*Меры безопасности, касающиеся обнаружения и реагирования инцидентам, которые могут произойти в средах Индустрии 4.0.*

* определить киберинциденты, актуальные для организации, на основе региона и диапазона деятельности компании и классифицировать их в соответствии с применимыми стандартами;
* рассмотреть возможность создания Операционного центра кибербезопасности (SOC), состоящего из специалистов по кибербезопасности ОТ и ИТ, для поддержки инцидентов кибербезопасности, разделив их на определенные линии поддержки с соответствующими ролями и обязанностями;
* установить процесс обработки инцидентов, который состоит из идентификации затронутых активов, идентификации и классификации уязвимостей, эскалации и уведомления.

*Меры безопасности в отношении процесса управления уязвимостями:*

* при устранении уязвимостей начинать с наиболее критичных с учетом критичности активов и систем;
* проводить тесты на проникновение новых решений IIoT в контролируемой среде или до/во время фазы ввода в эксплуатацию, а также регулярно и после важного обновления системы.

*Меры безопасности в отношении рекомендуемого подхода, связанного с обучением безопасности и повышением осведомленности сотрудников, работающих с устройствами и системами IIoT:*

* принять целостный подход к обучению безопасности и повышению осведомленности сотрудников, охватывающий сотрудников на всех уровнях организации и устранение новых угроз, связанных с Индустрией 4.0;
* обеспечить всех вновь нанятых сотрудников обучением по вопросам кибербезопасности до начала работы;
* обеспечить непрерывное, регулярное и часто обновляемое обучение по вопросам безопасности;
* обучить пользователей IIoT безопасному использованию своих устройств, объясняя им технологии, развернутые для защиты устройств IIoT и экосистемы.

**1.4 Анализ основных методов оценки рисков информационной безопасности промышленных IoT-систем**

Сталкиваясь с различными типами рисков, оценка рисков сетевой безопасности помогает отслеживать текущее состояние безопасности сети, прогнозировать риск и предлагать соответвующие меры. Существует множество методов оценки риска, которые в основном делятся на методы качественной оценки, методы количественной оценки и методы комплексной оценки:

*Методы качественной оценки риска* – это метод оценки текущего состояния безопасности сети в рамках данного теоретического анализа, основанный на неколичественных факторах, таких как знания и опыт оценщика, исторические данные о нарушениях и защите сети. К качественным методам анализа, которые широко используются, относятся метод матрицы рисков, метод экспертной оценки, метод анализа дерева отказов, метод Дельфи [31-34].

*Методы количественной оценки риска* – это метод оценки, который обычно использует численные значения в качестве стандарта для оценки сетевых рисков, количественно оценивает оценку риска и выполняет расчеты для определения вероятности рисков сетевой безопасности, а также потерь, которые могут быть вызваны. Типичные методы количественной оценки риска включают факторный анализ, анализ основных компонентов, дерево решений, марковский анализ и т.д. [35, 36].

*Методы комплексной оценки рисков* – это метод оценки, который сочетает в себе качественные и количественные показатели и может объективно и эффективно оценивать риски сетевой безопасности. К методам комплексной оценки рисков относятся иерархический анализ, вероятностная оценка риска и нечеткая логика [37, 38].

Рассмотрим каждый из методов оценки риска поподробнее, а также определим их достоинства и недостатки.

*Метод матрицы рисков.* Этот метод предполагает создание матрицы, в которой пересекаются вероятность возникновения определенного события (например, ущерба) и его потенциальные последствия. Для каждой ячейки матрицы определяется величина риска, например, умножением вероятности на потенциальный ущерб [32, р. 270-280].

Достоинства:

* простота и понятность;
* позволяет визуализировать риски и приоритизировать их.

Недостатки:

* не всегда удается количественно оценить вероятность и ущерб;
* не учитывает взаимосвязи между рисками;
* не учитывает изменения во времени.

*Метод экспертной оценки*. Этот метод основан на опросе экспертов или специалистов в области, связанной с рисками. Эксперты оценивают вероятность и потенциальные последствия рисков на основе своего опыта и знаний [33].

Достоинства:

* учитывает опыт и знания специалистов;
* может быть применен в случаях, когда данных для статистической оценки недостаточно;
* позволяет быстро получить оценку рисков.

Недостатки:

* возможна субъективность оценок экспертов;
* не всегда доступны квалифицированные эксперты.

*Метод Дельфи*. Этот метод также основан на экспертной оценке, но он структурирован и итеративен. Группа экспертов предоставляет свои оценки рисков, после чего результаты анализируются и предоставляются экспертам для дополнительных оценок. Процесс повторяется несколько раз до достижения консенсуса [34].

Достоинства:

* структурированный итеративный процесс способствует улучшению оценок;
* может быть применен для прогнозирования долгосрочных рисков.

Недостатки:

* требует больших затрат времени и ресурсов;
* могут возникнуть сложности при выборе экспертов и их координации.

*Метод дерева решений.* Метод дерева решений представляет собой графическую модель принятия решений, которая разбивает проблему на последовательность бинарных решений. На каждом шаге анализируется определенный аспект риска, и на основе определенных критериев принимается решение о том, какой путь следует выбрать. Дерево строится сверху вниз, и каждый узел представляет собой решение, которое влияет на дальнейший ход анализа [35].

Достоинства:

* простота интерпретации: деревья решений легко интерпретировать, что делает их полезными для обучения и взятия решений;
* возможность учета различных факторов: метод позволяет учитывать множество факторов при оценке риска.

Недостатки:

Неустойчивость к изменениям данных: Малые изменения в данных могут привести к большим изменениям в структуре дерева.

*Марковский анализ.* Марковский анализ является математической моделью, которая используется для моделирования случайных процессов, где будущее зависит только от текущего состояния системы и не зависит от предыдущих состояний. Он особенно полезен в оценке риска, когда имеется последовательность событий [36].

Достоинства:

* моделирование последовательных событий: марковский анализ позволяет учитывать последовательность событий и их взаимосвязь;
* подходит для долгосрочных прогнозов: этот метод может использоваться для оценки риска в долгосрочной перспективе.

Недостатки:

* высокая вычислительная сложность: для больших и сложных систем марковский анализ может потребовать значительных вычислительных ресурсов;
* ограниченность модели: этот метод может не учитывать влияние внешних факторов, которые могут влиять на риск.

*Метод анализа иерархий (AHP).*Метод анализа иерархий разработан Томасом Саати и используется для оценки и сравнения различных альтернатив в многокритериальных решениях. Он основан на представлении иерархической структуры критериев и альтернатив, а затем на применении математических методов для определения наилучших решений [37].

Достоинства:

* структурированность: позволяет учитывать сложные взаимосвязи между критериями и альтернативами, разделяя их на более простые уровни;
* учет экспертного мнения: позволяет включать мнение экспертов в процесс принятия решений с использованием шкалы сравнения;
* многокритериальность: Этот метод может быть полезен в случаях, когда существует большое количество критериев и альтернатив, и их взаимосвязи сложны.

Недостатки:

* субъективность: результаты могут сильно зависеть от экспертного мнения и выбора шкалы сравнения;
* сложность: применение AHP может быть сложным и требует высокой квалификации для проведения анализа;
* чувствительность к изменениям: малые изменения в данных или приоритетах могут привести к изменению ранжирования альтернатив.

*Нечеткая логика.* Нечеткая логика, или теория нечетких множеств, разработана Лотфи Заде в 1965 году. Этот метод позволяет учитывать неопределенность и нечеткость в данных и оценках [38].

Достоинства:

* учет неопределенности: позволяет работать с данными, которые не имеют четких значений, а имеют степень принадлежности к разным категориям.
* простота использования: нечеткая логика часто более интуитивна и менее сложна в применении по сравнению с другими методами.
* гибкость: метод подходит для различных типов данных и может быть применен в разных областях.

Недостатки:

* требует экспертных знаний: выбор функций принадлежности и определение нечетких правил требуют экспертных знаний и опыта;
* высокая вычислительная сложность: в некоторых случаях, особенно при большом объеме данных, нечеткая логика может потребовать больших вычислительных ресурсов.

В таблице 4 описаны преимущества и недостатки методов оценки риска.

Исходя из сравнительного анализа, выбор в пользу экспертного метода на основе нечеткой логики обусловлен рядом преимуществ, которые этот подход может предоставить:

1. Учет неопределенности и нечеткости: Нечеткая логика позволяет учесть нечеткость и неопределенность входных данных и принимать решения на основе приближенных и нечетких значений. Это особенно полезно в случаях, когда точные данные ограничены или недоступны.
2. Интеграция экспертных знаний: Метод на основе нечеткой логики позволяет учесть экспертные знания и опыт специалистов в процессе принятия решений. Эксперты могут предоставить оценки и описания в форме лингвистических переменных, которые затем могут быть введены в модель нечеткой логики.
3. Гибкость и адаптивность: Нечеткая логика позволяет моделировать различные типы нечетких и лингвистических переменных, а также учитывать различные аспекты проблемы. Это делает метод гибким и способным адаптироваться к различным ситуациям и условиям.
4. Интерпретируемость результатов: Результаты, полученные с использованием нечеткой логики, могут быть легко интерпретированы и объяснены. Они отражают уровень принадлежности и степень уверенности в принятых решениях, что помогает принимающим решения лучше понять и использовать полученные выводы.
5. Обработка нечетких и неоднозначных данных: Метод на основе нечеткой логики может обрабатывать нечеткую и неоднозначную информацию, которая часто присутствует в реальных ситуациях принятия решений. Это позволяет учесть различные факторы и условия, которые могут влиять на результаты принятия решений.

Таблица 4 – Преимущества и недостатки методов оценки риска

|  |  |  |
| --- | --- | --- |
| Метод | Преимущества | Недостатки |
| Метод матрицы рисков | Простота в использовании | Неточность |
| Метод экспертной оценки | Расчет прост и интуитивно понятен | Субъективность |
| Метод Дельфи | Гибкость и адаптивность | Ресурсозатратность, слож ность выбора экспертов |
| Метод дерева решений | Интерпретируемость | Чувствительность к изменениям данных |
| Марковский анализ | Простота и интерпретируемость | Ограниченность модели, высокая вычислительная сложность |
| Метод анализа иерархий (AHP) | Структурированность, многокритериальность | Субъективность, зависи мость от структуры иерар хии, чувствительность к изменениям |
| Нечеткая логика | Обработка нечеткой и неопреде ленной информации, гибкость | Сложность вычислений |
| Примечание – Составлено по источнику [38] | | |

Ниже представлен обзор исследований, в которых для оценки риска информационных систем был применен метод нечеткой логики.

В [39] была предложена нечеткая экспертная система оценки рисков информационной безопасности на примере систем управления аналитическим обучением. Построенная нечеткая экспертная система имеет расширенную классификацию критериев оценки риска, основанную на анализе таких стандартов как ISO/IEC 27000, ISO/IEC 27002, ISO 15408 и др.

Предлагаемая оценка риска в [40] представляет собой качественный подход в соответствии со стандартом ISO/IEC 27005. В этой модели были рассмотрены основные цели и процессы бизнеса, а также проведена оценка риска на управленческом и операционном уровнях. Вероятность возникновения угроз и интенсивность их воздействия являются двумя основными факторами при оценке уровня риска.

Wang и Elhag [41] предложили нечеткий метод TOPSIS, основанный на наборах альфа-уровней, и применили его для оценки риска. В этом примере вероятность и влияние различных угроз определяются в формах лингвистических переменных, а затем применяются в оценке риска моста путем умножения соответствующих нечетких значений.

В [42] для оценки риска применяется метод, сочетающий в себе метод МАИ и метод нечеткой логики. Каждый фактор риска оценивается в аспекте вероятности, степени воздействия и неуправляемости.

Концепция применения нечеткой экспертной системы для оценки информационной безопасности является хорошо известной. Основные работы, основанные на нечеткой логике, сконцентрированы на стандартных подходах к оценке информационной безопасности и установленных формулах расчета рисков. Однако, в связи с учетом специфических аспектов IIoT, таких как его сложная архитектура, широкий спектр угроз и особенности промышленных процессов, возникает необходимость в разработке экспертной системы на основе нечеткой логики для оценки риска информационной безопасности промышленных IoT-систем.

Использование экспертной системы на основе нечеткой логики позволит учесть различные неопределенности и нечеткости, которые присущи IIoT. Она позволит учесть экспертные знания и опыт специалистов, адаптировать модели оценки рисков под конкретные контексты и условия IIoT. Благодаря гибкости и адаптивности нечеткой логики, такая экспертная система сможет обрабатывать разнородные данные и предоставлять более точные и надежные результаты оценки рисков информационной безопасности в IIoT.

**2 РАЗРАБОТКА МОДЕЛИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ НЕЧЕТКОЙ ЛОГИКИ**

Оценка риска информационной безопасности нацелена на предотвращение угроз и нарушений информационной безопасности промышленных систем.

Существует несколько современных подходов к оценке рисков информационной безопасности предприятия, которые включают в себя следующие шаги:

1. Идентификация активов.
2. Идентификация угроз активам.
3. Расчет риска ИБ на основе определения вероятностей реализации угроз и оценки их последствий.
4. Формирование предложений по обработке выявленных рисков

Для идентификации защищаемых активов и угроз будут использованы классификации, предложенные в разделе 1.2.2, 1.2.3.

**2.1 Описание основных этапов создания нечеткой системы вывода**

На сегодняшний день одним из наиболее перспективных инструментов для научных исследований в области анализа, прогнозирования и моделирования слабоструктурированных и плохо формализуемых явлений и процессов является теория нечетких множеств и нечеткая логика (fuzzy logic), впервые предложенная американским ученым Лотфи Заде [43]. Эта теория значительно расширяет возможности учета различных форм неопределенности, которые неизбежно сопутствуют математическому описанию реальности. Такой подход обеспечивает решение задач улучшения функционирования различных систем в условиях неполной и неточной информации о происходящих процессах, ограниченных и ненадежных знаний, а также при наличии субъективности в оценках.

В отличие от традиционной математики, которая требует точных и однозначных формулировок закономерностей на каждом этапе моделирования, нечеткая логика предлагает альтернативный уровень мышления. В этом подходе творческий процесс моделирования происходит на более высоком уровне, где постулируется лишь минимальный набор закономерностей [44].

В сфере информационной безопасности (ИБ) эта проблема остается весьма актуальной. С одной стороны, точность и оптимальность в принятии решений играют ключевую роль в успешной стратегии обеспечения безопасности, что обеспечивает максимальную эффективность. С другой стороны, в оценке и управлении ИБ присутствуют факторы случайности и неточности. Поэтому математическая модель должна быть разработана не только с учетом наилучшего отражения сущности моделируемых процессов и явлений, но и с учетом условий неопределенности [45].

Для разработки нечеткой модели, пригодной для оценки информационной безопасности (ИБ), необходимо проанализировать возможности существующих моделей, основанных на теории нечётких множеств.

Под нечётким множеством понимается множество упорядоченных пар , где – функция принадлежности элемента , характеризующая степень принадлежности элемента этому множеству [46].

Возможны следующие три случая по формуле (1):

|  |  |
| --- | --- |
|  | (1) |

где , если элемент *x* не включен в подмножество *A*,

, если *x* частично принадлежит *A*,

, если *x* полностью принадлежит *A*.

Существует свыше десятка типовых форм кривых для задания функций принадлежности. В данной работе будут использоваться следующие типы: трапецеидальная, линейная Z-образная и линейная S-образная функции принадлежности.

В настоящее время наиболее часто используемым типом нечёткой модели является модель Мамдани [47]. Данная модель основана на нечетком логическом выводе, который позволяет избегать чрезмерно большого объема вычислений. Этот алгоритм получил большое практическое применение в задачах нечеткого моделирования и примечателен тем, что он работает по принципу «черного ящика». На вход поступают количественные значения, на выходе те же количественные значения. На промежуточных этапах используется аппарат нечеткой логики и теории нечетких множеств. Выбор в пользу модели Мамдани обусловлен хорошей лингвистической интерпретируемостью, что во многом определяет удобство ее использования в промышленных IoT-системах.

Модель Мамдани состоит из следующих этапов [48]:

1. *Фаззификация: определение нечетких переменных и функций принадлежности*.
2. *Формирование базы правил нечетких продукций.*
3. *Агрегация подусловий в правилах нечетких продукций.*
4. *Аккумулирование заключений правил нечетких продукций.*
5. *Дефаззификация выходного значения.*

Рассмотрим каждый из блоков поподробнее.

Первый этап модели Мамдани заключается в *определении нечетких переменных и функций принадлежности*. Нечеткие переменные описывают входы и выходы системы и характеризуются своими значениями и функциями принадлежности. Функции принадлежности определяют степень принадлежности элементов к каждому значению переменной и представляются в виде графиков, где ось x отражает значение переменной, а ось y – степень принадлежности. Целью фаззификации является установление соответствия между конкретным, обычно численным значением отдельной входной переменной системы нечеткого вывода и значением функции принадлежности соответствующего ей терма входной лингвистической переменной. После завершения этого этапа для всех входных переменных должны быть определены конкретные значения функций принадлежности по каждому из лингвистических термов, которые используются в подусловиях базы правил системы нечеткого вывода [49].

Для построения функций принадлежности нечетких множеств существуют прямые и косвенные методы. В прямых методах эксперт либо группа экспертов задают или определеют по соответствующей формуле каждое значение функции принадлежности. Как правило, прямые методы построения функций принадлежности используются для таких свойств, которые могут быть измерены в некоторой количественной шкале.

Как правило, косвенные методы определения значений функции принадлежности используются в тех случаях, когда отсутствуют очевидные измеримые свойства, которые могут быть использованы для построения нечетких моделей рассматриваемой предметной области. В общем случае, собирается мнение экспертов относительно какого-то нечеткого аспекта будущей системы [50]. К таким методам относятся метод опроса, метод лингвистических термов, метод попарного количественного сравнения и другие.

Этап фаззификации включает:

1. Определить число входных и выходных лингвистических переменных (ЛП).
2. Установить число термов для каждой ЛП.
3. Построить ФП для каждого терма каждой ЛП.

Второй этап состоит в *формировании базы правил системы нечеткого вывода*, которые связывают входные и выходные переменные. Правила формулируются в виде условий-заключений с использованием лингвистических термов и операторов нечеткой логики, таких как "И", "ИЛИ" и "НЕ". Каждое правило определяет, какой вывод должен быть сделан в зависимости от текущих значений входных переменных.

Нечеткой базой правил (нечетких продукций) называется совокупность нечетких правил "ЕСЛИ-ТО", определяющих взаимосвязь между входами и выходами исследуемого объекта [51]. Вес входной лингвистической переменной в составлении базы правил важен, поскольку он определяет степень влияния каждой переменной на выходную переменную. Вес должен быть выбран исходя из экспертных знаний области, которая описывается системой. Для определения весовых коэффициентов входных ЛП использовался метод парных сравнений.

Третий этап – *агрегация подусловий и аккумулирование выводов*: Агрегирование подусловий в правилах нечетких продукций заключается в объединении нескольких подусловий в одно, более общее условие. Это позволяет упростить правила и сделать их более лаконичными. В этом этапе объединяются активированные правила и их выводы для получения общего вывода нечеткой системы. Далее, происходит *аккумулирование заключений правил нечетких продукций.* Аккумулирование заключений означает, что выводы нечетких правил объединяются вместе для получения более точного результата.

Последний этап – *дефаззификация*. Дефаззификация выходного значения заключается в преобразовании его из нечеткого в точное значение. Для этого используются различные методы, такие как центр тяжести, среднее значение, максимальное значение и т.д. Методом дефаззификации в модели Мамдани является метод центра тяжести, который вычисляет центр масс нечеткого вывода для определения конкретного значения выходной переменной [52].

Существует несколько методов дефаззификации. В рамках данной работы будет использоваться метод средневзвешенного максимума. Этот метод дает средневзвешенное значение по степени принадлежности значений, при которых все применимые функции принадлежности достигают своего максимального значения. Для расчета используется формула (2) [52, с. 16-18]:

(2)

где *n* – количество квантованных выходных выводов;

*xi* – опорное значение *i*-й функции принадлежности;

– степень принадлежности *i*-й функции

**2.2 Описание нечеткой модели расчета риска ИБ промышленной IoT-системы**

Уровень риска ИБ – это степень вероятности возникновения угроз и ущерба для информационной системы или организации.

Как уже отмечалось, существует несколько общепризнанных стандартов и методологий, которые используются для расчета риска ИБ:

ISO/IEC 27001: Этот стандарт предоставляет требования для системы управления информационной безопасностью (СУИБ) и помогает организациям разрабатывать и поддерживать политику информационной безопасности [53].

ISO/IEC 27005: Этот стандарт предоставляет руководство по управлению рисками информационной безопасности и описывает процесс оценки рисков ИБ, включая идентификацию, анализ и оценку рисков [54].

NIST SP 800-39: Руководство по проведению оценки риска, разработанное Национальным институтом стандартов и технологий США (NIST). Оно предоставляет подробный подход к оценке риска ИБ и управлению рисками на основе стандартов NIST [55].

FAIR (Factor Analysis of Information Risk): Это методология оценки риска ИБ, которая помогает организациям количественно оценивать и анализировать риски, связанные с информационной безопасностью [56].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Это методология оценки риска, разработанная CERT/CC, которая предоставляет структурированный подход к идентификации, оценке и управлению рисками ИБ [57].

Согласно документу “Interoperable EU Risk Management Toolbox” [58] значение уровня риска ИБ есть произведение вероятности реализации угроз на уровень нанесенного ущерба формула (3):

(3)

где *R* – значение уровня риска ИБ,

– вероятность реализации угроз,

– уровень нанесенного ущерба.

Правильное определение критериев риска является важным шагом в процессе оценки рисков, поскольку это позволяет более точно определить вероятность возникновения рисков и потенциальный ущерб. Кроме того, выделение критериев риска также является важным этапом для последующего планирования и реализации мер по управлению рисками.

*Оценка вероятности реализации угроз* – это процесс определения вероятности того, что угроза произойдет в будущем. Вероятность реализации угроз может зависеть от различных факторов, таких как важность информационных активов, наличие соответствующих средств безопасности на программно-техническом, административном и процедурном уровне контроля, а также предыдущие случаи нарушения безопасности.

Согласно стандарту ISO/IEC 27005:2018 "Информационная технология. Методы оценки рисков информационной безопасности" [54] критерии, предназначенные для оценки вероятности реализации угроз, включают:

1. привлекательность актива;
2. доступность актива;
3. ценность актива;
4. конфиденциальность актива;
5. целостность актива;
6. программно-технический контроль;
7. административный контроль;
8. процедурный контроль;
9. соответствие мер контроля стандартам ИБ;
10. предшествующие инциденты.

Предлагаемая модель информационной безопасности рассматривает активы системы промышленного интернета вещей в качестве главного компонента, поэтому были выделены несколько критериев для анализа информационной безопасности активов IIoT-системы. Рассмотрим каждый из них в отдельности

Привлекательность актива – характеристика, показывающая, насколько данный актив интересен для потенциальных злоумышленников, которые могут попытаться получить несанкционированный доступ к активу или его информации.

Доступность актива – характеристика, характеризующая, насколько легко к активу можно получить доступ. Другими словами, если актив легкодоступен, то для данного актива вероятность реализации угроз будет очень высока.

Ценность актива – характеристика, показывающая, насколько важен актив для организации. Ценность актива может быть определена как его стоимость или важность для бизнес-процессов организации. Если актив имеет высокую ценность, то это может стать причиной высокой вероятности реализации угроз.

Конфиденциальность актива – характеристика степени важности сохранения конфиденциальности информации, относящейся к активу. Таким образом, если актив является источником конфиденциальной информации, то это может сделать его более привлекательным для потенциальных злоумышленников.

Целостность актива – характеристика, показывающая, что актив остается в своем первоначальном состоянии и не подвергается несанкционированным изменениям или повреждениям. Если актив имеет высокую целостность, то он сохраняет длительное время свои свойства и функциональность без изменений.

Объединение этих 5 критериев (привлекательность актива, доступность актива, ценность актива, конфиденциальность актива, целостность актива) в один критерий – *значимость актива* - облегчает анализ и понимание безопасности активов в рамках системы IIoT. Включение этих критериев в один общий критерий оценки актива обусловлено их взаимосвязью и консолидированным влиянием на оценку актива в контексте информационной безопасности.

По этой же причине 4 критерия: 1) программно-технический контроль, 2) административный контроль, 3) процедурный контроль, 4) соответствие мер контроля стандартам ИБ – можно объединить еще в один критерий *– существующий контроль*.

Критерии программно-технический контроль, административный контроль, процедурный контроль, соответствие мер контроля стандартам ИБ можно объединить в один критерий - существующего контроля, поскольку они связаны с тем, как управляются и обеспечиваются меры информационной безопасности в организации.

Программно-технический контроль – это меры безопасности, связанные с техническими аспектами ИБ, такими как использование антивирусного программного обеспечения, фаервола и т.д.

Административный контроль – это меры безопасности, связанные с правилами и политиками безопасности, такими как процедуры управления доступом, обучение сотрудников и т.д.

Процедурный контроль – это меры безопасности, связанные с выполнением задач и процедур в рамках информационной безопасности, таких как резервное копирование данных, проверка безопасности системы и т.д.

Соответствие мер контроля стандартам ИБ связано с тем, насколько хорошо организация следует стандартам и рекомендациям в области ИБ промышленных IoT-систем.

Таким образом, все эти критерии можно объединить в один критерий *существующий контроль*, так как они оценивают и описывают уровень контроля, существующего в организации в настоящее время.

В качестве третьего критерия выберем *предшествующие инциденты*. Этот критерий оценивает, были ли ранее совершены атаки на данный актив промышленной IoT-системы. Если были, то вероятность реализации угрозы будет выше, поскольку злоумышленник уже знаком с этим активом и может использовать опыт прошлых атак для более успешной атаки.

*Оценка уровня нанесенного ущерба* – это процесс определения финансовых, операционных, репутационных и других потерь, которые могут возникнуть в результате нарушения информационной безопасности. Потенциальный ущерб складывается из всех затрат, которые понесет организация при реализации угроз на активы промышленной IoT-системы.

Согласно методологии FAIR [56] критерии, предназначенные для оценки потенциального ущерба, включают:

1. ущерб, связанный с затратами на замену оборудования;
2. ущерб от простоя системы;
3. ущерб, связанный с затратами на реагирование;
4. репутационный ущерб.

Первые три критерия имеют консолидированное влияние на ущерб с финансовой точки зрения, поэтому их целесообразно выделить отдельно как *финансовый ущерб.* Таким образом, для оценки уровня нанесенного ущерба нами выбраны два критерия: *финансовый ущерб* и *репутационный ущерб* (нематериальные потери).

Критерий «финансовый ущерб» включает в себя издержки, связанные с восстановлением и ремонтом технических систем, компенсациями, связанными с утратой данных или финансовой информации, а также возможными санкциями или штрафами, применяемыми в случае нарушения соглашений или контрактов. Данный критерий также может охватывать затраты на внедрение дополнительных мер безопасности и предотвращение повторения подобных инцидентов.

Критерий «репутационный ущерб» отражает возможные негативные последствия на имидж организации, доверие клиентов и общественное мнение.

Схематически выбор критериев для оценки риска ИБ представлен на рисунке 3.

ущерб от простоя системы

ценность актива

привлекательность актива

доступность актива

конфиденциальность актива

целостность актива

*Критерий 1*

*Значимость актива*

административный контроль

программно-технический контроль

процедурный контроль

соответствие мер стандартам ИБ

*Критерий 2 Существующий контроль*

предшествующие инциденты

*Критерий 3 Предшествующие инциденты*

*Вероятность реализации угроз*

ущерб, связанный с затратами на реагирование

ущерб, связанный с затратами на замену оборудования

репутационный ущерб

*Критерий 4 Финансовый ущерб*

*Критерий 5 Репутационный ущерб*

**Уровень нанесенного ущерба**

Рисунок 3 – Выбор критериев для оценки риска ИБ

Примечание – Составлено автором

С учетом выбранных критериев была разработана модель для оценки уровня информационного риска в промышленных IoT-системах [59, 60]. В этой модели процесс оценки информационного риска разделен на три последовательных этапа. На первом этапе происходит оценка вероятности появления угроз У1, на втором этапе – вычисление оценка нанесенного ущерба защищаемым активам IIoT-систем У2. На третьем этапе вычисляется оценка риска информационной безопасности *R*.

К1 Значимость актива

К2 Существующий контроль

К3 - Предшествующие инциденты

База нечетких продукционных правил R

для оценки вероятности появления угроз

Дефаззификация

Фаззификация

Агрегирование

Y1 Вероятность реализации угроз

Y2 Уровень нанесенного ущерба

Значение риска ИБ = Вероятность реализации угроз × Уровень нанесенного ущерба

К4 Финансовый ущерб

К5 Ущерб репутации

База нечетких продукционных правил R для оценки проявления нанесенного ущерба

Дефаззифика-ция

Фаззификация

Агрегирование

Рисунок 4 – Система нечеткого логического вывода

Примечание – Составлено автором

Графическая схема модели для оценки уровня риска ИБ промышленной IoT-системы изображена на рисунке 4. Рассмотрим подробнее алгоритм реализации модели.

2.2.1 Определение нечетких переменных и функций принадлежности

На этапе фаззификации определим количество входных и выходных нечетких лингвистических переменных (ЛП) для оценки вероятности реализации угроз и уровня нанесенного ущерба.

*Входными лингвистическими переменными* системы нечеткого вывода для оценки вероятности реализации угроз являются:

− критерий 1 (К1) – значимость актива;

− критерий 2 (К2) – существующий контроль;

− критерий 3 (К3) – предшествующие инциденты.

*Выходная переменная (Y1)* **–** вероятность реализации угроз.

В качестве*входных лингвистических переменных* для оценки нанесенного ущерба были использованы следующие критерии:

− критерий 4 (К4) – финансовый ущерб;

− критерий 5 (К5) – репутационный ущерб.

В качестве *выходной переменной (Y2) –*уровень нанесенного ущерба.

После определения входных и выходных лингвистических переменных необходимо установить число термов для каждой ЛП и построить функцию принадлежности (ФП) для каждого терма каждой ЛП.

*ЛП «Значимость актива»*

Для определения критерия “Значимость актива” был подготовлен опросник с ответами "да" или "нет". Каждый утвердительный ответ равен 1, отрицательный – 0.

1. Имеет ли актив значимость для бизнес-процессов организации?
2. Является ли актив важным для достижения целей организации?
3. Является ли актив уникальным для организации?
4. Есть ли альтернативы, которые могут заменить актив?
5. Содержит ли актив конфиденциальные данные?
6. Есть ли меры защиты, которые защищают конфиденциальность информационного актива?
7. Является ли актив целостным и не подвержен изменению?
8. Есть ли меры защиты, которые защищают целостность актива?
9. Является ли актив легко доступным для нужных пользователей?

Есть ли меры защиты, которые защищают актив от несанкционированного доступа?

Максимальное количество баллов согласно этому опроснику – 10, минимальное – 0. Для определения значений множества ЛП “Значимость актива” данный опросник был предложен 10 экспертам в области информационной безопасности, которые дали оценку (в баллах) тому или иному терму ЛП.

Термы «Очень низкая» (ОН), «Низкая» (Н), «Средняя» (Ср), «Высокая» (В), «Очень высокая» (ОВ) ЛП «Значимость актива» описаны в таблице 5.

Таблица 5 – Описание термов ЛП«Значимость актива»

|  |  |
| --- | --- |
| Значение лингвистического терма | Описание |
| Очень низкая (ОН) | Потеря или изменение актива не имеет последствий для деятельности организации. |
| Низкая (Н) | Актив представляет небольшую значимость, а его потеря имеет небольшое влияние на деятельность организации. |
| Средняя (Ср) | Актив важен, но может быть заменен. Потеря имеет умеренные последствия |
| Высокая (В) | Актив особенно важен для организации и его уничтожение может иметь серьезные последствия для организации |
| Очень высокая (ОВ) | Потеря или изменение актива приводят к критичным последствиям для деятельности организации. |
| Примечание – Составлено автором | |

Результаты опроса экспертов в виде вспомогательной матрицы представлены в таблице 6 (например, 10 экспертов отнесли количество баллов, равное 1, к терму “Очень низкая”, количество баллов – 2 к терму “Очень низкая” 7 экспертов и 3 эксперта к терму “Низкая” и т.д.)

Таблица 6 – Вспомогательная матрица

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Значения базовых термов | Количество баллов | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Очень низкая (ОН) | 10 | 7 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Низкая (Н) | 0 | 3 | 7 | 5 | 2 | 0 | 0 | 0 | 0 | 0 |
| Средняя (Ср) | 0 | 0 | 1 | 5 | 8 | 6 | 3 | 0 | 0 | 0 |
| Высокая (В) | 0 | 0 | 0 | 0 | 0 | 4 | 5 | 6 | 1 | 0 |
| Очень высокая (ОВ) | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 9 | 10 |
| Примечание – Составлено автором | | | | | | | | | | |

Далее по формуле (4) найдем нормализованные значения ЛП «Значимость актива» [43, р. 112]:

(4)

где – нормализованные значения ЛП «Значимость актива»,

– элемент матрицы,

– максимальный элемент строки.

Нормализованные значения ЛП «Значимость актива» представлены в таблице 7.

Таблица 7 – Результирующая матрица

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Значения базовых термов | Количество баллов | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Очень низкая (ОН) | 1 | 0,7 | 0,2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Низкая (Н) | 0 | 0,43 | 1 | 0,71 | 0,29 | 0 | 0 | 0 | 0 | 0 |
| Средняя (Ср) | 0 | 0 | 0,125 | 0,625 | 1 | 0,75 | 0,375 | 0 | 0 | 0 |
| Высокая (В) | 0 | 0 | 0 | 0 | 0 | 0,5 | 0,8 | 1 | 0,17 | 0 |
| Очень высокая (ОВ) | 0 | 0 | 0 | 0 | 0 | 0 | 0,2 | 0,4 | 0,9 | 1 |
| Примечание – Составлено автором | | | | | | | | | | |

С помощью данных таблицы 7 строим график функции принадлежности ЛП «Значимость активов», где по оси *x* отложены нормализованные значения баллов, отданных за тот или иной терм, а по оси *y* – значения функции принадлежности ЛП (рисунок 5).

Рисунок 5 – График ФП ЛП «Значимость актива»

Примечание – Составлено автором

*ЛП «Существующий контроль»*

Значения входной ЛП «Существующий контроль» определяются по количеству мер безопасности в промышленных системах и изменяются в диапазоне [0, 8]. К данным мерам, которые были проанализированы в разделе 1.2, относятся:

1. Защита сетевых узлов: сетевые узлы IIoT системы должны быть защищены с помощью различных методов, таких как использование механизмов аутентификации, авторизации и шифрования данных. Для этого можно использовать различные технологии, такие как VPN, SSL, TLS и другие.
2. Мониторинг сетевой активности: для обнаружения аномальной активности в сети IIoT системы необходимо использовать механизмы мониторинга сетевой активности. Такие механизмы могут помочь быстро обнаружить атаку и принять меры по ее устранению.
3. Аутентификация и авторизация: запрет чтения данных или управляющих сообщений для неавторизованных людей или систем.
4. Защита от физических атак: Физическая защита является важным аспектом безопасности IIoT систем. Для этого необходимо использовать физические механизмы защиты, такие как камеры видеонаблюдения, контроль доступа и другие.
5. Защита от вредоносных программ: для защиты IIoT систем от вредоносных программ необходимо использовать антивирусные программы, брандмауэры и другие средства защиты.
6. Безопасность данных: для обеспечения безопасности данных в IIoT системе необходимо использовать средства шифрования данных, управления доступом и механизмы аудита.
7. Резервное копирование данных: регулярное резервное копирование данных является важным аспектом безопасности IIoT систем. Это поможет минимизировать потери данных в случае угрозы безопасности.
8. Обучение персонала: для обеспечения безопасности IIoT систем необходимо обучать персонал основам безопасности информации. Это поможет повысить уровень осведомленности о возможных угрозах и принимаемых мерах защиты.

Лингвистические термы ЛП «Существующий контроль» описаны в таблице 8.

Таблица 8 – Описание термов ЛП «Существующий контроль»

|  |  |
| --- | --- |
| Значение лингвистического терма | Описание |
| Очень низкий (ОН) | В промышленной IoT-системе только 2 из описанных метода обеспечения информационной безопасности |
| Низкий (Н) | В промышленной IoT-системе используется от 1 до 4 из описанных методов обеспечения информационной безопасности |
| Средний (Ср) | В промышленной IoT-системе используется от 3 до 6 из описанных методов обеспечения информационной безопасности |
| Высокий (В) | В промышленной IoT-системе используется от 5 до 7 из описанных методов обеспечения информационной безопасности |
| Очень высокий (ОВ) | В промышленной IoT-системе используется все 8 из описанных методов обеспечения информационной безопасности |
| Примечание – Составлено автором | |

Таким образом, нормализованные значения ЛП «Существующий контроль» можно задать по формуле (5).

(5)

где – количество методов ИБ, используемых на промышленном объекте.

Нормализованные значения ЛП «Существующий контроль» представлены в таблице 9.

Таблица 9 – Нормализованные значения К2норм

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| *К*2норм | 0,125 | 0,25 | 0,375 | 0,5 | 0,625 | 0,75 | 0,875 | 1 |

Тогда функции принадлежности термов входной лингвистической переменной «Существующий контроль» аналитически задаются следующим образом (6):

|  |  |
| --- | --- |
|  | (6) |
|  |  |
|  |  |
|  |  |
|  |  |

График функций принадлежности ЛП «Существующий контроль» представлен на рисунке 6.

Рисунок 6 – График ФП ЛП «Существующий контроль»

Примечание – Составлено автором

*ЛП* «*Предшествующие инциденты*»

Числовые значения переменной *К3* изменяются в диапазоне [0, 100] и определяются по проценту атакованных компьютеров промышленной системы IIoT за год. На основе анализа отчетов центра реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) [17, р. 1-4] значения терма *К*3 «Предшествующие инциденты», можно выразить формулой (7):

(7)

где – процент атакованных компьютеров промышленной системы IIoT за год,

40% – максимальное пороговое значение.

В таблице 10 описаны термы ЛП «Предшествующие инциденты».

Таблица 10 – Описание термов ЛП «Предшествующие инциденты»

|  |  |
| --- | --- |
| Значение лингвистического терма | Описание |
| Очень низкий (ОН) | Статистика по фактам реализации угроз в защищаемом активе и мотивации к ее реализации не превышает 10%. |
| Низкий (Н) | Статистика по фактам реализации угроз в защищаемом активе и мотивации к ее реализации превышает 5%, но меньше, чем 20%. |
| Средний (Ср) | Статистика по фактам реализации угроз в защищаемом активе и мотивации к ее реализации превышает 15%, но меньше, чем 30%. |
| Высокий (В) | Статистика по фактам реализации угроз в защищаемом активе и мотивации к ее реализации превышает 25%, но меньше, чем 40%. |
| Очень высокий (ОВ) | Статистика по фактам реализации угроз в защищаемом активе и мотивации к ее реализации превышает 35%. |
| Примечание – Составлено автором | |

Нормализованные значения ЛП «Предшествующие инциденты» представлены в таблице 11.

Таблица 11 – Нормализованные значения *К*3норм

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 5% | 10% | 15% | 20% | 25% | 30% | 35% | 40% и выше |
| *К3норм* | 0,125 | 0,25 | 0,375 | 0,5 | 0,625 | 0,75 | 0,875 | 1 |

Тогда функции принадлежности термов входной лингвистической переменной «Предшествующие инциденты» аналитически задаются следующим образом (8):

|  |  |
| --- | --- |
|  | (8) |
|  |  |
|  |  |
|  |  |
|  |  |

График функций принадлежности ЛП «Предшествующие инциденты» представлен на рисунке 7.

Рисунок 7 – График ФП ЛП «Предшествующие инциденты»

*ЛП «Вероятность реализации угроз»*

Установим число термов для выходной ЛП «Вероятность реализации угроз» и построим ФП для каждого терма.

Для задания выходной ЛП«Вероятность реализации угроз» используем пять термов: “Очень низкая”, “Низкая”, “Средняя”, “Высокая”, “Очень высокая”. Границы термов определим, как показано в таблице 12.

Таблица 12 – Описание термов ЛП «Вероятность появления угроз»

|  |  |  |
| --- | --- | --- |
| Терм | Значение | Описание |
| Очень низкая | 0-0,3 | отсутствуют объективные предпосылки для осуществления угрозы |
| Низкая | 0,2-0,5 | объективные предпосылки для реализации угроз существуют, но принятые меры существенно затрудняют ее реализаци |
| Средняя | 0,4-0,7 | объективные предпосылки для реализации угроз существуют, но принятые меры обеспечения безопасности недостаточны |
| Высокая | 0,6-0,9 | объективные предпосылки для реализации угроз существуют |
| Очень высокая | 0,8-1 | объективные предпосылки для реализации угроз существуют, и меры по обеспечению безопасности не приняты |

Функции принадлежности термов выходной лингвистической переменной «Вероятность реализации угроз» аналитически задаются следующим образом (9):

(9)

На рисунке 8 представлен график функций принадлежности выходной переменной «Вероятность реализации угроз».

Рисунок 8 – График ФП выходной переменной

«Вероятность реализации угроз»

Примечание - Составлено автором

В результате были заданы входные лингвистические переменные для первого этапа, определены множества термов и их функции принадлежности. С помощью этих переменных определяется значение вероятности реализации угроз.

Также была задана выходная лингвистическая переменная «Вероятность реализации угроз», определены и описаны терм-множества. Как было описано выше, выходная переменная «Вероятность реализации угроз» является одной из двух критических составляющих для нахождения уровня риска ИБ IIoT-систем.

*ЛП* «*Финансовый ущерб*»

Числовое значение переменной [0, 100] и определяется в процентах затрат на реагирование на атаку и восстановление систем, штрафы, стоимость услуг мониторинга и ущерб от простоя и срыва операций. Для расчета используем формулу (10) [61]:

(10)

где ALE – annual loss expectancy, ожидаемые годовые потери,

D – годовой доход.

Описание термов ЛП «Финансовый ущерб» приведено в таблице 13.

Таблица 13 – Описание термов ЛП «Финансовый ущерб»

|  |  |
| --- | --- |
| Значение терма | Описание |
| Очень низкая | Незначительные затраты, связанные с восстановлением ресурсов, менее 1% годового дохода |
| Низкая | Низкие затраты, связанные с восстановлением ресурсов, 2-4% годового дохода |
| Средняя | Заметные затраты, связанные с восстановлением ресурсов, 4-7% годового дохода |
| Высокая | Большие затраты, связанные с восстановлением ресурсов, 7-10% годового дохода |
| Очень высокая | Очень большие затраты, связанные с восстановлением ресурсов, более 10% годового дохода |

Нормализованные значения *К*4 приведены в таблице 14.

Таблица 14 – Нормализованные значения *К*4

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *К*4 | 1% | 2% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% |
| *К*4норм | 0,1 | 0,2 | 0,3 | 0,4 | 0,5 | 0,6 | 0,7 | 0,8 | 0,9 | 1 |

Функции принадлежности термов входной лингвистической переменной «Финансовый ущерб» аналитически задаются следующим образом (11):

(11)

Рисунок 9 – График функции принадлежности переменной «Финансовый ущерб»

Примечание – Составлено автором

График ФП переменной К4 «Финансовые затраты» представлен на рисунке 9.

*ЛП «Репутационный ущерб»*

Числовое значение переменной *К5* определяется в процентах потерь из-за негативного отношения клиентов, партнёров и инвесторов к компании.

Для расчета используем формулу (12):

(12)

где P – потери из-за негативного отношения клиентов, партнёров и инвесторов к компании за последний год.

D – годовой доход.

Описание термов ЛП «Репутационный ущерб» приведено в таблице 15.

Таблица 15 – Описание термов ЛП «Репутационный ущерб»

|  |  |
| --- | --- |
| Значение терма | Описание |
| Очень низкая | Незначительные затраты, связанные с восстановлением ресурсов, менее 1% годового дохода |
| Низкая | Низкие затраты, связанные с восстановлением ресурсов, 2-4% годового дохода |
| Средняя | Заметные затраты, связанные с восстановлением ресурсов, 4-7% годового дохода |
| Высокая | Большие затраты, связанные с восстановлением ресурсов, 7-10% годового дохода |
| Очень высокая | Очень большие затраты, связанные с восстановлением ресурсов, более 10% годового дохода |
| Примечание – Составлено автором | |

Нормализованные значения *К*5 приведены в таблице 16.

Таблица 16 – Нормализованные значения *К*5

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *К*5 | 1% | 2% |  | 3% | 5% | 6% | 7% | 8% | 9% | 10% |
| *К*5норм | 0,1 | 0,2 | 0,3 | 0,4 | 0,5 | 0,6 | 0,7 | 0,8 | 0,9 | 1 |

Функции принадлежности термов входной лингвистической переменной «Репутационный ущерб» аналитически задаются следующим образом (13):

(13)

Рисунок 10 – График ФП ЛП «Ущерб репутации»

Примечание – Составлено автором

График ФП переменной «Репутационный ущерб» представлен на рисунке 10.

*ЛП «Уровень нанесенного ущерба»*

То же самое проделаем для *выходной ЛП* «Уровень нанесенного ущерба».

Установим число термов для *выходной ЛП «*Уровень нанесенного ущерба» и построим ФП для каждого терма.

Для задания выходной ЛП«Уровень нанесенного ущерба» используем пять термов: “Очень низкий”, “Низкий”, “Средний”, “Высокий”, “Очень высокий”.

Описание термов ФП *выходной ЛП* «Уровень нанесенного ущерба» представлены в таблице 17.

Таблица 17 – Описание термов ЛП «Уровень нанесенного ущерба»

|  |  |  |
| --- | --- | --- |
| Терм | Значение | Описание |
| Очень низкий | 0-0,3 | Уровень нанесенного ущерба практически не влияет на деятельность объекта |
| Низкий | 0,2-0,5 | Уровень нанесенного ущерба немного влияет на деятельность объекта |
| Средний | 0,4-0,7 | Уровень нанесенного ущерба затрудняет деятельность объекта |
| Высокий | 0,6-0,9 | Ущерб достаточно высокий |
| Очень высокий | 0,8-1 | Уровень нанесенного ущерба очень сильно на деятельность объекта |
| Примечание – Составлено автором | | |

Функции принадлежности термов выходной лингвистической переменной «Уровень нанесенного ущерба» аналитически задаются следующим образом (14):

(14)

На рисунке 11 показан график ФП переменной «Уровень нанесенного ущерба».

Рисунок 11 – График ФП выходной переменной «Уровень нанесенного ущерба»

Примечание – Составлено автором

В результате были заданы входные лингвистические переменные для второго этапа, определены множества термов и их функции принадлежности. При помощи данных переменных определяется уровень нанесенного ущерба.

Также была задана выходная лингвистическая переменная «Уровень нанесенного ущерба», определены и описаны терм-множества. Как было описано выше, уровень риска ИБ промышленных IoT-систем есть произведение двух величин: вероятности реализации угроз и уровня нанесенного ущерба.

2.2.2 Определение весов критериев

После того как были заданы лингвистические переменные, необходимо определить вес каждой входной ЛП (критерия), поскольку это определяет степень влияния каждой переменной в формировании значения выходной переменной.

Для расчета веса каждого критерия был использован метод парных сравнений [62]. Для применения метода парных сравнений нужно построить матрицу парных сравнений, представляющая собой матрицу, которая строится путем сравнения определенного элемента в верхнем слое со всеми элементами, связанными с ним в этом слое. Таким образом, матрица суждения представлена в формуле (15).

(15)

В приведенной выше матрице относится к отношению важности элемента i и элемента j с точки зрения критерия H и удовлетворяет . могут быть предоставлены экспертами, знакомыми с проблемами, лицами, принимающими решения, или аналитиками посредством технических консультаций. Пусть задано *n* элементов, или объектов, *a1, …, an*. Для каждого элемента определен некоторый вес ω*i*, *i = 1, …, n*, и выполняется условие ω*1* + … + ω*m* = 1. Тогда можно построить матрицу V относительных весов.

Каждый элемент *vij* > 0 матрицы относительных весов представляет собой отношение веса *i*-го объекта *аi* к весу *j*-го объекта *аj*, т.е. *vij* = ω*i* / ω*j* для любых *i, j* =1,...*n*. Элементы матрицы, расположенные симметрично относительно главной диагонали, являются обратными по отношению друг к другу, т.е. *vij* = 1/ *vji* для любых *i, j* =1,...*n*.

При заполнении матрицы парных сравнений обычно эксперт определяет только *n* (*n* – 1)/2 элементов матрицы. Это могут быть, например, элементы выше диагонали. Элементы ниже диагонали вычисляются из условия *vij* = 1/ *vji*. Элементы, принадлежащие диагонали матрицы равны единице. Для того чтобы упростить процедуру получения экспертных оценок элементов матрицы парных сравнений, значения *vij*; могут выбираться из фиксированной шкалы, например, 1/9, 1/8, 1/7, …1/2, 1, 2, 3, …, 8, 9.

В процессе аналитической иерархии сравнение двух элементов может стать количественным в соответствии с методом шкалы Саати от 1 до 9, как показано в таблице 18.

Таблица 18 – Метод шкалы Саати от 1 до 9

|  |  |
| --- | --- |
| Значение | Сравнение двух элементов |
| 1 | оба элемента одинаково важны |
| 3 | один элемент немного важнее другого элемента |
| 5 | один элемент явно важнее другого |
| 7 | один элемент значительно важнее другого элемента |
| 9 | один элемент абсолютно важнее другого элемента |
| 2, 4, 6, 8 | промежуточные случаи |
| обратное число выше | отношение важности элемента i и элемента j равно , поэтому отношение важности элемента j и элемента i равно |
| Примечание – Составлено по источнику [50, с. 99] | |

По формуле (16) рассчитываем собственный вектор [63].

(16)

Далее для нахождения весов критериев используем формулу (17):

|  |  |
| --- | --- |
|  | (17) |

Рассчитаем веса для критериев, оценивающих вероятность реализации угроз. В оценке критериев принимало участие 5 экспертов – инженеров ИБ с практическим опытом работы не менее 3 лет. В таблицах 19, 20, 21, 22 ,23 представлены комплексные результаты попарного сравнения экспертов.

Таблица 19 – Результаты попарного сравнения эксперта 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | К1 | К2 | К3 |  | ω |
| Привлекательность актива | 1 | 0,5 | 3 | 1,14 | 0,348739 |
| Существующий контроль | 2 | 1 | 2 | 1,59 | 0,483604 |
| Предшествующие инциденты | 0,33333 | 0,5 | 1 | 0,55 | 0,167656 |

Таблица 20 – Результаты попарного сравнения эксперта 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | К1 | К2 | К3 |  | ω |
| Привлекательность актива | 1 | 1 | 2 | 1,26 | 0,387371 |
| Существующий контроль | 1 | 1 | 3 | 1,44 | 0,443429 |
| Предшествующие инциденты | 0,5 | 0,33333 | 1 | 0,55 | 0,1692 |

Таблица 21 – Результаты попарного сравнения эксперта 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | К1 | К2 | К3 |  | ω |
| Привлекательность актива | 1 | 2 | 1 | 1,26 | 0,412599 |
| Существующий контроль | 0,5 | 1 | 2 | 1,00 | 0,32748 |
| Предшествующие инциденты | 1 | 0,5 | 1 | 0,79 | 0,259921 |

Таблица 22 – Результаты попарного сравнения эксперта 4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | К1 | К2 | К3 |  | ω |
| Привлекательность актива | 1 | 0,5 | 2 | 1,00 | 0,371053 |
| Существующий контроль | 0,5 | 1 | 3 | 1,14 | 0,424749 |
| Предшествующие инциденты | 0,5 | 0,33333 | 1 | 0,55 | 0,204198 |

Таблица 23 – Результаты попарного сравнения эксперта 5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | К1 | К2 | К3 |  | ω |
| Привлекательность актива | 1 | 3 | 2 | 1,82 | 0,539615 |
| Существующий контроль | 0,3333 | 1 | 3 | 1,00 | 0,296961 |
| Предшествующие инциденты | 0,5 | 0,3333 | 1 | 0,55 | 0,163424 |

Таблица 24 – Веса критереив

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Критерии | Э1 | Э2 | Э3 | Э4 | Э5 | ω |
| Привлекательность актива | 0,34874 | 0,38737 | 0,4126 | 0,37105 | 0,53961 | 0,412 |
| Существующий контроль | 0,4836 | 0,44343 | 0,32748 | 0,42475 | 0,29696 | 0,395 |
| Предшествующие инциденты | 0,16766 | 0,1692 | 0,25992 | 0,2042 | 0,16342 | 0,193 |
| Итого |  |  |  |  |  | 1 |
| Примечание – Составлено автором | | | | | | |

Результаты сравнения весов критериев приведены в таблице 24. На рисунке 12 показана диаграмма весовых коэффициентов критериев, оценивающих вероятность реализации угроз.

Рисунок 12 – Веса критериев для оценки вероятности появления угроз

Примечание – Составлено автором

Аналогично рассчитаем веса для критериев, оценивающих уровень потенциального ущерба. В таблице 25 приведены результаты сравнения весов критериев. На рисунке 13 показана диаграмма весовых коэффициентов критериев, оценивающих уровень нанесенного ущерба.

Таблица 25 – Веса критериев

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Критерии |  | Э1 | Э2 | Э3 | Э4 | Э5 | ω |
| Финансовые затраты | К4 | 0,6667 | 0,3333 | 0,6667 | 0,75 | 0,5 | 0,58334 |
| Ущерб репутации | К5 | 0,3333 | 0,6667 | 0,3333 | 0,25 | 0,5 | 0,41666 |
| Итого | |  |  |  |  |  | 1 |
| Примечание – Составлено автором | | | | | | | |

Рисунок 13 – Вес критериев для оценки для оценки проявления нанесенного ущерба

Примечание – Составлено автором

Были определены весовые коэфициенты каждой входной лингвистической переменной, что позволит составить корректную базу нечетких продукционных правил, учитывая степень влияния каждой переменной в формировании значения выходной переменной.

2.2.3 Формирование базы нечетких продукционных правил

На этапе формирования базы правил системы нечеткого вывода необходимо определить связь между входными и выходными лингвистическими переменными.

После того, как определены нечеткие входные и выходные переменные, функции принадлежности, а также весовые коэффициенты критериев К1 – К5 создадим *базу продукционных правил для оценки вероятности появления угроз* (таблица 26), где К1 … К3 – значения термов входных лингвистических переменных, с соответствующими весовыми коэффициентами, У1 – значение терма выходной лингвистической переменной.

Таблица 26 – База нечетких продукционных правил для оценки вероятности появления угроз

|  |  |  |  |
| --- | --- | --- | --- |
| К1 Привлекательность активов  ω1 =0,412 | К2 Существующий контроль  ω2 =0,395 | К3 предшествующие инциденты  ω3 =0,193 | У1 Вероятность возникновения угрозы |
| 1 | 2 | 3 | 4 |
| ОН | ОН | ОН | Ср |
| ОН | ОН | Н | Ср |
| ОН | ОН | Ср | Ср |
| ОН | ОН | В | Ср |
| ОН | ОН | ОВ | Ср |
| ОН | Н | ОН | Н |
| ОН | Н | Н | Ср |
| ОН | Н | Ср | Ср |
| ОН | Н | В | Ср |
| ОН | Н | ОВ | Ср |
| ОН | Ср | ОН | Н |
| ОН | Ср | Н | Н |
| ОН | Ср | Ср | Н |
| ОН | Ср | В | Ср |
| ОН | Ср | ОВ | Ср |
| ОН | В | ОН | ОН |
| ОН | В | Н | ОН |
| ОН | В | Ср | Н |
| ОН | В | В | Н |
| ОН | В | ОВ | Н |
| ОН | ОВ | ОН | ОН |
| ОН | ОВ | Н | ОН |
| ОН | ОВ | Ср | Н |
| ОН | ОВ | В | Н |
| Продолжение таблицы 26 | | | |
| 1 | 2 | 3 | 4 |
| ОН | ОВ | ОВ | Н |
| Н | ОН | ОН | Ср |
| Н | ОН | Н | Ср |
| Н | ОН | Ср | Ср |
| Н | ОН | В | В |
| Н | ОН | ОВ | В |
| Н | Н | ОН | Ср |
| Н | Н | Н | Ср |
| Н | Н | Ср | Ср |
| Н | Н | В | Ср |
| Н | Н | ОВ | Ср |
| Н | Ср | ОН | Н |
| Н | Ср | Н | Н |
| Н | Ср | Ср | Ср |
| Н | Ср | В | Ср |
| Н | Ср | ОВ | Ср |
| Н | В | ОН | Н |
| Н | В | Н | Н |
| Н | В | Ср | Н |
| Н | В | В | Н |
| Н | В | ОВ | Ср |
| Н | ОВ | ОН | ОН |
| Н | ОВ | Н | Н |
| Н | ОВ | Ср | Н |
| Н | ОВ | В | Н |
| Н | ОВ | ОВ | Н |
| Ср | ОН | ОН | В |
| Ср | ОН | Н | В |
| Ср | ОН | Ср | В |
| Ср | ОН | В | В |
| Ср | ОН | ОВ | В |
| Ср | Н | ОН | Ср |
| Ср | Н | Н | Ср |
| Ср | Н | Ср | В |
| Ср | Н | В | В |
| Ср | Н | ОВ | В |
| Ср | Ср | ОН | Ср |
| Ср | Ср | Н | Ср |
| Ср | Ср | Ср | Ср |
| Ср | Ср | В | Ср |
| Ср | Ср | ОВ | Ср |
| Ср | В | ОН | Н |
| Ср | В | Н | Ср |
| Ср | В | Ср | Ср |
| Ср | В | В | Ср |
| Продолжение таблицы 26 | | | |
| 1 | 2 | 3 | 4 |
| Ср | В | ОВ | Ср |
| Ср | ОВ | ОН | Н |
| Ср | ОВ | Н | Н |
| Ср | ОВ | Ср | Ср |
| Ср | ОВ | В | Ср |
| Ср | ОВ | ОВ | Ср |
| В | ОН | ОН | В |
| В | ОН | Н | В |
| В | ОН | Ср | В |
| В | ОН | В | ОВ |
| В | ОН | ОВ | ОВ |
| В | Н | ОН | В |
| В | Н | Н | В |
| В | Н | Ср | В |
| В | Н | В | В |
| В | Н | ОВ | В |
| В | Ср | ОН | Ср |
| В | Ср | Н | Ср |
| В | Ср | Ср | В |
| В | Ср | В | В |
| В | Ср | ОВ | В |
| В | В | ОН | Ср |
| В | В | Н | Ср |
| В | В | Ср | Ср |
| В | В | В | Ср |
| В | В | ОВ | Ср |
| В | ОВ | ОН | Ср |
| В | ОВ | Н | Ср |
| В | ОВ | Ср | Ср |
| В | ОВ | В | Ср |
| В | ОВ | ОВ | Ср |
| ОВ | ОН | ОН | В |
| ОВ | ОН | Н | В |
| ОВ | ОН | Ср | ОВ |
| ОВ | ОН | В | ОВ |
| ОВ | ОН | ОВ | ОВ |
| ОВ | Н | ОН | В |
| ОВ | Н | Н | В |
| ОВ | Н | Ср | В |
| ОВ | Н | В | В |
| ОВ | Н | ОВ | ОВ |
| ОВ | Ср | ОН | В |
| ОВ | Ср | Н | В |
| ОВ | Ср | Ср | В |
| ОВ | Ср | В | В |
| Продолжение таблицы 26 | | | |
| 1 | 2 | 3 | 4 |
| ОВ | Ср | ОВ | В |
| ОВ | В | ОН | Ср |
| ОВ | В | Н | Ср |
| ОВ | В | Ср | Ср |
| ОВ | В | В | В |
| ОВ | В | ОВ | В |
| ОВ | ОВ | ОН | Ср |
| ОВ | ОВ | Н | Ср |
| ОВ | ОВ | Ср | Ср |
| ОВ | ОВ | В | Ср |
| ОВ | ОВ | ОВ | В |
| Примечание – Составлено автором | | | |

Учитывая имеющееся разбиение диапазона значений аргумента *Кi* , *i* =1,5 и значений функции У1 (У2), сформулируем высказывания на естественном языке. Для составления лингвистического правила вида “ЕСЛИ.., ТО …” требуется в соответствии с грамматикой лингвистических переменных выбрать термы, соответствующие табличным значениям *Кi* и У1 (У2). (Если система обладает двумя или более входами, то используем логическую связку “И”). Генерация базы правил происходит для каждого столбца таблично заданной функции следующим образом: каждому значению ставим в соответствие элемент терм-множества, к которому оно относится.

Так как 3 входных лингвистических переменных могут принимать 5 значений термов, рассмотрев всевозможные варианты, всего в базу было внесено 53=125 нечетких продукционных правил.

После формирования базы правил системы нечеткого выводанеобходимо агрегировать подусловия в правилах нечетких продукций, т.е. объединенить несколько подусловий в одно, более общее условие. Агрегация правил нечеткой продукции осуществляется при помощи классической нечеткой логической операции «И» двух элементарных высказываний [64]. В результате агрегации получившихся правил были получены нечеткие причинно-следственные отношения между антецедентами и консеквентом (Таблица 27).

Например, для правила R1 в таблице 27 антецедентом является объединенные при помощи конъюнкции условия правил 16, 17, 21, 22, 46 (таблица 26), а консеквентом – следствие этих правил, равное значению “очень низкий”.

Таблица 27 – Агрегированные нечеткие правила для оценки вероятности возникновения угрозы

|  |  |  |
| --- | --- | --- |
| Правило | Антецедент | Консеквент |
| 1 | 2 | 3 |
| R1 | (К1=ОН) ∧ (К2=В) ∧ (К3=ОН) ∨  (К1=ОН) ∧ (К2=В) ∧ (К3=Н) ∨  (К1=ОН) ∧ (К2=ОВ) ∧ (К3=ОН) ∨  (К1=ОН) ∧ (К2=ОВ) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=ОВ) ∧ (К3=ОН) | У1=ОН |
| R2 | (К1=ОН) ∧ (К2=Н) ∧ (К3=ОН) ∨  (К1=ОН) ∧ (К2=Ср) ∧ (К3=ОН) ∨  (К1=ОН) ∧ (К2= Ср) ∧ (К3=Н) ∨  (К1=ОН) ∧ (К2=Ср) ∧ (К3=Ср) ∨  (К1=ОН) ∧ (К2=В) ∧ (К3=Ср) ∨  (К1=ОН) ∧ (К2=В) ∧ (К3=В) ∨  (К1=ОН) ∧ (К2=В) ∧ (К3=ОВ) ∨  (К1=ОН) ∧ (К2=ОВ) ∧ (К3=Ср) ∨  (К1=ОН) ∧ (К2=ОВ) ∧ (К3=В) ∨  (К1=ОН) ∧ (К2=ОВ) ∧ (К3=ОВ) ∨  (К1=Н) ∧ (К2=Ср) ∧ (К3=ОН) ∨  (К1=Н) ∧ (К2=Ср) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=В) ∧ (К3=ОН) ∨  (К1=Н) ∧ (К2=В) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=В) ∧ (К3=Ср) ∨  (К1=Н) ∧ (К2=В) ∧ (К3=В) ∨  (К1=Н) ∧ (К2=ОВ) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=ОВ) ∧ (К3=Ср) ∨  (К1=Н) ∧ (К2=ОВ) ∧ (К3=В) ∨  (К1=Н) ∧ (К2=ОВ) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=В) ∧ (К3=ОН) ∨  (К1=Ср) ∧ (К2=ОВ) ∧ (К3=ОН) ∨  (К1=Ср) ∧ (К2=ОВ) ∧ (К3=Н) | У1=Н |
| R3 | (К1=ОН) ∧ (К2=ОН) ∧ (К3=ОН) ∨  (К1=ОН) ∧ (К2=ОН) ∧ (К3=Н) ∨  (К1=ОН) ∧ (К2=ОН) ∧ (К3=Ср) ∨  (К1=ОН) ∧ (К2=ОН) ∧ (К3=В) ∨  (К1=ОН) ∧ (К2=ОН) ∧ (К3=ОВ) ∨  (К1=ОН) ∧ (К2=Н) ∧ (К3=Н) ∨  (К1=ОН) ∧ (К2=Н) ∧ (К3=Ср) ∨  (К1=ОН) ∧ (К2=Н) ∧ (К3=В) ∨  (К1=ОН) ∧ (К2=Н) ∧ (К3=ОВ) ∨  (К1=ОН) ∧ (К2= Ср) ∧ (К3=В) ∨  (К1=ОН) ∧ (К2= Ср) ∧ (К3=ОВ) ∨  (К1=Н) ∧ (К2=ОН) ∧ (К3=ОН) ∨  (К1=Н) ∧ (К2=ОН) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=ОН) ∧ (К3=Ср) ∨  (К1=Н) ∧ (К2=Н) ∧ (К3=ОН) ∨  (К1=Н) ∧ (К2=Н) ∧ (К3=Н) ∨  (К1=Н) ∧ (К2=Н) ∧ (К3=Ср) ∨  (К1=Н) ∧ (К2=Н) ∧ (К3=В) ∨ | У1=СР |
| Продолжение таблицы 27 | | |
| 1 | 2 | 3 |
|  | (К1=Н) ∧ (К2=Н) ∧ (К3=ОВ) ∨  (К1=Н) ∧ (К2=Ср) ∧ (К3=Ср) ∨  (К1=Н) ∧ (К2= Ср) ∧ (К3=В) ∨  (К1=Н) ∧ (К2= Ср) ∧ (К3=ОВ) ∨  (К1=Н) ∧ (К2=В) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=Н) ∧ (К3=ОН) ∨  (К1=Ср) ∧ (К2=Н) ∧ (К3=Н) ∨  (К1=Ср) ∧ (К2=Ср) ∧ (К3=ОН) ∨  (К1=Ср) ∧ (К2=Ср) ∧ (К3=Н) ∨  (К1=Ср) ∧ (К2=Ср) ∧ (К3=Ср) ∨  (К1=Ср) ∧ (К2=Ср) ∧ (К3=В) ∨  (К1=Ср) ∧ (К2=Ср) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=В) ∧ (К3=Н) ∨  (К1=Ср) ∧ (К2=В) ∧ (К3=Ср) ∨  (К1=Ср) ∧ (К2=В) ∧ (К3=В) ∨  (К1=Ср) ∧ (К2=В) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=ОВ) ∧ (К3=Ср) ∨  (К1=Ср) ∧ (К2=ОВ) ∧ (К3=В) ∨  (К1=Ср) ∧ (К2=ОВ) ∧ (К3=ОВ) ∨  (К1=В) ∧ (К2=Ср) ∧ (К3=ОН) ∨  (К1=В) ∧ (К2=Ср) ∧ (К3=Н) ∨  (К1=В) ∧ (К2=В) ∧ (К3=ОН) ∨  (К1=В) ∧ (К2=В) ∧ (К3=Н) ∨  (К1=В) ∧ (К2=В) ∧ (К3=Ср) ∨  (К1=В) ∧ (К2=В) ∧ (К3=В) ∨  (К1=В) ∧ (К2=В) ∧ (К3=ОВ) ∨  (К1=В) ∧ (К2=ОВ) ∧ (К3=ОН) ∨  (К1=В) ∧ (К2=ОВ) ∧ (К3=Н) ∨  (К1=В) ∧ (К2=ОВ) ∧ (К3=Ср) ∨  (К1=В) ∧ (К2=ОВ) ∧ (К3=В) ∨  (К1=В) ∧ (К2=ОВ) ∧ (К3=ОВ) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=ОН) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=Н) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=Ср) ∨  (К1=ОВ) ∧ (К2=ОВ) ∧ (К3=ОН) ∨  (К1=ОВ) ∧ (К2=ОВ) ∧ (К3=Н) ∨  (К1=ОВ) ∧ (К2=ОВ) ∧ (К3=Ср) ∨  (К1=ОВ) ∧ (К2=ОВ) ∧ (К3=В) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=ОВ) |  |
| R4 | (К1=Н) ∧ (К2=ОН) ∧ (К3=В) ∨  (К1=Н) ∧ (К2=ОН) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=ОН) ∧ (К3=ОН) ∨  (К1=Ср) ∧ (К2=ОН) ∧ (К3=Н) ∨  (К1=Ср) ∧ (К2=ОН) ∧ (К3=Ср) ∨  (К1=Ср) ∧ (К2=ОН) ∧ (К3=В) ∨  (К1=Ср) ∧ (К2=ОН) ∧ (К3=ОВ) ∨  (К1=Ср) ∧ (К2=Н) ∧ (К3=Ср) ∨  (К1=Ср) ∧ (К2=Н) ∧ (К3=В) ∨ | У1=В |
| Продолжение таблицы 27 | | |
| 1 | 2 | 3 |
|  | (К1=Ср) ∧ (К2=Н) ∧ (К3=ОВ) ∨  (К1=В) ∧ (К2=ОН) ∧ (К3=ОН) ∨  (К1=В) ∧ (К2=ОН) ∧ (К3=Н) ∨  (К1=В) ∧ (К2=ОН) ∧ (К3=Ср) ∨  (К1=В) ∧ (К2=Н) ∧ (К3=ОН) ∨  (К1=В) ∧ (К2=Н) ∧ (К3=Н) ∨  (К1=В) ∧ (К2=Н) ∧ (К3=Ср) ∨  (К1=В) ∧ (К2=Н) ∧ (К3=В) ∨  (К1=В) ∧ (К2=Н) ∧ (К3=ОВ) ∨  (К1=В) ∧ (К2=Ср) ∧ (К3=Ср) ∨  (К1=В) ∧ (К2=Ср) ∧ (К3=В) ∨  (К1=В) ∧ (К2=Ср) ∧ (К3=ОВ) ∨ (К1=ОВ) ∧ (К2=ОН) ∧ (К3=ОН) ∨  (К1=ОВ) ∧ (К2=ОН) ∧ (К3=Н) ∨  (К1=ОВ) ∧ (К2=ОН) ∧ (К3=Ср) ∨  (К1=ОВ) ∧ (К2=Н) ∧ (К3=ОН) ∨  (К1=ОВ) ∧ (К2=Н) ∧ (К3=Н) ∨  (К1=ОВ) ∧ (К2=Н) ∧ (К3=Ср) ∨  (К1=ОВ) ∧ (К2=Н) ∧ (К3=В) ∨  (К1=ОВ) ∧ (К2=Ср) ∧ (К3=ОН) ∨  (К1=ОВ) ∧ (К2= Ср) ∧ (К3=Н) ∨  (К1=ОВ) ∧ (К2= Ср) ∧ (К3=Ср) ∨  (К1=ОВ) ∧ (К2= Ср) ∧ (К3=В) ∨  (К1=ОВ) ∧ (К2= Ср) ∧ (К3=ОВ) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=В) ∨  (К1=ОВ) ∧ (К2=В) ∧ (К3=ОВ) ∨ |  |
| R5 | (К1=В) ∧ (К2=ОН) ∧ (К3=В) ∨  (К1=В) ∧ (К2=ОН) ∧ (К3=ОВ) ∨  (К1=ОВ) ∧ (К2=ОН) ∧ (К3=В) ∨  (К1=ОВ) ∧ (К2=ОН) ∧ (К3=ОВ) ∨  (К1=ОВ) ∧ (К2=Н) ∧ (К3=ОВ) | У1=ОВ |
| Примечание – Составлено автором | | |

Аналогично сформируем базу правил *системы нечеткого вывода* для оценки проявления нанесенного ущерба угрозами на защищаемые активы IIoT-систем. База правил нечетких продукций представлена в таблице 28, где по горизонтали К4,К5 – это значения термов входных лингвистических переменных, У2 – значение терма выходной лингвистической переменной, по вертикали 1…9 – правила нечеткой базы [65].

Таблица 28 – База нечетких продукционных правил для оценки проявления нанесенного ущерба

|  |  |  |
| --- | --- | --- |
| К4 Финансовые затраты  ω4 =0,583 | К5 Ущерб репутации  ω5 = 0,417 | У2 Проявление нанесенного ущерба |
| ОН | ОН | ОН |
| ОН | Н | ОН |
| ОН | Ср | Н |
| ОН | В | Ср |
| ОН | ОВ | Ср |
| Н | ОН | Н |
| Н | Н | Н |
| Н | Ср | Н |
| Н | В | Ср |
| Н | ОВ | Ср |
| Ср | ОН | Н |
| Ср | Н | Ср |
| Ср | Ср | Ср |
| Ср | В | В |
| Ср | ОВ | В |
| В | ОН | Ср |
| В | Н | Ср |
| В | Ср | В |
| В | В | В |
| В | ОВ | ОВ |
| ОВ | ОН | Ср |
| ОВ | Н | В |
| ОВ | Ср | В |
| ОВ | В | ОВ |
| ОВ | ОВ | ОВ |
| Примечание – Составлено автором | | |

Всего в базу было внесено 25 нечетких продукционных правил. В результате агрегации получившихся правил, были получены нечеткие причинно-следственные отношения между антецедентами и консеквентом (таблица 29).

Таблица 29 – Агрегированные нечеткие правила для оценки проявления нанесенного ущерба

|  |  |  |
| --- | --- | --- |
| Правило | Антецедент | Консеквент |
| 1 | 2 | 3 |
| R6 | (К4=ОН) ∧ (К5=ОН) ∨  (К4=ОН) ∧ (К5=Н) | У2=ОН |
| R7 | (К4=ОН) ∧ (К5=Ср) ∨  (К4=Н) ∧ (К5=ОН) ∨  (К4=Н) ∧ (К5=Н) ∨  (К4=Н) ∧ (К5=СР) ∨ | У2=Н |
| Продолжение таблицы 29 | | |
| 1 | 2 | 3 |
|  | (К4=Ср) ∧ (К5=ОН) (К4=Ср) ∧ (К5=ОН) |  |
| R8 | (К4=ОН) ∧ (К5=В) ∨  (К4=ОН) ∧ (К5=ОВ) ∨  (К4=Н) ∧ (К5=В) ∨  (К4=Н) ∧ (К5=ОВ) ∨  (К4=СР) ∧ (К5=Н) ∨  (К4=СР) ∧ (К5=СР) ∨  (К4=В) ∧ (К5=ОН) ∨  (К4=В) ∧ (К5=Н) ∨  (К4=ОВ) ∧ (К5=ОН) | У2=СР |
| R9 | (К4=СР) ∧ (К5=В) ∨  (К4=СР) ∧ (К5=ОВ) ∨  (К4=В) ∧ (К5=Ср) ∨  (К4=В) ∧ (К5=В) ∨  (К4=ОВ) ∧ (К5=Н) ∨  (К4=ОВ) ∧ (К5=Ср) | У2=В |
| R10 | (К4=В) ∧ (К5=ОВ) ∨  (К4=ОВ) ∧ (К5=В) ∨  (К4=ОВ) ∧ (К5=ОВ) | У2=ОВ |
| Примечание – Составлено автором | | |

В результате мы получили базы нечетких правил для определения оценки вероятности возникновения угрозы Y1 и оценки нанесенного ущерба Y2. Эти параметры (Y1 и Y2) можно использовать для вычисления чёткого выходного значения уровня риска *R* по формуле (3).

Для перевода чёткого выходного значения уровня риска используем таблицу 30.

Таблица 30 – Расчетные уровни риска

|  |  |  |
| --- | --- | --- |
| Рассчитанный уровень риска | Границы | Описание |
| 1 | 2 | 3 |
| Очень низкий | [0; 0,1) | Очень низкий риск означает, что можно ожидать незначительное неблагоприятное воздействие на деятельность организации, активы организации. |
| Низкий | [0,1; 0,25) | Низкий риск означает, что можно ожидать ограниченное неблагоприятное воздействие на деятельность организации, активы организации. |
| Средний | [0,25; 0,4225) | Средний риск означает, что угрозы могут оказать серьезное неблагоприятное воздействие на деятельность организации, активы организации, отдельных лиц, другие организации. |
| Высокий | [0,4225; 0,7225) | Высокий риск означает, что угрозы могут оказать серьезное или катастрофическое неблагоприятное воздействие на деятельность организации, активы организации. |
| Продолжение таблицы 30 | | |
| 1 | 2 | 3 |
| Очень высокий | [0,7225; 1] | Очень высокий риск означает, что можно ожи дать, угрозы привести к множественным серьез ным или катастрофически неблагоприятным последствия для деятельности организации, активов организации. |
| Примечание – Составлено автором | | |

Теперь оценим корректность работы предложенной модели нечеткого вывода на нескольких примерах.

*Пример 1.*

Пусть на вход системы поступили значения, представленные в таблице 31.

Таблица 31 – Входные значения системы нечеткого вывода

|  |  |
| --- | --- |
| Лингвистические переменные | Нормализованные значения |
| Значимость актива | 0.25 |
| Существующий контроль | 0.2 |
| Предшествующие инциденты | 0.55 |
| Финансовый ущерб | 0.7 |
| Репутационный ущерб | 0.3 |

Сначала найдём степени истинности µА(х) для данных входных лингвистических переменных. Для этого рассмотрим процесс фаззификации пяти нечетких высказываний: «Значимость актива очень низкая», «Значимость актива низкая», «Значимость актива средняя», «Значимость актива высокая» и «Значимость актива очень высокая» для входной ЛП «Значимость актива».

Используя построенные ФП (см. рисунок 5), определим степени истинности ЛП «Значимость актива» (рисунок 14).

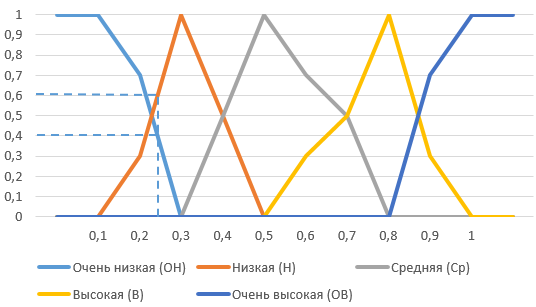


Рисунок 14 – Определение функции принадлежности ЛП

«Значимость актива»

Примечание – Составлено автором

µк1\_он = 0,4, µк1\_н = 0,6, µк1\_ср = 0, µк1\_в = 0, µк1\_ов = 0

Аналогично найдём степени истинности µА(х) для входных ЛП «Существующий контроль», «Предшествующие инциденты». Результаты фаззификации представлены в таблице 32.

Таблица 32 – Значения степени истинности µА(х) входных переменных для оценки вероятности появления угроз

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| Значимость актива | ОН | 0,4 |
| Н | 0,6 |
| Ср | 0 |
| В | 0 |
| ОВ | 0 |
| Существующий контроль | ОН | 0,3 |
| Н | 0,7 |
| Ср | 0 |
| В | 0 |
| ОВ | 0 |
| Предшествующие инциденты | ОН | 0 |
| Н | 0 |
| Ср | 1 |
| В | 0 |
| ОВ | 0 |
| Примечание – Составлено автором | | |

Далее, необходимо провести агрегацию заключений правил нечетких продукций. Для этого объединим выводы нечетких правил вместе для получения более точного результата следующим образом:

1. Если условие нечеткого продукционного правила является простым нечетким высказыванием, то степень его истинности соответствует значению функции принадлежности соответствующего терма ЛП.
2. Если условие представляет составное высказывание, то степень истинности сложного высказывания определяется при помощи логической операции конъюнкции.

В нечеткой логике оператор минимума используется вместо классической логической операции “И”. Так как для операции “И” справедливо правило: если одна входных переменных равна 0, то и значение на выходе равно 0.

Найдем степени истинности продукционных правил 3, 8, 28, 33, представленных в таблице 20. Значения степеней истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать:

Правило 3. Y1 =Ср: µ(R3)=min(0,4; 0,3; 1)=0,3.

Правило 8. Y1 =Ср: µ(R8)=min(0,4; 0,7; 1)=0,4.

Правило 28. Y1 =Ср: µ(R28)=min(0,6; 0,3; 1)=0,3.

Правило 33. Y1 =Ср: µ(R33)=min(0,6; 0,7; 1)=0,6.

Например, для правила 3, если К1=ОН, К2=ОН, К3=Ср, степени истинности которых соответственно равны 0,4; 0,3; 1, (см. таблицу 26) выберем минимальное значение.

Далее, для получения более точного результата объединим вместе выводы нечетких правил.

Объединение функций принадлежности всех подзаключений проводится как правило классически по формуле (18):

(18)

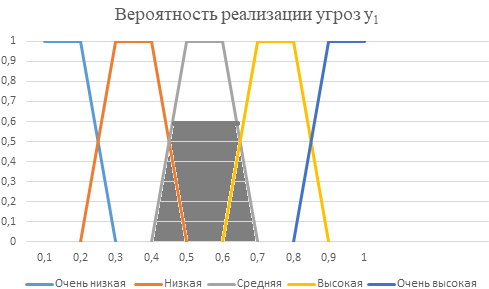


Рисунок 15 – Результаты процесса агрегирования

Примечание – Составлено автором

В соответствии с рисунком 15, далее все нечеткие подмножества, присвоенные каждой выходной переменной, объединяются вместе, чтобы сформировать одно нечеткое подмножество для каждой выходной переменной.

Для того, чтобы получить четкое значение используем формулу (19):

(19)

имеем

Повторим все действия для определения уровня нанесенного ущерба *Y2*. Аналогично по заданным значениям входных параметров найдём степени истинности µА(х) (таблица 33).

Таблица 33 – Значения функции принадлежностей входных переменных для определения уровня нанесенного ущерба

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| Финансовый ущерб | ОН | 0 |
| Н | 0 |
| Ср | 0,3 |
| В | 0,7 |
| ОВ | 0 |
| Репутационный ущерб | ОН | 0 |
| Н | 0,2 |
| Ср | 0,8 |
| В | 0 |
| ОВ | 0 |
| Примечание – Составлено автором | | |

Определим степени истинности условий по каждому из правил системы нечеткого вывода на основе операции конъюнкции. Найдем степени истинности продукционных правил 12, 13, 17, 18, представленных в таблице 28:

Правило 12. Y2 =Ср: µ(R12)=min(0,3; 0,2)=0,2.

Правило 13. Y2 =Ср: µ(R13)=min(0,3; 0,8)=0,3.

Правило 17. Y2 =Ср: µ(R17)=min(0,7; 0,2)=0,2.

Правило 18. Y2 =В: µ(R18)=min(0,7; 0,8)=0,7.

Значения истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать.

Найдем четкое значение :

Мы нашли значения вероятности появления угроз и уровня возможного ущерба, теперь, используя формулу (3), найдем значение риска ИБ.

Согласно таблице 30, данное значение соответствует *среднему* значению риска ИБ.

*Пример 2.*

Пусть на вход системы поступили значения, представленные в таблице 34.

Таблица 34 – Входные значения системы нечеткого вывода

|  |  |
| --- | --- |
| Лингвистические переменные | Нормализованные значения |
| Значимость актива | 0,85 |
| Существующий контроль | 0,7 |
| Предшествующие инциденты | 0,9 |
| Финансовый ущерб | 0,7 |
| Репутационный ущерб | 0,5 |

Также по заданным значениям входных параметров найдём степени истинности µА(х).

Таблица 35 – Значения степени истинности µА(х) входных переменных для оценки вероятности появления угроз

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| Значимость актива | ОН | 0 |
| Н | 0 |
| Ср | 0 |
| В | 0,5 |
| ОВ | 0,5 |
| Существующий контроль | ОН | 0 |
| Н | 0 |
| Ср | 0,08 |
| В | 0,12 |
| ОВ | 0 |
| Предшествующие инциденты | ОН | 0 |
| Н | 0 |
| Ср | 0 |
| В | 0,2 |
| ОВ | 0,6 |
| Примечание – Составлено автором | | |

В соответствии с таблицей 35, представлены Степени истинности µА(х) для входных лингвистических переменных.

Найдем степени истинности продукционных правил 89, 90, 94, 95, 114, 115, 119, 120. Значения истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать:

Правило 89. Y1 = В: µ(R89)=min(0,5; 0,08; 0,2)=0,08.

Правило 90. Y1 = В: µ(R90)=min(0,5; 0,08; 0,6)=0,08.

Правило 94. Y1 = Ср: µ(R94)=min(0,5; 0,12; 0,2)=0,12.

Правило 95. Y1 = Ср: µ(R95)=min(0,5; 0,12; 0,6)=0,12.

Правило 114. Y1 = В: µ(R114)=min(0,5; 0,08; 0,2)=0,08.

Правило 115. Y1 = В: µ(R115)=min(0,5; 0,08; 0,6)=0,08.

Правило 119. Y1 = В: µ(R119)=min(0,5; 0,12; 0,2)=0,12.

Правило 120. Y1 = В: µ(R120)=min(0,5; 0,12; 0,6)=0,12.

Объединение функций принадлежности всех подзаключений:

Далее получим четкое значение .

Повторим все действия для определения уровня нанесенного ущерба. Аналогично по заданным значениям входных параметров найдём степени истинности µА(х), представленные в таблице 36.

Таблица 36 – Значения функции принадлежностей входных переменных для определения уровня нанесенного ущерба

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| Финансовый ущерб | ОН | 0 |
| Н | 0 |
| Ср | 0 |
| В | 1 |
| ОВ | 0 |
| Репутационный ущерб | ОН | 0 |
| Н | 0 |
| Ср | 1 |
| В | 0 |
| ОВ | 0 |
| Примечание – Составлено автором | | |

Определим степени истинности условий по каждому из правил системы нечеткого вывода на основе операции конъюнкции.

Правило 18. Y2 =В: µ(R18)=min(1; 1)=1.

Значения истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать.

Найдем четкое значение :

Мы нашли значения вероятности появления угроз и уровня возможного ущерба, теперь, используя формулу (3), найдем значение риска ИБ.

Согласно таблице 30, данное значение соответствует *высокому* значению риска ИБ.

*Пример 3.*

Пусть на вход системы поступили значения, представленные в таблице 36.

Таблица 36 – Входные значения системы нечеткого вывода

|  |  |
| --- | --- |
| Лингвистические переменные | Нормализованные значения |
| Значимость актива | 0,15 |
| Существующий контроль | 0,4 |
| Предшествующие инциденты | 0,5 |
| Финансовый ущерб | 0,16 |
| Репутационный ущерб | 0,2 |

Сначала по заданным значениям входных параметров найдём степени истинности µА(х). Результаты фаззификации представлены в таблице 37.

Таблица 37 – Значения степени истинности µА(х) входных переменных для оценки вероятности появления угроз

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| 1 | 2 | 3 |
| Значимость актива | ОН | 0,8 |
| Н | 0,2 |
| Ср | 0 |
| В | 0 |
| ОВ | 0 |
| Существующий контроль | ОН | 0 |
| Н | 0,5 |
| Ср | 0,5 |
| В | 0 |
| ОВ | 0 |
| Предшествующие инциденты | ОН | 0 |
| Н | 0 |
| Ср | 1 |
| В | 0 |
| ОВ | 0 |
| Примечание – Составлено автором | | |

Найдем степени истинности продукционных правил 8, 13, 33, 38 (таблица 26), степени истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать:

Правило 8. Y1 = Ср: µ(R8)=min(0,8; 0,5; 1)=0,5.

Правило 13. Y1 = Н: µ(R13)=min(0,8; 0,5; 1)=0,5.

Правило 33. Y1 = Ср: µ(R33)=min(0,2; 0,5; 1)=0,2.

Правило 38. Y1 = Ср: µ(R38)=min(0,2; 0,5; 1)=0,2.

Далее все нечеткие подмножества, присвоенные каждой выходной переменной, объединяются вместе, чтобы сформировать одно нечеткое подмножество для каждой выходной переменной.

Далее определим четкое значение :

Повторим все действия для определения уровня нанесенного ущерба. Степени истинности µА(х) представлены в таблице 38.

Таблица 38 – Значения функции принадлежностей входных переменных для определения уровня нанесенного ущерба

|  |  |  |
| --- | --- | --- |
| Входные переменные | Термы | µА(х) |
| Финансовый ущерб | ОН | 0,4 |
| Н | 0,6 |
| Ср | 0 |
| В | 0 |
| ОВ | 0 |
| Репутационный ущерб | ОН | 0 |
| Н | 1 |
| Ср | 0 |
| В | 0 |
| ОВ | 0 |
| Примечание – Составлено автором | | |

Определим степени истинности условий по каждому из правил системы нечеткого вывода на основе операции конъюнкции. Найдем степени истинности продукционных правил 4, 9. Значения истинности всех остальных правил равны нулю, поэтому нет необходимости их учитывать.

Правило 2. Y2 =ОН: µ(R2)=min(0,4; 0,6)=0,4.

Правило 7. Y2 =Н: µ(R7)=min(0,6; 1)=0,6.

В результате дефаззификации по формуле (2) имеем

Мы нашли значения вероятности появления угроз и уровня возможного ущерба, найдем значение риска ИБ.

Согласно таблице 30, данное значение соответствует **низкому** значению риска ИБ.

Объединим все полученные результаты в таблице 39.

Таблица 39 – Результаты оценки корректности модели

|  |  |  |  |
| --- | --- | --- | --- |
| Критерии | Входные значения | Входные значения | Входные значения |
| Значимость актива | 0,25 | 0,85 | 0,15 |
| Существующий контроль | 0,2 | 0,7 | 0,4 |
| Предшествующие инциденты | 0,55 | 0,9 | 0,5 |
| Финансовый ущерб | 0,7 | 0,7 | 0,16 |
| Репутационный ущерб | 0,3 | 0,5 | 0,2 |
| Уровень риска | Средний | Высокий | Низкий |
| Примечание – Составлено автором | | | |

Таким образом, предложенная модель позволяет получить корректные значения риска ИБ для промышленных IoT-систем, которые соответствуют различным сценариям развития событий.

**2.3 Моделирование нечеткой системы оценки риска информационной безопасности с помощью пакета Fuzzy Logic Toolbox**

Алгоритм оценивания риска, основанный на положениях нечеткой логики и теории нечетких множеств, предлагается реализовать с помощью пакета Fuzzy Logic Toolbox системы MATLAB [66, 67]. Задачей является моделирование нечеткой эскпертной системы для анализа риска информационной безопасности промышленных IoT-систем. Система эксперимента состоит из двух этапов: разработка экспертной системы и оценка эффективности с использованием данных для испытаний.

Предложенная модель имеет пять входных переменных и две выходные [68]. Структура модели показана на рисунке 16.

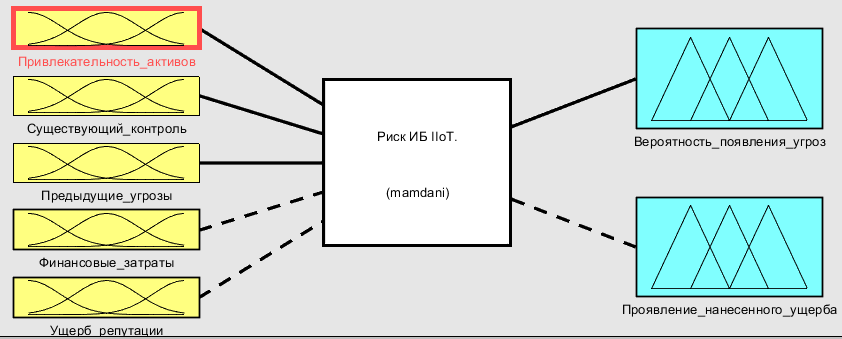


Рисунок 16 – Структура нечеткой модели

Примечание – Составлено автором

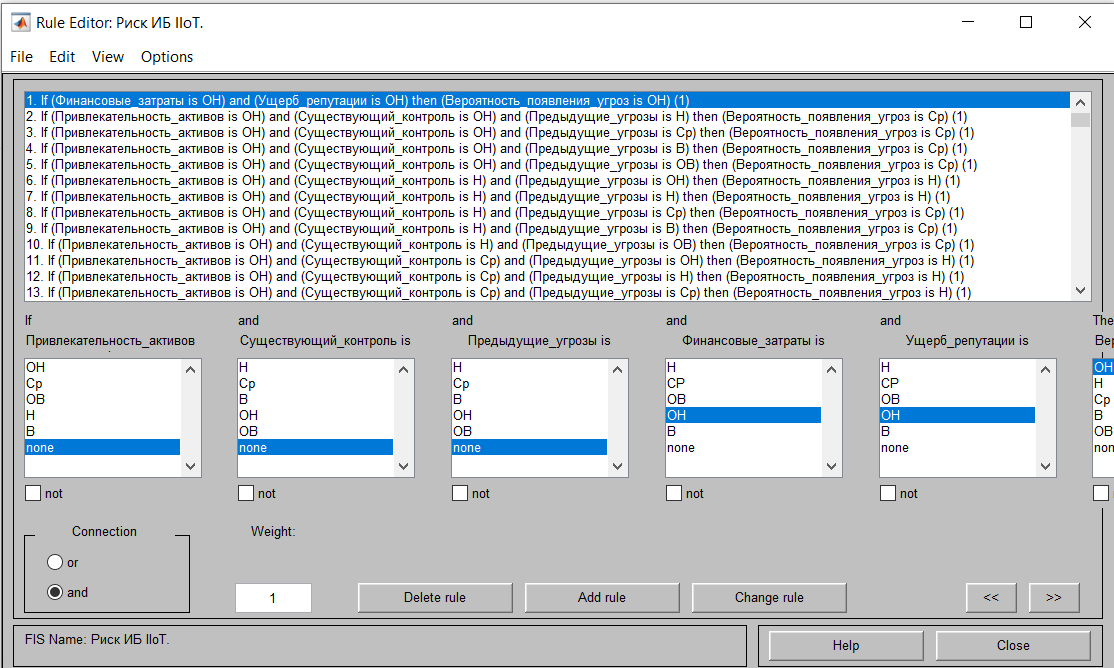


Рисунок 17 – Продукционные правила

Примечание – Составлено автором

На рисунке 17 представлены продукционные правила, вводимые с использованием нечеткой базы правил.

|  |  |
| --- | --- |
| а | б |
| в | г |

а - от привлекательности активов и существующего контроля; б - от предыдущих угроз и привлекательности активов; в - от предыдущих угроз и существующего контроля; г - зависимость уровня нанесенного ущерба от финансовых затрат и ущерба репутации

Рисунок 18 – Зависимость вероятности появления угроз

Примечание – Составлено автором

На рисунке 18а показана 3D-визуалиазация зависимости вероятности появления угроз от привлекательности активов и существующего контроля. Самая нижняя часть, в данном случае синего цвета, представляет собой *низкую вероятность появления угроз*, которая возможна при низкой привлекательности актива предприятия и достаточно высоком уровне существующего контроля. Следует отметить, что самый верхний угол, желтое поле является участком, определяющим самую *высокую вероятность появления угроз*.

На рисунке 18б приведен трехмерный график зависимости вероятности появления угроз от предыдущих угроз и привлекательности активов. По графику видно, что низкая привлекательность активов IIoT-систем для злоумышленников и нечастые предыдущие угрозы определяют низкую вероятность появления угроз.

Трехмерный график зависимости вероятности появления угроз от предыдущих угроз и существующего контроля приведен на рисунке 18в. По графику видно, что желтая зона соответствует высокой вероятности появления угроз, при частых предыдущих угрозах и недостаточном уровне существующего контроля.

На рисунке 18г приведен график, полученный при моделировании на основе нечеткой логики зависимости уровня нанесенного ущерба от финансовых затрат и ущерба репутации. Самая нижняя темно-синяя часть графика представляет минимальный уровень нанесенного ущерба, вызванный сценариями, которые происходят при низких финансовых и репутационных затратах, в то время как самый верхний угол, желтое поле соответствует высокому уровню нанесенного ущерба при высоких финансовых и репутационных затратах.

Была создана программная реализация, основанная на предложенном методе оценки риска информационной безопасности в системах промышленного интернета вещей.

**3 Создание экспертно-аналитической системы оценки рисков информационной безопасности в промышленных IoT-системах**

**3.1 Выбор и разработка алгоритма работы экспертно-аналитической системы оценки рисков информационной безопасности IIoT-систем**

При анализе риска информационной безопасности промышленных систем встает вопрос об оценке защищенности информационных активов промышленных IoT-систем, а также о выработке рекомендаций, выполнение которых может способствовать повышению уровня защищенности.

Разрабатываемая система решает следующие задачи:

* автоматизация процедуры оценки риска ИБ;
* облегчение работы или полная замена экспертов ИБ;
* использование накопленного ранее опыта;
* выработка максимально эффективных рекомендаций;
* снижение стоимости проведения аудита.

В ходе работ по созданию ЭС сложилась определенная технология их разработки, включающая шесть следующих этапов: идентификация, концептуализация, формализация, выполнение, тестирование, опытная эксплуатация [69]. На рисунке 19 изображены данные этапы.

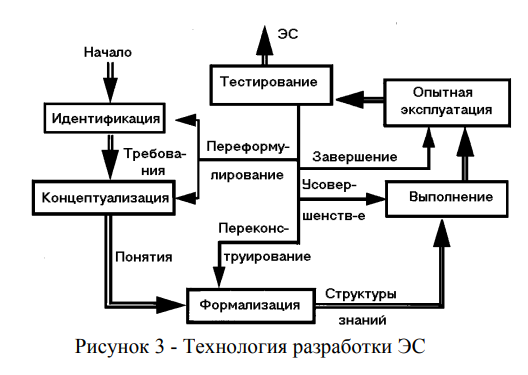


Рисунок 19 – Технология разработки ЭС

Примечание – Составлено по источнику [69, с. 15]

Первый этап – *идентификация*. На этом этапе определяются задачи, которые подлежат решению, выявляются цели разработки, определяются и типы пользователей.

На этапе *концептуализации* проводится содержательный анализ проблемной области, выявляются используемые понятия и их взаимосвязи, определяются методы решения задач.

На этом этапе определяются следующие особенности задачи:

* типы доступных данных;
* исходные и выводимые данные;
* подзадачи общей задачи;
* используемые стратегии и гипотезы;
* виды взаимосвязей между объектами проблемной области;
* типы используемых отношений (иерархия, причина/следствие, часть/целое и т.п.);
* процессы, используемые в ходе решения задачи;
* типы ограничений, накладываемых на процессы, используемые в ходе решения;
* состав знаний, используемых для решения задачи и для объяснения решения.

Для выявления указанных характеристик задачи рекомендуется создать подробный протокол действий и рассуждений эксперта, который проводит анализ хотя бы одной конкретной задачи. Такой протокол не только предоставит инженеру по знаниям словарь терминов и представление о стратегиях, используемых экспертом, но также поможет ответить на различные вопросы, возникающие в процессе разработки. На этой стадии инженер по знаниям рассматривает вопросы, связанные с представлением знаний и методами решения, однако выбор конкретных методов и подходов осуществляется на более поздних этапах.

*Формализация* включает в себя выбор информационных систем и определение способов представления всех видов знаний, формализацию ключевых понятий, определение методов интерпретации знаний, моделирование работы системы и оценку адекватности системы целям, учитывая закрепленные понятия, методы решений, средства представления и обработки знаний.

Основными задачами в процессе формализации являются проблемы структуризации исходной задачи и знаний в выбранном формализме, а именно:

1) структуризация общей задачи на связанные подзадачи;

2) структуризация предметной области на основе иерархии классов;

3) структуризация знаний на декларативные и процедурные;

4) структуризация приложения на основе иерархии «часть/целое».

Важность модульной организации экспертной системы определяется тем, что разбиение приложения на модули существенно ускоряет разработку, снижает затраты на сопровождение и поддержку, упрощает повторное использование модулей базы знаний в последующих разработках. С другой стороны, разбиение прикладной экспертной системы на модули несколько повышает накладные расходы на загрузку и сборку прикладной системы, например, восстановление после сбоев и перезапуск системы [70].

На этапе *выполнения* происходит наполнение базы знаний экспертной системы. Этот этап является ключевым и трудоемким в процессе разработки, поскольку основой для функционирования ЭС служат знания. Процесс приобретения знаний включает в себя извлечение экспертных знаний, их организацию для эффективной работы системы, а также представление знаний в форме, понятной для экспертной системы. Инженер по знаниям осуществляет этот процесс, анализируя деятельность эксперта при решении реальных задач.

Этап *тестирования экспертной системы* рассматривается как завершающая стадия разработки, представляющая собой операционное прототипирование с возможностью внесения изменений в целях проектирования на протяжении разработки. Этот этап предъявляет специфические требования к демонстрации корректности и соответствия системы установленным стандартам. В сравнении с процессом тестирования традиционных программных систем, верификация (логическое тестирование) экспертной системы ассоциируется с альфа-тестированием, а концептуальное тестирование – с бета-тестированием. Но следует отметить, что тестирование экспертных систем отличается от тестирования традиционных систем. В то время как для традиционных систем строгие предварительные спецификации позволяют программистам самостоятельно проводить верификацию, тестирование экспертных систем требует участия экспертов в предметной области. [71].

Выделяют три аспекта тестирования экспертных систем:

* тестирование исходных данных;
* логическое тестирование базы знаний;
* концептуальное тестирование прикладной системы.

На *этапе опытной эксплуатации и внедрения* проверяется пригодность экспертной системы для конечного пользователя. Система решает широкий спектр задач с различными пользователями. Переход к этому этапу следует осуществлять только после успешного решения всех требуемых задач системой, чтобы предотвратить создание у пользователя негативного восприятия из-за ошибок в решениях. Пригодность системы для пользователя оценивается, в основном, по удобству её использования и полезности.

Этапы разработки предложенной экспертной системы применительно к решению задачи оценки риска информационной безопасности промышленных IoT систем представлены на рисунке 20.

Проблемой является практическая потребность в обеспечении высокого уровня информационной безопасности цифровых промышленных систем. Структура системного анализа применимости разработанного метода в данной проблемной области представлена на рисунке 21.

Анализ проблемной области

Определение цели разработки системы

Детализация структуры системы

Определение исходных данных для формализации БЗ

Определение методов представления знаний данных

Выбор среды разработки системы

Алгоритмы расчета

Прототипная версия программной реализации системы

Тестирование программы

Программная реализация

Рисунок 20 – Этапы разработки системы

Примечание – Составлено автором

Целью является оценка при помощи лингвистических переменных уровня риска ИБ для своевременного реагирования на различные инциденты, а также выработка необходимых рекомендаций с целью повышению уровня ИБ.

Для построения ЭС используем разработанную модель определения уровня риска информационной безопасности методом простого аддитивного взвешивания, которая и является основой будущей БЗ, определяя ее адекватность, эффективность и быстродействие. Исходными данными для построения БЗ являются данные о защищаемых активах, их критичности, угрозах, мерах по снижению риска. Выбор среды разработки ЭС для полноценного приложения, которое в дальнейшем сможет расти и развиваться – задача, требующая тщательного анализа всех достоинств и недостатков той или иной среды. В конечном итоге средой разработки была выбрана IDE Sublime Text, так как обладает огромными возможностями разработки ПО с бесплатной лицензией и гибкой библиотекой встроенный средств, инструментов и фреймоворков. Sublime Text является проприетарным текстовым редактором, поддерживающим плагины на языке программирования Python.

*Исследования на уместность:*

1. Решение задачи опирается на использование как фактов, так и продукционных правил и алгоритмов.
2. Данная проблема является трудноформализуемой задачей.
3. Задача обеспечения информационной безопасности промышленных IoT-систем имеет практическую значимость.
4. Задача можеть быть решена с использованием ЭВМ.

*Исследования на возможность разработки:*

1. Решение задачи требует рассуждений, а не действий. Подсистема логического вывода генерирует рекомендации по решению задачи.
2. Существуют эксперты в данной проблемной области.

Анализ проблемной области

Рисунок 21 – Структура системного анализа на применимость метода в данной проблемной области

Примечание – Составлено автором

Системные требования для работы системы:

– процессор 300 MHz или выше;

– оперативная память – 128 Мб RAM или выше;

– видеоадаптер и монитор – SuperVGA (1024х720) или выше;

– свободное место на HDD – 20 Мб или выше;

– клавиатура и мышь;

– операционная система Windows 7 / 8 / 8.1 / 10.

Одним из важнейших этапов разработки системы является разработка алгоритмов работы ЭС в различных ситуациях и механизма получения решений.

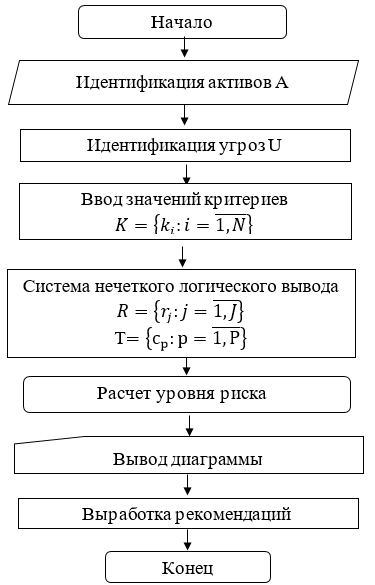


Рисунок 22 – Алгоритм оценки уровня риска информационной безопасности

Примечание – Составлено автором

На рисунке 22 представлен алгоритм предложенной модели оценки риска информационной безопасности IIoT. Данная модель включает основные этапы и процессы, необходимые для решения многокритериальной задачи.

Как видно из рисунка, реализация модели включает следующие шаги:

1. Определение защищаемых информационных активов промыщленной IoT-системы. В модели предлагаются 7 групп активов: промышленные системы управления (ICS), оконечные устройства IioT, коммуникационные сети и компоненты промышленной системы управления, информация, серверы и системы, человеческие ресурсы, программное обеспечение и лицензии.
2. Определение угроз для каждой группы активов.
3. Определение критериев, влияющих на проявление нанесенного ущерба. Всего 2 критерия: финансовые затраты, ущерб репутации.
4. Определение критериев, влияющих на вероятность возникновения угрозы. Всего 3 критерия: привлекательность актива, существующий контроль, предыдущие угрозы.
5. Ввод значений каждого критерия при помощи лингвистических переменных.
6. Анализ полученных результатов, вывод диаграммы.
7. Выработка рекомендаций взависимости от рассчитанного уровня риска.

**3.2 Технология разработки экспертно-аналитической системы**

Нечеткая экспертная система может не только учитывать неопределенность и стохастичность предметной области, но и моделировать ее параметры на основе профессиональных знаний эксперта (группы экспертов). Поведение системы определяется на основе входных данных, представленных в виде правил или отношений, которые можно выразить в форме нечеткой базы знаний. На основе этой модели поведения нечеткая логика выводит состояние системы или ее тенденции развития. Сформированная нечеткая база знаний, отражающая взаимосвязи системы с известными входными параметрами, может быть использована для определения ее состояний. Нечеткий логический вывод представляет собой аппроксимацию зависимости y = f (x1, x2 ..., xn) с использованием нечеткой базы знаний и операций над нечеткими множествами. Процесс нечеткого логического вывода представляет собой процедуру или алгоритм получения нечеткого вывода на основе нечетких условий или предпосылок [72].

Для оценки уровня риска информационной безопасности промышленных IoT-систем применение нечеткой логики обеспечивает работу с имеющейся неопределенностью, неполнотой и размытостью информации. Принятие решений в условиях неопределенности (риска), связанное с множеством возможных результатов и известными условными вероятностями, становится актуальным. Поэтому использование нечеткой логики при разработке механизмов вывода экспертной системы формализует процедуру оценки технического состояния на основе фрагментарной, ненадежной и возможно неточной информации, обосновывая принятие решений по выявлению неисправностей. Нечеткая экспертная система оперирует знаниями в виде нечетких продукций и лингвистических переменных. Она не только учитывает неопределенность, но и моделирует рассуждения, что сложно реализовать в системах, основанных на классической логике. Таким образом, основной целью применения нечеткой логики является создание инструмента способного моделировать человеческие рассуждения и объяснять принятые методы принятия решений [73, 74].

В экспертной системе условия и логические выводы различных правил формируются в виде нечетких утверждений о значениях тех или иных лингвистических переменных на рисунке 23 представлена структурная схема методики вывода на базе нечёткой логики.

Рассмотрим представленную схему подробнее [75, с. 57-68]:

1. Интерфейс пользователя предназначен для сотрудников компании, производящих оценку риска ИБ. Через интерфейс сотрудник передает ЭС запрашиваемые данные: сведения о системе, защищаемых информационных активах, информационных угрозах. Через этот же интерфейс осуществляется выбор защищаемых активов, определение угроз ИБ, для которых будет проводиться анализ. Вся информация, вводимая пользователем через интерфейс, передается в рабочую память. ЭС использует интерфейс пользователя для предоставления итоговых отчетов с результатами аудита и выработанными рекомендациями. Для разработки интерфейса пользователя, а также блока вычисления уровня риска ИБ использовался высокоуровневый язык программирования общего назначения Python.

Пользователь

ввод исходных данных

вывод результатов и рекомендаций

Интерфейс

Фаззификация

Дефаззификация

Рабочая память

Блок вычисления уровня риска ИБ

у четкое

множество

х четкое

множество

нечеткое

множество

нечеткое

множество

Экспертная система

Рисунок 23 – Структурная схема формирования результатов с использованием нечеткой системы вывода

Примечание – Составлено по источнику [75]

2. Фаззификация представляет собой процесс определения значений функции принадлежности для нечеткого набора данных, принадлежащего исходному информационному множеству. На завершающем этапе данного процесса требуется определить конкретные значения функции принадлежности для всех входных переменных каждой нечеткой переменной, используемой во входных данных.

Этап фаззификации осуществляет преобразование четкого множества входных данных в нечеткое множество, определяемое значениями функций принадлежности. Основной целью фаззификации является установление соответствия между конкретным числовым значением каждой входной переменной системы нечеткого вывода и значением функции принадлежности соответствующего терма входной лингвистической переменной. Входными данными, где - число диагностируемых параметров, выступают значения, полученные с системы сбора контроля. Затем каждый параметр подвергается лингвистической оценке в соответствии с предопределенными в системе функциями принадлежности. После этого четкое множество входных параметров преобразуется в нечеткое множество и используется в качестве лингвистических переменных в логических правилах базы знаний. Дефаззификация, в свою очередь, представляет собой обратное преобразование нечеткого множества в четкое множество B. В связи с этим, значениями системы являются вероятности каждой неисправности , где j – число неисправностей (состояний). Нечёткое множество представляет зависимость  μ(х) = μÃ→B (y) как функцию от выходной переменной у. Поэтому, производится идентификация неисправностей с оценкой вероятностей. Данная система логического вывода называется системой Мамдани-Заде. Выбор нечёткой модели типа Мамдани обусловлен тем, что правила базы знаний являются прозрачными и интуитивно понятными, тогда как для моделей типа Сугэно не всегда ясно какие линейные зависимости «входы – выход» необходимо использовать и как их получить.

3. Рабочая память предназначена для хранения исходных и промежуточных данных решаемой в текущий момент задачи.

4. Блок вычисления уровня риска ИБ.

5. Процесс аккумулирования выводов включает в себя активацию и накопление. Активация означает определение степени истинности каждого базового условия нечеткого правила. В случае, если оценка правила является нечетким множеством, значение функции принадлежности равно произведению соответствующей степени истинности его составляющих условий. Накопление, в свою очередь, включает поиск вспомогательной функции для каждой из выходных лингвистических переменных. Цель процесса заключается в агрегировании функций принадлежности всех выбранных условий и получении общего значения истинности для нечеткой переменной. Условия, связанные с одними и теми же переменными исходного языка, представляют собой различные правила для систем нечеткого вывода.

6. Дефаззификация представляет собой процесс определения типичного (строгого) значения выходной лингвистической переменной. В конечном итоге требуется получить количественные значения для каждой выходной переменной, используя все нечеткие функции, полученные на этапе аккумулирования.

**3.3 Применение экспертно-аналитической системы для оценки степени рисков для информационной безопасности IIoT-систем**

Программное средство разработано в виде десктопного приложения. Язык программирования – Python.

Для создания приложения с графическим интерфейсом пользователя использовалась стандартная графическая библиотека Python – Tkinter. Она кроссплатформенная, то есть с ее помощью можно писать приложения для Windows, Linux, macOS (рисунок 24).

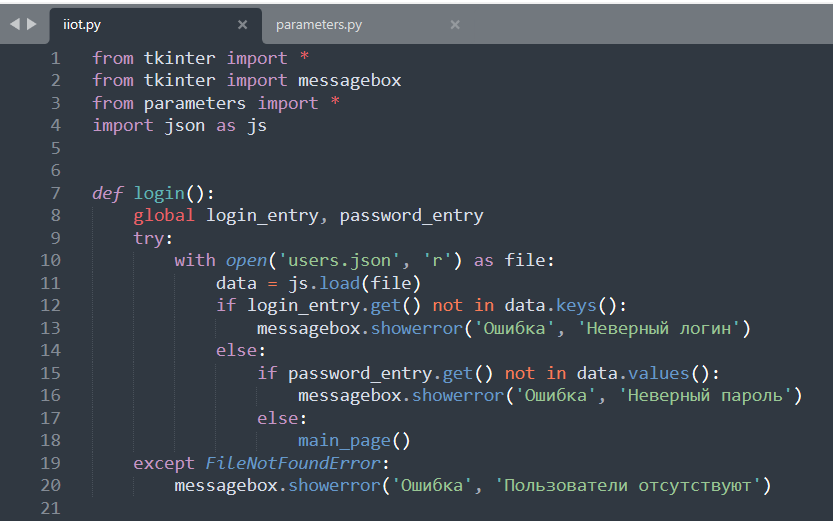


Рисунок 24 – Часть кода программы

Примечание – Разработано автором

Часть кода программы приведена в (Приложении В).

Ниже приведено пошаговое описание, позволяющее описать технические возможности программного средства:

Шаг 1: Авторизация. Во время запуска программного средства заполняются сведения, необходимые при регистрации (рисунок 25).



Рисунок 25 – Регистрация

Примечание – Разработано автором

Далее ввод логина и пароля позволяют войти в программное средство (рисунок 26).

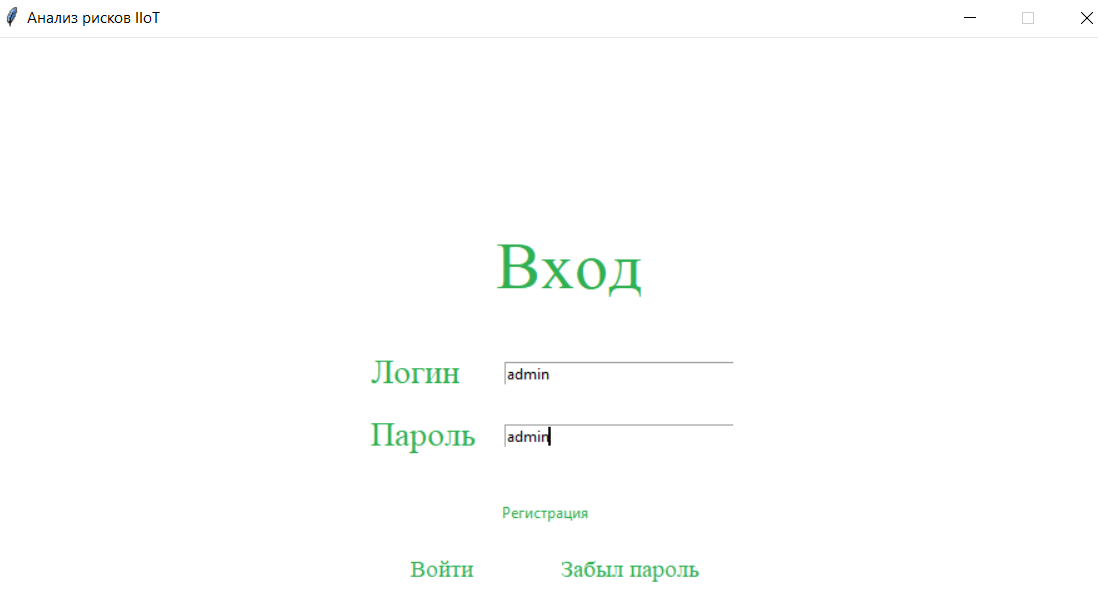


Рисунок 26 – Авторизационная форма

Примечание – Разработано автором

Шаг 2: Выбор актива. В следующем окне предоставляется список всех защищаемых активов, для которых можно рассчитать уровень риска информационной безопасности. Установка флажка позволяет осуществить выбор одного, нескольких или всех предложенных вариантов (рисунок 27).

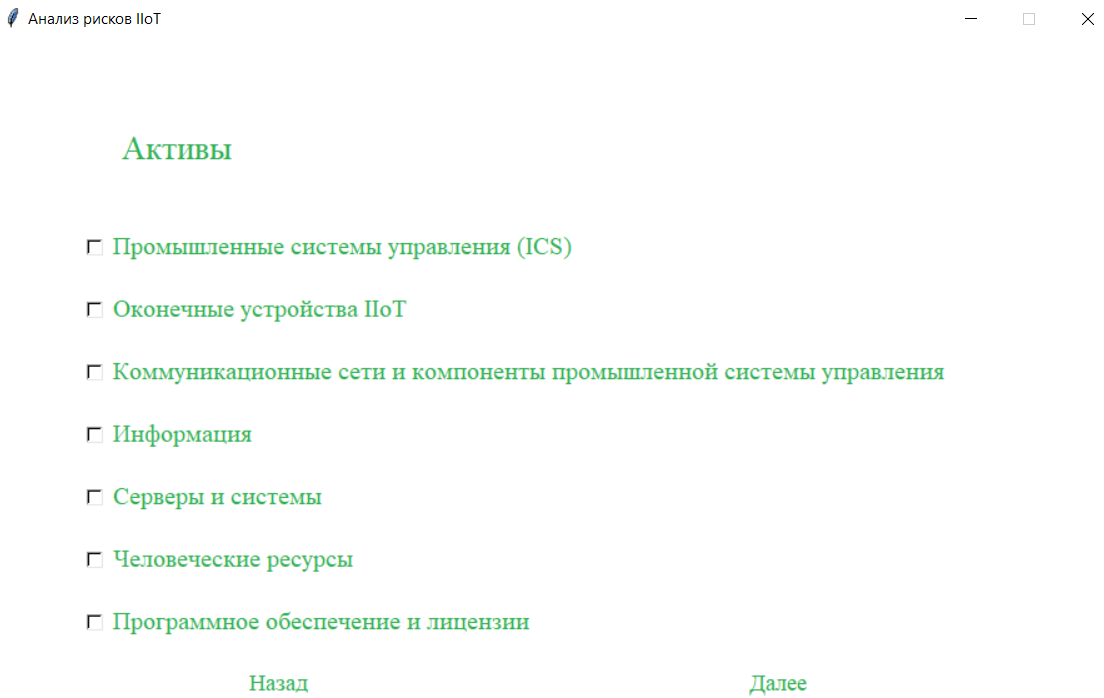


Рисунок 27 – Выбор активов

Примечание – Разработано автором

Шаг 3: Определение угроз для выбранного актива. После выбора актива в следующем окне отображаются все угрозы, которые относятся к данной категории актива (рисунок 28).

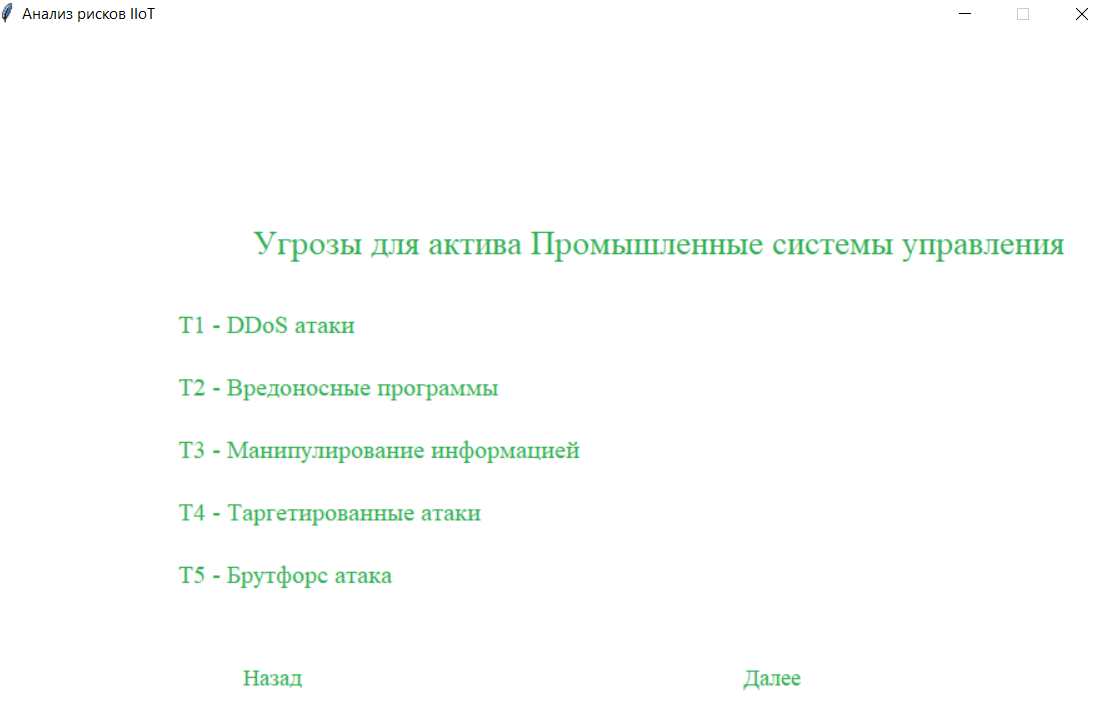


Рисунок 28 – Определение угроз

Примечание – Разработано автором

1. Шаг 4: Ввод сведений. Заполняются для 5 критериев привлекательность актива, существующий контроль, предыдущие угрозы, финансовые затраты, ущерб репутации (рисунки 29, 30).

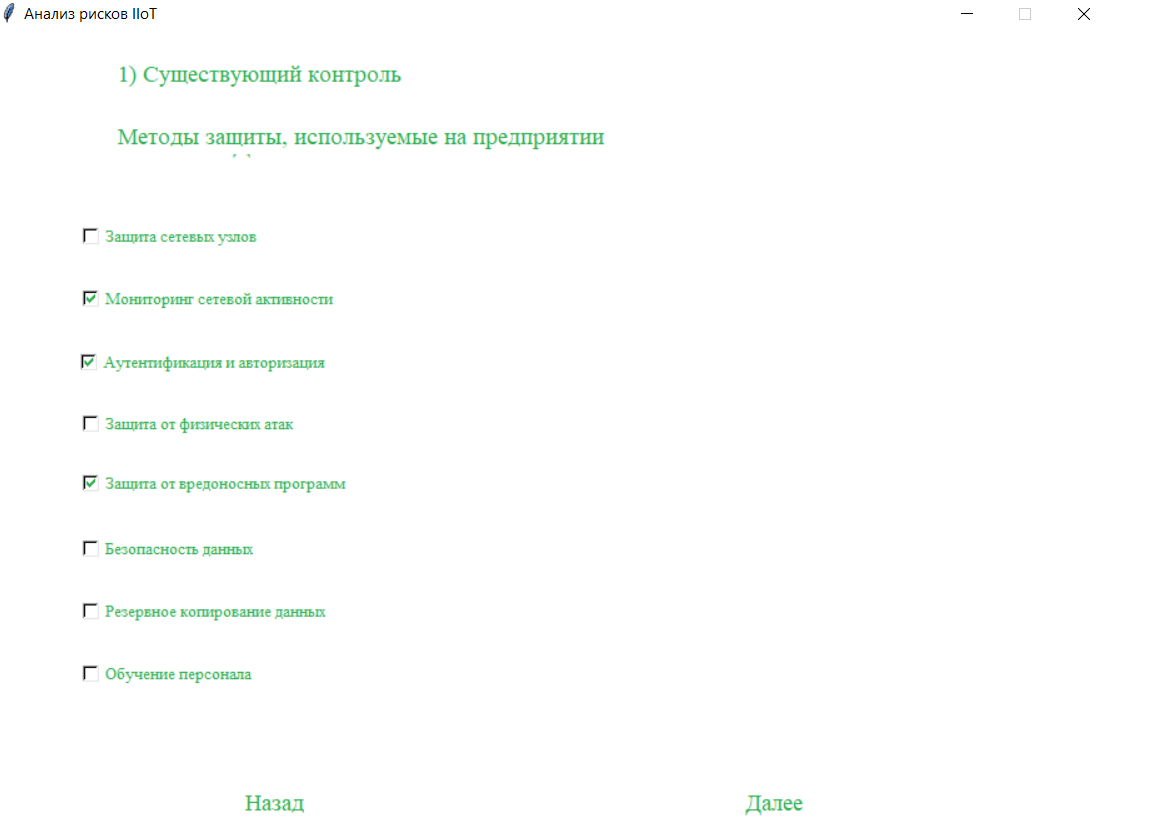


Рисунок 29 – Ввод исходных данных

Примечание – Разработано автором

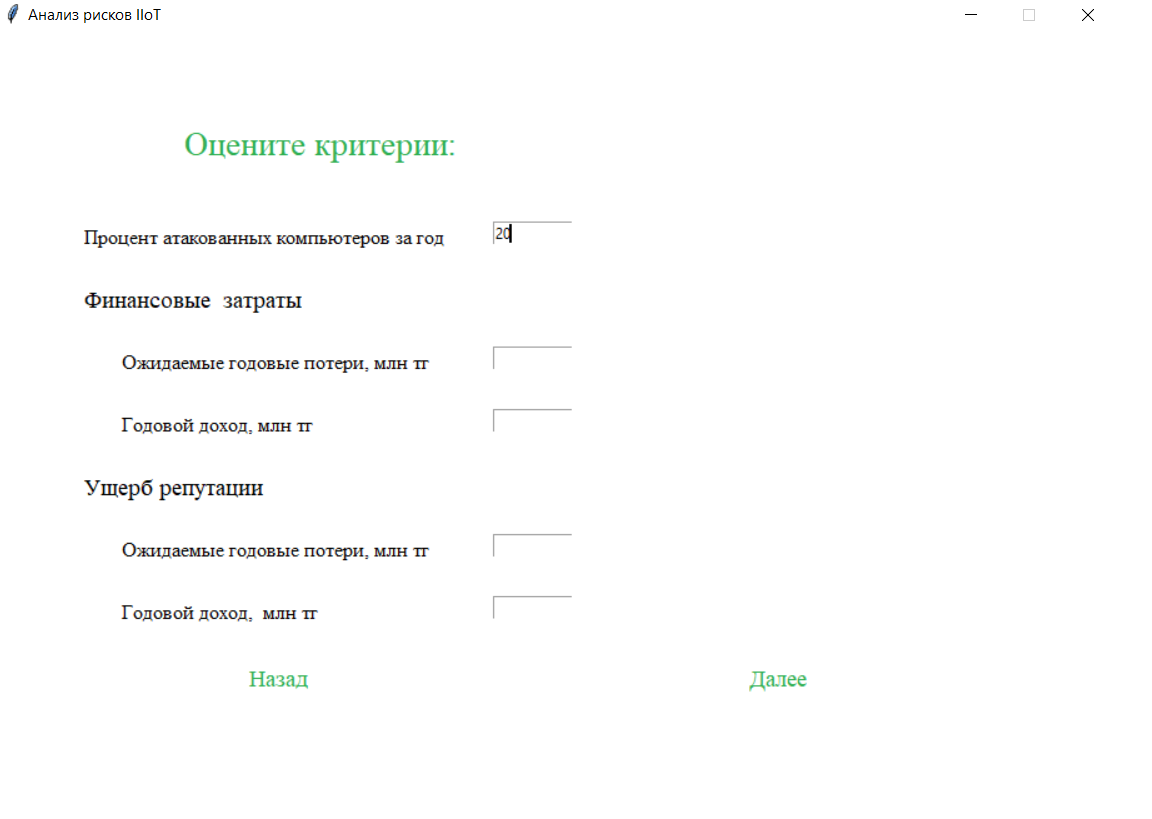


Рисунок 30 – Ввод исходных данных

Примечание – Разработано автором

Шаг 5: Вывод результатов. Результатом использования данного программного средства является расчет уровня риска (рисунок 31). Возможные варианты:

* очень низкий;
* низкий;
* средний;
* высокий;
* очень высокий.

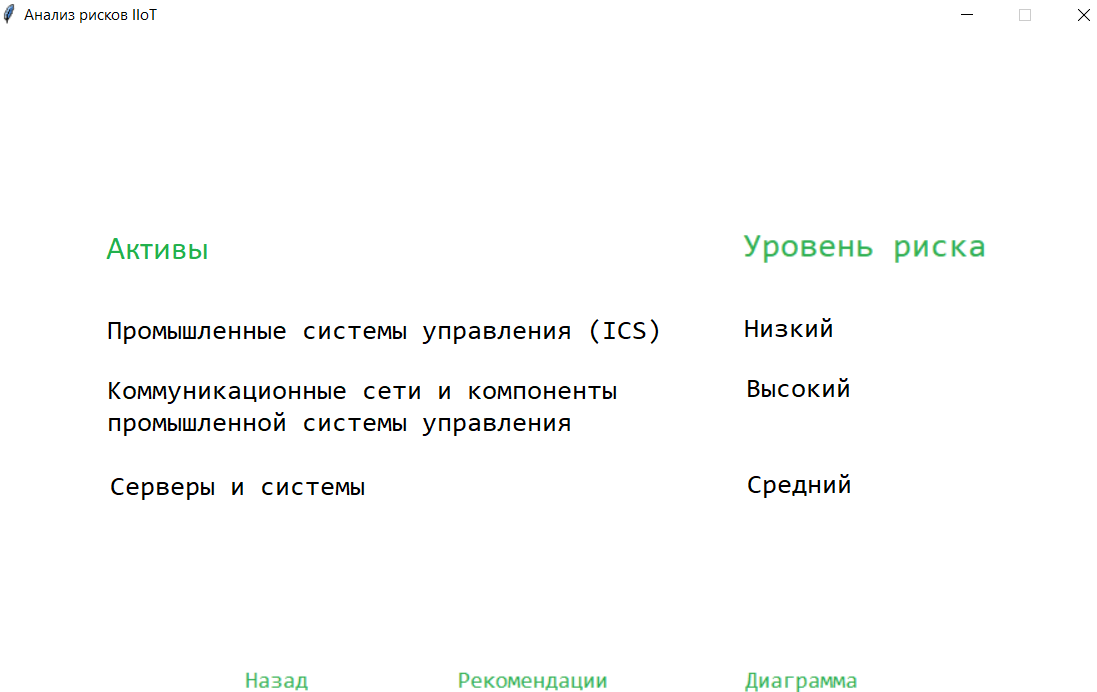


Рисунок 31 – Вывод результатов

Примечание – Разработано автором

Для наглядного отображения результатов есть возможность вывода столбчатой диаграммы с итоговым расчетом риска (рисунок 32).

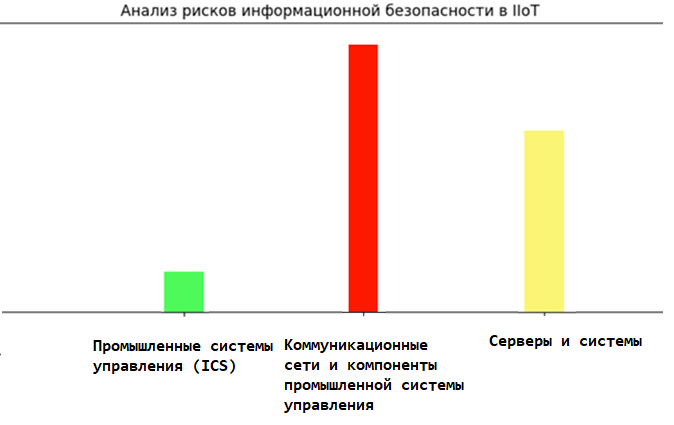


Рисунок 32 – Диаграмма с итоговыми расчетами

Также программа выдает необходимые рекомендации для устранения последствий соответственно рассчитанному риску информационной безопасности (рисунок 33).

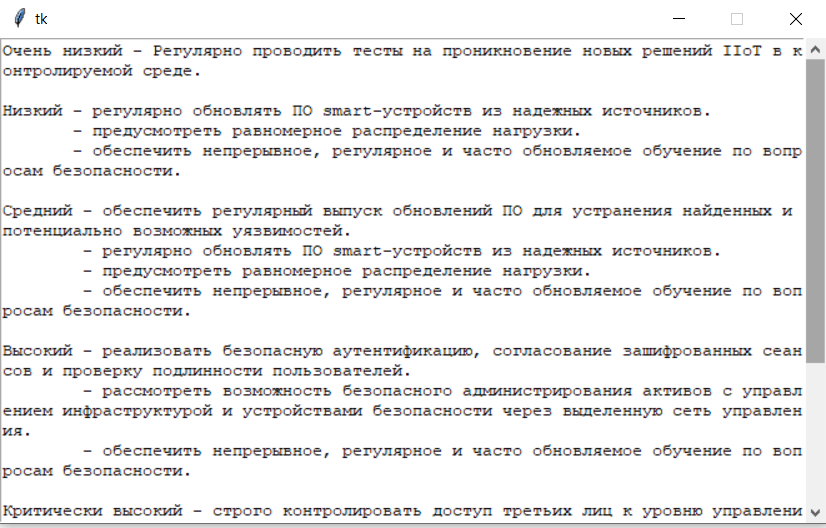


Рисунок 33 – Рекомендации программы

Примечание – Разработано автором

**ЗАКЛЮЧЕНИЕ**

Диссертационное исследование посвящено решению задачи анализа рисков информационной безопасности в промышленных IoT-системах. Для решения данной задачи использовались методы нечеткой логики, так как именно данный подход позволяет решать задачи совершенствования функционирования различных систем в условиях неполноты и неточности информации, при наличии субъективности оценок, что актуально в ИБ.

Разработанная экспертно-аналитическая система представляет собой широкодоступный инструмент для оценки рисков информационной безопасности в промышленных IoT-системах. Предлагаемая система может быть использована для оценки рисков информационной безопасности, которую должны выполнять специалисты по кибербезопасности. Она может быть полезна для прогнозирования и приоритезации рисков. Кроме того, она предоставляет важную информацию в области контроля риска и реализации мер по повышению информационной безопасности систем. К преимуществам предложенного метода оценки рисков можно отнести доступность и ясность предоставляемого формата результатов анализа для любого пользователя. Также к достоинствам метода оценки рисков является возможность оценки рисков на ранней стадии разработки промышленных IoT-систем.

Проведенные исследования позволяют сформулировать следующие основные **выводы** и результаты:

– исследованы существующие угрозы информационной безопасности промышленных IoT-систем и построена классификация данных угроз;

– разработанf модель анализа рисков информационной безопасности в IIoT-систем, работающая на основе нечеткой логики;

– создана система поддержки принятия решения по определению уровня информационной безопасности в промышленных IoT-системах;

* разработаны научно-практические рекомендации, направленные на повышение информационной безопасности в сетях промышленного Интернета вещей.

Результаты диссертационной работы могут быть использованы в работах по исследованию проблемы информационной безопасности в промышленных IoT-системах.

По результатам работы на объект «Расчет уровня риска информационной безопасности в промышленных системах IIoT» было получено Авторское свидетельство о внесении сведений в Государственный реестр прав РК на объекты, охраняемые авторским правом №27868 от 18 июля 2022 года.

Таким образом, поставленные в диссертационной работе задачи исследования полностью решены.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1 Росляков А.В., Ваняшин С.В., Гребешков А.Ю. и др.  Интернет вещей. – Самара: ПГУТИ, 2014. – 340 с.

2 Stouffer K., Pillitteri V., Lightman S. Guide to Industrial Control Systems. – Gaithersburg, 2023. – 248 р.

3 Тарасов И.В. Индустрия 4.0: понятие, концепции, тенденции развития // Стратегии бизнеса. – 2018. – №6. – С. 14-19.

4 Амирова А.С., Тохметов А.Т. Проблемы безопасности промышленного интернета вещей // Матер. 5-й междунар. науч.-практ. конф. «Наука и образование в современном мире: вызовы ХХI века». – Астана, 2019. – С. 164-168. 5 4 Амирова А.С., Тохметов А.Т. Проблемы безопасности промышленного интернета вещей // Матер. 5-й междунар. науч.-практ. конф. «Наука и образование в современном мире: вызовы ХХI века». – Астана, 2019. – С. 164-168.

5 Амирова А.С., Тохметов А.Т., Жанасбаева А.С. Исследование требований для построения модели обеспечения безопасности промышленного интернета вещей // Известия научно-технического общества «КАХАК». – 2020. – №3. – С. 8-16.

6 Bakhshi Z., Balador A., Mustafa J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models // Procced. IEEE Wireless Communications and Networking conf. Workshops (WCNCW). – Barcelona, 2018. – P. 173-178.

7 Wollschlaeger M., Sauter T., Jasperneite J. The future of industrialcommunication: Automation networks in the era of the internet of thingsand industry 4.0 // EEE Ind. Electron. Mag. – 2017. – №1. – P. 17-27.

8 Искусственный интеллект и цифровые фабрики: как внедряются элементы Индустрии 4.0 на казахстанских предприятиях // <https://primeminister.kz/ru/news/reviews/iskusstvennyy-intellekt-i>. 11.02.2022.

9 Постановление Правительства Республики Казахстан. Об утверждении Государственной программы «Цифровой Казахстан»: утв. 12 декабря 2017 года, №827 // <https://adilet.zan.kz/rus/docs/P1700000827>. 11.02.2022.

10 Амирова А.С., Тохметов А.Т. Проблемы и перспективы использования BIG DATA в промышленности Казахстана // Сб. матер. 6-й междунар. науч.-практ. конф. «Вig data and advanced analytics». – Минск, 2020. – С. 374-378.

11 Hofer F. Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study // 12th ACM/IEEE internat. symp. Empirical Softw. Eng. Meas. – NY., 2018. – P. 1-10.

12 Sisinni E., Saifullah A., Han S. Industrial Internet of Things: Challenges, opportunities, and directions // IEEE Trans. Ind. Informat. – 2018. – Vol. 14, Issue 11. – P. 4724-4734.

13 Tange K., De Donno M., Fafoutis X. et al. Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, Issue 4. – P. 2489-2520.

14 Yu X., Guo H. A Survey on IIoT Security // Procced. IEEE VTS Asia Pacific Wireless Communications sympos. – Singapore, 2019. – P. 1-5.

15 Panchal A., Khadse V., Mahalle P. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures // Procced. 2018 IEEE Global conf. on Wireless Computing and Networking (GCWCN). – Lonavala, 2018. – P. 124-130.

16 Shah Y., Sengupta S. A survey on Classification of Cyber-attacks on IoT and IIoT devices // Procced. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication conf. (UEMCON). – NY., 2020. – P. 406-413.

17 Tamy S., Belhadaoui H., Rabbah M. A. An evaluation of machine learning algorithms to detect attacks in SCADA network // Procced 7th Mediterr. congr. Telecommun. – Morocco, 2019. – P. 1-5.

18 Al-Hawawreh M., Sitnikova E. Industrial Internet of Things based ransomware detection using stacked variational neural network // Procced 3rd internat. conf. Big Data Internet Things. – Melbourne, 2019. – P. 126-130.

19 Wang H., Chen Z., Zhao J. A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow // IEEE Access. – 2018. – Vol. 6. – P. 8599-8609.

20 Li Z., Kang J., Yu R. et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14, Issue 8. – P. 3690-3700.

21 Huang Y. -L., Sun W. -L. An AHP-Based Risk Assessment for an Industrial IoT Cloud // Procced. IEEE internat. conf. on Software Quality, Reliability and Security Companion. – Lisbon, 2018. – P. 637-638.

22 Hassani H. Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443 // Procedia Comput. Sci. – 2021. – №191. – Р. 33-40.

23 Potter B. Microsoft SDL Threat Modelling Tool // Network Security. – 2009. – №1. – P. 15-18.

24 Schrecker S., Molina J. Industrial Internet of Thinds. – Boston, 2018. − Vol. G4. – 174 p.

25 Good Practices for Security of Internet of Things in the context of Smart Manufacturing / ENISA. – Attiki, 2018. – 118 p.

26 Амирова А.С., Тохметов А.Т., Жанасбаева А.С. Разработка онтологии информационных атак и угроз промышленного интернета вещей в программной среде PROTÉGÉ 5.0 // Известия научно-технического общества «КАХАК». – 2020. – №4(71). – С. 4-13.

27 Амирова А.С., Тохметов А.Т., Жанасбаева А.С. Основные проблемы безопасности в промышленном интернете вещей // Вестник Восточно-Казахстанского технического университета им. Д.Серикбаева. – 2021. – №1(91). – С. 82-91.

28. СТ РК 34.023-2006. Информационная технология. Методика оценки соответствия информационных систем требованиям безопасности // https://online.zakon.kz/Document/?doc\_id=30447694. 14.03.2022.

29 ISO/IEC 29147. Информационные технологии. Методы обеспечения безопасности. Раскрытие уязвимостей // https://www.iso.org/ru. 14.03.2022.

30 Комитет по статистике Министерства национальной экономики Республики Казахстан // http://stat.gov.kz. 01.04.2022.

31 Peiyu L., Dong L. The new risk assessment model for information system in cloud computing environment // Procedia Engineering. – 2011. – Vol. 15. – Р. 3200-3204.

32 Pan L., Tomlinson A. A systematic review of information security risk assessment // International Journal of Safety and Security Engineering. – 2016. – Vol. 6, Issue 2. – P. 270-281.

33 Павленко А.В., Ковалева Е.Г., Радоуцкий В.Ю. Анализ подходов к оценке риска // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. – 2015. – №3. – С. 106-109.

34. Файзулаев Д., Морозов Б. Методы и средства анализа рисков информационной безопасности предприятия // Безопасность информационных технологий. – 2017. – Т. 24, №3. – С. 72-77.

35 Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. – 2020. – Т. 4, №1. – С. 31-37.

36 Львова А.В. Методы анализа и управления рисками безопасности защищено информационной системы: дис. ... канд. техн. наук: 05.13.01. – М., 2009. – 198 с.

37 Корнилов Д.А., Зайцев Д.А. Оценка эффективности внедрения системы информационной безопасности с использованием метода анализа иерархий // Экономическая безопасность России: проблемы и перспективы: матер. междунар. науч.-практ. конф. – Нижний Новгород, 2014. – С. 407-412.

38 Wang L.X. Analysis and design of hierarchical fuzzy systems // IEEE Transactions on Fuzzy Systems. – 1999. – Vol. 7, Issue 5. – P. 617-624.

39 Abdymanapov S.A., Muratbekov M. et al. Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems // IEEE Access. – 2021. – Vol. 9, Issue 3. – Р. 556-565.

40 Shameli-Sendi A., Shajari M., Hassana badi M. et al. Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment // The Open Cybernetics & Systemics Journal. – 2012. – №6. – Р. 26-37.

41 Wang Y. M., Elhag T. M. Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment // Expert systems with applications. – 2006. – Vol. 31, Issue 2. – P. 309-319.

42 Zhao D.-M., Wang J.-H., Ma J.-F. Fuzzy Risk Assessment of the Network Security // Procced. Internat. conf. on Machine Learning and Cybernetics. – Dalian, 2006. – Р. 4400-4405.

43 Saaty T. What is the Analytic Hierarchy Process? // Mathematical Models for Decision Support. – 1988. – Vol. 48. – P. 109-121.

44 Курейчик В.М. Особенности построения систем поддержки принятия решений // Известия ЮФУ. Технические науки. – 2012. – №7(132). – С. 92-98.

45 Ani U., Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective // Journal of Cyber Security Technology. – 2017. – Vol. 1, Issue 1. – P. 32-74.

46 Новак В., Перфильева И.Г., Мочкорж И. Математические принципы нечеткой логики. – М.: Физматлит, 2006. – 352 с.

47 Абалдова С.Ю., Волынский В.Ю. Разработка системы нечеткого вывода оценки результативности системы менеджмента качества предприятия на основе алгоритма Мамдани // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. – 2011. – №1. – С.86-93.

48 Голосовский М.С., Богомолов А.В., Теребов Д.С. и др. Алгоритм настройки системы нечёткого логического вывода типа Мамдани // Вестник Южно-Уральского государственного университета. – 2018. – №3. – С. 19-29.

49 Горбачев С.В. Фаззификация экспертных лингвистических данных, заданных в порядковой шкале // Матер. докл. 4-й междунар. заочн. Науч.-практ. конф. «Интеллектуальные информационные системы: тенденции, проблемы, перспективы (ИИС-2016). – Курск, 2017. – С. 47-49.

50 Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ Петербурr, 2005. – 736 с.

51 Belarbi K. Design of Mamdani fuzzy logic controllers with rule base minimisation using genetic algorithm // Engineering applications of artificial intelligence. – 2005. – Vol. 18, Issue 7. – P. 875-880.

52 Грибин М.А. Применение алгоритма Мамдани в системах автоматического управления // Развитие современной науки: теоретические и прикладные аспекты. – 2019. – №22. – С. 16-19.

53 ISO/IEC 27001:2022. Информационная безопасность, кибербезопасность и защита персональных данных // https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2022.pdf. 14.12.2022.

54 ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection // https://www.iso.org/standard/80585. 14.12.2022.

55 NIST SP 800-39. Managing Information Security Risk // https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication. 14.12.2022.

56 Методология FAIR (Factor Analysis of Information Risk) // <https://www.risklens.com/hubfs/uploads/2019/04/An_Adoption_Guide.> 14.12.2022.

57 Методология OCTAVE для оценки информационных рисков // <http://www.risk24.ru/octave.htm>. 14.12.2022.

58 Interoperable EU risk management framework // <https://www.enisa>. europa.eu/publications/interoperable-eu-risk-management-framework. 14.12.2022.

59 Amirova A., Tokhmetov A. A model for risk analysis in the industrial internet of things // Journal of Theoretical and Applied Information Technology. – 2021. – Vol. 14. – P. 3449-3459.

60 Kerimkhulle S., Dildebayeva Zh., Tokhmetov А., Amirova А., Tussupov J., Makhazhanova U., Adalbek А., Taberkhan R., Zakirova А., Salykbayeva А. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things // Symmetry. – 2023. – №10. – Р. 1-29.

61 Александрович Г.Я., Нестеров С.А., Петренко С.А. Автоматизация оценки информационных рисков компании // Защита информации. – 2003. – №2. – С. 78-81.

62 Амирова А.С., Тохметов А.Т. Комбинированная модель обнаружения угроз в сетях промышленного интернета вещей // Procced. internat. scient. conf. «Global science and innovations 2022: Central Asia». – Астана, 2022. – С. 91-95.

63 Даниярулы Ж., Кажиманова М.К. Оценка весов информационных активов ииот-системы на основе метода анализа иерархий // Research forum сб. ст. 3-й междунар. науч.-практ. конф. – Петрозаводск, 2023. – С. 101-111.

64 Амирова А.С., Тохметов А.Т. Заттар өнеркәсіптік интернетіндегі қауіпті анықтаудың аралас моделі // Вестник КазНПУ им. Абая. – 2022. – №1(77). – С. 70-77.

65 Копырин А.С., Копырина А.О. Построение типовой системы правил вывода по базе знаний // Программные системы и вычислительные методы. – 2021. – №1. – С. 1-9.

66 Штовба С.Д. Проектирование нечетких систем средствами МАТLАВ. – М., 2007. – 288 с.

67 Дьяконов В. Математические пакеты расширения MATLAB: cпециальный справочник. – СПб.: Питер, 2001. – 480 с.

68 Амирова А.С., Тохметов А.Т. Анализ рисков информационной безопасности в сетях промышленного интернета вещей // Вестник Национальной инженерной академии Республики Казахстан. – 2022. – №1(83). – С. 10-20.

69 Татжибаева О.А. Разработка экспертных систем: метод. указ. – Оренбург: ГОУ ОГУ, 2005. – 23с.

70 Глушань В.М., Карелин В.П., Кузьменко О.Л. Нечёткие модели и методы многокритериального выбора в интеллектуальных системах поддержки принятия решений // Известия ЮФУ. Технические науки. – 2009. – №4(93). – С. 106-113.

71 Интеллектуальные системы: коллективная монография / под ред. В.М. Курейчик и др. – М.: Физматлит, 2009. – Вып. 3. – 196 с.

72 Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. – М., 2007. – 284 с.

73 Курейчик В.В., Курейчик В.М., Ковалев С.М. Оптонечёткие системы // Известия ЮФУ. Технические науки. – 2009. – №4(93). – С. 99-105.

74 Полковникова Н.А., Курейчик В.М. Разработка модели экспертной системы на основе нечёткой логики. Известия ЮФУ. Технические науки. – 2014. – №1(150). – С. 83-92.

75 Коробулина О.Ю., Иванова Н.В. Экспертная система аудита информационной безопасности // Программные продукты и системы. – 2010. – №4. – С. 57-69.

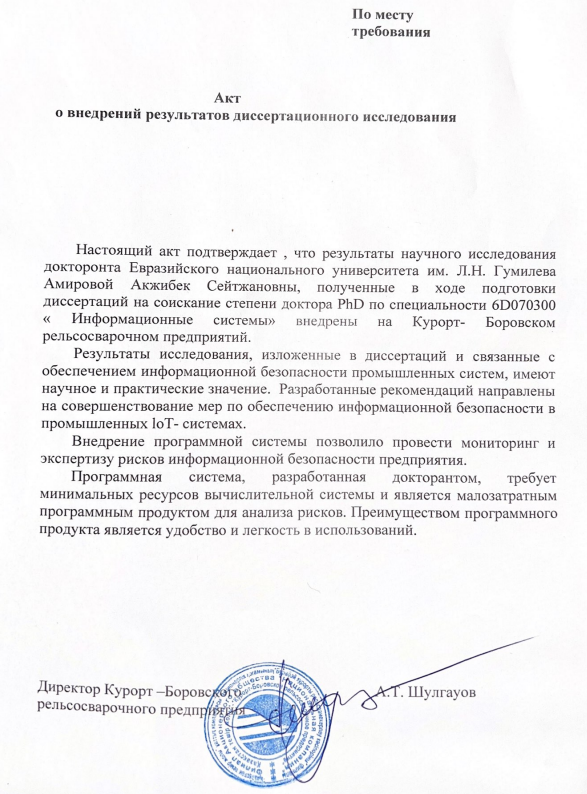
**ПРИЛОЖЕНИЕ А**

Свидетельство об авторском праве



**ПРИЛОЖЕНИЕ Б**

Акт внедрения



**ПРИЛОЖЕНИЕ В**

Часть кода программы

from tkinter import \*

from tkinter import messagebox

from parameters import \*

import json as js

import matplotlib.pyplot as plt

def login():

global login\_entry, password\_entry

try:

with open('users.json', 'r') as file:

data = js.load(file)

if login\_entry.get() not in data.keys():

messagebox.showerror('Ошибка', 'Неверный логин')

else:

if password\_entry.get() not in data.values():

messagebox.showerror('Ошибка', 'Неверный пароль')

else:

main\_page()

except FileNotFoundError:

messagebox.showerror('Ошибка', 'Пользователи отсутствуют')

def register(user={}):

global login\_entry, password\_entry, password\_entry\_2

try:

with open('users.json','r') as file:

data = js.load(file)

if login\_entry.get() in data.keys():

messagebox.showerror('Ошибка', 'Пользователь с таким именем уже существует')

else:

if password\_entry.get() == password\_entry\_2.get():

user[login\_entry.get()] = password\_entry.get()

with open('users.json', 'w') as file:

js.dump(user, file)

messagebox.showinfo('ОК', 'Регистрация завершена')

sign\_in()

else:

messagebox.showerror('Ошибка', 'Пароли не совпадают')

except FileNotFoundError:

if password\_entry.get() == password\_entry\_2.get():

user[login\_entry.get()] = password\_entry.get()

with open('users.json', 'w') as file:

js.dump(user, file)

messagebox.showinfo('ОК', 'Регистрация завершена')

sign\_in()

else:

messagebox.showerror('Ошибка', 'Пароли не совпадают')

def get\_password():

global login\_entry, password\_entry, password\_entry\_2

try:

with open('users.json','r+') as file:

data = js.load(file)

if login\_entry.get() not in data.keys():

messagebox.showerror('Ошибка', 'Данный пользователь не зарегистрирован')

else:

if password\_entry.get() == password\_entry\_2.get():

data[login\_entry.get()] = password\_entry.get()

file.seek(0)

js.dump(data, file)

file.truncate()

messagebox.showinfo('ОК', 'Пароль изменён')

sign\_in()

else:

messagebox.showerror('Ошибка', 'Пароли не совпадают')

except FileNotFoundError:

messagebox.showerror('Ошибка', 'Пользователи отсутствуют')

sign\_in()

def show\_diagram(colors=[]):

global risks, ro

if ro == 5:

data = dict(list(risks.items())[:4])

elif ro == 6:

data = dict(list(risks.items())[:3])

else:

data = risks

courses = list(data.keys())

values = list(data.values())

for value in values:

if 0 <= value < 2:

colors.append('#4dfa59')

elif 2 <= value < 3.5:

colors.append('#75fa7e')

elif 3.5 <= value < 7.1:

colors.append('#faf575')

elif 7.1 <= value < 11:

colors.append('#fc6d00')

else:

colors.append('#fc1900')

fig = plt.figure(figsize = (10, 5))

plt.bar(courses, values, color = colors, width = 0.2)

plt.xlabel('Угрозы')

plt.ylabel('Уровень риска')

plt.title('Анализ рисков информационной безопасности в IIoT')

plt.show()

def show\_attacks():

global var, ro, json

root = Tk()

root.title('Анализ рисков IIoT')

root.geometry('900x700')

root.resizable(False, False)

root.config(bg='white')

danger = Label(root, text='Угрозы', font=('Consolas', 20), bg='white', fg='#31b053')

danger.place(x=210, y=150)

x = 150

y = 220

for i,j in json.items():

desc = Label(root, text=f'{i} - {j}', font=('Consolas', 15), bg='white', fg='#31b053')

desc.place(x=x, y=y)

y += 50

root.mainloop()

def show\_recommendations():

file = open("recommendations.txt", encoding='UTF-8')

data = file.read()

file.close()

root = Tk()

root.resizable(False, False)

widget = Text(root)

scrollbar = Scrollbar(root)

scrollbar.pack(side=RIGHT, fill=Y)

widget.pack(side=LEFT, fill=Y)

scrollbar.config(command=widget.yview)

widget.config(yscrollcommand=scrollbar.set)

widget.insert(END, data)

root.mainloop()

def show\_results():

global root, risks, json

root.destroy()

root = Tk()

root.title('Анализ рисков IIoT')

root.geometry('900x700')

root.resizable(False, False)

root.config(bg='white')

danger = Label(root, text='Угроза', font=('Consolas', 20), bg='white', fg='#31b053')

risk\_level = Label(root, text='Уровень риска', font=('Consolas', 20), bg='white', fg='#31b053')

diagram\_button = Button(root, text='Диаграмма', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=show\_diagram)

recommendations\_button = Button(root, text='Рекомендации', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=show\_recommendations)

back\_button = Button(root, text='Назад', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=t\_page\_7)

danger.place(x=80, y=150)

risk\_level.place(x=600, y=150)

diagram\_button.place(x=600, y=500)

recommendations\_button.place(x=370, y=500)

back\_button.place(x=200, y=500)

x = 80

y = 220

for i,j in json.items():

if 0 <= risks[i] < 0.2:

risk = 'Очень низкий'

elif 0.2 <= risks[i] < 3.5:

risk = 'Низкий'

elif 3.5 <= risks[i] < 7.1:

risk = 'Средний'

elif 7.1 <= risks[i] < 11:

risk = 'Высокий'

elif risks[i] >= 11:

risk = 'Критически высокий'

desc = Label(root, text=f'{j+" "\*(53-len(j))} - {risk}', font=('Consolas', 15), bg='white', fg='black')

desc.place(x=x, y=y)

y += 50

root.mainloop()

def calculate\_risks():

global risks

risks = {'T1':0, 'T2':0, 'T3':0, 'T4':0, 'T5':0}

risks['T1'] = (sum([cr\_1\_3['T1'][0]\*cr\_4\_7['T1'][0], cr\_1\_3['T1'][1]\*cr\_4\_7['T1'][1], cr\_1\_3['T1'][2]\*cr\_4\_7['T1'][2]]) / 3) \* 100

risks['T2'] = (sum([cr\_1\_3['T2'][0]\*cr\_4\_7['T2'][0], cr\_1\_3['T2'][1]\*cr\_4\_7['T2'][1], cr\_1\_3['T2'][2]\*cr\_4\_7['T2'][2]]) / 3) \* 100

risks['T3'] = (sum([cr\_1\_3['T3'][0]\*cr\_4\_7['T3'][0], cr\_1\_3['T3'][1]\*cr\_4\_7['T3'][1], cr\_1\_3['T3'][2]\*cr\_4\_7['T3'][2]]) / 3) \* 100

risks['T4'] = (sum([cr\_1\_3['T4'][0]\*cr\_4\_7['T4'][0], cr\_1\_3['T4'][1]\*cr\_4\_7['T4'][1], cr\_1\_3['T4'][2]\*cr\_4\_7['T4'][2]]) / 3) \* 100

risks['T5'] = (sum([cr\_1\_3['T5'][0]\*cr\_4\_7['T5'][0], cr\_1\_3['T5'][1]\*cr\_4\_7['T5'][1], cr\_1\_3['T5'][2]\*cr\_4\_7['T5'][2]]) / 3) \* 100

show\_results()

def options\_handle(check\_list = []):

if cnt == 0:

check\_list = [value\_inside\_1.get(), value\_inside\_2.get(), value\_inside\_3.get(), value\_inside\_4.get(), value\_inside\_5.get(), value\_inside\_6.get(), value\_inside\_7.get()]

for i in check\_list:

if i in cr\_options\_default:

messagebox.showerror("Ошибка", "Пожалуйста, заполните все параметры.")

break

else:

t\_page\_1()

else:

if ro == 5:

check\_list = [value\_1.get(), value\_2.get(), value\_3.get(), value\_4.get()]

elif ro == 6:

check\_list = [value\_1.get(), value\_2.get(), value\_3.get()]

else:

check\_list = [value\_1.get(), value\_2.get(), value\_3.get(), value\_4.get(), value\_5.get()]

for i in check\_list:

if i == 'Выбрать':

messagebox.showerror("Ошибка", "Пожалуйста, заполните все параметры.")

break

else:

if cnt == 1:

t\_page\_2()

elif cnt == 2:

t\_page\_3()

elif cnt == 3:

t\_page\_4()

elif cnt == 4:

t\_page\_5()

elif cnt == 5:

t\_page\_6()

elif cnt == 6:

t\_page\_7()

else:

calculate\_risks()

def t\_page\_7():

global root, cnt, value\_1, value\_2, value\_3, value\_4, value\_5, cr\_4\_7, page, t\_values\_6, t\_values\_7

cnt = 7

t\_values\_6 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()]]

if ro != 6:

t\_values\_6 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()]]

if ro != 5 and ro != 6:

t\_values\_6 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()], t\_json[value\_5.get()]]

if page == 7:

weight = cr\_json[value\_inside\_7.get()]

t1 = [i\*weight for i in t\_values\_3[0]]

cr\_4\_7['T1'] = [round(cr\_4\_7['T1'][0]-t1[0], 3), round(cr\_4\_7['T1'][1]-t1[1], 3), round(cr\_4\_7['T1'][2]-t1[2], 3)]

t2 = [i\*weight for i in t\_values\_3[1]]

cr\_4\_7['T2'] = [round(cr\_4\_7['T2'][0]-t2[0], 3), round(cr\_4\_7['T2'][1]-t2[1], 3), round(cr\_4\_7['T2'][2]-t2[2], 3)]

t3 = [i\*weight for i in t\_values\_3[2]]

cr\_4\_7['T3'] = [round(cr\_4\_7['T3'][0]-t3[0], 3), round(cr\_4\_7['T3'][1]-t3[1], 3), round(cr\_4\_7['T3'][2]-t3[2], 3)]

if ro != 6:

t4 = [i\*weight for i in t\_values\_3[3]]

cr\_4\_7['T4'] = [round(cr\_4\_7['T4'][0]-t4[0], 3), round(cr\_4\_7['T4'][1]-t4[1], 3), round(cr\_4\_7['T4'][2]-t4[2], 3)]

if ro != 5 and ro != 6:

t5 = [i\*weight for i in t\_values\_3[4]]

cr\_4\_7['T5'] = [round(cr\_4\_7['T5'][0]-t5[0], 3), round(cr\_4\_7['T5'][1]-t5[1], 3), round(cr\_4\_7['T5'][2]-t5[2], 3)]

page = 6

try:

weight = cr\_json[value\_inside\_6.get()]

t1 = [i\*weight for i in t\_json[value\_1.get()]]

cr\_4\_7['T1'] = [round(cr\_4\_7['T1'][0]+t1[0], 3), round(cr\_4\_7['T1'][1]+t1[1], 3), round(cr\_4\_7['T1'][2]+t1[2], 3)]

t2 = [i\*weight for i in t\_json[value\_2.get()]]

cr\_4\_7['T2'] = [round(cr\_4\_7['T2'][0]+t2[0], 3), round(cr\_4\_7['T2'][1]+t2[1], 3), round(cr\_4\_7['T2'][2]+t2[2], 3)]

t3 = [i\*weight for i in t\_json[value\_3.get()]]

cr\_4\_7['T3'] = [round(cr\_4\_7['T3'][0]+t3[0], 3), round(cr\_4\_7['T3'][1]+t3[1], 3), round(cr\_4\_7['T3'][2]+t3[2], 3)]

if ro != 6:

t4 = [i\*weight for i in t\_json[value\_4.get()]]

cr\_4\_7['T4'] = [round(cr\_4\_7['T4'][0]+t4[0], 3), round(cr\_4\_7['T4'][1]+t4[1], 3), round(cr\_4\_7['T4'][2]+t4[2], 3)]

if ro != 5 and ro != 6:

t5 = [i\*weight for i in t\_json[value\_5.get()]]

cr\_4\_7['T5'] = [round(cr\_4\_7['T5'][0]+t5[0], 3), round(cr\_4\_7['T5'][1]+t5[1], 3), round(cr\_4\_7['T5'][2]+t5[2], 3)]

except KeyError:

pass

root.destroy()

root = Tk()

root.title('Анализ рисков IIoT')

root.geometry('900x700')

root.resizable(False, False)

root.config(bg='white')

criterion = Label(root, text='Критерий:', font=('Consolas', 20), bg='white', fg='#31b053')

danger = Label(root, text='Угроза:', font=('Consolas', 20), bg='white', fg='#31b053')

cr = Label(root, text='Предыдущие угрозы', font=('Consolas', 20), bg='white', fg='#31b053')

next\_button = Button(root, text='Далее', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=options\_handle)

show\_t = Button(root, text='Список угроз', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=show\_attacks)

show\_t.place(x=370, y=500)

back\_button = Button(root, text='Назад', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=t\_page\_6)

criterion.place(x=50, y=100)

cr.place(x=300, y=100)

danger.place(x=50, y=200)

next\_button.place(x=600, y=500)

back\_button.place(x=200, y=500)

x = 200

for i in json.keys():

threat = Label(root, text=f'{i}', font=('Consolas', 20), bg='white', fg='grey')

threat.place(x=x, y=200)

x += 150

value\_1 = StringVar(root)

value\_1.set('Выбрать')

cr\_menu\_1 = OptionMenu(root, value\_1, \*t\_list)

cr\_menu\_1.config(bg='white')

cr\_menu\_1.config(width=10)

cr\_menu\_1.config(height=2)

value\_2 = StringVar(root)

value\_2.set('Выбрать')

cr\_menu\_2 = OptionMenu(root, value\_2, \*t\_list)

cr\_menu\_2.config(bg='white')

cr\_menu\_2.config(width=10)

cr\_menu\_2.config(height=2)

value\_3 = StringVar(root)

value\_3.set('Выбрать')

cr\_menu\_3 = OptionMenu(root, value\_3, \*t\_list)

cr\_menu\_3.config(bg='white')

cr\_menu\_3.config(width=10)

cr\_menu\_3.config(height=2)

value\_4 = StringVar(root)

value\_4.set('Выбрать')

cr\_menu\_4 = OptionMenu(root, value\_4, \*t\_list)

cr\_menu\_4.config(bg='white')

cr\_menu\_4.config(width=10)

cr\_menu\_4.config(height=2)

value\_5 = StringVar(root)

value\_5.set('Выбрать')

cr\_menu\_5 = OptionMenu(root, value\_5, \*t\_list)

cr\_menu\_5.config(bg='white')

cr\_menu\_5.config(width=10)

cr\_menu\_5.config(height=2)

cr\_menu\_1.place(x=160, y=300)

cr\_menu\_2.place(x=310, y=300)

cr\_menu\_3.place(x=460, y=300)

if ro != 6:

cr\_menu\_4.place(x=610, y=300)

if ro != 5 and ro != 6:

cr\_menu\_5.place(x=760, y=300)

root.mainloop()

def t\_page\_6():

global root, cnt, value\_1, value\_2, value\_3, value\_4, value\_5, cr\_4\_7, page, t\_values\_5, t\_values\_6

cnt = 6

t\_values\_5 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()]]

if ro != 6:

t\_values\_5 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()]]

if ro != 5 and ro != 6:

t\_values\_5 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()], t\_json[value\_5.get()]]

if page == 6:

weight = cr\_json[value\_inside\_6.get()]

t1 = [i\*weight for i in t\_values\_3[0]]

cr\_4\_7['T1'] = [round(cr\_4\_7['T1'][0]-t1[0], 3), round(cr\_4\_7['T1'][1]-t1[1], 3), round(cr\_4\_7['T1'][2]-t1[2], 3)]

t2 = [i\*weight for i in t\_values\_3[1]]

cr\_4\_7['T2'] = [round(cr\_4\_7['T2'][0]-t2[0], 3), round(cr\_4\_7['T2'][1]-t2[1], 3), round(cr\_4\_7['T2'][2]-t2[2], 3)]

t3 = [i\*weight for i in t\_values\_3[2]]

cr\_4\_7['T3'] = [round(cr\_4\_7['T3'][0]-t3[0], 3), round(cr\_4\_7['T3'][1]-t3[1], 3), round(cr\_4\_7['T3'][2]-t3[2], 3)]

if ro != 6:

t4 = [i\*weight for i in t\_values\_3[3]]

cr\_4\_7['T4'] = [round(cr\_4\_7['T4'][0]-t4[0], 3), round(cr\_4\_7['T4'][1]-t4[1], 3), round(cr\_4\_7['T4'][2]-t4[2], 3)]

if ro != 5 and ro != 6:

t5 = [i\*weight for i in t\_values\_3[4]]

cr\_4\_7['T5'] = [round(cr\_4\_7['T5'][0]-t5[0], 3), round(cr\_4\_7['T5'][1]-t5[1], 3), round(cr\_4\_7['T5'][2]-t5[2], 3)]

page = 5

try:

weight = cr\_json[value\_inside\_5.get()]

t1 = [i\*weight for i in t\_json[value\_1.get()]]

cr\_4\_7['T1'] = [round(cr\_4\_7['T1'][0]+t1[0], 3), round(cr\_4\_7['T1'][1]+t1[1], 3), round(cr\_4\_7['T1'][2]+t1[2], 3)]

t2 = [i\*weight for i in t\_json[value\_2.get()]]

cr\_4\_7['T2'] = [round(cr\_4\_7['T2'][0]+t2[0], 3), round(cr\_4\_7['T2'][1]+t2[1], 3), round(cr\_4\_7['T2'][2]+t2[2], 3)]

t3 = [i\*weight for i in t\_json[value\_3.get()]]

cr\_4\_7['T3'] = [round(cr\_4\_7['T3'][0]+t3[0], 3), round(cr\_4\_7['T3'][1]+t3[1], 3), round(cr\_4\_7['T3'][2]+t3[2], 3)]

if ro != 6:

t4 = [i\*weight for i in t\_json[value\_4.get()]]

cr\_4\_7['T4'] = [round(cr\_4\_7['T4'][0]+t4[0], 3), round(cr\_4\_7['T4'][1]+t4[1], 3), round(cr\_4\_7['T4'][2]+t4[2], 3)]

if ro != 5 and ro != 6:

t5 = [i\*weight for i in t\_json[value\_5.get()]]

cr\_4\_7['T5'] = [round(cr\_4\_7['T5'][0]+t5[0], 3), round(cr\_4\_7['T5'][1]+t5[1], 3), round(cr\_4\_7['T5'][2]+t5[2], 3)]

except KeyError:

pass

root.destroy()

root = Tk()

root.title('Анализ рисков IIoT')

root.geometry('900x700')

root.resizable(False, False)

root.config(bg='white')

criterion = Label(root, text='Критерий:', font=('Consolas', 20), bg='white', fg='#31b053')

danger = Label(root, text='Угроза:', font=('Consolas', 20), bg='white', fg='#31b053')

cr = Label(root, text='Ущерб репутации', font=('Consolas', 20), bg='white', fg='#31b053')

next\_button = Button(root, text='Далее', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=options\_handle)

show\_t = Button(root, text='Список угроз', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=show\_attacks)

show\_t.place(x=370, y=500)

back\_button = Button(root, text='Назад', font=('Consolas', 14), bg='white', fg='#31b053', borderwidth=0, command=t\_page\_5)

criterion.place(x=50, y=100)

cr.place(x=300, y=100)

danger.place(x=50, y=200)

next\_button.place(x=600, y=500)

back\_button.place(x=200, y=500)

x = 200

for i in json.keys():

threat = Label(root, text=f'{i}', font=('Consolas', 20), bg='white', fg='grey')

threat.place(x=x, y=200)

x += 150

value\_1 = StringVar(root)

value\_1.set('Выбрать')

cr\_menu\_1 = OptionMenu(root, value\_1, \*t\_list)

cr\_menu\_1.config(bg='white')

cr\_menu\_1.config(width=10)

cr\_menu\_1.config(height=2)

value\_2 = StringVar(root)

value\_2.set('Выбрать')

cr\_menu\_2 = OptionMenu(root, value\_2, \*t\_list)

cr\_menu\_2.config(bg='white')

cr\_menu\_2.config(width=10)

cr\_menu\_2.config(height=2)

value\_3 = StringVar(root)

value\_3.set('Выбрать')

cr\_menu\_3 = OptionMenu(root, value\_3, \*t\_list)

cr\_menu\_3.config(bg='white')

cr\_menu\_3.config(width=10)

cr\_menu\_3.config(height=2)

value\_4 = StringVar(root)

value\_4.set('Выбрать')

cr\_menu\_4 = OptionMenu(root, value\_4, \*t\_list)

cr\_menu\_4.config(bg='white')

cr\_menu\_4.config(width=10)

cr\_menu\_4.config(height=2)

value\_5 = StringVar(root)

value\_5.set('Выбрать')

cr\_menu\_5 = OptionMenu(root, value\_5, \*t\_list)

cr\_menu\_5.config(bg='white')

cr\_menu\_5.config(width=10)

cr\_menu\_5.config(height=2)

cr\_menu\_1.place(x=160, y=300)

cr\_menu\_2.place(x=310, y=300)

cr\_menu\_3.place(x=460, y=300)

if ro != 6:

cr\_menu\_4.place(x=610, y=300)

if ro != 5 and ro != 6:

cr\_menu\_5.place(x=760, y=300)

root.mainloop()

def t\_page\_5():

global root, cnt, value\_1, value\_2, value\_3, value\_4, value\_5, cr\_4\_7, page, t\_values\_4, t\_values\_5

cnt = 5

t\_values\_4 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()]]

if ro != 6:

t\_values\_4 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()]]

if ro != 5 and ro != 6:

t\_values\_4 = [t\_json[value\_1.get()], t\_json[value\_2.get()], t\_json[value\_3.get()], t\_json[value\_4.get()], t\_json[value\_5.get()]]

if page == 5:

weight = cr\_json[value\_inside\_5.get()]

t1 = [i\*weight for i in t\_values\_3[0]]

cr\_4\_7['T1'] = [round(cr\_4\_7['T1'][0]-t1[0], 3), round(cr\_4\_7['T1'][1]-t1[1], 3), round(cr\_4\_7['T1'][2]-t1[2], 3)]

t2 = [i\*weight for i in t\_values\_3[1]]

cr\_4\_7['T2'] = [round(cr\_4\_7['T2'][0]-t2[0], 3), round(cr\_4\_7['T2'][1]-t2[1], 3), round(cr\_4\_7['T2'][2]-t2[2], 3)]

t3 = [i\*weight for i in t\_values\_3[2]]

cr\_4\_7['T3'] = [round(cr\_4\_7['T3'][0]-t3[0], 3), round(cr\_4\_7['T3'][1]-t3[1], 3), round(cr\_4\_7['T3'][2]-t3[2], 3)]

if ro != 6:

t4 = [i\*weight for i in t\_values\_3[3]]

cr\_4\_7['T4'] = [round(cr\_4\_7['T4'][0]-t4[0], 3), round(cr\_4\_7['T4'][1]-t4[1], 3), round(cr\_4\_7['T4'][2]-t4[2], 3)]

if ro != 5 and ro != 6:

t5 = [i\*weight for i in t\_values\_3[4]]

cr\_4\_7['T5'] = [round(cr\_4\_7['T5'][0]-t5[0], 3),