На правах рукописи

Кириллова Анастасия Дмитриевна

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП ПРОМЫШЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2023

Работа выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий»

Научный руководитель: доктор технических наук, профессор, **Васильев Владимир Иванович**

Официальные оппоненты:

Аралбаев Ташбулат Захарович, доктор технических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», заведующий кафедрой вычислительной техники и защиты информации
Баранкова Инна Ильинична, доктор технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова», заведующая кафедрой информатики и информационной безопасности

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Омский государственный технический университет», г. Омск

Защита диссертации состоится 30 июня 2023 года в 10^{00} часов на заседании диссертационного совета 24.2.479.07, на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450008, г. Уфа, ул. К. Маркса, д. 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский университет науки и технологий» и на сайте *https://uust.ru/*.

Автореферат разослан «___» _____ 2023 года.

Ученый секретарь
диссертационного совета,
д-р техн. наук, доцент Виноградова Ирина Леонидовна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Развитие промышленности 4.0 основывается на технологиях промышленного Интернета вещей (IIoT) и киберфизических систем, направленных на объединение физического и цифрового производства. Современные промышленные системы автоматизации претерпевают цифровую трансформацию, что существенно обостряет проблему обеспечения информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Внедрение новых технологий, а также унификация и тесная интеграция производства с корпоративной информационной системой и внешней средой влечет за собой возникновение множества новых уязвимостей, угроз и рисков ИБ, ранее не характерных для АСУ ТП.

Об актуальности проблемы обеспечения ИБ АСУ ТП промышленных объектов свидетельствует статистика последних лет, отражающая стабильный рост числа инцидентов и целенаправленных атак на АСУ ТП с целью промышленного шпионажа, мошенничества и нарушения функционирования предприятия. Так, по материалам исследований «Лаборатории Касперского» во втором полугодии 2022 г. в России зафиксировано самое значительное среди всех стран мира изменение удельного веса (увеличение на 9 %) компьютеров АСУ ТП, подвергшихся компьютерным атакам. С 39,2 % Россия поднялась по этому показателю на третье место в рейтинге стран. Промышленные системы привлекают нарушителей своими масштабами, значимостью выполняемых бизнес-процессов, их влиянием на окружающий мир и жизнь граждан. В 45 % случаев атаки во втором полугодии 2022 г. привели к нарушению основной деятельности промышленных предприятий, что связано с недоступностью их инфраструктуры в результате атак шифровальщиков. Потеря управления над промышленными объектами может привести к нежелательным последствиям в отдельном субъекте государства или отразиться на экономических показателях страны в целом, а также снизить безопасность жизнедеятельности населения. Соответственно, вопросы обеспечения ИБ АСУ ТП промышленных объектов приобретают большое значение. Особое внимание при этом должно уделяться оценке рисков ИБ как необходимой составляющей комплексного подхода к обеспечению ИБ, позволяющей оценить реализуемость сценариев нарушения ИБ и выявить их возможные последствия для построения эффективной системы защиты. За последнее десятилетие активно развивалась нормативно-правовая база обеспечения ИБ АСУ ТП, но предложенные решения ориентированы, в первую очередь, на качественную оценку рисков ИБ и не позволяют в полной мере ранжировать риски по степени критичности.

Сегодня существенно выросли требования регуляторов, направленные на повышение ИБ АСУ ТП и объектов критической информационной инфраструктуры (КИИ). Необходимо обеспечить частичную или полную автоматизацию процессов обработки больших объемов накапливаемых в современных системах обеспечения ИБ данных о состоянии АСУ ТП промышленных объектов, что позволит в конечном итоге повысить оперативность не только качественной, но и количественной оценки рисков ИБ и будет способствовать повышению защищенности этих объектов в условиях воздействия возможных потенциальных угроз.

Таким образом, тема диссертационной работы, посвященная разработке метода и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов и обеспечения интеллектуальной поддержки принятия решений на этапе выбора эффективных контрмер по защите информации, является актуальной.

Степень разработанности темы исследований. Проблема обеспечения ИБ АСУ ТП отражена в ряде российских и международных нормативно-методических документов, а также в работах ряда российских и зарубежных исследователей. Вопросам обеспечения ИБ АСУ ТП и объектов КИИ посвящены серия стандартов ГОСТ Р 62443, Приказы ФСТЭК

России №№ 31, 235, 239, Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021 г.

Методы оценки рисков ИБ АСУ ТП и объектов КИИ, как одного из основных этапов в обеспечении ИБ промышленных систем, анализируются в работах Ажмухамедова И.М., Аникина И.В., Аралбаева Т.З., Баранковой И.И., Болодуриной И.П., Катасёва А.С., Костогрызова А.И., Лившица И.И., Максимовой Е.А., Милославской Н.Г., Flaus J.M., и др. Вместе с тем, в настоящее время можно считать отработанными лишь методики качественной оценки рисков ИБ, применяемые для предварительной (качественной) оценки уровня ИБ объекта защиты, а также определенные методики, отражающие общий подход к количественной оценке рисков ИБ и не учитывающие конкретные аспекты, характерные для АСУ ТП промышленных объектов.

В работах Васильева В.И., Вульфина А.М., Гузаирова М.Б., Ложникова П.С., Машкиной И.В., Шелупанова А.А., Salmeron J.L., Papageorgiou E.I. и др. предложены методы и технологии оценки и анализа рисков ИБ, основанные на использовании новых методов, моделей и технологий интеллектуального анализа данных. Наибольшую сложность в данном случае вызывает недостаточный объем располагаемой статистической информации об угрозах и уязвимостях, ее противоречивость и неполнота, что затрудняет формирование достоверных оценок рисков ИБ и получение итоговых показателей уровня защищенности АСУ ТП.

Вопросы моделирования сценариев компьютерных атак на промышленные системы автоматизации отражены в исследованиях Котенко И.В., Саенко И.Б., Чечулина А.А., Noel S., Yeboah-Ofori A., Zografopoulos I. и др. В этих работах предложены инструменты для автоматизации отдельных этапов процесса построения сценариев атак, однако комплексное решение задачи моделирования сценариев атак на АСУ ТП промышленных объектов с учетом накопленной информации в открытых международных базах знаний до сих пор отсутствует.

Проведенный анализ опубликованных работ в целом показывает, что, несмотря на значительный объем исследований в данной предметной области, проблема адекватной количественной оценки рисков ИБ АСУ ТП и выбора надлежащего состава контрмер нуждается в дальнейшей проработке. По мере увеличения статистических данных и разработки математических моделей риска ИБ, угроз и инцидентов безопасности, актуальной становится задача разработки методов и алгоритмов количественной оценки рисков ИБ АСУ ТП, обеспечивающих возможность достоверной оценки уровня защищенности АСУ ТП промышленных объектов и его соответствия требованиям нормативных документов.

Объектом исследования являются автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных объектов.

Предметом исследования являются методы, модели и алгоритмы количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе методов когнитивного моделирования.

Целью исследования является повышение оперативности и достоверности оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования и методов машинного обучения.

Для достижения поставленной цели в работе решались следующие **задачи исследования:**

1. Провести анализ современного состояния проблемы обеспечения ИБ АСУ ТП промышленных объектов с учетом требований существующей нормативно-методической базы.

2. Разработать и исследовать нечеткую когнитивную модель количественной оценки рисков ИБ АСУ ТП с учетом воздействия факторов неопределенности и алгоритм ее построения в классе вложенных серых нечетких когнитивных карт.

3. Разработать метод, алгоритм и методику количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения.

4. Разработать инструментальные средства автоматизации моделирования сценариев атак на АСУ ТП в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ АСУ ТП промышленных объектов.

5. Разработать методику и практические рекомендации применения разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач.

Научная новизна

1. Предложена нечеткая когнитивная модель оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт для зональных моделей АСУ ТП, которые, в отличие от существующих, отражают особенности многоуровневой организации АСУ ТП промышленных объектов (многообразие применяемых протоколов, программного и аппаратного обеспечения, продолжительный жизненный цикл, иерархическую структуру объекта с различными уровнями логической и физической изоляции, специфику применения используемых средств защиты), позволяя формализовать сценарии компьютерных атак с требуемым уровнем их детализации в пределах выделенных зон, что позволяет повысить достоверность и обоснованность количественной оценки рисков ИБ и, как следствие, обеспечить выбор эффективных контрмер.

2. Разработан метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, отличающийся применением шаблонов открытых баз знаний для формализации описания объекта атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей и баз данных, что позволяет автоматизировать и унифицировать их представление в виде последовательности действий, совокупности методов и средств (тактик и техник), позволяющих потенциальному нарушителю реализовать атаку на АСУ ТП промышленного объекта.

3. Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак, отличающиеся применением нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон АСУ ТП промышленного объекта, что позволяет определить оптимальное (рациональное) распределение затрат на реализацию, внедрение и сопровождение контрмер 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 достоверность и оперативность оценки рисков ИБ и, в конечном итоге, эффективность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации АСУ ТП промышленного объекта.

Практическая значимость результатов исследований заключается в разработке методики и инструментальных средств автоматизации моделирования сценариев атак и оценки рисков ИБ в составе ИСППР, в решении с их помощью прикладных задач оценки рисков ИБ АСУ ТП промышленных объектов, повышении обоснованности полученных количественных оценок рисков ИБ с учетом воздействия факторов неопределенности. Применение программной реализации разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП позволило после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшить на 70-80 % разброс экспертных оценок, а также повысить уровень защищенности АСУ ТП конкретного промышленного объекта, снизить предварительную

оценку стоимости эксплуатации предлагаемых защитных мер. Временные затраты на моделирование сценариев атак и оценку рисков ИБ при этом сократились в 2,5 раза.

Методы исследования. В качестве методов решения поставленных в диссертационной работе задач использовались методы системного анализа, оценки рисков ИБ, теории графов, когнитивного моделирования и машинного обучения.

Положения, выносимые на защиту:

1. Нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП и алгоритм ее построения.
2. Метод количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак.
3. Алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе иерархии вложенных нечетких когнитивных моделей и сценарного моделирования атак.
4. Архитектура и программная реализация разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов в составе исследовательского прототипа ИСППР.
5. Методика и практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов при решении прикладных задач.

Степень достоверности научных положений и выводов подтверждается корректной постановкой задач и выбором методов исследования, результатами практического применения разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП при решении ряда прикладных задач, апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях.

Апробация результатов диссертации. Основные положения и результаты диссертационной работы докладывались и обсуждались на научных конференциях: X, XIV Всероссийская молодежная научная конференция «Мавлютовские чтения» (г. Уфа, 2016, 2020); VI, VII Всероссийская научная конференция с международным участием «Информационные технологии и системы» (г. Ханты-Мансийск, 2017, 2019); V, VIII, IX Всероссийская конференция «Информационные технологии интеллектуальной поддержки принятия решений» (г. Уфа, 2017, 2020, 2021); VII Всероссийская заочная Интернет-конференция «Проблемы информационной безопасности» (г. Ростов-на-Дону, 2018); V, VII, VIII Международная конференция и молодежная школа «Информационные технологии и нанотехнологии» (г. Самара, 2019, 2021, 2022); 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS) (г. Уфа, 2020); XXVIII Международная научно-практическая конференция «Приоритетные направления развития науки и технологий» (г. Тула, 2021); II International Scientific and Practical Conference «Information Technologies and Intelligent Decision Making Systems» (г. Москва, 2021).

Отраженные в диссертации исследования проведены в рамках реализации грантов РФФИ № 19-07-00972, № 20-08-00668, № 20-38-90078.

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим 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».

Публикации результатов работы. По материалам исследования опубликована 31 работа, в том числе 8 статей в научных изданиях из Перечня рецензируемых научных

изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI, 4 научные работы в изданиях, включенных в базу Scopus, 16 статей в других изданиях, получено 3 свидетельства о государственной регистрации программы для ЭВМ.

Структура и объем диссертации. Диссертация включает в себя введение, 4 главы, заключение, список сокращений и условных обозначений, словарь терминов, список литературы и приложения. Основной текст диссертации изложен на 167 страницах, содержит 83 рисунка, 32 таблицы, 8 приложений. Список литературы включает в себя 184 наименования.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении к диссертации обоснована актуальность темы исследования, дана оценка степени ее научной разработанности, определены объект и предмет исследования, сформулированы цель и решаемые задачи. Отмечена научная новизна диссертационной работы, ее практическая значимость, представлены положения, выносимые на защиту.

В первой главе проводится анализ современного состояния нормативно-правового и методического обеспечения работ в области ИБ АСУ ТП. Представлен обзор существующих методов и алгоритмов оценки рисков ИБ.

Отмечается отсутствие формализованных методик детальной оценки рисков ИБ АСУ ТП промышленных объектов. Существующие нормативные и методические документы в целом направлены на построение статической модели нарушителя, формирование фиксированного перечня угроз, экспертной оценки реализации и уровня значимости угроз. Результаты применения этих методов и алгоритмов затруднительно использовать в практических задачах управления рисками ИБ промышленного предприятия, поскольку они носят, как правило, качественный характер и не позволяют оценить реальные потери от реализации угроз ИБ АСУ ТП и, как следствие, обосновать эффективный выбор контрмер. Кроме того, анализ показал, что их применение осложнено высокой степенью неопределенности и трудоемкости процедуры формализации факторов, влияющих на уровень ИБ АСУ ТП промышленных объектов.

Во второй главе разработана и исследована нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов в условиях воздействия факторов неопределенности и разброса экспертных оценок.

Характерной особенностью АСУ ТП как объекта защиты является ее многоуровневая иерархическая структура, что определяет специфичность подхода к вопросу обеспечения ИБ автоматизированных промышленных систем. Построение моделей АСУ ТП как объекта защиты основано на стандартах серии ГОСТ Р 62443, предусматривающих выделение в рамках иерархической структуры АСУ ряда зон безопасности, связанных между собой трактами. Зональная модель базовой архитектуры АСУ ТП позволяет при этом для распределенных и гетерогенных промышленных систем с большим количеством узлов и уязвимостей производить оценку рисков ИБ не только для отдельных зон, но и для всей системы в целом, позволяя выявить наиболее уязвимые группы информационных ресурсов и обосновать эффективный выбор контрмер.

Разработана функциональная модель процесса оценки рисков ИБ АСУ ТП промышленных объектов (рисунок 1), основанная на Методике оценки угроз безопасности информации ФСТЭК России, в соответствии с которой предложено реализовать данный процесс путем построения иерархии нечетких когнитивных карт применительно к зональной модели АСУ ТП и формализовать таким образом процедуру количественной оценки рисков ИБ АСУ ТП и моделирования сценариев атак как в пределах каждой из зон, так и для всего объекта в целом.

Для реализации процесса оценки рисков ИБ АСУ ТП предложено использовать приведенные в Методике ФСТЭК России и базе знаний MITRE ATT&CK тактики и техники (Tackts, Techs), а также дополнительную информацию из Банка данных угроз безопасности информации (БДУ) ФСТЭК России (Threats) и баз данных шаблонов компьютерных атак (CPE, CVE, CWE, CAPEC). Использование открытых баз данных угроз и уязвимостей позволяет при этом формально описать сценарии эксплуатации уязвимостей и автоматизировать построение цепочки возможных действий нарушителя на промежуточных узлах АСУ ТП.

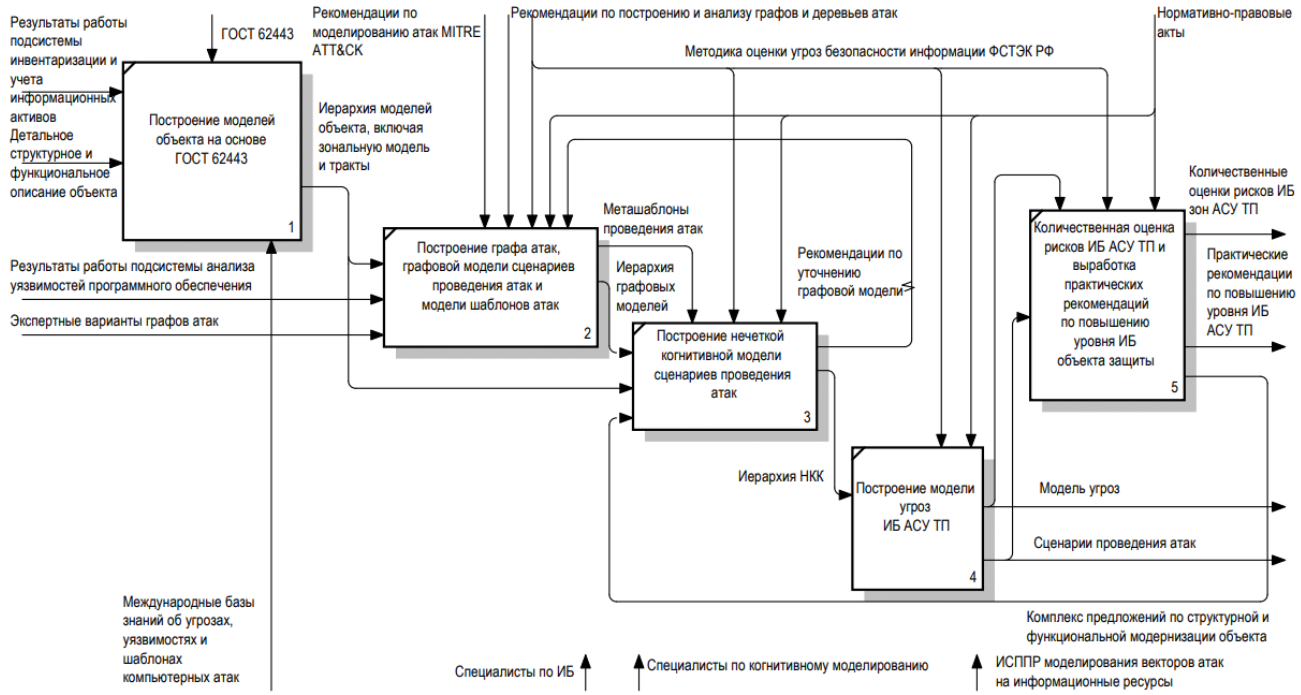


Рисунок 1 – Функциональная модель процесса оценки рисков ИБ АСУ ТП промышленных объектов на основе иерархии нечетких когнитивных моделей, формализующих сценарии атак

Количественная оценка рисков ИБ в пределах каждой выделенной зоны безопасности АСУ ТП основана на построении нечеткой серой когнитивной карты (НСКК) (рисунок 2), которая может быть представлена в виде взвешенного ориентированного графа, заданного с помощью кортежа множеств:

$$\text{НСКК} = \langle C, E, W \rangle,$$

где $C = \{C_i\}$ – множество концептов (вершин графа), $(i = 1,2, \dots, n)$; $E = \{E_{ij}\}$ – множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ – множество весов связей, $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, j_1), (i_2, j_2), \dots, (i_S, j_S)\}$–множество пар индексов смежных ,т.е. связанных между собой вершин графа, $S \le n(n-1)$.

Веса связей НСКК и состояния концептов задаются с помощью серых чисел $\otimes W_{ij}$, определяемых как $\otimes W_{ij} \in [\underline{W}_{ij}, \overline{W}_{ij}]$, где $\underline{W}_{ij} < \overline{W}_{ij}, \{\underline{W}_{ij}, \overline{W}_{ij}\} \in [-1,1]$, где $\underline{W}_{ij}$ и $\overline{W}_{ij}$ – соответственно нижняя и верхняя граница серого числа $\otimes W_{ij}$. Таким образом, вес связи между i-м и j-м концептами $(C_i \to C_j)$ может принимать любое значение в пределах заданного диапазона $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1,1]$.

Состояния концептов C_i характеризуются переменными X_i, принимающими значения в интервале $[0,1]$:

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{(j \ne i)}^{n} \otimes W_{ji} \otimes X_j(k)\right), \qquad (1)$$

где функции активации концептов $f(\cdot)$ – двухполярные сигмоиды: $f(X) = (1 - e^{-x})/(1 + e^{-x})$.

Значение переменной состояния концепта C_R НСКК определяет итоговую оценку риска ИБ X_R для моделируемых сценариев проведения атак C_S^1 и C_S^2. Значения весовых коэффициентов $W_{C_C^1,C_S^1}$, $W_{C_C^1,C_S^2}$, $W_{C_C^2,C_S^2}$ характеризуют распределение ограниченных ресурсов на реализацию контрмер C_C^1 и C_C^2 при моделировании сценариев атак в пределах выделенных зон безопасности АСУ ТП промышленного объекта. Установившиеся значения переменных состояния концептов C_E^1 и C_E^2 позволяют оценить эффективность интеграции и использования каждой контрмеры.

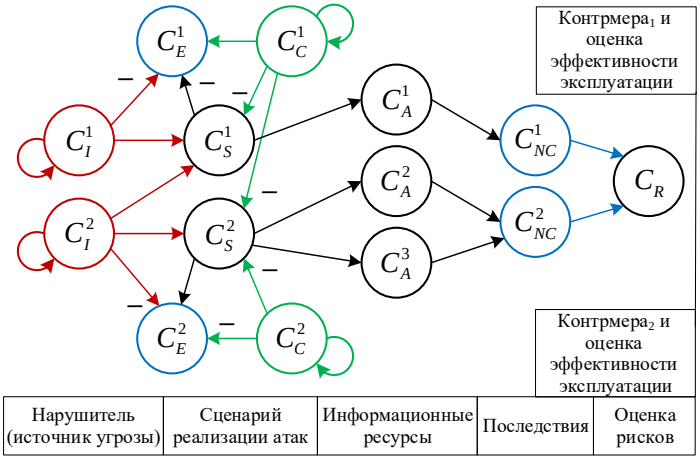


Рисунок 2 – НСКК для оценки рисков ИБ АСУ ТП и оценки эффективности распределения ресурсов на реализацию контрмер: C_I – нарушители; C_E – стоимость развертывания и сопровождения контрмер; C_S – выбор способа проведения атаки посредством эксплуатации уязвимостей; C_A – определение информационных ресурсов; C_{NC} – определение негативных последствий для АСУ ТП; C_C – выбор рационального способа защиты с учетом ограничений; C_R – оценка риска ИБ

Для моделирования возможных действий нарушителя в каждой из выделенных зон безопасности АСУ ТП на различных этапах реализации атаки (наиболее трудоемкий и сложный этап согласно Методике ФСТЭК) предлагается использовать графовые модели реализации атак, формализуемые с помощью иерархии вложенных НКК. Предложена процедура «сворачивания» исходной детализированной НКК, раскрывающей последовательность действий нарушителя на каждом этапе реализации атаки, до результирующей НКК уровня представления атаки.

Алгоритм построения результирующей НКК на основе графовых моделей реализации атаки включает в себя следующие шаги:

1) Построение НКК детализированного уровня графовой модели на основе анализа матрицы переходов между компонентами в пределах одного узла и между узлами выделенной зоны АСУ ТП (рисунок 3, I).

2) Построение НКК для представления различных сценариев атаки (рисунок 3, II).

3) Построение НКК для обобщенного представления варианта проведения отдельной атаки (рисунок 3, III).

4) Построение результирующей НКК (рисунок 4) для моделирования набора возможных сценариев атак на выделенные целевые узлы в пределах отдельных зон и всего объекта в целом, с оценкой вероятности реализации и значимости возможных последствий.

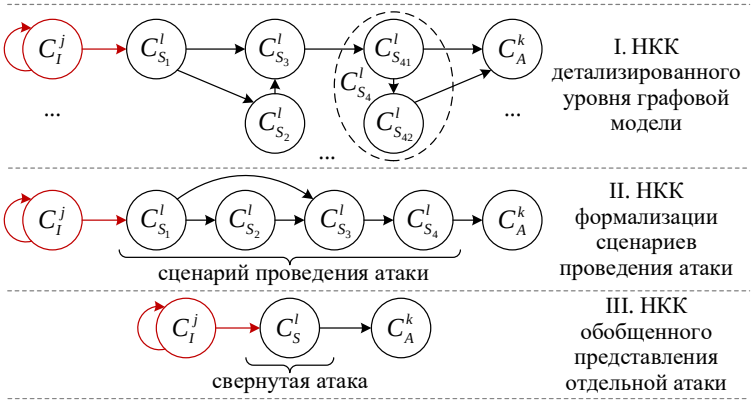


Рисунок 3 – Этапы построения результирующей НКК

Детализированный уровень НКК отражает последовательность возможных действий нарушителя на каждом этапе проведения атаки, что обеспечивает получение развернутой итоговой оценки рисков ИБ для АСУ ТП. Каждая атака укрупняется

до концепта НКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность ее реализации в каждом из возможных сценариев.

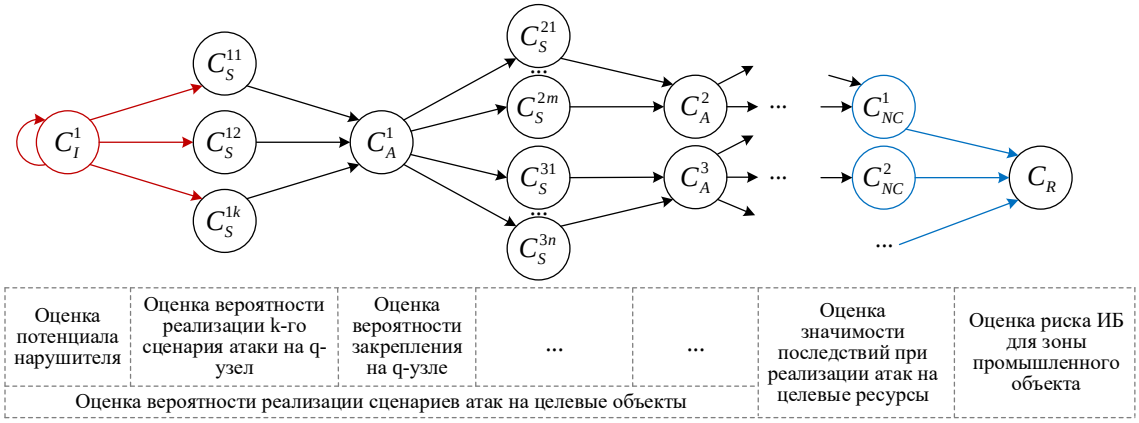


Рисунок 4 – НКК для моделирования множества возможных атак на целевые концепты

Результирующая НКК позволяет получить оценку рисков ИБ АСУ ТП при реализации нарушителем совокупности атак на целевые ресурсы как в выделенной зоне безопасности объекта, так и для рассматриваемой АСУ ТП в целом.

Рассмотрены особенности использования предложенной методики количественной оценки рисков ИБ с помощью НКК на примере АСУ ТП пункта приема-сдачи подготовленной нефти.

В третьей главе предложен метод сценарного моделирования атак, реализующий заключительные этапы Методики ФСТЭК России, основанный на построении и анализе комплекса моделей объекта и действий нарушителя, позволяющих формализовать декомпозировать возможные сценарии проведения атак в выделенной зоне безопасности (промышленной сети) АСУ ТП с количественной оценкой соответствующих рисков ИБ.

Иерархия разработанного комплекса моделей представлена на рисунке 5. На основе зональной модели базовой архитектуры АСУ ТП промышленного объекта (1) строится ряд графовых моделей, раскрывающих детали (отдельные аспекты) реализации атаки. Графовые модели сценариев атак (2) формируются на основе графа атак на промышленную сеть (3) (рисунок 6, а), перекрестных ссылок и матрицы переходов между выделенными идентификаторами баз данных.

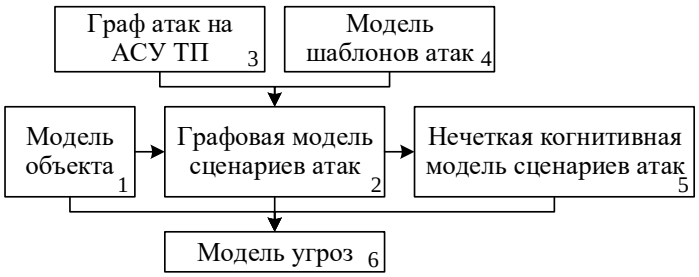
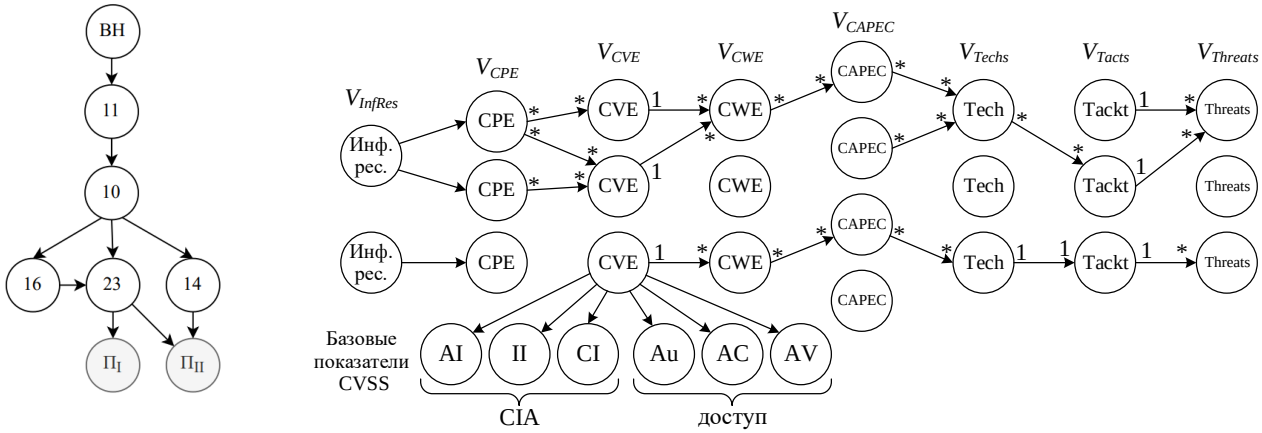


Рисунок 5 – Иерархия моделей построения сценариев проведения атак

Графовые модели различной степени детализации строятся исходя из анализа модели объекта, профиля вероятного нарушителя, наиболее вероятных атак и наиболее уязвимых ресурсов системы (рисунок 6, б): V_{InfRes} – множество вершин, соответствующих информационным активам и компонентам АСУ ТП промышленного объекта; V_{CPE} – множество вершин, соответствующих идентификаторам платформ и конфигураций для программно-аппаратного обеспечения системы; V_{CVE} – множество вершин, соответствующих идентификаторам выявленных уязвимостей для каждого элемента системы; V_{CWE} – множество вершин, соответствующих идентификаторам CWE, представляющим недостатки программного и аппаратного обеспечения системы; V_{CAPEC} – множество вершин,

соответствующих шаблонам атак CAPEC, описывающим типовые атаки; V_{Techs} – множество вершин, соответствующих техникам реализации атаки, которые описывают инструменты и технологии, используемые в процессе реализации атаки; V_{Tackts} – множество вершин, соответствующих тактикам, т.е. действиям нарушителя на различных этапах реализации атаки; $V_{Threats}$ – множество вершин, соответствующих угрозам безопасности информации из БДУ ФСТЭК.



а) б)

Рисунок 6 – а) Граф атак на промышленную сеть АСУ ТП (ВН – нарушитель, $П_1$, $П_2$ – последствия от реализации атак); б) Графовая модель сценариев проведения атак, описывающая взаимосвязь CPE-CVE-CWE-CAPEC-ATT&CK

Модель шаблонов атак (4) (рисунок 7), построенная на основе открытой базы шаблонов атак CAPEC, используется для детализации графовой модели и анализа возможностей нарушителя, т.к. графовая модель конструируется в виде цепочки вероятностных переходов между узлами CAPEC (рисунок 8) и представляет собой последовательности действий, совокупность методов и средств, при помощи которых нарушитель достигает поставленной цели воздействия на каждом этапе проведения атаки.

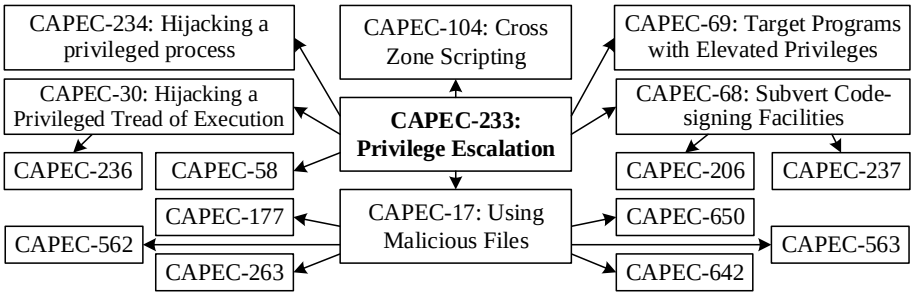


Рисунок 7 – Модель шаблонов атак для CAPEC-233

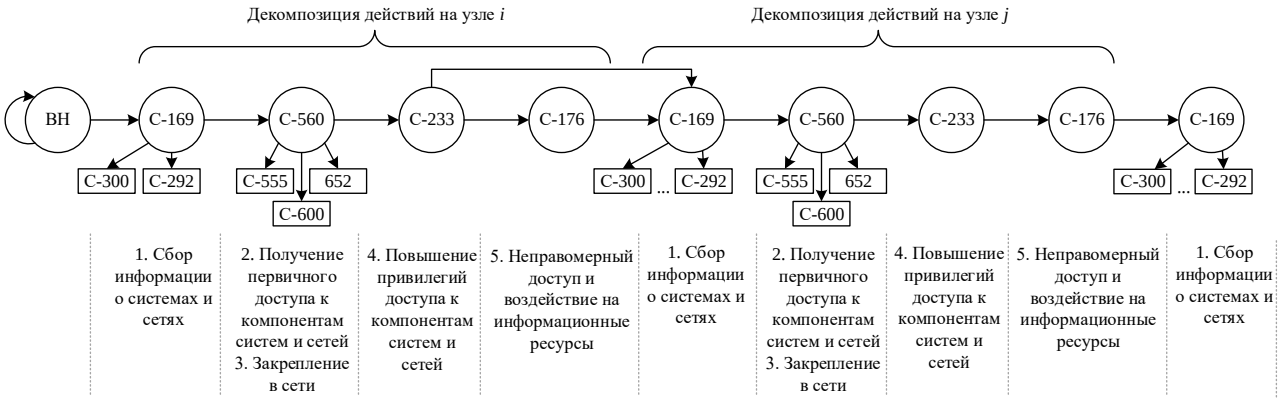


Рисунок 8 – Графовая модель проведения атаки на основе шаблонов атак CAPEC

На рисунке 9 представлена структура подсистемы анализа графовых моделей. Нечеткая когнитивная модель сценариев проведения атаки (5) позволяет анализировать сценарии атак с требуемым уровнем детализации за счет механизмов декомпозиции и композиции действий нарушителя и формировать оценку рисков реализации атаки в целом или на каждом этапе ее исполнения. Модель угроз (6) объединяет всю информацию об объекте, полученную из рассмотренных моделей, результаты анализа профиля вероятного нарушителя, а также результаты применения предлагаемого метода сценарного моделирования (перечень актуальных угроз и сценарии их реализации, а также количественную оценку рисков ИБ АСУ ТП).

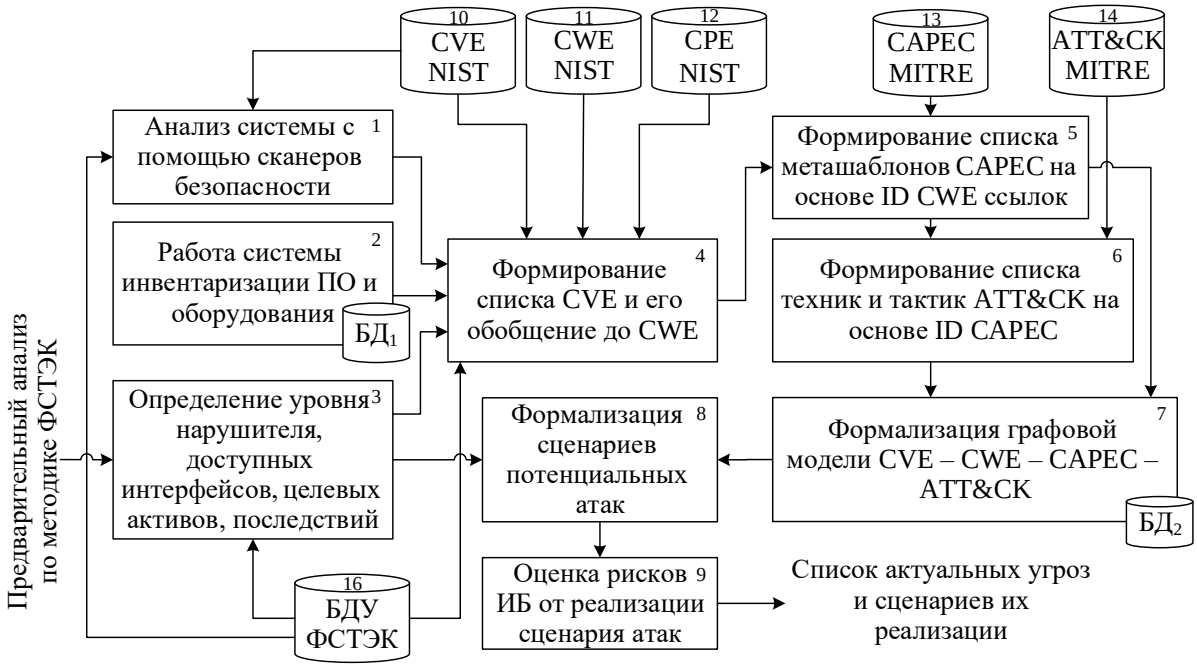


Рисунок 9 – Структура подсистемы построения и анализа графовых моделей

Разработана методика количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак в выделенных зонах АСУ ТП, позволяющая определить оценки рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

Приведена формальная постановка задачи многокритериальной оптимизации (2), учитывающей возможность минимизации оценки риска ИБ для выделенной зоны промышленного объекта и оценку эффективности использования контрмер в различных сценариях моделирования при разных вариантах задания целевой функции:

$$\text{а) } X_R \to min, \quad \text{б) } \sum X_R \to min, \text{ в) } \Phi\left(W_{C_C^i, C_S^j}\right) \to min, \tag{2}$$

где $\Phi(\cdot)$ – критерий эффективности использования контрмер; X_R – оценка риска ИБ (установившееся значение переменной состояния концепта C_R). В качестве оптимизируемых параметров рассматриваются веса НСКК $W_{C_C^i, C_S^j}$, характеризующие распределение выделенных ресурсов на реализацию контрмеры C_C^i с целью снижения вероятности проведения сценария атаки C_S^j. Для оптимизации весовых коэффициентов НСКК использован генетический алгоритм (ГА), обеспечивающий нахождение оптимального решения поставленной задачи.

Анализ полученных оценок рисков ИБ в пределах выделенных зон безопасности АСУ ТП и затрат на контрмеры (мероприятия по снижению рисков) позволяет определить механизмы управления защищенностью информационных ресурсов объекта и поддерживать необходимый уровень ИБ, а также оценивать требуемые затраты на интеграцию и

сопровождение необходимых контрмер. Рассмотрен пример использования предложенной методики сценарного моделирования атак с последующей оценкой рисков ИБ для выделенной зоны АСУ ТП пункта приема-сдачи подготовленной нефти.

В четвертой главе разработаны инструментальные средства автоматизации оценки рисков ИБ АСУ ТП и моделирования сценариев атак, интегрированные в составе ИСППР. Рассмотрены особенности практического применения полученных результатов, включая анализ угроз и уязвимостей объекта, моделирование сценариев проведения атак на основе открытых баз угроз, уязвимостей и компьютерных атак, построение и визуализацию НКК, с возможностью оптимизации весовых коэффициентов НКК, оценку рисков ИБ в результате возможных действий нарушителя.

Разработанное программное обеспечение (ПО) обеспечивает:

– интеллектуальную поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак, что позволяет специалистам, выявив конкретные уязвимости объекта, построить наглядную графовую модель реализации атаки (свидетельство о регистрации ПО № 2021614134);

– анализ сценариев проведения атак с требуемым уровнем детализации и оптимизации весовых коэффициентов НКК с помощью методов машинного обучения для решения задачи распределения ресурсов на реализацию контрмер (свидетельство о регистрации ПО № 2021619894).

В работе представлен фрагмент логической модели данных, описывающей структуру и взаимосвязь основных сущностей предметной области, используемой для создания хранилища данных об угрозах, уязвимостях и сценариях их реализации, а также фрагмент диаграммы классов в нотации UML, раскрывающей имплементацию результатов объектно-ориентированного анализа предметной области моделирования сценариев реализации атак. На рисунке 10 представлен фрагмент архитектуры ИСППР в нотации диаграммы компонентов UML с реализацией паттерна MVC.

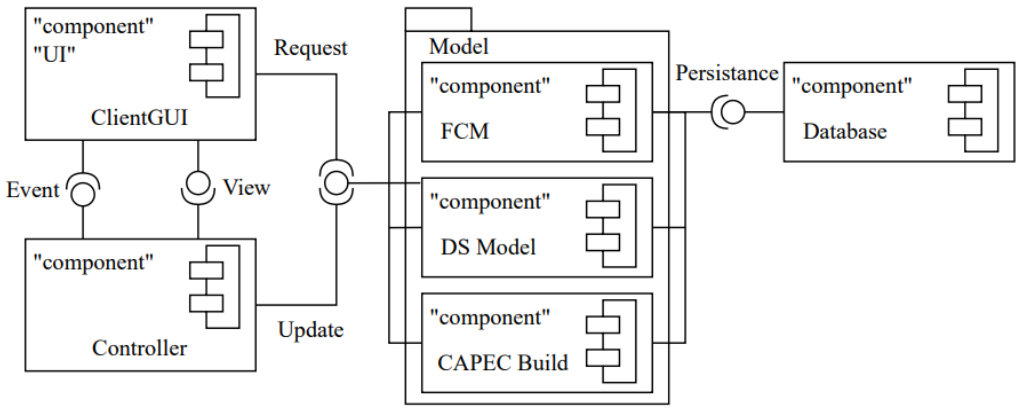


Рисунок 10 – Фрагмент архитектуры ИСППР (диаграмма компонентов UML)

Рассмотрен пример применения инструментального средства автоматизации моделирования сценариев атак с последующей оценкой рисков ИБ для АСУ ТП нефтедобывающего предприятия, базовая архитектура которой представлена на рисунке 11. Подсистемы АСУ ТП, согласно терминологии ГОСТ Р 62443, рассматривались в данном случае как отдельные зоны безопасности.

В таблице 1 представлены результаты вычислительных экспериментов по оценке риска ИБ АСУ ТП для различных сценариев проведения атак. С помощью ГА получен набор весовых коэффициентов НСКК, характеризующих оптимальное распределение затрат на реализацию необходимых контрмер по снижению риска ИБ. Величина риска ИБ здесь оценивалась в относительных единицах по отношению к стоимости целевых информационных ресурсов АСУ ТП, эффективность применения контрмер оценивалась по критерию снижения достигнутого уровня риска ИБ.

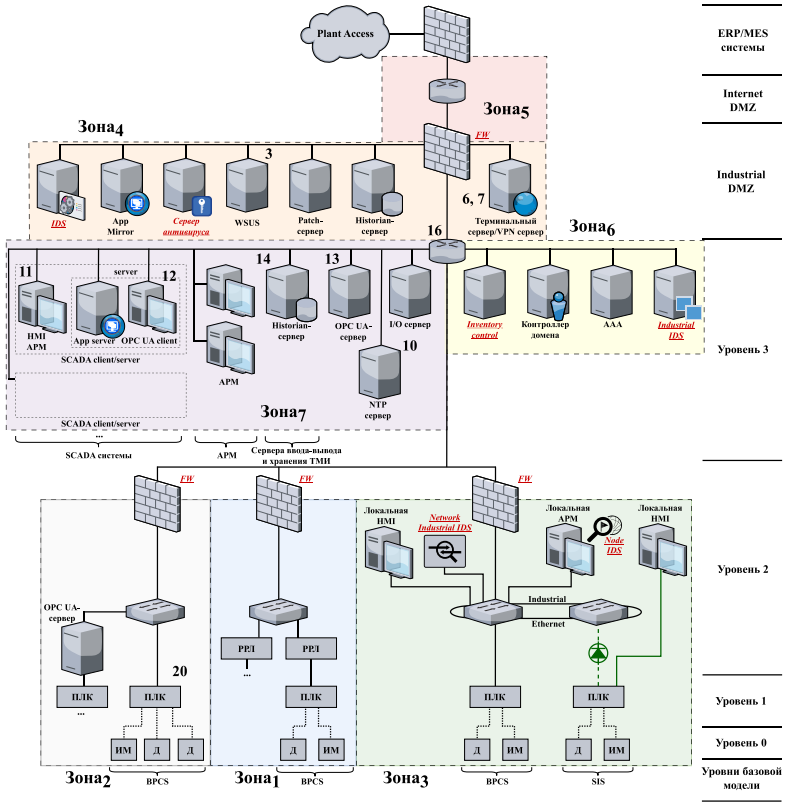


Рисунок 11 – Модель базовой архитектуры АСУ ТП нефтедобывающего предприятия

Таблица 1 – Результаты оценки рисков ИБ АСУ ТП с оптимизацией весов НСКК

Характеристика целевых концептов	Оценка рисков ИБ в диапазоне серых чисел		
	штатные контрмеры	контрмеры выбраны на основе рекомендаций ИСППР для сценарного уровня моделирования	оптимизация ресурсов контрмер с помощью ГА
Оценка риска ИБ для объекта в целом	[0,15; 0,63]	[0,16; 0,52]	[0,09; 0,5]
Оценка эффективности применения контрмер	[0,22; 0,72]	[0,3; 0,78]	[0,33; 0,86]

Сравнение предложенной в работе методики оценки рисков ИБ АСУ ТП с существующими аналогами показало, что применение известных методик осложняется высокой степенью неопределенности в формализации основных факторов, влияющих на защищенность АСУ ТП: появлением новых угроз и уязвимостей, возможностью потери актуальности данных в ходе анализа рисков, что в значительной степени устраняется при использовании предложенной методики.

В заключении представлены основные выводы и результаты проведенного исследования.

Перспективы дальнейшего использования результатов. Дальнейшее направление исследований связано с совершенствованием предложенных алгоритмов, моделей и методик оценки рисков ИБ АСУ ТП и развитием разработанного прототипа ИСППР с целью повышения оперативности и достоверности получения количественных оценок рисков ИБ АСУ ТП для различных промышленных объектов, а также совершенствование методических рекомендаций по выбору эффективного набора контрмер.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ современного состояния в области оценки рисков ИБ АСУ ТП. Выявлены достоинства и недостатки существующих методов и алгоритмов оценки рисков

применительно к АСУ ТП. Разработана функциональная модель процесса оценки рисков ИБ АСУ ТП, основанная на Методике ФСТЭК России, описывающая процессы формализации зональной модели базовой архитектуры АСУ ТП в виде иерархии нечетких когнитивных карт и формирования количественной оценки рисков ИБ АСУ ТП.

2. Предложена нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт применительно к зональной модели базовой архитектуры АСУ ТП, которая, в отличие от существующих методов и подходов оценки рисков ИБ, учитывает многоуровневую организацию промышленных объектов и позволяют формализовать сценарии атак с требуемым уровнем детализации в пределах выделенных зон, что позволяет повысить достоверность и обоснованность количественной оценки рисков ИБ и, как следствие, обеспечить обоснованный выбор эффективных контрмер.

3. Разработан метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, позволяющий получить формализованное описание объекта атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей, что существенно повышает обоснованность и полноту сценарного моделирования за счет представления последовательности тактик и техник, позволяющих нарушителю реализовать атаку на АСУ ТП. Решается задача оптимизации параметров когнитивных моделей, отражающих распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений. Оптимизация распределения ресурсов, выделенных на контрмеры, позволяет повысить эффективность эксплуатации контрмер и снизить количественную оценку риска ИБ для объекта защиты в целом.

4. Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак, отличающиеся применением нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон АСУ ТП. Анализ сценариев атак с требуемым уровнем детализации действий нарушителя позволяет формировать оценку рисков реализации атаки в целом или на каждом этапе ее исполнения. Предложена методика количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак в выделенных зонах АСУ ТП промышленного объекта, позволяющая определить оценки рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

5. Разработана архитектура исследовательского прототипа ИССПР и программная реализация инструментальных средств автоматизации оценки рисков ИБ и моделирования сценариев атак., позволяющая извлечь информацию о слабых местах инфраструктуры АСУ ТП, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные потенциальные сценарии атак, оценить их последствия для промышленного предприятия.

6. Разработана методика и практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач. Проведенные вычислительные эксперименты показали, что на этапах проектирования и внедрения контрмер временные затраты на моделирование сценариев реализации атак сократились более чем в 2,5 раза; на 15 % повысилась эффективность эксплуатации контрмер за счет оптимизации распределения ресурсов их применения; на 10 % снизилась количественная оценка уровня риска ИБ для объекта защиты в целом; предложенные решения позволяют сформировать расширенный список контрмер на основе баз знаний БДУ ФСТЭК России, ATT&CK, NVD для каждой из выделенных зон безопасности.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI

1. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами / В.И. Васильев, В.Е. Гвоздев, М.Б. Гузаиров, А.Д. Кириллова // Информация и безопасность. – 2017. – Т. 20, № 4. – С. 618–623.

2. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова // Информационные технологии. – 2018. – Т. 24, № 10. – С. 657–664. – DOI: 10.17587/it.24.657-664.

3. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4(30). – С. 66–74. – DOI: 10.14529/secur180410.

4. Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков инновационных проектов / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Л.Р. Черняховская // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4(34). – С. 45–57. – DOI: 10.14529/secur190406.

5. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Н.В. Кучкарова // Системы управления, связи и безопасности. – 2021. – № 3. – С. 110–134. – DOI: 10.24412/2410-9916-2021-3-110-134.

6. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. – 2021. – № 2(42). – С. 2–16. – DOI: 10.21681/2311-3456-2021-2-2-16.

7. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2(37). – С. 1–18. – DOI 10.26102/2310-6018/2022.37.2.022.

8. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова // Инфокоммуникационные технологии. – 2017. – Т. 15, № 4. – С. 319–325. – DOI: 10.18469/ikt.2017.15.4.02.

Публикации в изданиях, включенных в международную базу Scopus

9. Decision support system in the task of ensuring information security of automated process control systems / A.D. Kirillova, V.I. Vasilyev, A.V. Nikonov, V.V. Berkholts // CEUR Workshop Proceedings DS-ITNT 2019 – Proceedings of the Data Science Session at the 5th International Conference on Information Technlogy and Nanotechnology. – 2019. – P. 477–486. – DOI: 10.18287/1613-0073-2019-2416-477-486.

10. Secure Data Exchange in the Industrial Internet of Things Network of the Fuel and Energy Complex / E.R. Hajrullin, A.M. Vulfin, K.V. Mironov, A.I. Frid, M.B. Guzairov, A.D. Kirillova // Proceedings ICOECS 2020 International Conference on Electrotechnical Complexes and Systems. USATU, Ufa, Russia 27-30 October 2020. – IEEE. – 2020. – P. 353–358. – DOI: 10.1109/ICOECS50468.2020.9278491.

11. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms / A.M. Vulfin, V.I. Vasilyev, S.N. Kuharev, E.V. Homutov, A.D. Kirillova // International Scientific and Practical Conference “Information Technologies and Intelligent Decision Making Systems” (ITIDMS-II 2021). – Journal of Physics: Conference Series. – 2021. –Vol. 2001. – 012004. – DOI: 10.1088/1742-6596/2001/1/012004.

12. Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS Score / V.I. Vasilyev, A.D. Kirillova, A.M. Vulfin, A.V. Nikonov // 2021 International Conference on Information Technology and Nanotechnology (ITNT). – IEEE. – 2021. – P. 1–6. – DOI: 10.1109/ITNT52450.2021.9649191.

Другие публикации по теме диссертации

13. Кириллова А.Д. О реализации системы требований ФСТЭК к защите информации в инфокоммуникационных системах специального назначения // Материалы Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: УГАТУ. – 2016. – Т. 5. – С. 213–215.

14. Кириллова А.Д. Применение экспертной системы поддержки принятия решений в аудите информационной безопасности АСУ ТП // Труды Шестой Международной научной конференции «Информационные технологии и системы». – 2017. – С. 129–131.

15. Кириллова А.Д. Экспертная система аудита информационной безопасности АСУ ТП // Материалы V Всероссийской конференции «Информационные технологии интеллектуальной поддержки принятия решений». – 2017. – Т. 2. – С. 172–175.

16. Кириллова А.Д., Васильев В.И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП // Материалы VII Всероссийской заочной Интернет-конференции «Проблемы информационной безопасности». – 2018. – С. 138–142.

17. Analysis of confidential data protection in critical information infrastructure and the use of biometric, neural network and cryptographic algorithms (standards review and perspectives) / V.I. Vasilyev, A.D. Kirillova, A.E. Sulavko, S.S. Zhumazhanova // Труды Седьмой Всероссийской научной конференции с международным участием «Информационные технологии и системы». – 2019. – С. 193–197.

18. Decision support system for ensuring information security of an automated process control system / A.D. Kirillova, V.I. Vasilyev, A.V. Nikonov, V.V. Berkholts // V международная конференция и молодежная школа «Информационные технологии и нанотехнологии». – 2019. – Т. 4. Науки о данных. – С. 391–398.

19. Анализ защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата / М.Б. Гузаиров, А.И. Фрид, А.М. Вульфин, В.В. Берхольц, А.Д. Кириллова // Вестник УГАТУ. – 2019. – Т. 23, № 4(86). – С. 132–146.

20. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования / В.И. Васильев, А.М. Вульфин, В.В. Берхольц, А.Д. Кириллова, С.М. Бельский // Вестник УГАТУ. – 2019. – Т. 23, № 4(86). – С. 122–131.

21. Система обнаружения атак в беспроводных сенсорных сетях промышленного интернета вещей / В.И. Васильев, А.М. Вульфин, В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 70–78. – DOI: 10.14357/20790279190409.

22. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности / М.Б. Гузаиров, А.М. Вульфин, В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 62–69. – DOI: 10.14357/20790279190408.

23. Васильев В.И., Кириллова А.Д., Вульфин А.М. Методы управления рисками кибербезопасности АСУ ТП промышленных объектов // Труды Восьмой Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений». – 2020. – Т. 1. – С. 185–191.

24. Кириллова А.Д. Анализ проекта методики моделирования угроз безопасности информации ФСТЭК России // Материалы XIV Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: РИК УГАТУ. – 2020. – С. 20.

25. Васильев В.И., Кириллова А.Д., Вульфин А.М. Моделирование кибератак на объекты АСУ ТП с помощью нечетких когнитивных карт // Приоритетные направления развития науки и технологий: доклады XXVIII международной науч.-практич. конф.; под общ. ред. В.М. Панарина. – Тула: Инновационные технологии. – 2021. – С. 132–136.

26. Modeling the cyber attacks vector based on fuzzy cognitive maps / V.I. Vasilyev, A.D. Kirillova, A.M. Vulfin, A.V. Nikonov // Сборник трудов VII Международной конференции и молодежной школы «Информационные технологии и нанотехнологии» (ИТНТ-2021). – 2021. – Т. 3. – С. 031372

27. Система проактивной защиты промышленного объекта на основе алгоритмов машинного обучения / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин, А.И. Фрид // Сборник докладов III Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (FISP-2021), Ставрополь, 30 ноября 2021 года. – С. 24-30.

28. Кириллова А.Д. Моделирование вектора атаки в базисе нечетких когнитивных карт с учетом оценок CVSS // Материалы XV Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: УГАТУ. – 2021. – С. 229–235.

Свидетельства о государственной регистрации программы для ЭВМ

29. Программа моделирования нечетких когнитивных карт: Свидетельство о государственной регистрации программы для ЭВМ 2021615069 Российская Федерация / А.М. Вульфин, Р.Р. Ягафаров, А.Д. Кириллова, В.И. Васильев. – № 2021614134; заявл. 26.03.2021; опубл. 02.04.2021.

30. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка: Свидетельство о государственной регистрации программы для ЭВМ 2021615080 Российская Федерация / А.М. Вульфин, А.В. Никонов, Д.Н. Габбасова, Н.В. Кучкарова, В.И. Васильев, А.Д. Кириллова. – № 2021614120; заявл. 26.03.2021; опубл. 02.04.2021.

31. Программа анализа и моделирования кибератак на основе меташаблонов в нечетком когнитивном базисе: Свидетельство о государственной регистрации программы для ЭВМ 2021619894 Российская Федерация / А.Д. Кириллова, А.М. Вульфин, Р.Р. Ягафаров, Л.Ю. Зиязетдинова. – № 2021618903; заявл. 07.06.2021; опубл. 18.06.2021.

Диссертант  А.Д. Кириллова