ОТЗЫВ

официального оппонента

доктора технических наук, профессора Аралбаева Ташбулата Захаровича

на диссертацию Кирилловой Анастасии Дмитриевны

на тему «**Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования**»,

представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Тематика исследований диссертационной работы Кирилловой А.Д. относится к категории проблем, решение которых имеет важное значение для эффективной работы АСУ промышленными объектами. Известно, что автоматизированные системы в настоящее время все чаще становятся мишенью целенаправленных кибератак со стороны различных категорий внешних и внутренних злоумышленников, нередко приводящих к ощутимому материальному и финансовому ущербу.

Значимость тематики исследований диссертации отражена, в частности, в таких руководящих документах, как: Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ, Приказы ФСТЭК России №235 и №239, стандарты серии ГОСТ Р МЭК 62443, вышедший в 2021 г. методический документ ФСТЭК России «Методика оценки угроз безопасности информации». В представленных документах особо отмечена необходимость детального анализа рисков множества угроз, уязвимостей и негативных последствий от воздействия этих угроз на информационные активы объекта.

Оценка рисков информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов представляет собой сложный, слабо структурированный и плохо

формализуемый процесс. Ввиду высокой степени неопределенности и большого числа факторов, влияющих на итоговый уровень защищенности системы, проблема оценки рисков ИБ АСУ ТП остается открытой и требует разработки и применения новых подходов, основанных на применении методов искусственного интеллекта. Специфика АСУ ТП создает дополнительные сложности при анализе и управлении рисками ИБ, поэтому необходимость использования данных методов связана с возможностью получения с их помощью объективной и достоверной оценки уровня защищенности промышленных автоматизированных систем с учетом влияния факторов неопределенности.

Таким образом, тема диссертационной работы, посвященная разработке метода и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе технологий когнитивного моделирования с целью обеспечения интеллектуальной поддержки принятия решений на этапе оценки уровня защищенности этих систем и выбора эффективных контрмер по защите информации, является актуальной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, библиографического списка и приложений. Основной текст диссертационной работы изложен на 167 страницах, содержит 83 рисунка, 32 таблицы, 8 приложений. Библиографический список включает в себя 184 наименования литературы. В приложениях содержатся акты внедрения и дополнительный материал по результатам исследований.

Во введении обоснована актуальность темы исследования, сформулирована цель и решаемые задачи, определена научная новизна, практическая значимость результатов исследования, представлены научные положения, выносимые на защиту.

В первой главе проведен анализ текущего состояние нормативно-правовой и методической базы в области обеспечения информационной безопасности (ИБ) АСУ ТП в условиях переменного характера угроз. Выявлены недостатки существующей научно-методической базы оценки рисков ИБ применительно к

автоматизированным системам промышленных объектов. Сделан вывод о возможности совершенствования существующих методов количественной оценки рисков ИБ как для подсистем так и для АСУ ТП в целом. Определены факторы повышения качества оценки риска на основе снижения неопределенности и трудоемкости процедуры формализации процессов, влияющих на уровень защищенности автоматизированных систем.

На основе Методики оценки угроз безопасности информации ФСТЭК России и Банка данных угроз безопасности информации (БДУ) ФСТЭК показана необходимость структурирования данных для автоматизации моделирования сценариев атак на АСУ ТП промышленных объектов с использованием баз данных MITRE. Сделан вывод о необходимости разработки метода, моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием методов когнитивного моделирования и машинного обучения.

Во второй главе представлена нечеткая когнитивная модель для количественной оценки рисков ИБ и алгоритм ее построения с использованием иерархии вложенных нечетких серых когнитивных карт применительно к зональной модели архитектуры АСУ ТП промышленного объекта.

Предложенная модель позволяет формализовать сценарии атак с требуемым уровнем детализации в пределах выделенных зон АСУ ТП с учетом ее многоуровневой организации, что позволяет повысить достоверность и обоснованность количественной оценки рисков ИБ и обеспечить выбор эффективных контрмер в условиях воздействия факторов неопределенности и разброса экспертных оценок.

В третьей главе представлен метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, реализующий заключительные этапы Методики оценки угроз безопасности ФСТЭК России.

Предложена методика количественной оценки рисков ИБ АСУ ТП на основе иерархии когнитивных моделей и алгоритма построения сценариев атак в выделенных зонах промышленного объекта, что позволяет определить количественные оценки рисков ИБ и оптимальное распределение затрат на

реализацию, внедрение и сопровождение контрмер с учетом их функциональны ограничений.

В четвертой главе разработана архитектура исследовательского прототип интеллектуальной системы поддержки принятия решений (ИСППР) и программна реализация инструментальных средств автоматизации оценки рисков ИБ моделирования сценариев атак. Рассмотрены особенности практическог применения разработанного метода, моделей, алгоритмов и инструментальны средств оценки рисков ИБ АСУ ТП промышленных объектов для решени прикладных задач.

В Заключении приводятся основные результаты и выводы по проделанно работе.

В приложениях приводятся результаты экспериментов**.**

Степень обоснованности научных положений, выводов и рекомендаций сформулированных в диссертации

Обоснованность научных положений и выводов, сформулированных диссертации, не вызывает сомнений. Это подтверждается опубликованными по материалам исследования работами, включая 8 статей в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, и в научных изданиях, индексируемых базой данных RSCI, 4 работы в изданиях, включенных в базу Scopus, 16 статей в других изданиях, а также получено 3 свидетельства о государственной регистрации программ для ЭВМ.

В целом, диссертационная работа имеет четкую логическую структуру основные разделы последовательны и взаимосвязаны.

Работа хорошо иллюстрирована, имеет список определений основных терминов. Приложения содержат необходимые таблицы с пояснениями основных результатов.

Автореферат достаточно полно раскрывает основное содержание диссертации. Полученные результаты соответствуют специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов

Достоверность полученных результатов и выводов основана на том, чт решения, предложенные в работе, подтверждаются корректной постановкой задач выбором методов исследования; результатами практического применени предложенного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП пр решении ряда прикладных задач; результатами сравнительного анализ количественных оценок рисков ИБ, полученных по итогам когнитивног моделирования, и экспертных оценок рисков ИБ АСУ ТП промышленного объекта апробацией на научных конференциях, публикацией результатов в ведущи рецензируемых научных изданиях.

Научная новизна работы

Наиболее существенные новые научные результаты, полученные диссертации, состоят в разработке метода и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологии когнитивного моделирования, отличающиеся от известных учетом особенностей многоуровневой организации АСУ ТП промышленных объектов, позволяющим формализовать сценарии компьютерных атак с требуемым уровнем их детализации а также повысить достоверность и обоснованность количественной оценки рисков ИБ.

К новым научным результатам, полученным в диссертационном исследовании, следует отнести следующие:

1) разработана нечеткая когнитивная модель оценки рисков ИБ АСУ ТП промышленных объектов, а также алгоритм ее построения, отражающая многоуровневую организацию промышленных систем автоматизации за счет использования иерархии вложенных серых НКК;

2) разработан метод количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием методов когнитивного моделирования и машинного обучения, в котором применяется информация из открытых баз данных угроз, уязвимостей и

компьютерных атак для формализации описания объекта защиты, актуальных угроз, уязвимостей в виде иерархии графовых моделей.

3) разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак с применением нечеткого когнитивного моделирования и методов машинного обучения для оценки рисков ИБ выделенных зон АСУ ТП с последующей оптимизацией распределения затрат на меры защиты с учетом их функциональных ограничений;

4) разработана архитектура ИСППР и программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП промышленных объектов.

Теоретическая и практическая значимость полученных автором результатов

В работе теоретически обоснован выбор концепции исследований, сформирован и разработан модельный базис для описания процедуры построения метода оценки рисков, доказана необходимость разработки алгоритмов и методики количественной оценки рисков ИБ АСУ ТП на основе технологий когнитивного моделирования а также программной реализации средств моделирования сценариев атак, применение которых позволит повысить достоверность и оперативность принимаемых управленческих решений по обеспечению ИБ АСУ ТП.

Практическая значимость результатов подтверждается разработкой методики и инструментальных средств автоматизации моделирования сценариев атак в составе интеллектуальной системы поддержки приятия решений, а также решением с их помощью прикладных задач оценки рисков ИБ АСУ ТП на примере анализа территориально распределенной системы обустройства месторождения и транспорта товарной нефти. Результаты работы внедрены и используются в ряде организаций, что подтверждается актами внедрения.

К достоинствам диссертационной работы следует отнести:

- системность научного подхода к проведению исследований;
- результаты исследований подтверждены большим экспериментальным материалом;

- большой спектр исследуемых вопросов и перечень авторских публикаций;
- возможность использования результатов исследований в учебном процессе вуза;
- из результатов диссертации особый интерес представляют сведения о моделировании характера изменения рисков с учетом различной специфики сценариев развития атаки, касающиеся количества циклов в работе генетического алгоритма, колебательности процесса установки интервалов оценок, наличия (отсутствия) установившего состояния оценок, разброса оценок экспертов. Пожелание диссертанту – учесть это в дальнейшей работе.

Замечания по диссертационной работе

1. В содержании текста диссертации не приведены результаты анализа возможности применения разработанной методики и ее аналогов применительно к распределенным в пространстве АСУ транспортными трубопроводами нефте-газового сырья и продуктов.

2. В работе решается задача сценарного моделирования графов реализации атаки с использованием графовой базы данных, однако желательно было бы уточнить порядок и формат формирования запросов к указанной базе данных с учетом требований по репрезентативности и достоверности исходных данных.

3. В работе недостаточно четко представлен механизм получения конкретных численных оценок снижения рисков при интервальной оценке параметров концептов.

4. Текст работы, в частности в главе 4, избыточно насыщен материалом пояснительного и иллюстративного характера, часть из которого без ущерба для представления и понимания результатов исследований может быть перемещен в приложение, например, рисунки: 4.7, 4.29. В тексте также встречаются отдельные выражения, редко используемые в научной литературе, в частности, как «эксплуатация контрмер».

Вместе с тем, отмеченные недостатки не носят принципиальный характер и не снижают общей положительной оценки работы, которая в целом выполнена на высоком научном уровне.

Заключение

Диссертация Кирилловой А.Д., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, в которой решена актуальная задача разработки метода и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования, результаты которой обладают существенной научной новизной и практической ценностью (значимость).

Считаю, что диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, а ее автор, Кириллова Анастасия Дмитриевна, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
доктор технических наук, профессор
заведующий кафедрой вычислительной
техники и защиты информации,
Федерального государственного бюджетного
образовательного учреждения высшего образования
«Оренбургский государственный университет»

Аралбаев Ташбулат Захарович

03.06.2023

Докторская диссертация защищена
по специальности 05.13.06 – Автоматизация и управление технологическими процессами

Даю согласие на обработку персональных данных.

Адрес места основной работы: 460018, г. Оренбург, просп. Победы, д. 13
Рабочий телефон: 8-902-365-73-53
Адрес эл. почты: atz1953@gmail.com

Подпись Аралбаева Т. З.
заверяю
Ведущий специалист по
документационному обеспечению
работы с персоналом
Дмитриенко

ОТДЕЛ КАДРОВ