УТВЕРЖДАЮ
Проректор по научной и инновационной деятельности ОмГТУ, к.х.н.

_____ В.Ф. Фефелов
«__16__» _____ 2023 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

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

Современный этап развития промышленности (Индустрия 4.0) связан с масштабной цифровой трансформацией, что значительно обостряет проблему обеспечения информационной безопасности (ИБ) промышленных объектов, и в том числе их автоматизированных систем управления технологическими процессами (АСУ ТП). Оценка рисков ИБ является важным этапом комплексного подхода к обеспечению этих систем. Несмотря на то, что в последнее десятилетие активно развивается нормативно-правовая база обеспечения ИБ АСУ ТП, предложенные нормативно-методические решения все еще отстают от реальной практики применения. Они ориентированы, как правило, на качественную оценку рисков ИБ и не позволяют в полной мере оценить реальный уровень защищенности автоматизированных промышленных систем и выработать адекватные контрмеры по защите информации на данных объектах.

В то же время, в последние годы значительно выросли требования регуляторов к обеспечению защищенности АСУ ТП и значимых объектов критической информационной инфраструктуры (КИИ). Возникла настоятельная необходимость обеспечить частичную или полную автоматизацию процессов обработки больших объемов данных о состоянии ИБ АСУ ТП промышленных объектов, накапливаемых в современных системах обеспечения ИБ, что позволит повысить оперативность и достоверность не только качественной, но и количественной оценки рисков

ИБ и будет в конечном итоге способствовать повышению защищенности этих объектов в условиях воздействия потенциальных внешних и внутренних угроз информационной безопасности.

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

Оценка структуры и содержания работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, словаря терминов, списка литературы и приложений. Основной текст диссертации изложен на 167 страницах, содержит 83 рисунка, 32 таблицы и 8 приложений. Список литературы содержит 184 наименования.

Первая глава является обзорной и посвящена анализу современного состояния проблемы обеспечения ИБ АСУ ТП, описанию основных особенностей АСУ ТП промышленных объектов как объектов защиты, обуславливающих необходимость разработки и применения эффективных методов и алгоритмов количественной оценки рисков ИБ АСУ ТП с целью обоснованного выбора контрмер, направленных на повышение уровня защищенности этих объектов.

Во второй главе разработана функциональная модель процесса количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе Методики угроз безопасности информации ФСТЭК России. Предложена иерархия нечетких когнитивных моделей для проведения количественной оценки рисков ИБ в пределах выделенных зон АСУ ТП в условиях воздействия факторов неопределенности и разброса экспертных оценок.

Третья глава посвящена разработке метода сценарного моделирования атак на основе комплекса моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием принципов когнитивного моделирования, реализующих основные положения и рекомендации заключительного этапа Методики оценки угроз безопасности информации ФСТЭК России.

Четвертая глава содержит результаты разработки инструментальных средств автоматизации моделирования сценариев атак в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ АСУ ТП, а также результаты практического применения разработанного метода, моделей, алгоритмов и инструментальных средств для решения ряда прикладных задач.

В Заключении сформулированы основные результаты и выводы, полученные в диссертационной работе.

Область исследования диссертации соответствует пунктам паспорта научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»;

п. 8 «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения»;

п. 10. «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Оформление диссертации соответствует ГОСТ Р 7.0.11-2011. Автореферат диссертации выполнен с соблюдением установленных требований, полностью отражает ее содержание, полученные в ней практические и теоретические результаты и выводы.

Новизна полученных результатов

1. В работе разработана нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт в качестве зональных моделей АСУ ТП, применение которых позволяет учитывать многоуровневую организацию АСУ ТП промышленных объектов и формализовать процедуру построения сценариев атак с требуемым уровнем детализации в пределах выделенных зон.

2. Разработан метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий нечеткого когнитивного моделирования и методов машинного обучения, применение которого позволяет формализовать описание объекта атаки, перечня актуальных угроз безопасности информации и уязвимостей программного обеспечения (ПО) в виде иерархии графовых моделей и представить их в конечном итоге в виде последовательности действий (тактик и техник) нарушителя.

3. Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе иерархии вложенных нечетких когнитивных моделей и сценарного моделирования атак, применение которых позволяет оценить уровень защищенности выделенных зон АСУ ТП и определить оптимальное распределение ресурсов на реализацию контрмер по защите информации.

4. Предложена архитектура исследовательского прототипа ИСППР и программная реализация его модулей на основе предложенного в работе метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов, применение которых позволит повысить достоверность и оперативность получения количественных оценок рисков ИБ и, как следствие, обеспечить выбор адекватных контрмер мер, направленных на повышение уровня защищенности объектов.

Степень достоверности результатов исследования

Достоверность научных положений, результатов и выводов подтверждается корректной постановкой задач и выбором методов исследования, практическим применением разработанного метода, моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов при решении ряда прикладных задач, обсуждением полученных результатов на научных конференциях.

Публикации. Основные результаты диссертации опубликованы в 31 работе, в том числе в 8 статьях в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, а также в научных изданиях, индексируемых базой данных RSCI, 4 работах в изданиях, включенных в базу данных Scopus, 16 статьях в других изданиях. Получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Теоретическая и практическая значимость результатов, полученных автором диссертации

Автор теоретически обосновал и практически доказал необходимость и эффективность разработанного ею метода, алгоритмов и методики количественной оценки рисков ИБ АСУ ТП, а также программной реализации средств автоматизации моделирования сценариев атак в составе исследовательского прототипа ИСППР, применение которых позволит повысить достоверность и оперативность принимаемых управленческих решений на этапах проектирования и внедрения комплексных систем защиты информации АСУ ТП промышленных объектов.

Практическая значимость работы состоит в разработке и внедрении методики и инструментальных средств автоматизации моделирования сценариев атак в составе ИСППР, а также в решении с их помощью прикладных задач оценки рисков ИБ на примере анализа территориально распределенной АСУ ТП обустройства месторождения и транспорта товарной нефти. Рассмотрены сценарии эксплуатации уязвимостей объекта защиты, сформирован перечень актуальных угроз безопасности информации, предложены рекомендации по выбору контрмер для повышения уровня защищенности АСУ ТП промышленного объекта. Результаты работы прошли

апробацию в ряде организаций, что подтверждается соответствующими актами внедрения.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационной работы рекомендуются к расширенному использованию в организациях, занимающихся проектами в области аудита ИБ и комплексной оценки защищенности АСУ ТП промышленных объектов, а также внедрения и сопровождения средств защиты для поддержания требуемого уровня защищенности промышленных систем автоматизации.

Замечания по диссертационной работе

1. Эффективность применения предложенных в работе инструментальных средств автоматизации моделирования сценариев атак с последующей оценкой рисков ИБ для АСУ ТП показана на примере АСУ ТП нефтедобывающего предприятия. Вместе с тем, в работе не уделено достаточно внимания вопросам переносимости и масштабируемости предложенных решений на другие промышленные объекты.

2. Применение аппарата нечетких когнитивных карт сопровождается в работе введением шкалы оценки силы связей между концептами (таблица 2.1, стр. 62), однако не поясняется выбор количества и границ термов, а также не раскрывается обоснование выбора структуры когнитивной модели на рисунке 2.7.

3. Недостаточно подробно раскрыт процесс выбора весовых коэффициентов вложенной когнитивной модели при оценке эффективности применения выбранных контрмер (рисунок 3.14 и таблица 3.6, стр. 93).

4. Не раскрыты оценки сравнительных временных затрат на формирование сценариев реализации актуальных угроз ИБ в процессе построения модели угроз для объекта защиты, без применения разработанных решений и с их использованием, приведена лишь оценка их соотношения.

5. Неясно, насколько оправданным при разработке прототипа ИСППР является использование сразу нескольких фреймворков и языковых средств (Matlab, Python, C#).

Заключение

Приведенные выше замечания в целом не снижают общей положительной оценки работы и не ставят под сомнение основные научные и практические результаты диссертационной работы.

Диссертация Кирилловой Анастасии Дмитриевны на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором

исследований разработан метод, модели и алгоритмы количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования и машинного обучения, применение которых позволяет повысить оперативность и достоверность принимаемых управленческих решений на этапе оценки их уровня защищенности и выбора эффективных контрмер по защите информации.

Диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), а её автор – Кириллова Анастасия Дмитриевна – заслуживает присуждения ей ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертационная работа Кирилловой А.Д. и отзыв обсужден на заседании кафедры «Комплексная защита информации» Федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». Протокол заседания № 9 от 22 мая 2023 года.

Отзыв составил:
Доктор технических наук, доцент
заведующий кафедрой комплексной
защиты информации
ФГАОУ ВО «Омский
государственный
технический университет» Ложников Павел Сергеевич

Докторская диссертация защищена
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Даю согласие на обработку персональных данных.

Адрес организации: 644050, г. Омск, пр-т Мира, д. 11
Рабочий телефон: +7 (3812) 65-34-07
Адрес эл. почты: info@omgtu.ru

Подписи:
Заверяю:
Начальник управления персоналом
Посмитная 26.05.2023