ОТЗЫВ

официального оппонента

доктора технических наук, доцента Баранковой Инны Ильиничны

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

Статистика последних лет свидетельствует о постоянном росте числа компьютерных атак на автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных объектов, целью которых является промышленный шпионаж, мошенничество, нарушение нормального функционирования предприятия. Потеря управления над промышленными системами автоматизации часто приводит к нежелательным последствиям в отдельных субъектах государства, отражается на экономических показателях страны в целом, снижает безопасность жизнедеятельности населения, поэтому обеспечение информационной безопасности (ИБ) АСУ ТП промышленных объектов имеет важное значение.

Оценка рисков ИБ является необходимым этапом комплексного подхода к обеспечению ИБ АСУ ТП промышленных объектов. Существующие подходы и методики в основном направлены на оценку качественных показателей рисков ИБ, что затрудняет возможность ранжирования рисков ИБ по степени их критичности и получения сколько-нибудь полной и точной картины последствий (ожидаемого ущерба) от воздействия угроз.

Таким образом, тема диссертации, посвященная разработке метода и алгоритмов количественной оценки рисков ИБ АСУ ТП с использованием методов когнитивного моделирования и машинного обучения, является актуальной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, словаря терминов, списка литературы и приложений. Основной текст диссертационной работы изложен на 167 страницах, содержит 83 рисунка, 32 таблицы, 8 приложений. Список литературы состоит из 184 наименований.

Структура и содержание диссертации соответствует поставленным задачам и цели исследования.

Во введении обоснована актуальность темы исследования, сформулирована цель и решаемые задачи, определен объект и предмет исследования, изложена научная новизна и практическая значимость результатов исследования.

В первой главе проанализировано современное состояние проблемы обеспечения ИБ АСУ ТП промышленных объектов с учетом требований существующей нормативно-правовой и методической базы. Выделены особенности обеспечения ИБ, характерные для АСУ ТП промышленных объектов. Определены достоинства и недостатки существующих методов и методик оценки рисков ИБ применительно к АСУ ТП промышленных объектов.

Подчеркивается важная роль «Методики оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г. для решения задачи оценки рисков ИБ АСУ ТП с использованием Банка данных угроз безопасности информации (БДУ) ФСТЭК России. Отмечена необходимость разработки инструментальных средств автоматизации моделирования, позволяющих анализировать возможные сценарии компьютерных атак на АСУ ТП промышленных объектов и их негативные последствия с использованием БДУ ФСТЭК России и баз данных MITRE.

Во второй главе рассмотрена функциональная модель IDEF0 процесса количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе Методики угроз безопасности информации ФСТЭК России. Разработана и исследована нечеткая когнитивная модель количественной оценки рисков ИБ

АСУ ТП, а также алгоритм ее построения в классе вложенных серых нечетких когнитивных карт, использование которых, в отличие от существующих методов и подходов к оценке рисков ИБ, позволяет учитывает многоуровневую структуру АСУ ТП промышленных объектов и формализовать сценарии реализации компьютерных атак с требуемым уровнем детализации.

В третьей главе предложен метод и алгоритм количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения. Разработанный метод существенно повышает достоверность и полноту сценарного моделирования на основании формализованного описания объекта защиты, перечня угроз и уязвимостей в виде иерархии графовых моделей. Рассмотрена задача оптимизации параметров нечетких когнитивных моделей, отражающих распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

В четвертой главе разработаны инструментальные средства автоматизации моделирования сценариев атак на АСУ ТП промышленных объектов в составе интеллектуальной системы поддержки принятия решений (ИСППР), позволяющие извлечь и обработать информацию о слабых местах инфраструктуры АСУ ТП, наиболее опасных уязвимостях и актуальных угрозах безопасности информации, выявить потенциальные наиболее успешные сценарии реализации атак, оценить их последствия для промышленного объекта.

Рассмотрены особенности практического применения разработанного метода, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач.

В Заключении сформулированы основные результаты работы и выводы работы.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, высокая. Это

подтверждается корректной постановкой цели и задач исследования, обоснованным выбором и использованием методов их решения; анализом широкого круга библиографических источников, содержащих исследования отечественных и зарубежных авторов по рассматриваемой проблеме.

Достоверность и новизна полученных результатов подтверждается обсуждением основных положений и результатов диссертационной работы на большом количестве российских и международных конференций, публикацией основных результатов в ведущих рецензируемых журналах, а также апробацией результатов исследований в профильных организациях, подтвержденной актами внедрения.

Результаты диссертации опубликованы в 31 работе, в том числе в 8 статьях в изданиях, входящих в Перечень научных изданий, рекомендованных ВАК, и в научных изданиях, индексируемых в базе данных RSCI, 4 публикациях в изданиях, включенных в базу Scopus, 16 статьях в других изданиях, кроме того, получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Научная новизна работы заключается в следующем:

1. Разработана нечеткая когнитивная модель оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт, которые отражают многоуровневую структуру АСУ ТП промышленных объектов, позволяя формализовать возможные сценарии компьютерных атак с требуемым уровнем их детализации.

2. Разработан метод количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием методов когнитивного моделирования и машинного обучения, отличающийся применением шаблонов открытых баз знаний для формализации описания объектов атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей, обладающих наглядностью и возможностью

интерпретации результатов сценарного моделирования с целью выработки рекомендаций по защите информации.

3. Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак с использованием нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон безопасности АСУ ТП с последующей оптимизацией распределения затрат на контрмеры с учетом их функциональных ограничений.

4. Разработана архитектура исследовательского прототипа ИСППР и программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП промышленных объектов, применение которых позволяет повысить оперативность и достоверность оценки рисков ИБ и, в конечном итоге, повысить эффективность выбора контрмер на этапах проектирования, внедрения и эксплуатации комплексных систем защиты информации АСУ ТП промышленного объекта.

Теоретическая и практическая значимость полученных автором результатов

В диссертационной работе разработаны научно обоснованные теоретические положения, составляющие основу предложенного автором метода, алгоритмов и методики количественной оценки рисков ИБ АСУ ТП с использованием методов когнитивного моделирования и машинного обучения, использование которых позволит повысить достоверность и оперативность управленческих решений по обеспечению ИБ АСУ ТП промышленных объектов.

Практическая значимость результатов диссертации подтверждается разработкой методики и инструментальных средств автоматизации моделирования сценариев компьютерных атак в составе исследовательского прототипа ИСППР, а также решением прикладных задач, связанных с оценкой рисков ИБ АСУ ТП, в частности на примере анализа рисков ИБ территориально распределенной системы обустройства месторождения и транспорта товарной

нефти. Полученные результаты работы внедрены и использованы в ряде организаций, о чем свидетельствуют соответствующие акты внедрения.

Замечания по диссертационной работе

1. При описании нарушителей в сценариях реализации атак следует пользоваться классификацией нарушителей согласно Методике оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г.

2. Разработка алгоритма построения иерархии когнитивных моделей в разд. 2.4 представлена лишь в виде схем сворачивания и декомпозиции нечётких серых когнитивных карт и перечисления этапов, но не представлена в виде итоговой блок-схемы, что затрудняет анализ предложенного решения.

3. В разделе 3.2 при описании алгоритма построения графовых моделей недостаточно внимания уделено способам сокращения размерности графовой модели – указано лишь на необходимость оперирования перекрестными ссылками компонентов баз данных CVE-CWE-CAPEC-ATT&CK, что не позволяет оценить эффективность данной процедуры.

4. Предложенный в диссертации метод демонстрирует эффективность в выборе наиболее эффективных вариантов средств защиты при минимальных либо допустимых затратах. Большое количество АСУ ТП относятся к критической информационной инфраструктуре, для этого типа АСУ ТП критерием оптимизации следует выбирать минимизацию ущерба.

5. В п.4.4 диссертации указывается, что предложенные решения позволяют: сформировать расширенный список контрмер на основе базы знаний ATT&CK, NVD для каждой из выделенных зон. Группа матриц ATT&CK for ICS описывает тактики и техники, которые используются в атаках на промышленные системы управления, но контрмер она не содержит

6. Схема структурно-функциональной организации ИСППР в задачах оценки рисков ИБ АСУ ТП содержит модуль оценки эффективности и выбора контрмер. В диссертации не указано, как этот выбор осуществляется и на какой стадии разработки находится модуль.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают общей положительной оценки работы.

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 методов когнитивного моделирования и машинного обучения, результаты которой обладают научной новизной и практической ценностью.

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, доцент
заведующий кафедрой информатики
и информационной безопасности,
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Магнитогорский государственный технический
университет им. Г.И. Носова»

Баранкова Инна Ильинична

03.08.2023

Докторская диссертация защищена
по специальности 05.09.10 – Электротехнология

ПОДПИСЬ ЗАВЕРЯЮ
Начальник отдела делопроизводства
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Д.Г. Семенова

Даю согласие на обработку персональных данных.

Адрес места основной работы: 455000, г. Магнитогорск, пр. Ленина 38, ауд. 368
Рабочий телефон: +7 (3519) 23-27-51
Адрес эл. почты: inna_barankova@mail.ru