Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский университет науки и технологий»

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

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, профессор
Васильев Владимир Иванович

Уфа – 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 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».

Личный вклад автора. Результаты исследования, составляющие новизну и выносимые на защиту, получены лично автором. Ключевые публикации подготовлены в соавторстве. Постановка задачи исследования осуществлялась совместно с научным руководителем д.т.н., профессором Васильевым В.И.

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.

Глава 1. Анализ современного состояния проблемы обеспечения ИБ АСУ ТП промышленных объектов

В первой главе диссертационной работы выполняется анализ общего состояния проблемы обеспечения ИБ АСУ ТП промышленных объектов и способов ее решения. Основное внимание уделяется сравнительному анализу существующей нормативно-методической и правовой базы обеспечения ИБ АСУ ТП. Приводится краткая характеристика основных положений ключевых документов в области ИБ систем промышленной автоматизации, определяющих процесс анализа и оценки рисков ИБ АСУ ТП. Выделяются особенности обеспечения ИБ, специфичные для АСУ ТП промышленных объектов. Проводится анализ методов и подходов к оценке рисков ИБ и моделированию сценариев атак на промышленные системы, а также ИСППР, как одного из вариантов решения проблем в области обеспечения ИБ АСУ ТП промышленных объектов.

1.1 Анализ проблемы обеспечения ИБ АСУ ТП промышленных объектов

В соответствии с федеральным законом № 187-ФЗ АСУ представляет собой комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и/или производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами [12].

В соответствии с нормативным документом ФСТЭК России [10] стандартная структура АСУ ТП строится по трехуровневому принципу:

– нижний уровень (полевой) – контрольно-измерительные приборы и исполнительные механизмы, установленные на технологическом оборудовании и предназначенные для сбора первичной информации о физических параметрах системы, о ходе ТП и передачи ее на следующий уровень иерархической структуры АСУ ТП;

– средний уровень (автоматического управления) состоит из программируемых логических контроллеров (ПЛК), которые выполняют функцию автоматизированного управления ТП – получают информацию с нижнего уровня и передают ее на верхний; управление исполнительными механизмами осуществляется по определенным алгоритмам путем обработки данных о состоянии технологических параметров, полученных посредством измерительных приборов;

– верхний уровень (операторского управления) представляет собой систему промышленных серверов, сетевого оборудования и автоматизированных рабочих мест (АРМ) операторов, на которых визуализируются все изменения параметров работы ТП, аварийное срабатывание оборудования, действия персонала; осуществляется сбор данных, визуализация и диспетчеризация хода ТП.

Связь между различными уровнями обеспечивается коммутационными узлами, а доступ к оборудованию нижнего уровня реализуется через полевые шины по специальным протоколам: Modbus, Profibus, Foundation Fieldbus, DeviceNet, HART и др. [58, 59]. На верхних уровнях архитектуры АСУ ТП используются IP- и Ethernet-сети, а промышленные устройства снабжаются стандартными портами и используют общие протоколы.

Таким образом, под АСУ ТП понимается многоуровневая система управления, которая может включать [108]:

– системы оперативно-диспетчерского управления;

– интегрированные и локальные АСУ ТП, а также системы автоматизации линейных (рассредоточенных) объектов;

– обслуживающие и смежные системы (инфраструктурные сервисы и системы корпоративной информационной системы, взаимодействующие с АСУ ТП).

В промышленной отрасли АСУ ТП применяются для повышения эффективности и безопасности производственных процессов, а также улучшения качества конечного продукта. На сегодняшний день автоматизация критически важных промышленных объектов достигает такого уровня, что безопасность их

функционирования неразрывно связана с ИБ АСУ ТП. В [8] ИБ АСУ ТП рассматривается как составная часть безопасности, отражающая влияние свойств информации, обрабатываемой и производимой АСУ ТП, на безопасность и надежность ее функционирования.

Ранее АСУ ТП функционировали в изолированном от внешних сетей сегменте на базе узкоспециализированного оборудования и ПО, поэтому задача обеспечения ИБ АСУ ТП сводилась, в первую очередь, к обеспечению физической защиты компонентов системы. С течением времени подходы к построению АСУ ТП изменились. Цифровая трансформация является ключевым направлением технологического развития промышленности, обеспечивающим конкурентоспособность промышленных предприятий, повышение производительности и снижение инвестиционных и эксплуатационных затрат [22]. Для повышения производительности и упрощения администрирования промышленных сетей и систем современные АСУ ТП должны иметь масштабируемую и унифицированную информационную инфраструктуру с возможностью удаленного управления и обслуживания, сбора диагностических данных (Рисунок 1.1).

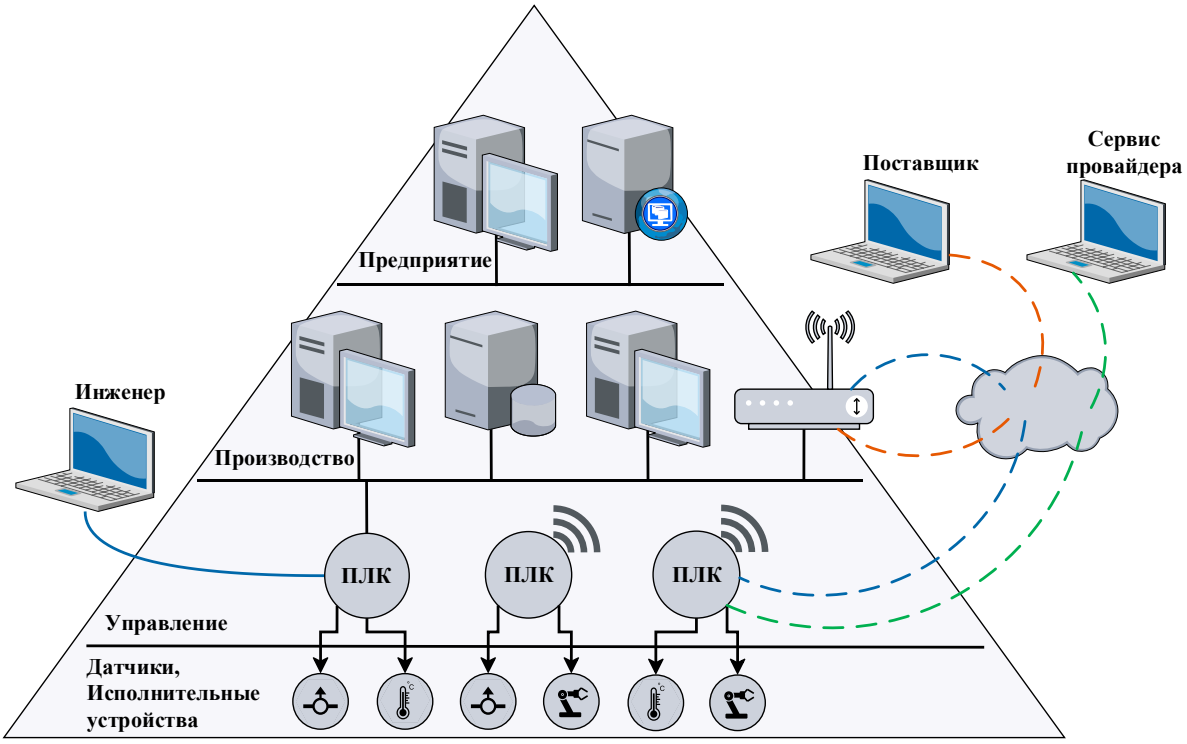


Рисунок 1.1 – Современная структура АСУ ТП

Эти изменения в первую очередь связаны с усложняющимися задачами, стоящими перед промышленными предприятиями:

– имея всю полноту данных о производстве в реальном режиме времени, сотрудники предприятия могут применять аналитическое ПО для решения задач управления производством, что сокращает объем рутинной работы;

– обеспечить контроль состояния, техническое обслуживание и ремонт оборудования, сократив работу в опасных зонах предприятия и на удаленных объектах [63, 95, 97].

Цифровая трансформация сред промышленной автоматизации привела к сопряжению технологических сегментов сети и корпоративных информационных систем предприятия, что повлекло за собой уменьшение степени изоляции АСУ ТП, возникновение новых уязвимостей, ранее не характерных для промышленных систем и увеличение числа компьютерных атак на их значимые компоненты.

«Лаборатория кибербезопасности АСУ ТП» компании «Ростелеком-Солар» за 2020-2021 гг. передала Банку данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК) информацию о 120 обнаруженных уязвимостях ПО, 115 из которых связаны с компонентами АСУ ТП зарубежных и отечественных поставщиков, причем значительная часть обнаруженных уязвимостей относится к встроенному ПО компонентов промышленных систем. В соответствии с международной системой оценки уязвимостей CVSS 3.0 [168], среднее значение критичности обнаруженных уязвимостей составляет 7,67 балла.

По данным компании Clatory, в I полугодии 2021 г. [123] было обнаружено 637 уязвимостей, затрагивающих компоненты АСУ ТП, что почти на 42 % больше, чем в прошлом полугодии (449 уязвимостей). Более 70 % уязвимостей были признаны критическими или получили высокую степень риска, а 61 % всех выявленных уязвимостей имеет сетевой вектор, то есть для их эксплуатации нужен только сетевой доступ к атакуемой системе. Подавляющее большинство этих уязвимостей не требуют специальных условий для эксплуатации: три четверти уязвимостей можно использовать без высоких прав, две трети – без взаимодействия с пользователем.

Согласно отчетам Лаборатории Касперского [81, 82] в первом полугодии 2022 г. около 30 % компьютеров в системах промышленной автоматизации России подвергались компьютерным атакам. Согласно отчетам Positive Technologies [17, 18] во II квартале 2022 года число атак на промышленные предприятия увеличилось на 53 % (75 атак) по сравнению с I кварталом (49 атак) и в 53 % случаев приводили к нарушениям функционирования промышленных предприятий. Основным методом атак во II квартале 2022 года стало использование вредоносного ПО (76 %), что свидетельствует о низком уровне ИБ промышленных систем, наличии большого числа уязвимостей и недостатков защиты как на периметре сети, так и во внутренней инфраструктуре. Так, по результатам реализации проектов Positive Technologies по анализу защищенности в 2020 г. было установлено, что в 91 % промышленных организаций внешний нарушитель может проникнуть в корпоративную сеть, где в 100 % случаев может получить учетные данные пользователей и полный контроль над инфраструктурой, а в 75 % – получить доступ в технологический сегмент сети. Это позволило нарушителям в 56 % случаев получить доступ к системам управления ТП [65].

Эксперты InfoWatch ARMA провели исследование доступных из сети Интернет компонентов АСУ ТП и обнаружили 4245 устройств, уязвимых для удаленных атак. Из них 2000 – это открытое коммутационное оборудование АСУ ТП, на 500 не настроена авторизация, а более 700 имеют критические уязвимости. По причине доступности компонентов АСУ ТП из сети Интернет у промышленных предприятий возрастают риски быть атакованными.

В настоящее время преобладают целевые атаки (APT) со сложной организацией и сложным многошаговым процессом реализации, доля которых в 2021 г. составила 74 % от общего числа атак. Такие атаки представляют собой набор последовательных действий (Рисунок 1.2), включающих в себя комплекс мероприятий и воздействий, направленных на достижения определенных целей, нарушающих ИБ предприятия [83].

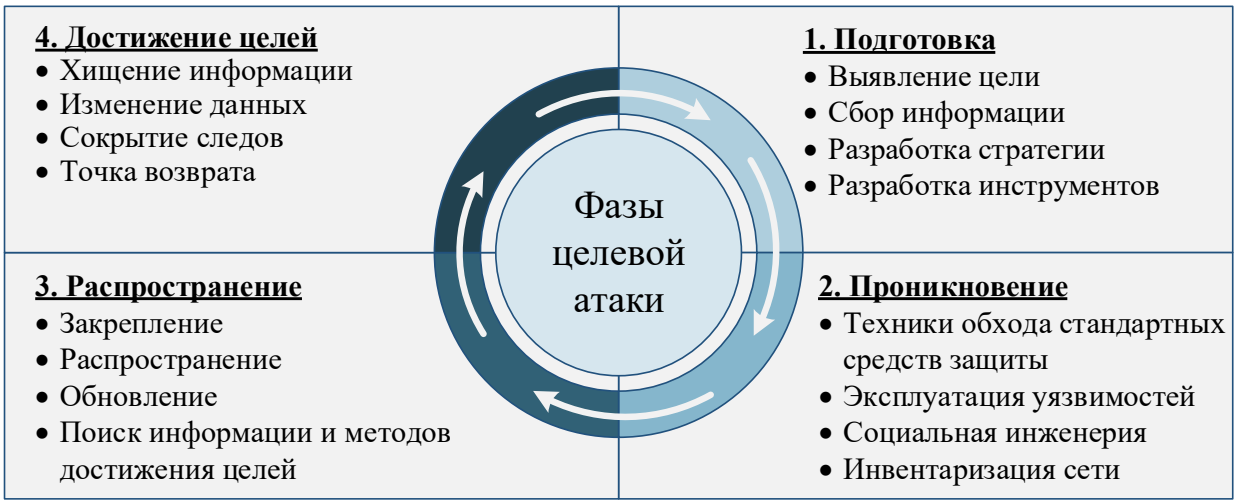


Рисунок 1.2 – Основные этапы целевой атаки

В подобном ландшафте угроз традиционные средства защиты информации (СЗИ) не обеспечивают необходимый уровень защиты, поскольку целевые атаки готовятся специально под конкретное предприятие и управляются вручную. Необходимо эффективное сочетание средств предотвращения, обнаружения и устранения угроз ИБ. Внимание акцентируется на создании интеллектуальных СЗИ, которые позволят обнаруживать сложные целевые атаки еще на начальных этапах их реализации, основываясь на множестве индикаторов компрометации (IOC, Indicator of Compromise) и индикаторы атак (IOA, Indicator of Attack). Такие индикаторы позволяют описывать отдельные вредоносные объекты, действия или подозрительное поведение системы, при совпадении с ними события ИБ помечаются как потенциальные элементы атаки. Основным инструментом становится моделирование сценариев атак на различных этапах их жизненного цикла: обнаружение уже совершенных вредоносных действий нарушителя, определение значимости и устранение последствий, формирование рекомендаций для предотвращения возникновения инцидентов ИБ в будущем [38, 40]. Определение сценариев предполагает установление последовательности возможных тактик (основных этапов реализации) и соответствующих им техник (определенные технические приемы реализации атаки), применение которых возможно нарушителем с соответствующим уровнем возможностей, а также доступность интерфейсов для использования соответствующих способов

реализации [6]. Возможные сценарии атаки должны быть оценены с точки зрения того, насколько вероятна их реализация нарушителем, поскольку знание того, какие сценарии представляют наибольшую угрозу для промышленной системы, позволяет повысить ее безопасность устранив их. Моделирование сценариев атак без использования инструментальных средств автоматизации является трудоемким процессом, требующим наличия высококвалифицированных специалистов по ИБ.

Международное сообщество и эксперты по ИБ заинтересованы в поиске эффективных способов решения проблемы обеспечения ИБ АСУ ТП промышленных объектов.

В 2018 году Координационным советом нефтегазовой отрасли совместно с Советом по природному газу США был подготовлен документ «Defense-in-Depth: Cybersecurity in the natural gas & oil industry» [129], в котором основное внимание уделяется обеспечению ИБ нефтегазовой промышленности. В рамках данного документа рассматривается подход эшелонированной защиты, основанный на лучших стандартах и проверенных системах. Компания Schneider Electric [113] также рекомендует промышленным предприятиям использовать подход эшелонированной защиты (Defense-in-Depth), поскольку эта стратегия гибридной многоуровневой защиты реализует комплексный подход к безопасности в масштабах всего промышленного предприятия и позволяет предотвратить прямые атаки на критические системы и значительно повысить сложность разведывательных действий нарушителей в промышленных сетях и системах. Однако меры глубокоэшелонированной защиты не защищают от эксплуатации всех уязвимостей и слабых мест в среде АСУ ТП, поскольку применяются, прежде всего, для того, чтобы замедлить нарушителя настолько, чтобы позволить специалистам по ИБ обнаружить и отреагировать на текущие угрозы, или усложнить действия нарушителей для достижения поставленной цели.

Разработка и внедрение инновационных технологий в сфере ИБ АСУ ТП рассматривается как приоритетная задача на государственном уровне, поскольку ИБ АСУ ТП напрямую связана с безопасной обстановкой в стране. Последствия сбоя в работе АСУ ТП промышленного объекта представляет серьезную опасность

для людей, оборудования, окружающей среды, могут иметь катастрофический характер. Следовательно, к критериям безопасности производства стратегически важно добавить нормативные составляющие для обеспечения грамотного подхода к проектированию и внедрению контрмер.

Задача обеспечения ИБ АСУ ТП отражена в ряде российских и международных нормативных и методических документов, а также отраслевых нормативных документах промышленных предприятий [7-9]. Наиболее существенные шаги для решения проблемы сделаны по пути разработки ряда международных и российских национальных стандартов [1, 10-12, 23, 87, 99, 116, 142, 164], определяющих терминологию, основные подходы и рекомендации по обеспечению ИБ промышленных автоматизированных систем.

Проблема обеспечения ИБ АСУ ТП активно освещается в научных работах российских и зарубежных ученых [20, 47, 51, 54, 67, 84, 119, 121, 122, 130, 149]. Также интерес у исследователей вызывает вопрос анализа и оценки рисков ИБ АСУ ТП [29, 30, 41, 46, 52, 64, 66, 73-75, 86, 90, 103, 140, 150, 164], как одного из этапов обеспечения ИБ АСУ ТП, так как анализ и оценка рисков позволяют определить уровень защищенности АСУ ТП, реализуемость сценариев атак, компоненты промышленной системы, нуждающиеся в защите, и угрозы, от которых требуется защита, а также достаточность и адекватность выбранных контрмер. То есть анализ и оценка рисков ИБ является основным начальным этапом в процессе построения и внедрения контрмер.

Таким образом, процедуры анализа и оценки рисков ИБ АСУ ТП является необходимой составляющей комплексного подхода к обеспечению ИБ АСУ ТП. Согласно Государственной программе «Цифровая экономика Российской Федерации» от 28.07.2017 г. актуальной является разработка методологий, моделей и методов комплексного анализа и управления рисками ИБ промышленных систем автоматизации с использованием технологий когнитивного моделирования и интеллектуального анализа структурированных и слабоструктурированных данных для обеспечения устойчивости и безопасности промышленной инфраструктуры предприятия на всех уровнях информационного пространства.

1.2 Анализ специфики структурно-функциональной организации АСУ ТП промышленных объектов как объекта защиты

Специфика промышленных систем автоматизации обуславливает наличие определенных трудностей в решении задач обеспечения ИБ АСУ ТП. В первую очередь эти трудности связаны со сложностью организации промышленной системы. Характерной особенностью АСУ ТП как объекта защиты является ее многоуровневая иерархическая структура [10].

Ранее было дано описание стандартной трехуровневой структуры АСУ ТП, которая лежит в основе нормативного документа ФСТЭК России [10]. Количество уровней АСУ ТП и их состав определяется назначением АСУ ТП и ее целевыми функциями. На каждом уровне АСУ ТП по функциональным, территориальным или иным признакам могут выделяться дополнительные сегменты. К наиболее критичным уровням в плане обеспечения ИБ относятся:

– верхний уровень, поскольку он чаще всего является единой точкой управления и мониторинга АСУ ТП и только он, как правило, взаимодействует с внешней сетью;

– средний уровень, поскольку обрабатывает и влияет на наиболее критичный тип данных АСУ ТП – контрольно-измерительную информацию.

Нижний уровень, как правило, изолирован логически и защищен физически, кроме того, он относительно малоизвестен среднестатистическим нарушителям.

Однако для таких сложных объектов, как АСУ ТП промышленных объектов, трехуровневая архитектура [10] не является достаточно информативной, поскольку включает в себя только описание уровней технологического сегмента и не дает целостного представления о современной системе промышленной автоматизации, для которой характерна тесная взаимосвязь с корпоративной сетью предприятия. Для защиты среды критической инфраструктуры важно рассматривать как корпоративную сеть промышленного предприятия, так и технологическую, исследовать системы и процессы в каждом сегменте сети, анализировать сценарии атак и риски ИБ, принимать достаточные меры безопасности.

На сегодняшний день актуальной моделью, описывающей общую архитектуру промышленной системы автоматизации, является модель PRM (Perdue Reference Model) [21, 94]. Модель PRM – это типовая эталонная модель сегментации системы промышленного управления, разработанная Университетом Пэрдью (США) и изложенная в отечественном отраслевом стандарте ГОСТ Р МЭК 62264-1-2010 «Интеграция систем управления предприятием. Модели и терминология» [5].

Модель PRM показывает взаимосвязь и взаимозависимость между основными компонентами типовой архитектуры промышленной системы, разделяя ее на три зоны, которые в свою очередь подразделяются на 6 уровней (Таблица 1.1, Рисунок 1.3). Две основные зоны, корпоративная и производственная, также называемые IT (информационные технологии) и OT (операционные технологии), разделены третьей – демилитаризованной зоной (ДМЗ), что предотвращает прямую связь между компонентами IT и OT зон. Эта мера, разделяющая архитектуру промышленной системы дополнительным уровнем, позволяет, в случае воздействия на АСУ ТП в ДМЗ, изолировать нарушение ИБ в этой же зоне.

Таблица 1.1 – Зоны и уровни архитектуры АСУ ТП на основе модели PRM

Зона / Уровень	Описание	Риски
Зона 1. IT-зона. Уровень 4 и 5. Корпоративная сеть	Представляют собой сеть предприятия, в которой существуют централизованные IT-системы, системы управления производством, системы планирования ресурсов предприятия (ERP), включая доступ в Интернет.	– атаки на сети АСУ ТП через IT-зону
Зона 2. Промышленная ДМЗ	Представлена зоной межсетевого взаимодействия между системами IT и OT. Содержит промежуточные узлы для безопасного удаленного доступа к компонентам АСУ ТП, а также серверы исторических данных (Historian), контроллеры домена и т.д. Используется для организации	– может потенциально привести к заражению наиболее критической части сети

Зона / Уровень	Описание	Риски
	удаленного доступа технического персонала.	
Зона 3. ОТ-зона. Уровень 3. Производственные операционные системы	Назначением является управление производственными процессами для создания желаемых продуктов. Оно включает в себя управление партиями; системы управления производством/операциями; лабораторные и инженерные станции, системы технического обслуживания и управления производительностью.	– нежелательные модификации ТП; – промышленный шпионаж; – непатентованные системы мониторинга; – недостаток информации о наличии уязвимого ПО
Зона 3. ОТ-зона. Уровень 2. Системы локального управления	Системы контролируют, мониторят и управляют физическими процессами. Уровень включает в себя средства управления и ПО реального времени; распределенную систему управления (DCS), человеко-машинный интерфейс (HMI); программное обеспечение системы диспетчерского контроля и сбора данных (SCADA).	– нежелательные модификации ТП; – промышленный шпионаж; – недостаток информации о наличии уязвимого ПО
Зона 3. ОТ-зона. Уровень 1. Управление процессом	Системы управляют физическими процессами. Уровень состоит из ПЛК, устройств связи с объектами (RTU), интеллектуальных электронных устройств (IED). Здесь HMI и ПЛК обмениваются данными по протоколам SCADA, а технический трафик направляется в ПЛК. Внедряя решение для обеспечения ИБ, необходимо принимать во внимание проблемы задержки передачи данных, время безотказной работы производственного оборудования, текущие процессы и чувствительность к любым	

Зона / Уровень	Описание	Риски
	изменениям, которые могут повлиять на производство.	
Зона 3. ОТ-зона. Уровень 0. Физический процесс	Состоит из широкого спектра датчиков, исполнительных механизмов и устройств, участвующих в базовом производственном процессе. Эти устройства выполняют основные функции промышленной автоматики и системы управления.	– нарушение или изменение физического процесса

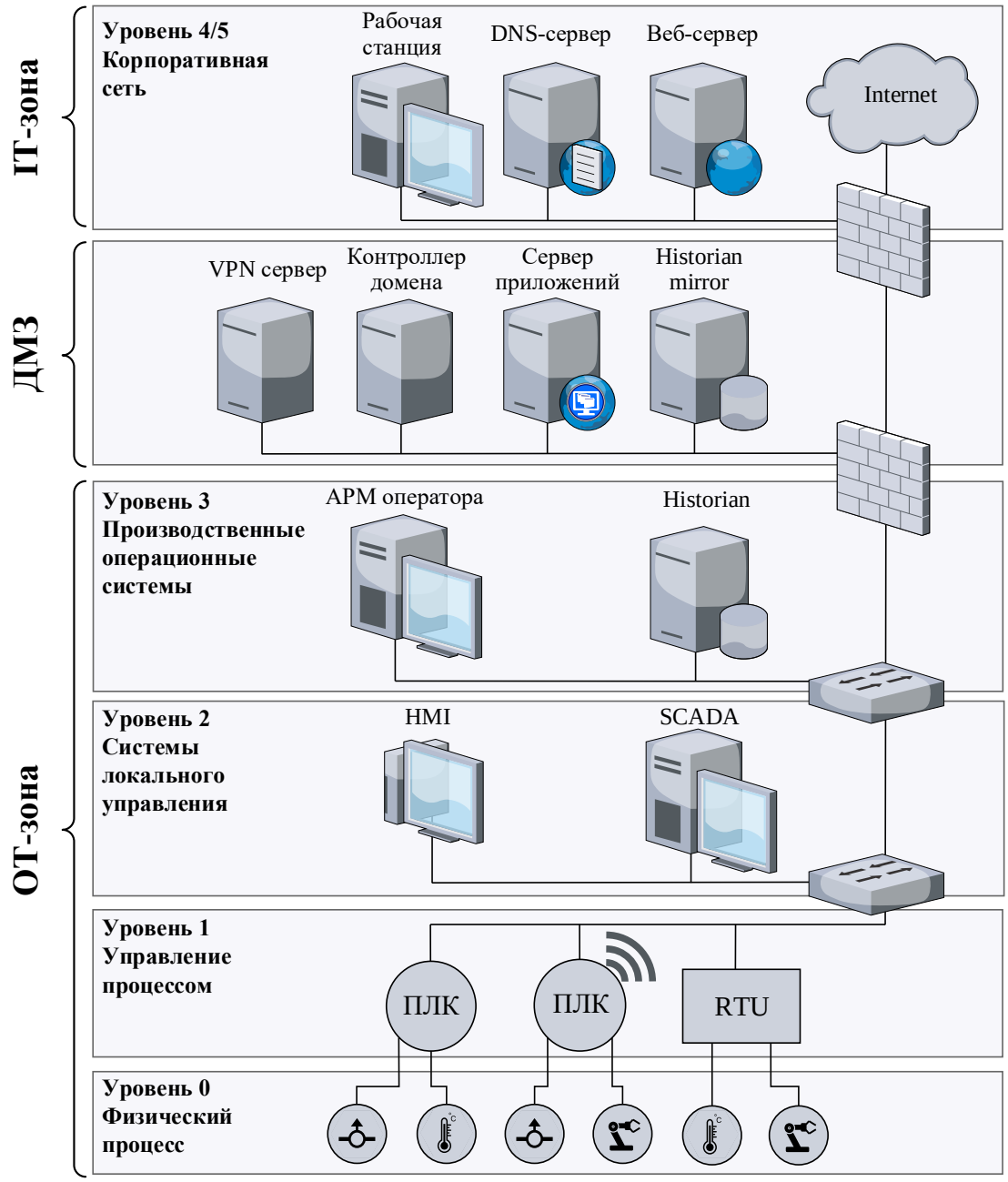


Рисунок 1.3 – Эталонная архитектура АСУ ТП согласно модели PRM

Принципиальная особенность архитектуры АСУ ТП – отсутствие встроенных актуальных механизмов обеспечения ИБ, соответствующих современному состоянию нормативно-правовой базы, что затрудняет их интеграцию с внешними корпоративными системами, имеющими выход в сеть Интернет.

Наиболее важным элементом АСУ ТП являются промышленные сети, связывающие оборудование промышленной системы управления [2, 4] (датчики, исполнительные механизмы, ПЛК и т.д.) между собой. Во многих случаях нижний и средний уровни АСУ ТП [10] объединяются «полевой шиной», представляющей собой сеть с гарантированным временем доставки пакетов, что позволяет создать распределенную систему управления, работающую в режиме реального времени. Для них недопустимо опоздание в выдаче управляющего сообщения, поскольку это может привести к авариям. Приложения верхнего уровня АСУ ТП обычно не требуют работы в режиме реального времени, поэтому оборудование здесь связано через сеть Ethernet, что позволяет АСУ ТП интегрировать с системой управления уровня АСУ предприятия, отправляя производственные данные в базы данных предприятия.

В настоящее время существует более 50 типов промышленных сетей (Profibus, Modbus, LonWorks, CANopen, DeviceNet, ControlNet, Seriplex, SDS, ArcNet, BACnet, FIP, FDDI, FF, ASI, Ethernet, Foundation Fieldbus, WorldFIP, Interbus, BitBus и др.), но широко используется только часть из них. В России большинство АСУ ТП используют сети Profibus и Modbus, а также возрос интерес к сетям на базе CANopen и DeviceNet [60].

Промышленная сеть АСУ ТП [4, 102] имеет следующие особенности, которые необходимо учитывать при обеспечении ИБ:

– простой в работе сети АСУ ТП может привести к остановке ТП;

– отказ сети АСУ ТП может привести к катастрофическим последствиям (человеческие жертвы, техногенные катастрофы);

– наличие проприетарных технологических протоколов производителей оборудования АСУ ТП, содержащих в себе уязвимости, которые сложно обнаружить и невозможно закрыть традиционными СЗИ;

– невозможно блокировать обмен данными с корпоративной сетью, предоставление удаленного доступа и управление сетью АСУ ТП со стороны подрядчиков.

В отличие от корпоративных систем, где защищаемым ресурсом является информация, подлежащая обработке, хранению и передаче, и основная цель – обеспечить ее конфиденциальность, в АСУ ТП объектом защиты является сам технологический процесс (ТП), и на первое место выходят вопросы обеспечения его непрерывности и целостности (в том числе передаваемой между узлами информации). Промышленные системы могут функционировать без установки обновлений для устранения критически важных уязвимостей, поскольку остановить работу АСУ ТП даже на короткое время невозможно. В таком случае каждый узел становится потенциальным источником угроз ИБ для всех остальных узлов промышленной сети. Кроме того, по-прежнему необходимо защищать периметр сети, несмотря на то что это понятие стало достаточно размытым и все чаще невозможно определить его границы. Это связано с использованием 3G/4G/5G-модемов и спутниковых систем связи в промышленных сетях, каналов подключения специалистов поставщиков АСУ, USB-накопителей, а также каналов подключения к сетям смежных предприятий.

Учитывая особенности, характерные для промышленных сетей, компания Cisco совместно с Rockwell Automation разработала подробную детализированную архитектуру Conwerged Plantwide Ethernet (CPwE) [126], представленную в Приложении Б на Рисунке Б.1, где учтены требования по отказоустойчивости, ограничения со стороны построения топологий, а также протоколы, используемые промышленным оборудованием. Назначение этого документа – определение эталонных сетевых архитектур, ориентированных на применение на промышленных предприятиях и облегчающих объединение промышленных и корпоративных сетей с учетом требований к обеспечению ИБ АСУ ТП.

Недостатки обеспечения ИБ АСУ ТП промышленных объектов обусловлены различными факторами, которые в большинстве случаев схожи с проблемами обеспечения ИБ типовой корпоративной сети, однако специфика АСУ ТП накладывает определенные ограничения на механизмы обеспечения ИБ промышленных систем автоматизации (Рисунок 1.4).

Рисунок 1.4 – Особенности АСУ ТП, затрудняющие обеспечение ИБ промышленных систем

С одной стороны доступ нарушителей к АСУ ТП может привести к таким последствиям, как остановка производства, выход промышленного оборудования из строя, порча продукции или авария, но с другой стороны, специфика отрасли не

позволяет проверить достижимость рисков на реальной инфраструктуре, так как это может негативно сказаться на ходе ТП.

1.2.1 Типовые атаки на АСУ ТП

Анализ структурно-функциональной организации АСУ ТП промышленных объектов с точки зрения обеспечения ИБ, позволяет сформулировать перечень основных методов атаки [81, 82]:

– отправка команд оборудованию – поскольку большая часть используемого в промышленности ПО не требует идентификации пользователя, то нарушителю достаточно проникнуть в технологическую сеть предприятия и установить связь с нужным объектом;

– использование специальных утилит, но в этом случае нарушители будут ограничены правами активного пользователя;

– внесение правок в базу данных, что в некоторых случаях позволяет также изменить и связанные с ней объекты;

– технология Man-in-the-Middle, которая используется в тех случаях, когда нарушителю известны параметры функционирования сети, что позволяет ему менять информацию на главном экране и получить полный контроль над любой системой;

– взлом датчиков и подача на них нарушителем неправильных данных, что приводит к некорректной работе промышленного оборудования.

Перечень основных атак на АСУ ТП, отмеченных в реальных инцидентах:

– на инфраструктуру и операционные системы (вирусы, черви, троянские программы, ARP-спуфинг, DDos-атаки);

– на базы данных (SQL-инъекция);

– на SCADA-системы;

– на ПЛК (пароль по умолчанию, неавторизованный доступ к фирменному ПО, удалённое изменение пароля и т.д.);

– на протоколы;

– другие атаки (отказ в доступе, переполнение буфера, отказ в представлении, отказ в управлении, подмена представления) [98].

С развитием АСУ ТП изменяются и совершенствуются атаки на них, появляются новые способы (сценарии) их реализации.

Сценарий 1. Атака на технологические сети через смежные системы.

Сложные целенаправленные атаки включают в себя три основных этапа [21]:

1) получение и повышение привилегий на узлах корпоративной сети;

2) развитие атаки и закрепление в корпоративной сети;

3) перемещение нарушителя внутри сети, получение доступа к критически важным системам и развитие атаки в технологической сети.

Проводя сбор информации на узлах сети, анализируя существующие системы и способы их использования, повышая в них привилегии, нарушитель может реализовать атаку на технологическую сеть через корпоративную сеть предприятия, поскольку она имеет к ней доступ.

Одной из целей нарушителя может оказаться, например, АРМ оператора, откуда он сможет:

– повысить привилегии и реализовать дальнейшие деструктивные воздействия на АРМ оператора;

– влиять на ТП;

– сканировать верхний уровень технологической сети и производить боковое перемещение внутри сети, то есть нарушитель может развить атаку вглубь технологической сети, переместиться на средний уровень и получить доступ к ПЛК [110].

Сценарий 2. Атака из технологической сети.

У нарушителя также есть возможность проникнуть и в изолированную технологическую сеть [82]:

– целенаправленное заражение USB-накопитель для распространения вредоносного ПО и переноса информации между АРМ (например, это было реализовано в атаках Stuxnet, Flame, Equation, ProjectSauron);

– компрометация локального ресурса в сети Интернет, который доступен из технологической сети, либо компрометация сетевого оборудования (это было реализовано в атаках BlackEnergy2);

– заражение АРМ подрядчиков, подключающихся в технологическую сеть.

Таким образом, ландшафт угроз для промышленных систем становится схожим с ландшафтом угроз для корпоративных сетей. Изоляция АСУ ТП промышленных объектов не может рассматриваться как мера их защиты.

1.2.2. Особенности обеспечения ИБ АСУ ТП промышленных объектов

В АСУ ТП промышленных объектов нарушителя ИБ необходимо выявлять на начальных этапах атаки, что требует понимания каждого ТП предприятия, поэтому необходимы инструменты анализа и защиты, результаты работы которых будут понятны как специалистам по ИБ, так и операторам АСУ ТП.

Средства защиты АСУ ТП промышленных объектов должны соответствовать ряду требований, основные из которых:

– глубокий анализ уязвимостей, характерных для компонентов АСУ ТП;

– возможность выявления многошаговых целевых атак;

– удобное представление результатов работы;

– учет специфики промышленного сегмента и компонентов АСУ ТП.

Средства обеспечения ИБ АСУ ТП должны полностью учитывать внутреннюю архитектуру управления промышленными процессами предприятия и соответствовать ей (Таблица 1.2).

Таблица 1.2 – Средства обеспечения ИБ АСУ ТП

Уровень промышленной системы	Средства защиты от угроз ИБ
Уровни корпоративной сети	Средства централизованного мониторинга и корреляции угроз ИБ (например, Positive Technologies MaxPatrol SIEM), комплекс решений по защите каналов передачи данных

Уровень промышленной системы	Средства защиты от угроз ИБ
Уровень ДМЗ	– сегментирование сети; – подсистема межсетевого экранирования и подсистемы предотвращения вторжений на стыке технологических, корпоративных и других не доверенных сетей; – безопасный удаленный доступ с использованием сертифицированных алгоритмов шифрования (например, Континент АП); – защита при передаче телеметрической информации сторонним организациям и контролирующим органам (Nateks); – однонаправленная передача информации; – анализ защищенности сети передачи данных
Уровень системы локального управления	– специализированные промышленные средства антивирусной защиты (Kaspersky Industrial Cyber Security for Nodes); – средства защиты от несанкционированного доступа (Код безопасности SecretNet, Dallas Lock); – средства контроля действий привилегированных пользователей; – расширенные средства аутентификации и авторизации (Indeed Enterprise Authentication); – средства контроля уровня защищенности (Positive Technologies MaxPatrol 8, Positive Technologies XSpider)
Уровень управления процессами	– контроль изменения состояния целостности ПЛК (например, Kaspersky Industrial Cyber Security for Nodes); – контроль целостности и конфиденциальности передаваемой информации (Positive technologies industrial security incident manager, Kaspersky Industrial Cyber Security for Networks)

В настоящее время на российском рынке ИБ представлены программные продукты производителей СЗИ, направленные на решение проблемы обеспечения ИБ на различных уровнях промышленных систем автоматизации.

Особенностью наложенных средств защиты АСУ ТП является их масштабируемость, множество настроек безопасности и подключаемых подсистем, способных осуществлять гибкое конфигурирование и учитывать каждый ТП предприятия, а также наличие оперативного централизованного управления

подсистемами безопасности и возможность своевременного оповещения о выявленных инцидентах ИБ [82].

В полном объеме отвечают требованиям регуляторов в области обеспечения ИБ АСУ ТП и имеют действующие сертификаты следующие средства защиты АСУ ТП [79]:

– Kaspersky Industrial CyberSecurity (Лаборатория Касперского) [93];

– PT Industrial Cybersecurity Suite (Positive Technologies) [163];

– DATAPK (Уральский Центр Систем Безопасности) [128, 144].

Российские наложенные средства защиты АСУ ТП позволяют в некоторой мере:

– обнаруживать активность нарушителей и непреднамеренные ошибочные действия операторов;

– контролировать целостность ПО и промышленного оборудования конечных точек информационной инфраструктуры;

– проводить непрерывный контроль сетевого окружения, анализ трафика и уровня ИБ АСУ ТП;

– выявлять инциденты ИБ и предоставлять сведения по ним;

– формировать необходимую отчетность.

1.3 Анализ нормативно-правовой базы и требований к обеспечению ИБ АСУ ТП промышленных объектов

Наиболее известными зарубежными нормативными документами в области ИБ промышленных систем автоматизации являются стандарты NIST SP 800-82, NERC CIP, ANSI/ISA-99, IEC 62443, а в нашей стране – Федеральный закон № 187-ФЗ, Приказы ФСТЭК России № 31 и № 239, серия стандартов ГОСТ Р МЭК 62443. Полный перечень и наименование нормативных документов представлено в Приложении В.

Стандарт **NIST SP 800-82 Rev. 2 «Guide to Industrial Control Systems (ICS) Security»** («Рекомендации по обеспечению безопасности промышленных систем

автоматизации») предоставляет подробный анализ отличия АСУ ТП от других информационных систем, кратко описывает эволюцию промышленных систем и их постепенную интеграцию с корпоративной сетью, а также описывает факторы, влияющие на ИБ АСУ ТП. Значительную часть стандарта составляет информация об оценке и управлении рисками ИБ АСУ ТП:

– идентификация и определение ценности активов;

– выбор мер защиты;

– анализ и оценка рисков;

– внедрение мер защиты.

В стандарте приведены лучшие практики и рекомендации, не зависимые от конкретных производителей СЗИ, что позволяет использовать их при проектировании систем защиты информации российских АСУ ТП.

Серия стандартов NERC-CIP [87] (Critical Infrastructure Protection) применяется для обеспечения надежной защиты от возможных атак на АСУ и сети коммуникации объектов энергетического сектора. Подобно стандарту NIST SP 800-82, данная серия содержит детально проработанные методические руководства по обеспечению ИБ АСУ ТП, которые успешно применяются во многих странах мира, включая Россию.

Семейство стандартов ANSI/ISA-99 [23, 164] («Безопасность промышленных систем автоматизации и управления») в качестве базовой концепции обеспечения ИБ АСУ ТП использует подход, основанный на сегментации сети передачи данных предприятия на зоны и связывающие их тракты (каналы связи). Стандарты предлагают набор требований по обеспечению ИБ в зависимости от уровня рисков предприятия, который определяется последствиями реализации атаки, а смягчение последствий достигается за счет их локализации в выделенных зонах, максимально изолированных от других сегментов.

Концепция обеспечения ИБ АСУ ТП на основе сегментации системы, предложенная в данной серии стандартов, впоследствии стала основой для разработки стандартов ISA/IEC 62443.

Серия международных стандартов ISA/IEC 62443 [99, 142] («Безопасность промышленных систем автоматизации и управления») в основе своих требований содержит риск-ориентированный подход, согласно которому проектирование системы управления ИБ АСУ ТП включает следующие этапы:

– высокоуровневая (ориентировочная) оценка рисков ИБ, связанная с реализацией атак ИБ;

– построение базовой модели АСУ ТП, описывающей классификацию основных видов деятельности, ТП и других активов промышленного предприятия;

– построение объектной модели, отражающей иерархию основных объектов и активов АСУ ТП, их взаимодействие с сетями, ключевыми подразделениями и т.п.;

– построение базовой архитектуры, отражающей все основные компоненты АСУ ТП, телекоммуникационное оборудование, линии связи и т.п.;

– построение зональной модели, разделяющей АСУ ТП на отдельные зоны;

– детальный анализ рисков ИБ для каждой выделенной зоны;

– определение текущего уровня безопасности для каждой зоны и требований к обеспечению целевого уровня безопасности зоны, реализуемые путем выбора соответствующих контрмер.

Перечисленные международные стандарты играют важную роль в разработке российской нормативно-методической базы в области ИБ АСУ ТП.

Серия стандартов ГОСТ Р МЭК 62443 [1, 116] «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» издается в России с 2015 г. в рамках политики гармонизации системы национальных стандартов и приведения ее в соответствие с системой международных стандартов в области обеспечения ИБ АСУ ТП.

Стандарты данной серии являются базовыми документами для формирования системного риск-ориентированного подхода к обеспечению ИБ автоматизированных промышленных систем.

Конкретные требования к обеспечению ИБ АСУ ТП промышленных объектов РФ установлены **Приказом ФСТЭК России от 14 марта 2014 г. № 31**

«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды» [10].

В соответствии с Приказом, объектами защиты в АСУ ТП являются:

– критически важная (технологическая) информация;

– программно-технический комплекс АСУ ТП.

Для формирования требований к обеспечению ИБ АСУ ТП Приказ № 31 определяет необходимость определения угроз безопасности информации (УБИ) и построения модели угроз, включая:

– оценку возможностей нарушителей (выявление источников угроз);

– анализ возможных уязвимостей АСУ ТП;

– анализ сценариев реализации УБИ;

– анализ последствий от реализации УБИ.

Преимуществом подхода к обеспечению ИБ АСУ ТП, предложенного в Приказе ФСТЭК № 31 является комплексное применение организационных и технических средств защиты на всех стадиях жизненного цикла АСУ ТП. В то же время требования Приказа № 31, хотя и в значительной степени коррелируют с перечисленными выше международными стандартами, также носят рекомендательный характер. Окончательное решение о необходимых мерах защиты принимает собственник АСУ ТП.

Важную роль в решении проблемы обеспечения ИБ АСУ ТП крупных промышленных предприятий играет **Федеральный закон от 26 июля 2017 г. № 187-ФЗ** [12] «О безопасности критической информационной инфраструктуры Российской Федерации». Под объектами КИИ здесь понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов РФ, функционирование которых критически важно для экономики государства.

В целях конкретизации требований, предусмотренных федеральным законом № 187-ФЗ, и условий их применения, выпущен **Приказ ФСТЭК России от 25 декабря 2017 г. № 239** «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [11]. Данный документ содержит рекомендации по обеспечению ИБ значимых объектов на различных этапах их жизненного цикла.

Как и в Приказе № 31, регламентирующем меры обеспечения ИБ АСУ ТП не относящихся к значимым объектам КИИ, анализ угроз должен включать выявление источников угроз, оценку возможностей нарушителей, анализ уязвимостей используемых систем, определение возможных способов реализации угроз и их последствий. Определение УБИ – основополагающий этап обеспечения ИБ АСУ ТП, однако официально принятый порядок моделирования и определение актуальности УБИ АСУ ТП в рассмотренных документах отсутствует.

1.4 Анализ методов оценки рисков ИБ и моделирования сценариев атак на АСУ ТП промышленных объектов

По результатам проведенного анализа нормативной базы [37, 39,42, 45, 49, 68, 71, 72, 173, 174] можно сделать вывод, что подходы к обеспечению ИБ промышленных систем автоматизации имеют общую структуру и их ключевым элементом является проведение анализа и оценки рисков ИБ, предполагающее определение сценариев атак с ненулевой вероятностью возникновения негативных последствий с существенным ущербом. Вследствие, в зависимости от величины потенциального ущерба и специфики сценариев атак, определяются контрмеры, позволяющие снизить выявленные риска ИБ.

В Таблице 1.3 представлено сравнение определений оценки рисков ИБ из различных источников.

Таблица 1.3 – Сравнение определений оценки рисков

Источник	Определение оценки рисков ИБ
NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security»	Процесс выявления рисков для деятельности агентства (включая миссию, функции, имидж или репутацию), активов агентства или отдельных лиц путем определения вероятности возникновения, результирующего воздействия и дополнительных мер безопасности, которые могли бы смягчить это воздействие. Включает анализ угроз и уязвимостей.
Серия международных стандартов ISA/IEC 62443	Процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения, и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации контрмер с целью минимизации общей уязвимости.
Серия стандартов ГОСТ Р МЭК 62443	
ГОСТ Р ИСО/МЭК 27005-2010 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»	Процесс, охватывающий идентификацию риска, анализ риска и оценивание риска.
ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»	Общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации.
ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»	Общий процесс анализа информационного риска и его оценивания.
ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»	Выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной

Источник	Определение оценки рисков ИБ
	системы, используемой для обработки этой информации

Проведенная на высоком уровне оценка рисков должна обеспечить:

– получение объективной и независимой оценки текущего уровня защищенности АСУ ТП с учетом требований законодательства РФ;

– планирование реализации комплекса мер защиты, направленных на повышение уровня защищенности АСУ ТП;

– выделение и обоснование актуальных требований к обеспечению ИБ АСУ ТП.

Использование моделей и методов оценки рисков ИБ АСУ ТП позволяет повысить оперативность и достоверность принимаемых управленческих решений.

1.4.1 Классификация существующих подходов и методов к оценке рисков ИБ АСУ ТП промышленных объектов

Всю совокупность известных на сегодняшний день методов оценки рисков ИБ можно разделить на две группы: основанные на качественном подходе оценки рисков и на количественном.

Качественные методы не позволяют определить численную оценку риска, вместо этого объекту оценки присваивается показатель, ранжированный по качественной шкале (например, «низкий», «средний», «высокий»), что чаще всего является основой для проведения дальнейших исследований с помощью количественных методов.

Методы количественной оценки рисков ИБ применяются, когда угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями. В этом случае объектом оценки может являться ценность актива в денежном выражении, вероятность реализации угрозы, ущерб от реализации угрозы, стоимость контрмер и др. В практических приложениях наиболее часто риск оценивается в стоимостном выражении путем перемножения вероятности

реализации той или иной угрозы и стоимости наносимого при этом ущерба. Встречаются и другие подходы к оценке рисков ИБ, в том числе предусматривающие его в виде некоторой безразмерной величины. Но в любом случае, количественная оценка рисков сводится к оценке двух параметров – вероятности реализации угрозы и возможного ущерба от этой реализации [89].

Целью и качественного, и количественного методов является понимание реальных рисков ИБ предприятия, определение перечня актуальных угроз, что в свою очередь позволит сделать выбор эффективных контрмер. Каждый метод оценки рисков имеет свои преимущества и недостатки:

– методы качественной оценки позволяют выполнить оценку рисков ИБ быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгоды от внедрения контрмер;

– методы количественной оценки дают наглядное представление по объектам оценки, однако они более трудоемки и в некоторых случаях неприменимы без автоматизации процесса.

Для автоматизации оценки рисков ИБ создано множество пакетов программ, сочетающих в себе как качественные, так и количественные методы оценки. Наиболее распространенными из них являются CRAMM, FRAP, MSAT и OCTAVE [25, 26, 59, 88, 91, 100, 101, 138, 148].

CRAMM является одним из первых методов анализа и оценки рисков ИБ, основанный на комплексном подходе к оценке рисков, сочетающем количественные и качественные методы [127].

Исследование ИБ системы с использованием CRAMM проводится в три этапа:

1) определение границ исследуемой системы, построение модели активов, описывающей взаимосвязь между программными, информационными и техническими активами, оценка их ценности на основе потенциального ущерба, который может понести предприятие в результате атаки;

2) проведение оценки рисков ИБ с идентификацией и оценкой вероятности реализации угроз, величины уязвимостей и расчетом рисков для каждого набора актив – угроза – уязвимость;

3) поиск адекватных контрмер и сравнение рекомендуемых и существующих контрмер.

Достоинства CRAMM: структурированный и широко опробованный метод; обладает гибкостью, что позволяет использовать его в проектах любой сложности; наличие понятного формализованного описания сводит к минимуму возможность возникновения ошибок при реализации процессов анализа и оценки рисков ИБ.

Недостатки CRAMM: применение подходит для уже сформированных систем; высокая сложность и трудоемкость сбора исходных данных; уровень угроз и уязвимостей оценивается на основе ответов из опросников (экспертная оценка); невозможность использования предыдущих результатов в качестве факторов, влияющих на уровень риска ИБ.

FRAP (Facilitated Risk Analysis Process) описывает подход к качественной оценке рисков ИБ и направлен на выявление, оценку и документирование состава рисков ИБ для заранее определенной области исследования [96, 161].

Анализ и оценка рисков ИБ проводится проектной командой на основе мозговых штурмов, в ходе которых определяются уязвимости, потенциальные угрозы, вероятность реализации этих угроз и возможный ущерб. Проектная команда не стремится получить оценки рисков ИБ при отсутствии данных для определения таких факторов, а полагается на общие знания об угрозах, уязвимостях и об их влиянии на деятельность предприятия.

Достоинства FRAP: минимизация трудозатрат; простота и прозрачность процесса анализа и оценки рисков ИБ.

Недостатки FRAP: отсутствие подробных вспомогательных материалов (каталога угроз, уязвимостей, последствий и контрмер); участникам проектной команды требуется достаточный опыт для выявления угроз и понимания их реализации; отсутствие возможности глубокой декомпозиции, подробной и точной оценки рисков затрудняет выбор минимально необходимых защитных мер.

MSAT (Microsoft Security Assessment Tool) [25] сочетает в себе элементы качественного и количественного подходов. Качественный подход используется для быстрого составления перечня всех рисков ИБ, в то время как количественный подход позволяет провести более глубокий анализ наиболее значимых рисков ИБ. Это позволяет сформировать перечень основных рисков ИБ, требующих глубокого изучения, и сконцентрировать усилия на этих рисках.

Исследование проводится в четыре этапа:

1) оценка рисков, включающая в себя планирование сбора данных, их непосредственный сбор и приоритезацию рисков ИБ;

2) поддержка принятия решений с определением функциональных требований для снижения рисков, выбором возможных решений, оценкой снижения риска и стоимости решения, а также выбором мер по нейтрализации риска;

3) реализация контроля;

4) оценка эффективности.

Достоинства MSAT: позволяет проводить периодическую оценку рисков ИБ и поддерживать в актуальном состоянии информацию о текущем уровне рисков ИБ и о необходимых мерах по контролю рисков.

Недостатки MSAT: трудоемкость требует привлечения значительных ресурсов и увеличения затрат на реализацию; применим для малых и средних систем.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [26] основан на качественном подходе к оценке рисков. Суть методики заключается в проведении оценки рисков ИБ сотрудниками предприятия без привлечения внешних консультантов.

Оценка рисков ИБ осуществляется в три этапа:

1) разработка профилей угроз, включающих в себя инвентаризацию и оценку ценности активов, выявление угроз и оценку вероятности их реализации;

2) выявление уязвимостей информационной системы и оценка их критичности;

3) оценка и обработка рисков ИБ, включающая в себя определение вероятности возникновения ущерба в результате реализации угроз, определение мер защиты, принятие решений по обработке рисков ИБ.

Достоинства OCTAVE: итеративный подход, позволяющий постепенно увеличивать глубину анализа рисков ИБ; документация в открытом доступе, то есть подходит для предприятий с жестко ограниченным бюджетом

Недостатки OCTAVE: в отсутствие вспомогательной документации (каталогов угроз, уязвимостей, последствий, контрмер) значимыми являются знания и компетентность исполнителей.

В Таблице 1.4 обобщены основные характеристики рассмотренных инструментальных средств оценки рисков ИБ, а также отмечаются недостатки при их использовании для оценки рисков ИБ АСУ ТП промышленных объектов.

Таблица 1.4 – Характеристики методов оценки рисков ИБ

Метод / Критерий	CRAMM	FRAP	MSAT	OCTAVE
Сложность применения				
Финансовые затраты	+	–	+	–
Высококвалифици-рованный сотрудник	+	+	+	+
Внешний эксперт	+	+	–	–
Этапы				
Идентификация риска	+	+	+	+
Анализ риска	+	+	+	+
Оценка риска	+	+	+	+
Обработка риска	+	+	–	+
Подход к оценке рисков ИБ				
Качественный	+	+	+	+
Количественный	+	–	+	–
Недостатки в использовании для АСУ ТП	– не учитывают специфику АСУ ТП промышленных объектов как объекта защиты; – нет согласованности с нормативной базой РФ в области обеспечения ИБ АСУ ТП; – не адаптированы к изменениям ландшафта угроз;			

Критерий \ Метод	CRAMM	FRAP	MSAT	OCTAVE
	– для достоверных результатов требуется полная и непротиворечивая информация; – не рассматривают сценарии атак.			

Методы и подходы к оценке рисков ИБ, предлагаемые российскими и зарубежными учеными рассмотрены в Приложении Г (Таблица Г.1). Большинство из них позволяют оценить риски ИБ отдельных уровней промышленной системы, но не все учитывают последствия для системы в целом, то есть при оценке рисков ИБ не рассматриваются негативные последствия реализации атак, использующих последовательность уязвимостей, что критично для АСУ ТП промышленных объектов. Подходы и методы к оценке рисков ИБ АСУ ТП промышленных объектов должны учитывать особенности современных атак, представляющих собой совокупность последовательных действий нарушителя.

Кроме того, специфика АСУ ТП промышленных объектов создает дополнительные сложности при оценке рисков ИБ и требует использование эффективных методов, несмотря на высокую формализованность объекта защиты с точки зрения моделирования оценки рисков ИБ промышленных систем автоматизации.

1.4.2 Методы интеллектуального анализа и моделирования в задаче оценки рисков ИБ АСУ ТП

Оценка рисков ИБ АСУ ТП промышленных объектов является сложным, слабо структурированным и плохо формализованным видом деятельности. Учитывая высокую неопределенность и сложность процедуры формализации факторов, влияющих на итоговые показатели уровня защищенности системы, проблема оценки рисков ИБ АСУ ТП остается открытой и требует разработки и применения новых подходов, среди которых в последние годы хорошо зарекомендовали себя методы и технологии интеллектуального анализа данных и

когнитивного моделирования. Подобные исследования включают в себя следующие направления:

– разработка моделей и алгоритмов оценки рисков ИБ на основе методов и технологий нечеткой логики и нейросетевого моделирования [19, 30, 53];

– разработка моделей и алгоритмов оценки рисков ИБ с использованием технологий когнитивного моделирования [16, 31, 44, 111];

– разработка моделей и алгоритмов оценки рисков ИБ с использованием динамических байесовских сетей и Марковских моделей [155, 162];

– разработка моделей и алгоритмов оценки рисков ИБ с использованием методов и технологий машинного обучения [139, 166, 167].

Анализ работ (Приложение Г, Таблица Г.2) в данном направлении показывает, что большинство из этих моделей и алгоритмов изначально не ориентированы на задачи оценки рисков ИБ АСУ ТП промышленных объектов, поскольку не учитывают в полной мере специфику объекта и не обладают системным характером.

Внимание исследователей привлекают возможности, предоставляемые для решения проблемы оценки рисков ИБ моделированием на основе построения нечетких когнитивных карт (НКК) (Fuzzy Cognitive Maps, FCM) [107, 147, 159, 160, 171], обеспечивающих простоту и наглядность, выявление структуры причинно-следственных связей между элементами сложной системы, трудно поддающиеся количественному анализу традиционными методами, использование знаний и опыта экспертов, адаптацию к неопределенности исходных данных и условий решаемой задачи [31]. В соответствии со сложившейся классификацией, различают: классические НКК [147, 171], обобщенные НКК [118], нечеткие продукционные НКК [28, 107], реляционные НКК [28] и другие. Для решения проблемы оценки силы связей в НКК рядом авторов были предложены специальные расширения НКК, связанные с представлением силы связей в НКК в виде некоторых интервальных оценок. К числу подобных НКК относятся: серые НКК [166], интервально-значные НКК [134], грубые НКК [131], интуиционистские НКК [135].

Известны примеры успешного применения НКК для решения задач оценки рисков ИБ [15, 31, 57, 111, 180], но основной проблемой при использовании рассмотренных методов когнитивного моделирования является недостаточный объем статистической информации об угрозах и уязвимостях, ее противоречивость и неполнота, что затрудняет формирование достоверных оценок рисков ИБ и приводит к неверным итоговым показателям уровня защищенности, что влечет за собой ошибки в выборе эффективных контрмер.

Современные системы поддержки принятия решений активно используются для своевременного и быстрого анализа больших объемов информации, на основе которого происходит принятие решений. Возможно применение методов и алгоритмов, используемых в построении системы поддержки принятия решений, для решения задач ИБ [49, 53], в частности, для автоматизации процесса оценки рисков и обеспечения достаточного уровня защищенности может выполняться разработка интеллектуальной СППР, основу которой составляют алгоритмы, позволяющие формализовать показатели параметров контрмер.

1.4.3 Анализ методики оценки угроз безопасности информации и инструментов моделирования сценариев атак

Перечисленные ранее методы и походы к оценке рисков ИБ могут эффективно использоваться коммерческими организациями, тогда как государственные организации, в частности промышленный сектор, при оценке рисков ИБ должен руководствоваться положениями нормативно-правовой базы РФ.

Методический документ ФСТЭК России «Методика оценки угроз безопасности информации» от 05.02.2021 г. [6] (далее – Методика ФСТЭК) ориентирован на определение актуальных УБИ в информационных системах и разработку модели угроз систем и сетей. Каждая УБИ в Методике ФСТЭК рассматривается как набор последовательных действий нарушителя в рамках некоторого сценария, определение которого включает установление

последовательности возможных тактик и соответствующих им техник. Для определения всех возможных сценариев реализации УБИ необходимо использовать тактики и техники, приведенные в Методике ФСТЭК, а также дополнительную информацию из БДУ ФСТЭК и иных информационных источников, опубликованных в сети Интернет (CAPEC, ATT&CK, OWASP, STIX, WASC и др.). В результате определяется уровень опасности каждой угрозы в рамках каждого сценария реализации для разработки перечня актуальных угроз.

Методика ФСТЭК не является пошаговой инструкцией по определению актуальных УБИ и разработке модели угроз, а содержит лишь перечень этапов с описанием основных действий без подробной детализации. Общая схема проведения оценки актуальности УБИ приведена на Рисунке 1.5.

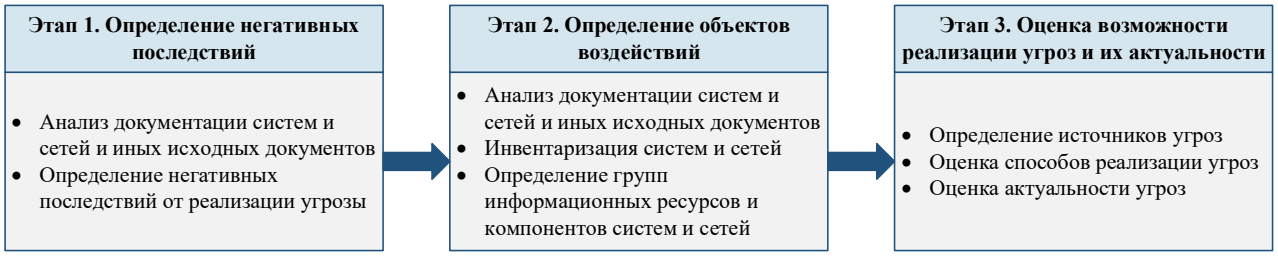


Рисунок 1.5 – Общая схема проведения оценки УБИ по Методике ФСТЭК

Описанный в Методике ФСТЭК подход к моделированию УБИ на основе тактик и техник должен был стать инструментом, значительно упрощающим процесс оценки рисков ИБ АСУ ТП на основе сценариев атак, однако этот вопрос все еще остается сложным по ряду причин [80, 109]:

– многое зависит от экспертной оценки, в том числе определение актуальности тактик и техник в зависимости от характеристик рассматриваемого объекта;

– рассматриваться должен каждый компонент информационной инфраструктуры, что трудоемко для масштабов АСУ ТП промышленных объектов;

– необходимо знать все методы воздействия нарушителей для разработки реалистичных сценариев;

– описание всех сценариев без применения инструментальных средств автоматизации займет много времени и не будет полезно без применения СППР в виду значительного объема обрабатываемых данных.

Чтобы упростить моделирование действий нарушителя, исследователи неоднократно пытались систематизировать известные сценарии атак и выделить их основные этапы. Cyber-Kill Chain (CKC) [115, 120] является одной из первых систематизированных моделей, предложенных компанией Lockheed-Martin в 2011 году. Она указывает на то, что для успешного осуществления атаки нарушитель всегда должен пройти основные этапы, представленные на Рисунке 1.6.

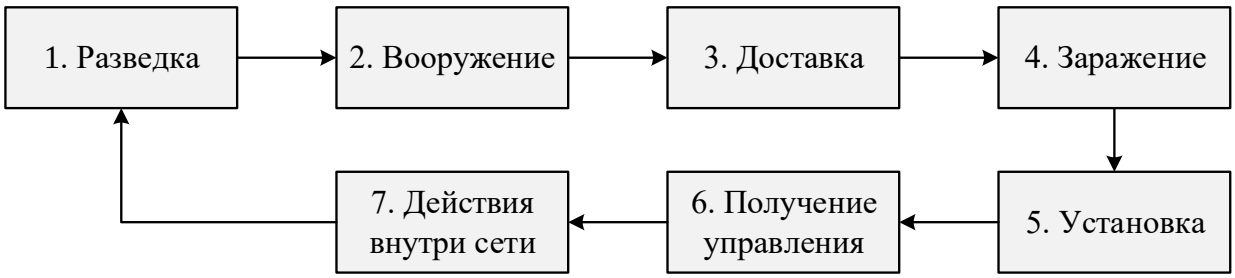


Рисунок 1.6 – Диаграмма этапов в CKC от периметра до цели

Особенностью CKC является ее круговой, а не линейный характер, то есть, как только нарушитель проник во внутреннюю сеть предприятия, все этапы цепочки повторяются, осуществляется дополнительная разведка и горизонтальное продвижение внутри сети предприятия. Фактически, после проникновения в сеть предприятия внешний нарушитель становится внутренним нарушителем (пользователем с определенными правами), что осложняет специалистам по ИБ работу по выявлению атаки [115].

Подобное разделение на этапы характерно для большинства современных целенаправленных атак, однако для моделирования сценариев атак подобная модель не совсем пригодна, поскольку она описывает проникновение нарушителя в инфраструктуру предприятия и закрепление в ней, но не позволяет спрогнозировать действия нарушителя, направленные на получение контроля над инфраструктурой и достижение им конечной цели [115]. Однако модель CKC дала

толчок к развитию методов моделирования сценариев атак, и на сегодняшний день основным инструментом моделирования является база знаний ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) [151] компании MITRE (Приложение Д), как наиболее систематизированный источник информации о действиях нарушителей.

Матрица MITRE ATT&CK для ICS представляет собой базу знаний, в которой собрана информация о нарушителях, тактиках, техниках целевых атак, применяемых для достижения нарушителем конечных или промежуточных целей в промышленных системах управления. В отличие от тактик и техник из Методики ФСТЭК, приведенные в матрице ATT&CK тактики подробно описывают возможные действия нарушителя, для каждой техники представляется подробное описание и известные случаи применения, а также методы обнаружения и контрмеры для нейтрализации атаки. Таким образом, база данных ATT&CK обеспечивает детальный анализ действий нарушителя при моделировании сценариев атак.

Для более полного изучения всех возможных действий нарушителей компания MITRE разработала **стандарт CAPEC** (Common Attack Pattern Enumeration and Classification) [78, 124], включающий в себя перечень и классификатор шаблонов типовых атак с описанием целей, уязвимостей и общих методов, используемых для реализации атак на компоненты информационных систем.

БДУ ФСТЭК во многом схож с базой шаблонов атак CAPEC, но он не имеет структурированной таксономии и не дает четкого понимания о том, как реализуется та или иная атака на компоненты информационной системы. Кроме того, при использовании БДУ ФСТЭК нет возможности перейти от общетеоретического и высокоуровневого описания атаки на уровень оценки конкретных действий нарушителя при ее реализации.

В настоящее время ведется разработка новой редакции Методики ФСТЭК и проводится опытная эксплуатация модернизированного раздела угроз БДУ ФСТЭК, направленного на автоматизацию формирования перечня возможных

УБИ применительно к конкретным автоматизированным системам. Новый раздел содержит сведения об объектах и компонентах воздействия, способах реализации УБИ, уровне возможностей нарушителей и мерах защиты от реализации угроз, сформированных в виде справочников и в целом схожих по структуре с базами данных компании MITRE, но в настоящее время менее информативных.

Поиск решения задачи моделирования сценариев атак отражен во многих российских и зарубежных исследованиях (Приложение Г, Таблица Г.3), предпринимаются попытки автоматизации процесса моделирования. Однако эти решения не предназначены для корректного моделирования сценариев атак на АСУ ТП промышленных объектов, поскольку:

– процесс моделирования затрудняет невысокая формализованность объекта исследования;

– в ходе автоматизированного моделирования может нарушаться непрерывность ТП;

– не содержат в своих базах данных параметров, характерных только для технологического сегмента;

– не руководствуются нормативно-правовой базой РФ в области обеспечения ИБ АСУ ТП.

В связи с этим представляется необходимым, в дополнение к существующей Методике ФСТЭК и БДУ ФСТЭК, структурировать исходные данные для автоматизации моделирования сценариев атак на АСУ ТП промышленных объектов с использованием баз данных MITRE, поскольку они ориентированы на безопасность программных приложений и описывают используемые нарушителем методы для эксплуатации известных уязвимостей программного и аппаратного обеспечения.

1.5 Выводы по главе

1. В первой главе проведен анализ современного состояния проблемы обеспечения ИБ АСУ ТП в условиях изменяющегося ландшафта угроз. Описаны

основные особенности АСУ ТП промышленных объектов обуславливающие необходимость поиска оптимального метода оценки рисков ИБ АСУ ТП с целью повышения уровня ИБ.

2. По результатам анализа нормативно-правовых и методических документов в области обеспечения ИБ АСУ ТП промышленных объектов выделены их основные недостатки [37]:

– отсутствие формализованных методик количественной оценки рисков ИБ;

– отсутствие автоматизации процесса получения количественной оценки рисков ИБ;

– обновления в законодательстве и нормативно-методической базе не отражены в существующих методиках оценки рисков ИБ.

Рассмотренные нормативные и методические документы в целом направлены на построение статической модели нарушителя, формирования фиксированного перечня угроз, экспертной оценки реализации и уровня значимости угроз.

3. Проведен анализ существующих методов и подходов качественной и количественной оценки рисков ИБ для дальнейшего определения рекомендаций по выбору контрмер, направленных на повышение уровня защищенности. Рассмотренные методы и подходы не позволяют проводить оценку рисков ИБ как отдельных зон промышленной системы, так и всей системы в целом; не рассматривают последствия реализации сложных многошаговых атак, использующих совокупность уязвимостей системы. Кроме того, их применение осложнено высокой степенью неопределенности и трудоемкости процедуры формализации факторов, влияющих на уровень защищенности АСУ ТП промышленных объектов, поэтому проблема обеспечения ИБ АСУ ТП промышленных объектов остается открытой и требует для своего решения применения все новых методов и подходов, базирующихся, в частности, на применении технологий интеллектуального анализа данных и когнитивного моделирования.

4. Моделирование сценариев атак позволяют без нарушения ТП корректно определить перечень возможных целенаправленных атак и последствия от их реализации, а также оценить вероятность их реализации, узнать условия, при которых нарушитель сможет атаковать, и определить необходимый перечень контрмер. Для этого требуется использовать низкоуровневые описания возможных способов воздействия нарушителя на объект защиты, представленных в открытых базах знаний. Анализ Методики ФСТЭК и БДУ ФСТЭК показал необходимость в структурировании исходных данных для автоматизации моделирования сценариев атак на АСУ ТП промышленных объектов с использованием баз данных MITRE, поскольку моделирование реалистичных сценариев на промышленные системы автоматизации по причине высокой сложности объекта исследования невозможно без применения инструментальных средств автоматизации.

На основе проведенного анализа сделан вывод о необходимости разработки метода, моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе методов когнитивного моделирования и машинного обучения.

Глава 2. Разработка комплекса моделей для оценки рисков ИБ АСУ ТП промышленных объектов на основе технологий когнитивного моделирования

В данной главе разрабатывается функциональная модель процесса количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе Методики ФСТЭК. В соответствии с серией стандартов ГОСТ Р 62443 строится комплекс моделей АСУ ТП, включающий в себя базовую, объектную и зональную модель объекта защиты. Разрабатывается и строится иерархия нечетких когнитивных моделей для проведения количественной оценки рисков ИБ в пределах выделенных зон АСУ ТП промышленного объекта в условиях воздействия факторов неопределенности и разброса экспертных оценок.

2.1. Разработка функциональной модели процесса оцени рисков ИБ АСУ ТП

Исходя из результатов анализа нормативно-методической базы в области обеспечения ИБ АСУ ТП, а также анализа методов и подходов оценки рисков ИБ сформирован порядок проведения оценки рисков ИБ АСУ ТП промышленных объектов и разработана функциональная модель в нотации IDEF0 (Рисунок 2.1), описывающая процесс количественной оценки рисков ИБ АСУ ТП промышленных объектов в виде иерархии НКК для зональной модели объекта защиты, позволяющих формализовать данный процесс и сценарии атак как в пределах выделенных зон, так и для всего объекта защиты в целом.

Декомпозиция первого уровня функциональной модели на рисунке 2.2 отображает структуру процесса получения количественной оценки рисков ИБ выделенных зон АСУ ТП и промышленной системы в целом.

Рисунок 2.1 – Функциональная модель процесса оценки рисков ИБ АСУ ТП промышленных объектов

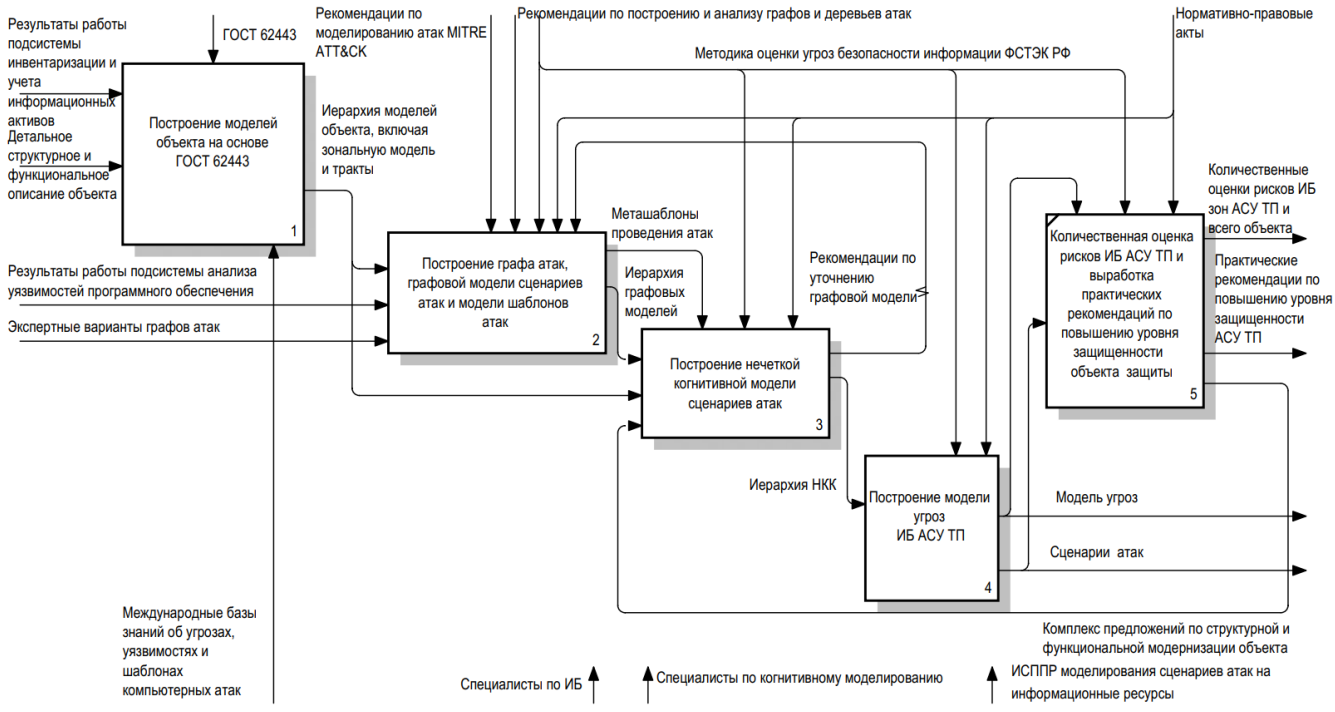


Рисунок 2.2 – Диаграмма декомпозиции первого уровня функциональной модели процесса оценки рисков ИБ АСУ ТП промышленных объектов

На основе данных, собранных подсистемой анализа уязвимостей и подсистемой инвентаризации активов, а также детального структурно-функционального описания объекта выполняется построение комплекса моделей согласно серии стандартов ГОСТ 62443, что позволяет декомпозировать задачу оценки рисков ИБ до ограниченного по сложности набора элементов каждой из выделенных зон.

На основе рекомендаций отечественных и зарубежных нормативных документов и баз знаний специалисты по ИБ выполняют построение графа атак, графовых моделей сценариев атак и моделей шаблонов атак с помощью предлагаемых в работе инструментальных средств. Иерархия графовых моделей является интегральным представлением сведений о возможных цепочках уязвимостей, недостатках реализации ПО и накапливаемых данных о сценариях реализации многошаговых атак активными группировками нарушителей. Особенностью графовых моделей является также возможность учета возможных контрмер (как организационных, так и технических), направленных на снижение уровня опасности моделируемых сценариев атак.

На этапе когнитивного моделирования отдельных сценариев атак специалистами по когнитивному моделированию и специалистами по ИБ выявляются требующие уточнения компоненты (узлы, связи) графовой модели, а также выполняется свертка сценариев в виде вложенных НСКК, описывающих выделенные меташаблоны атак.

На основе иерархии НКК выполняется построение фрагментов модели ИБ АСУ ТП, позволяющей интегрировать согласно методике ФСТЭК России сведения о возможностях нарушителя, последствиях реализации атак и актуальных угрозах ИБ. Фрагменты модели угроз и сценарии атак используются для количественной оценки рисков ИБ для выделенных зон АСУ ТП и формирования комплексной оценки риска ИБ для объекта в целом. На основе сведений о сценариях атак, эксплуатирующих имеющиеся или потенциальные уязвимости и/или недостатки ПО, выполняется выбор возможных контрмер и подбор параметров их развертывания и эксплуатации с целью повышения уровня защищенности объекта.

На основе нескольких итераций моделирования, учитывающих различные сценарии атак, а также перечни контрмер и распределение их ресурсов, вырабатываются практические рекомендации по повышению уровня защищенности АСУ ТП промышленного объекта.

2.2 Построение комплекса моделей АСУ ТП промышленного объекта как объекта защиты

Предварительный анализ особенностей АСУ ТП промышленных объектов, затрудняющих процесс количественной оценки рисков ИБ, показал необходимость в разработке комплекса моделей промышленного объекта защиты [34, 35], позволяющих облегчить понимание функциональных особенностей объекта защиты, взаимосвязь и взаимозависимость между его основными компонентами и взаимодействие с внешними сетями и системами, что в свою очередь облегчит процесс обеспечения ИБ АСУ ТП промышленного объекта.

На основе этапов анализа и моделирования объекта защиты, представленных в серии стандартов ГОСТ 62443, предлагается построить комплекс моделей АСУ ТП промышленного объекта, состоящий из базовой, объектной и зональной моделей на примере фрагмента территориально распределенной системы – АСУ ТП пункта сдачи приема нефти (ПСП) в системе магистральных трубопроводов, предназначенной для автоматизации управления и оперативного контроля ТП, включая сбор данных о технологических параметрах процесса: расход, уровень, температура, давление, плотность и влажность перекачиваемой нефти. Структурная схема рассматриваемого объекта защиты представлена на рисунке 2.3, где УПП – установка подогрева продукта; $Д_1$ – датчики системы измерения количества нефти (СИКН); $Д_2$ – датчики на входе нефтеперекачивающей станции (НПС); НО – насосное оборудование.

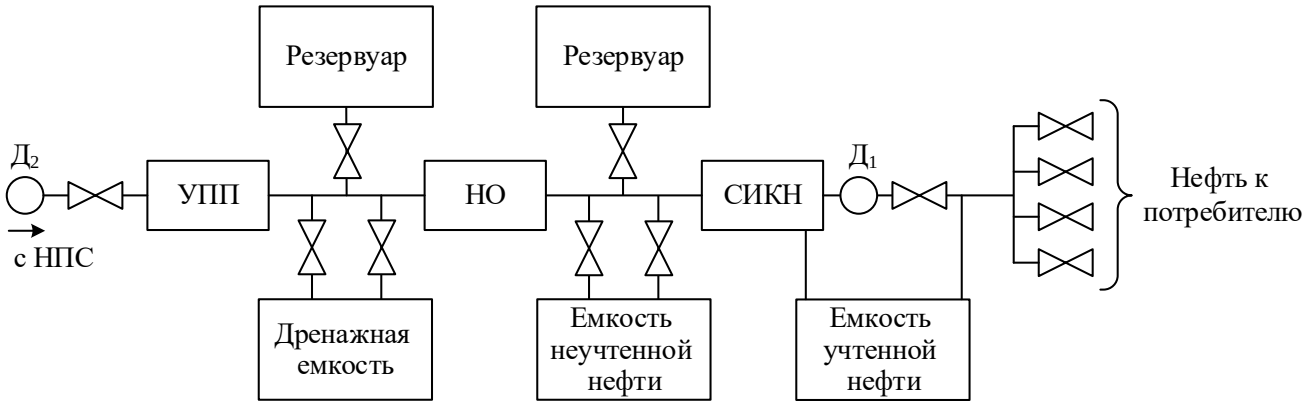


Рисунок 2.3 – Структурная схема АСУ ТП ПСП

Базовая модель объекта защиты, представленная на рисунке 2.4, описывает деление основных видов деятельности промышленной системы, ТП и других активов на пять логических уровней.

Рисунок 2.4 – Базовая модель объекта защиты

Каждый уровень соответствует определенному классу функциональности и описывает функции и действия от систем масштаба предприятия до физических процессов:

– корпоративное управление на уровне 4 включает в себя обеспечение централизованного управления бизнес- и производственными процессами, управление безопасностью, персоналом, а также эксплуатацией и обслуживанием энергосети;

– на уровне 3 система пересылает информацию о количестве переданных нефтепродуктов в систему диспетчерского контроля и управления (СДКУ) ТП транспортировки нефти; система выгрузки в общую информационную систему первичного пункта сбора нефти (ОИС ППСН) передает данные с серверов СИКН и АСУ ТП на центральный сервер предприятия;

– на уровне 2 перед передачей данных на верхний уровень предприятия проводится визуализация и контроль уровней нефтепродукта в нефтесборных пунктах (НСП), измерение количества и показателей качества нефти, нефтепродуктов и газа, а также осуществляется управление задвижками после СИКН до приема нефтепродукта и мониторинг состояния трубопровода и физического воздействия на трубопровод системой обнаружения утечек и контроля активности (СОУиКА);

– уровень 1 включает в себя функции, отвечающие за контроль и управление физическими процессами: проводится контроль положения (КП) задвижек, а также производится управление насосным оборудованием для подачи смеси пожаротушения;

– уровень 0 соответствует физическому процессу и распространяется на датчики и исполнительные механизмы, задействованные в ТП.

Следующим шагом на основе базовой модели строится объектная модель, описывающая иерархию основных объектов и активов предприятия, взаимодействие с сетями, ключевыми подразделениями и системами, задействованными в ТП, системами контроля и другим промышленным оборудованием.

Объектная модель обеспечивает понимание структуры АСУ ТП и связь процессов для анализа объекта защиты, наглядность и возможность определить его критические процессы и активы.

На рисунке 2.5. представлена объектная модель АСУ ТП ПСП.

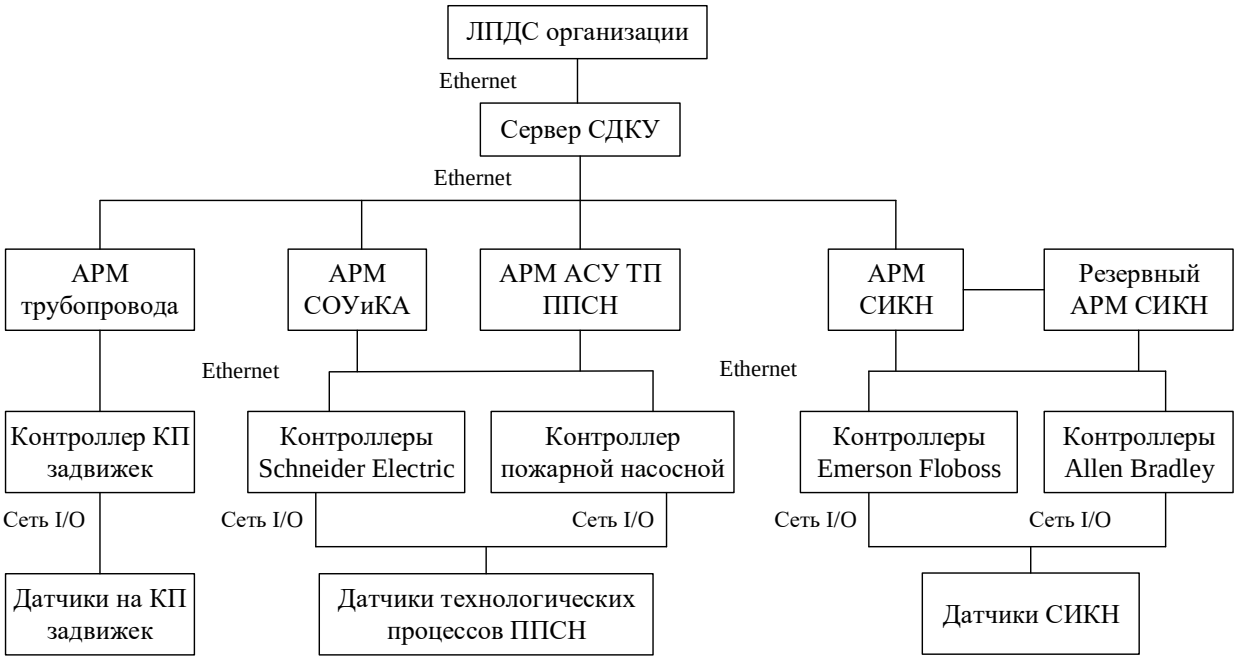


Рисунок 2.5 – Объектная модель объекта защиты

В соответствии с терминологией ГОСТ 62443 подсистемы АСУ ТП ПСП можно рассматривать как выделенные зоны безопасности, объединенные общими показателями риска, функциональными и/или техническими характеристиками, логическими или физическими границами, сетями передачи данных и т.д. Зональная модель строится на основе базовой архитектуры сети АСУ ТП, отражающей все основные компоненты объекта, телекоммуникационное оборудование и линии связи, с учетом рассмотренных ранее моделей объекта защиты. На рисунке 2.6 показано зонирование АСУ ТП ПСП по принципу единства выполняемых функций и требований к безопасности их реализации:

– зона 0 – зона корпоративной информационной сети предприятия;

– зона 1 – зона сервера СДКУ SCADA;

– зона 2 – зона критических устройств управления;

– зона 3 – зона управления задвижками;

– зона 4 – зона управления ТП ПСП;

– зона 5 – зона СИКН;

– зона 6 – зона датчиков.

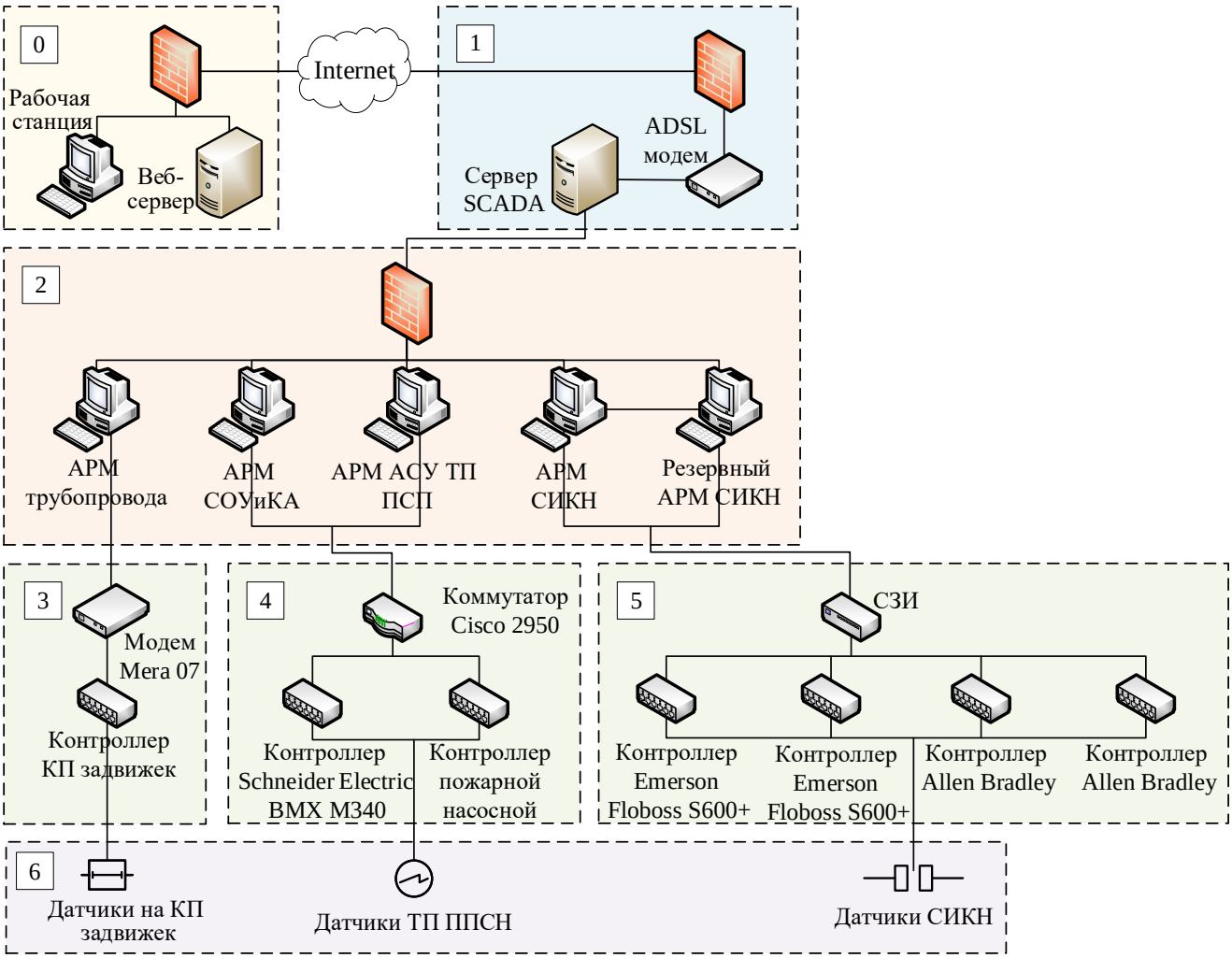


Рисунок 2.6 – Зональная модель объекта защиты

Для каждой выделенной зоны в дальнейшем необходимо провести идентификацию и классификацию активов, анализ угроз и уязвимостей, построение модели нарушителя, сценариев атак и проведение количественной оценки рисков ИБ для определения уровня защищенности АСУ ТП промышленного объекта.

Корректно построенный и проанализированный комплекс моделей АСУ ТП промышленного объекта является основой для выбора адекватных контрмер, эффективность которых напрямую будет зависеть от проведенного исследования и анализа объекта защиты.

2.3 Разработка модели оценки рисков ИБ АСУ ТП на основе иерархии нечетких когнитивных карт

В основе проанализированных нормативно-методических документов лежит методология системного риск-ориентированного подхода к обеспечению ИБ АСУ ТП. Данная методология близка методологии когнитивного моделирования, суть которой заключается в построении и последующем анализе НКК с использованием знаний и опыта экспертов-специалистов в рассматриваемой предметной области.

Предложен подход к оценке рисков ИБ АСУ ТП промышленных объектов, основанный на применении методов когнитивного моделирования с использованием НСКК, в которых в отличие от классических способов построения НКК, для оценки силы взаимосвязей между концептами используются интервальные оценки («серые» числа), характеризующие некоторую меру естественной неопределенности (размытости) в суждениях эксперта или группы экспертов относительно взаимовлияния указанных концептов [36]. Операции нечеткой логики заменяются при этом интервальной арифметикой над серыми (интервальными) числами.

НСКК считаются удачным расширением НКК, поскольку они в большей степени соответствуют представлениям экспертов, обладают большей интерпретируемостью и предоставляют больше степеней свободы лицу, принимающему решение (ЛПР) на основании результатов моделирования. Очевидно, что применение НСКК к задаче интервального оценивания рисков ИБ является перспективным.

НСКК – это когнитивная модель системы в виде ориентированного графа, заданного с помощью следующего набора множеств (2.1):

$$\text{НСКК} = \langle C, E, W \rangle, \tag{2.1}$$

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 (то есть связанных между собой) вершин графа, $S \leq n(n-1)$.

Веса связей НСКК и состояния концептов задаются с помощью «серых» (интервальных) чисел $\otimes W_{ij}$, определяемых как $\otimes W_{ij} \in \left[\underline{W}_{ij}, \overline{W}_{ij}\right]$, 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 $\left[\underline{W}_{ij}, \overline{W}_{ij}\right] \in [-1,1]$.

Изменение состояния концептов C_i во времени описывается уравнением (2.2):

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), (i = 1,2,\dots,n) \qquad (2.2)$$

где $\otimes X_i(k)$ – «серая» (интервальная) переменная состояния i-го концепта C_i, которая в каждый момент времени $k = 0,1,2,\dots$ принимает некоторое значение внутри определенного интервала (диапазона изменения), заданного границами $\underline{X}_i(k)$ и $\overline{X}_i(k)$; $f(\cdot)$ – нелинейная функция активации i-го концепта, отображающая значения аргумента в интервал $[-1,1]$. В качестве функции активации $f(\cdot)$, как правило, принимаются:

а) линейная функция с ограничением (2.3):

$$f(x) = \begin{cases} x, \text{если } |x| \leq 1, \\ \text{Sign } x, \text{если } |x| > 1; \end{cases} \qquad (2.3)$$

б) двухполярная сигмоидная функция (гиперболический тангенс) (2.4):

$$f(x) = (1 - e^{-x})/(1 + e^{-x}) = \text{th}\left(\frac{x}{2}\right); \qquad (2.4)$$

в) однополярная сигмоида (2.5):

$$f(x) = 1/(1 + e^{-x}). \qquad (2.5)$$

Для решения системы уравнений (2.2) требуется задать начальные значения переменных состояния $\otimes X_i(0)$, которые также должны рассматриваться как серые числа $\otimes X_i(0) \in \left[\underline{X}_i(0), \overline{X}_i(0)\right]$. Наибольший интерес представляет получение равновесного (установившегося) решения, которое представляет собой «серый»

вектор $\lim_{k\to\infty}[\otimes X_i(k)] = \otimes X^* \in \left[\underline{X}^*, \overline{X}^*\right]$ или предельный цикл (странный аттрактор).

При выборе серых значений весов $\otimes W_{ij}$ экспертам необходимо ориентироваться на нечеткую шкалу (таблица 2.1).

Таблица 2.1 – Оценка силы (весов) связей между концептами

Лингвистическое значение силы связи	Обозначение терма	Значение терма	Числовой диапазон
Не влияет	Z	Zero	0
Очень_слабая	VS	Very Small	(0; 0,15]
Слабая	S	Small	(0,15; 0, 35]
Средняя	M	Middle	(0,35; 0,6]
Сильная	L	Large	(0,6; 0,85]
Очень_сильная	VL	Very Large	(0,85; 1]

Построение НСКК для количественной оценки рисков ИБ в пределах выделенных зон АСУ ТП промышленного объекта [35, 56, 58] представлена на рисунке 2.7, где C_I – нарушители; C_E –стоимость развертывания и сопровождения контрмер; C_S – определение способов проведения атак по средствам эксплуатации уязвимостей; C_A – определение информационных ресурсов; C_{NC} – определение негативных последствий для АСУ ТП промышленного объекта; C_C – выбор рациональной контрмеры с учетом ограничений; C_R – оценка рисков ИБ.

Концепты C_I^1 и C_I^2 на рисунке 2.7 имеют собственные циклы положительной обратной связи, что указывает на то, что данные концепты выступают в качестве независимых источников входных сигналов НСКК, отражающих воздействия на смежные концепты со стороны внешней среды, и в [36] названы драйверами.

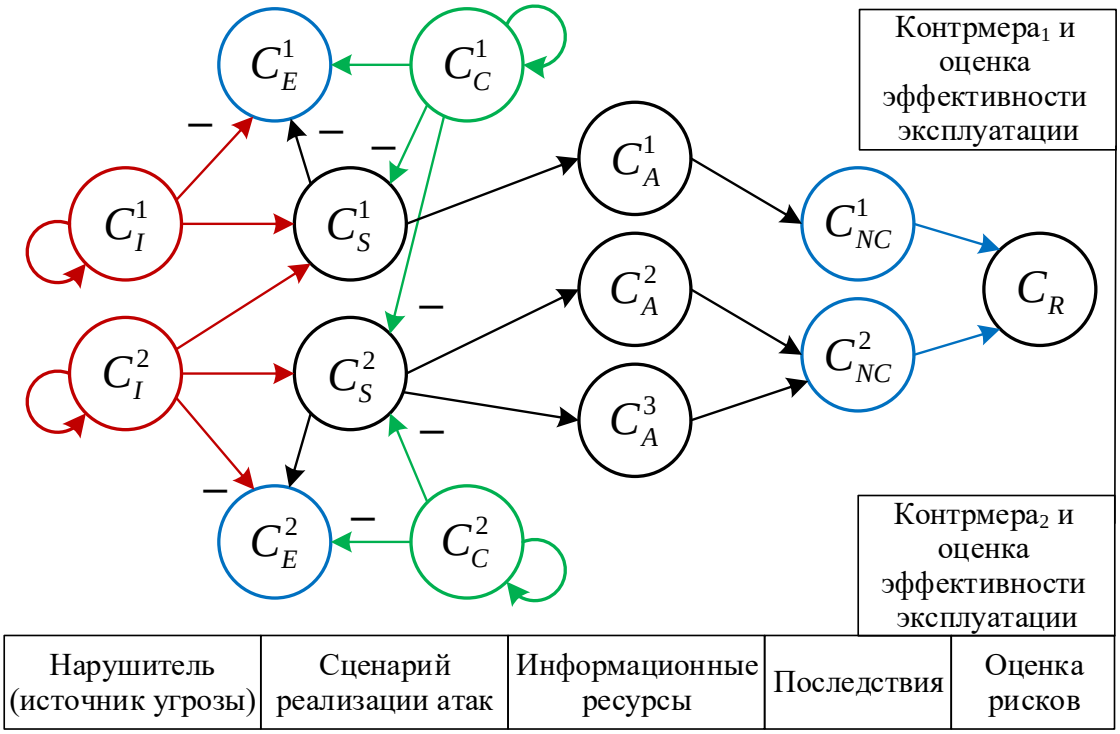


Рисунок 2.7 – НСКК для оценки рисков ИБ АСУ ТП промышленных объектов и оценки эффективности распределения ресурсов контрмер

Значение переменной состояния концепта C_R НСКК на рисунке 2.7 определяет итоговую оценку рисков ИБ X_R для моделируемых сценариев 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 контрмер C_C^1 и C_C^2 при моделировании сценариев атак в пределах выделенных зон АСУ ТП промышленного объекта. Установившиеся значения переменных состояния концептов C_E^1 и C_E^2 позволяют оценить эффективность интеграции и использования каждой контрмеры.

2.4 Разработка алгоритма построения иерархии когнитивных моделей

Как отмечается в [40], на практике исследование реального сложного объекта с помощью методов нечеткого когнитивного моделирования встречается с рядом трудностей [33]: высокая размерность пространства состояний исследуемой системы и ее подсистем, неоднозначность выбора состава базовых концептов и выявления наиболее значимых связей между ними, неопределенность в оценке

силы этих связи и др. Попытки решить эту проблему связаны с представлением исходной НСКК путем ее «сворачивания» (перехода от частного к общему), и, наоборот, с построением НСКК путем ее «развертывания», декомпозиции (от общего к частному) [183].

Использование вложенных (многослойных) НСКК [34, 152-154 170], основанных на декомпозиции некоторой исходной (укрупненной) НСКК, которая представляется в виде совокупности нескольких вложенных друг в друга частных НСКК, позволяет экспертам раскрыть неопределенности на более развернутых уровнях НСКК с детализацией последствий от рассматриваемых факторов рисков. Это дает более точный результат оценки рисков ИБ АСУ ТП промышленных объектов за счет того, что есть возможность рассмотреть процесс реализации атаки внутри каждой выделенной зоны объекта защиты, что впоследствии поможет экспертам при подборе контрмер для каждой зоны безопасности и объекта в целом.

Разбиение НСКК (Рисунок 2.8) на уровни (слои) производится экспертом или группой экспертов таким образом, что каждый уровень (L_i) описывает определенный аспект понимания, глубины изучения проблемы и, следовательно, число уровней (d) вложенной НСКК будет определяться числом принимаемых во внимание аспектов.

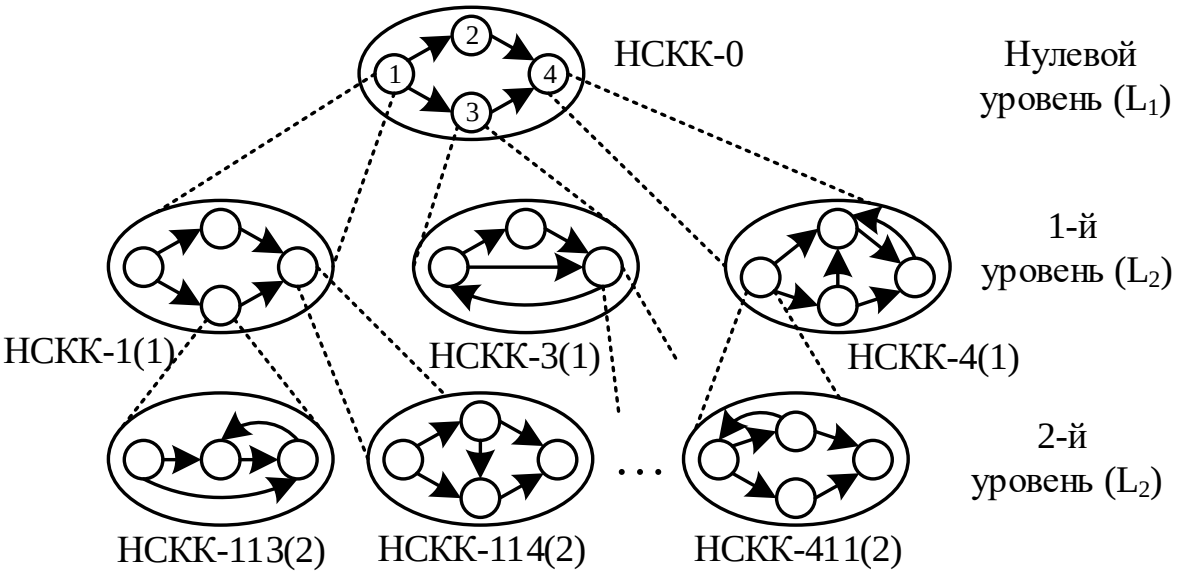


Рисунок 2.8 – Архитектура вложенной НСКК

В общем виде, вложенная НСКК представляет собой многослойный ориентированный граф G, определяемый кортежем множеств

$$G = \{V_M, E_M, V, L\}, \tag{2.10}$$

где V_M – множество вершин графа (концептов НСКК), участвующих в формировании уровней в соответствии с принятым способом декомпозиции НСКК; E_M – множество дуг, связывающих вершины графа (концепты НСКК), входящие в V_M; V – множество всех вершин (концептов НСКК); L – множество уровней НСКК.

В свою очередь, множества L, V_M, E_M определяются с помощью следующих отношений:

$$L = \{L_a\}_{a=0}^{d-1} = L_0 \times L_1 \times \ldots \times L_{d-1}; \tag{2.11}$$

$$V_M \subseteq V \times L_0 \times L_1 \times \ldots \times L_{d-1};$$

$$E_M \subseteq V_M \times V_M.$$

Общее количество концептов, входящих во вложенную НСКК, равно $D = \sum_{a=0}^{d-1} |L_a|$, где $|L_a|$ – число концептов, принадлежащих уровню L_a.

В качестве базового подхода для построения вложенных НСКК используется теория декомпозиции больших НСКК предложенная в [183]. Согласно этой теории, процедура когнитивного моделирования начинается с построения подробной (развернутой) НСКК исследуемой системы, которая принимается в качестве исходной. Затем множество концептов исходной НСКК декомпозируется на ряд отдельных блоков в соответствии с отношением эквивалентности. Рассматривая полученные блоки в качестве вершин укрупненной НСКК, получаем новое блочное представление НСКК.

На рисунке 2.9,а представлен пример сворачивания НСКК, где слева – исходная НСКК, состоящая из шести блоков (частных НСКК), связанных между собой определенным образом, а справа – укрупненная НСКК, каждая из концептов которой отражает множество концептов соответствующей частной НСКК.

На рисунке 2.9,б продемонстрирована декомпозиция вложенной НСКК на примере замещения родительского концепта C_1 частной НСКК, состоящей из пяти концептов C_1^1, C_1^2, C_1^3, C_1^4, C_1^5.

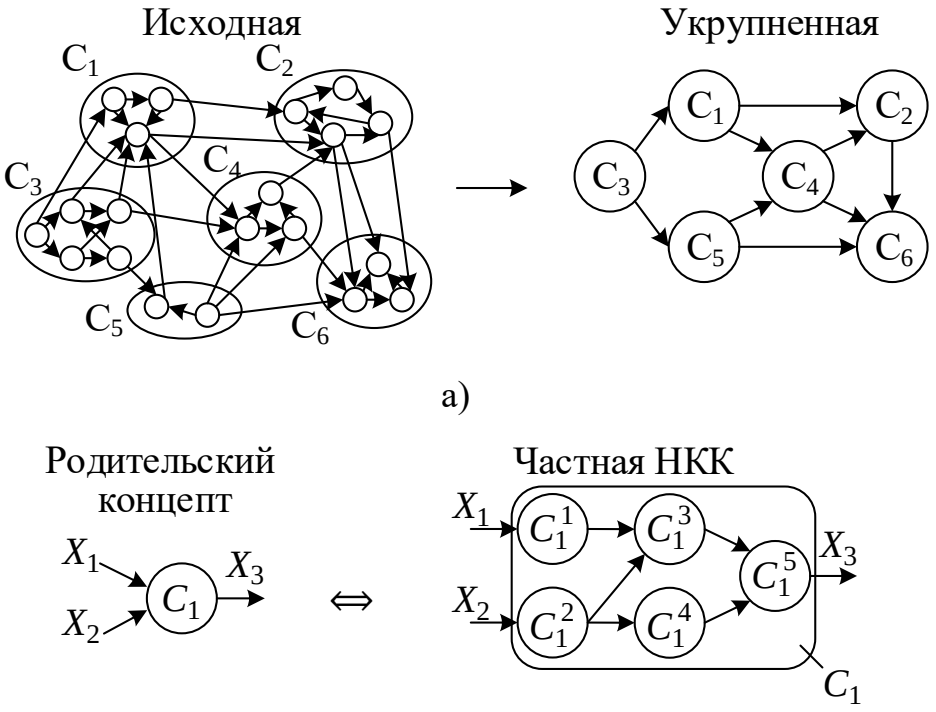


Рисунок 2.9 – Пример сворачивания (а) и декомпозиции (б) вложенной НСКК

Данные преобразования основаны на отношении эквивалентности [183], согласно которому родительский концепт и замещающая его частная НСКК считаются эквивалентными, если они имеют одинаковые входы и выходы, реализуют эквивалентные (то есть взаимно преобразуемые) схемы логического вывода и одинаково интерпретируемы (хотя и с разной глубиной понимания) в рамках общей (укрупненной) НСКК исследуемой проблемы.

Исходная (укрупненная) НСКК соответствует объекту защиты в целом и отображает общую многослойную структуру объекта защиты и его разбиение на зоны безопасности (Рисунок 2.10). НСКК первого уровня декомпозиции исходной НСКК раскрывают содержание (внутреннюю структуру) «родительских» концептов и представляют собой НСКК каждой выделенной зоны объекта защиты.

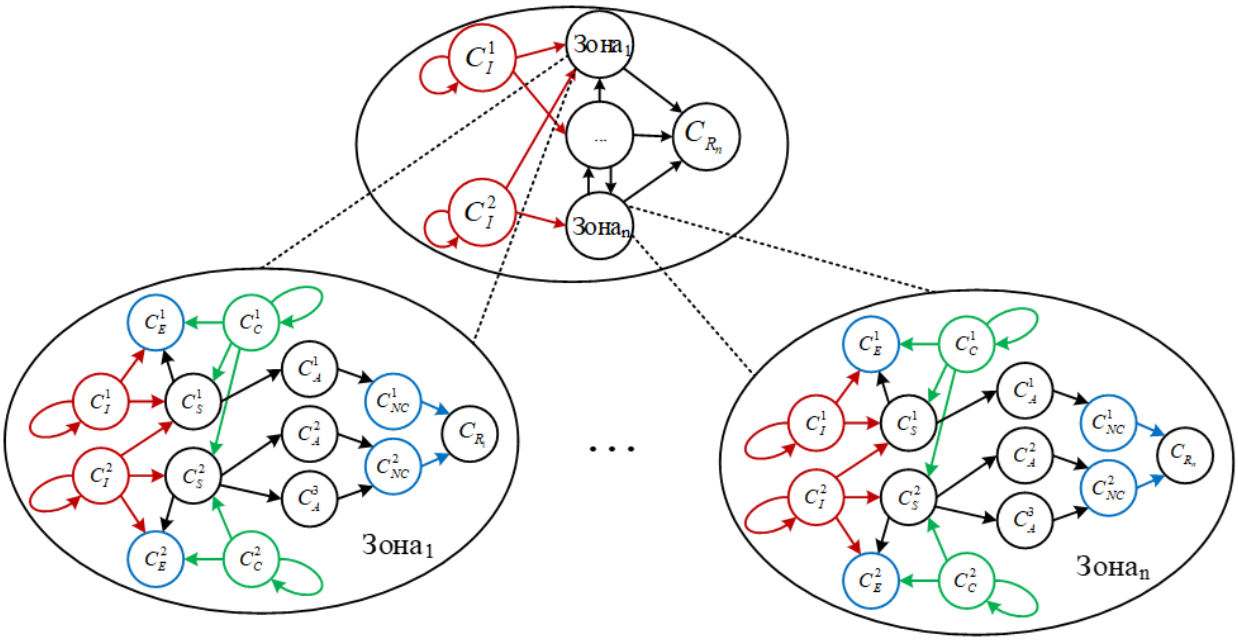


Рисунок 2.10 – Архитектура НСКК зональной модели объекта

НСКК второго уровня декомпозиции (Рисунок 2.11) детализируют сценарии реализации атаки в каждой зоне на уровне последовательности эксплуатируемых уязвимостей компонентов зональной модели.

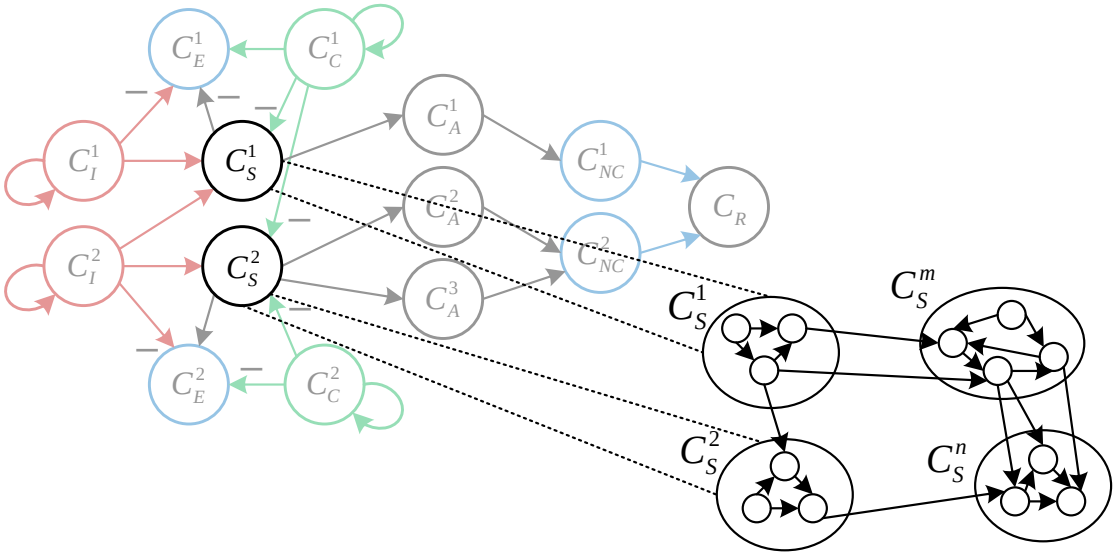


Рисунок 2.11 – Декомпозиция концептов сценариев атак

Возможна дальнейшая декомпозиция НСКК раскрывающая сценарии атак с применением открытых баз данных CAPEC, ATT&CK и БДУ ФСТЭК.

Для моделирования возможных действий нарушителя в каждой из выделенных зон АСУ ТП на различных этапах реализации атаки (наиболее

трудоемкий и сложный этап согласно Методике ФСТЭК [6]) предлагается использовать графовые модели атак, формализуемые с помощью вложенных НСКК. Предложена процедура «сворачивания» исходной детализированной НСКК, раскрывающей последовательность действий нарушителя на каждом этапе реализации атаки, до результирующей НСКК уровня представления атаки.

Алгоритм построения результирующей НСКК на основе графовых моделей проведения атаки включает в себя следующие шаги:

1) Построение НСКК детализированного уровня графовой модели на основе анализа матрицы переходов между компонентами в пределах одного узла и узлами выделенной зоны промышленного объекта (рисунок 2.12, I).

2) Построение НСКК для представления различных сценариев атаки (рисунок 2.12, II).

3) Построение НСКК для обобщенного представления варианта отдельной атаки (рисунок 2.12, III).

4) Построение результирующей НСКК (рисунок 2.13) для моделирования набора возможных сценариев атак на выделенные целевые узлы в пределах отдельных зон и всего промышленного объекта с оценкой вероятности реализации и значимости возможных последствий.

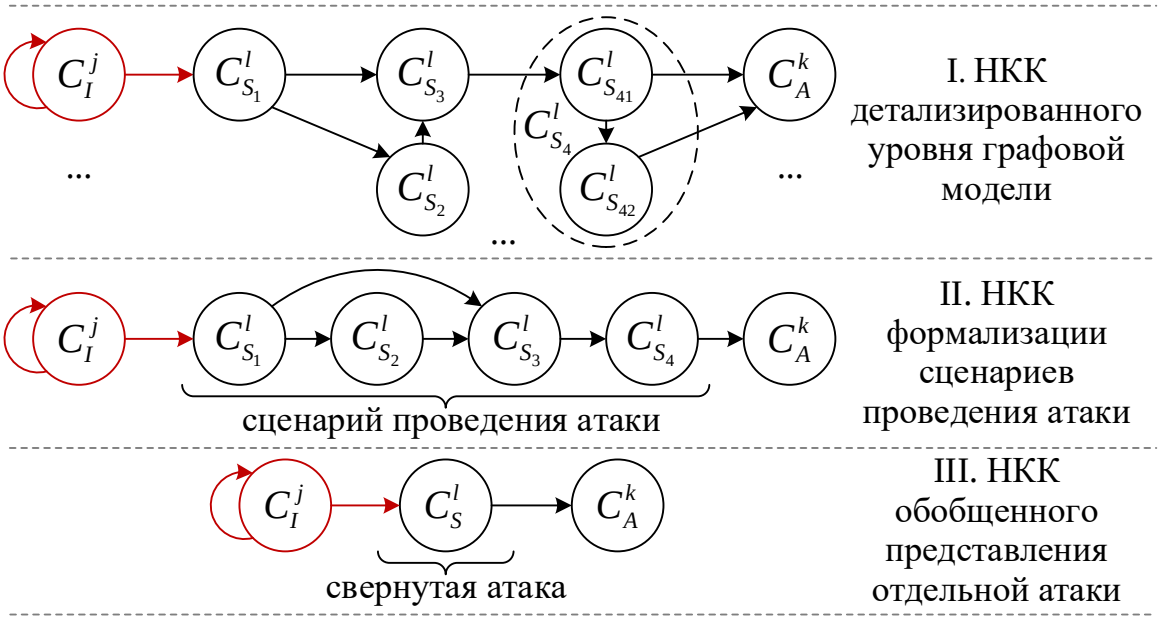


Рисунок 2.12 – Этапы построения результирующей НСКК

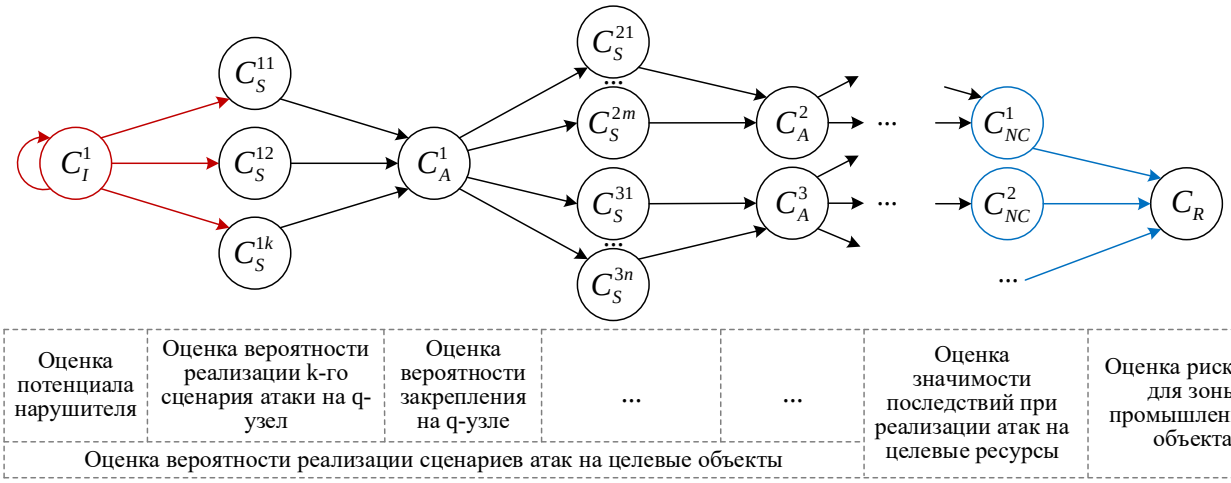


Рисунок 2.13 – НСКК для моделирования набора возможных атак на выделенные целевые концепты

Множество маршрутов из начальной вершины НСКК в конечную отражает множество сценариев атак, то есть последовательность перемещений нарушителя между компонентами АСУ ТП промышленного объекта. Поскольку сценарий атаки характеризуется наличием уязвимостей на всем пути нарушителя до цели, а также метриками CVSS этих уязвимостей, то на основании НСКК, моделирующей все возможные атаки на активы промышленной системы, формируются:

– оценка вероятности реализации атаки на внешний сервис, как первый шаг нарушителя, нацеленный на проникновении в систему предприятия;

– оценка вероятности успешного закрепления на узле;

– оценка реализации каждого этапа сценария атаки в отдельности;

– оценка реализации атаки на целевой актив, определяющая возможность реализации воздействий нарушителя на информационную инфраструктуру предприятия для достижения целевого актива;

– оценка вероятности неправомерного доступа к целевому активу, что говорит о успешности реализации конкретного сценария атаки;

– оценка вероятности реализации сложной целенаправленной атаки;

– оценка значимости последствий, на основании которых эксперт может сделать выводы о критичности последствий реализации атаки.

Детализированный уровень НСКК отражает множество действий нарушителя на каждом этапе проведения атаки, что обеспечивает получение развернутой итоговой оценки рисков ИБ для целевых активов АСУ ТП промышленного объекта. Каждая атака укрупняется до концепта НСКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность ее реализации в каждом из возможных сценариев. Результирующая НСКК позволяет получить оценку рисков ИБ АСУ ТП при реализации нарушителем совокупности атак на целевые активы как в выделенной зоне объекта защиты, так и для промышленного объекта в целом.

2.5 Пример использования модели когнитивной оценки рисков ИБ АСУ ТП ПСП

На основе полученной зональной модели (Рисунок 2.6) следующим этапом проводится идентификация и классификация активов, анализ угроз и уязвимостей, построение модели нарушителей и количественная оценка рисков ИБ [42].

Данные с датчиков СИКН, установленных на двух трубопроводах, поступают на два контроллера Emerson Floboss S600+. С двух других датчиков, установленных на третьем и четвертом трубопроводе СИКН, данные поступают на контроллер Allen Bradley 5561. Два АРМ (основной и резервный) хранят состояние и показатели всех четырех СИКН и отображают их на мнемосхеме. Дополнительно к оперативной установлен АРМ с данными по СИКН для принимающей стороны. Нарушение целостности накапливаемых данных учета принятой нефти может привести к финансовым потерям и репутационному ущербу. Проводится количественная оценка рисков ИБ АСУ ТП ПСП, связанную с нарушением целостности телеметрических данных вследствие воздействия угроз на компоненты АСУ ТП рассматриваемого объекта. Для этого строится НСКК, позволяющая оценивать риски ИБ в каждой их выделенных зон и результаты которой могут быть обобщены в виде интервальных оценок рисков ИБ.

На рисунке 2.14 изображена укрупненная НСКК для оценки рисков ИБ АСУ ТП ПСП, где в качестве факторов риска рассматриваются: C_1 – атаки на АРМ; C_2 – атаки на сетевое оборудование; С3 – атаки на ПЛК. Перечисленные факторы риска могут привести к нарушению целостности телеметрической информации: C_4 – в зоне сервера SCADA; C_5 – в зоне критических устройств управления; C_6 – в зоне управления задвижками; C_7 – в зоне управления ТП первичного пункта сбора нефти; C_8 – в зоне управления системой измерения количества нефти; C_9 – в зоне датчиков. В качестве интегрального показателя риска рассматривается: C_{10} – оценка риска нарушения целостности данных телеметрии.

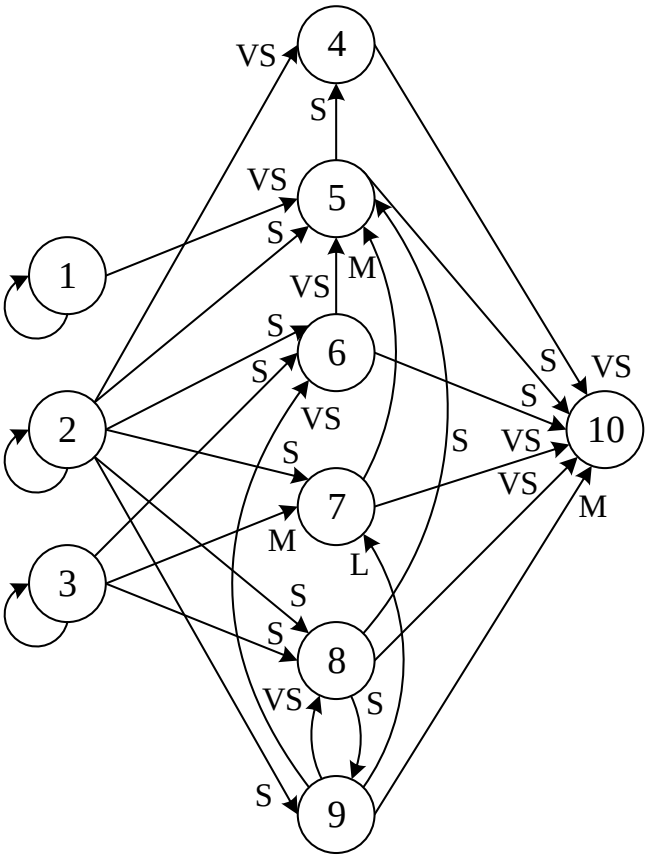


Рисунок 2.14 – Укрупненная НСКК для оценки рисков ИБ АСУ ТП ПСП

Значения весов связей между концептами НСКК представлено в таблице 2.2.

Таблица 2.2 – Веса связей укрупненной НСКК

Вес связи	Терм	Диапазон
W_{15}	VS	[0, 0,15]
W_{24}	VS	[0, 0,15]

W_{25}	S	[0,15, 0,35]
W_{26}	S	[0,15, 0,35]
W_{27}	S	[0,15, 0,35]
W_{28}	S	[0,15, 0,35]
W_{29}	S	[0,15, 0,35]
W_{36}	S	[0,15, 0,35]
W_{37}	M	[0,35, 0,6]
W_{38}	S	[0,15, 0,35]
$W_{4\,10}$	VS	[0, 0,15]
W_{54}	S	[0,15, 0,35]
$W_{5\,10}$	S	[0,15, 0,35]
W_{65}	VS	[0, 0,15]
$W_{6\,11}$	S	[0,15, 0,35]
W_{75}	M	[0,35, 0,6]
$W_{7\,10}$	VS	[0, 0,15]
W_{85}	S	[0,15, 0,35]
W_{89}	S	[0,15, 0,35]
$W_{8\,10}$	VS	[0, 0,15]
W_{96}	VS	[0, 0,15]
W_{98}	VS	[0, 0,15]
$W_{9\,10}$	M	[0,35, 0,6]

На рисунке 2.15 приведен пример декомпозиции концепта укрупненной НСКК, соответствующего нарушению целостности данных в зоне 5, характеризующей СИКН и передачу данных на предприятие (показатели температуры, массы, давления, влажности, плотности, расхода нефти).

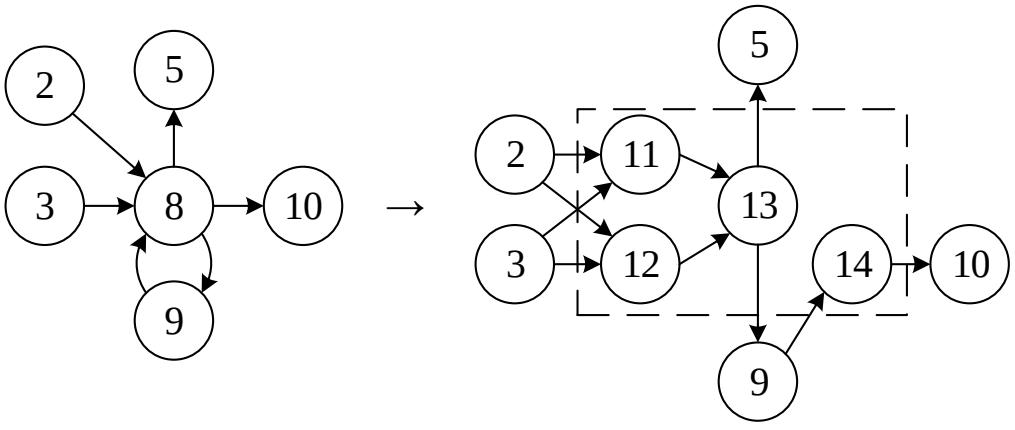


Рисунок 2.15 – Декомпозиция концепта C_8 укрупненной НСКК

На рисунке 2.15: C_{11} – подмена сервера FTP резервного копирования конфигураций ПЛК; C_{12} – перехват учетных данных привилегированного

пользователя на ПЛК; C_{13} – модификация прошивки ПЛК; C_{14} – нарушение целостности данных в зоне 5.

Все остальные концепты укрупненной НСКК возможно декомпозировать аналогичным способом.

По результатам расчетов оценки рисков ИБ АСУ ТП ПСП в таблицах 2.3 и 2.4 показаны изменения состояния концептов НСКК при активации трех концептов-драйверов C_1, C_2 и C_3, соответствующих комплексной атаке внешнего нарушителя на элементы промышленного объекта.

Таблица 2.3 – Нижняя граница оценок состояния

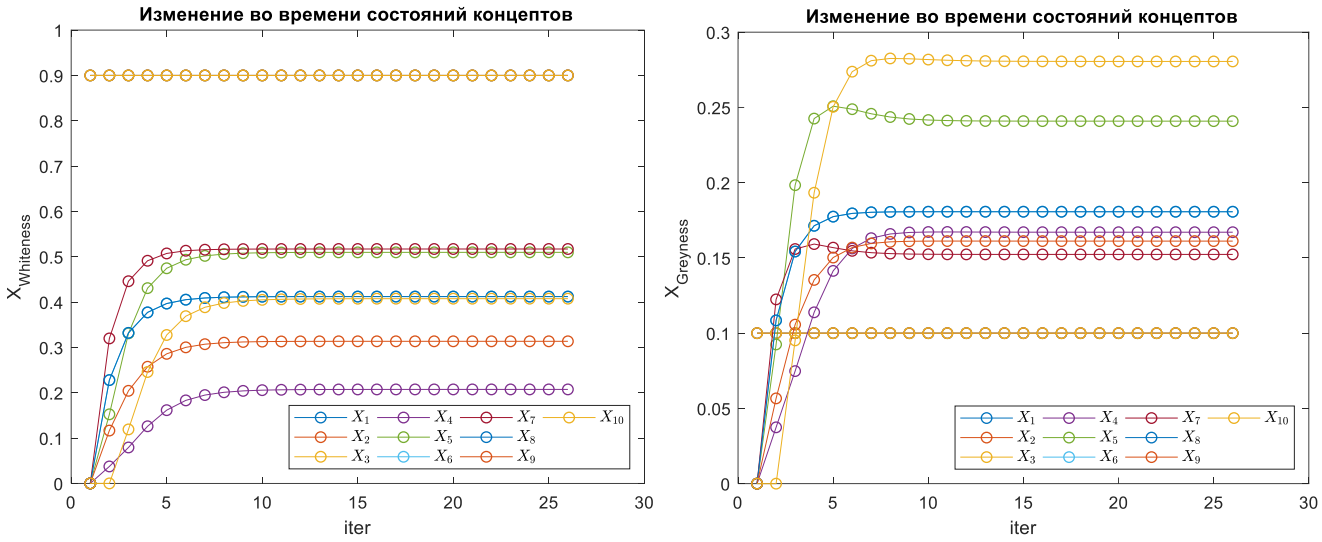
$\underline{X}_i$ \ k	1	2	3	4	5	6	7	8	9	11	12	13	14
$\underline{X}_1$	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800
$\underline{X}_2$	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800
$\underline{X}_3$	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800	0,800
$\underline{X}_4$	0,000	0,005	0,012	0,020	0,027	0,032	0,035	0,037	0,039	0,039	0,040	0,040	0,040
$\underline{X}_5$	0,060	0,133	0,188	0,224	0,245	0,256	0,262	0,266	0,267	0,268	0,268	0,269	0,269
$\underline{X}_6$	0,119	0,178	0,206	0,219	0,226	0,229	0,230	0,231	0,231	0,231	0,231	0,231	0,231
$\underline{X}_7$	0,197	0,290	0,332	0,351	0,359	0,362	0,364	0,364	0,365	0,365	0,365	0,365	0,365
$\underline{X}_8$	0,119	0,178	0,206	0,219	0,226	0,229	0,230	0,231	0,231	0,231	0,231	0,231	0,231
$\underline{X}_9$	0,060	0,099	0,122	0,136	0,143	0,148	0,150	0,151	0,152	0,152	0,152	0,152	0,152
$\underline{X}_{10}$	0,000	0,024	0,053	0,077	0,095	0,108	0,115	0,120	0,123	0,125	0,126	0,126	**0,127**

Таблица 2.4 – Верхняя граница оценок состояния

$\overline{X}_i$ \ k	1	2	3	4	5	6	7	8	9	11	12	13	14
$\overline{X}_1$	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
$\overline{X}_2$	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
$\overline{X}_3$	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
$\overline{X}_4$	0,075	0,154	0,240	0,303	0,339	0,358	0,367	0,371	0,373	0,374	0,374	0,374	0,374
$\overline{X}_5$	0,245	0,529	0,673	0,725	0,742	0,748	0,750	0,750	0,750	0,751	0,751	0,751	0,751
$\overline{X}_6$	0,336	0,486	0,549	0,574	0,585	0,589	0,591	0,592	0,593	0,593	0,593	0,593	0,593
$\overline{X}_7$	0,442	0,602	0,650	0,664	0,668	0,669	0,669	0,669	0,669	0,669	0,669	0,669	0,669
$\overline{X}_8$	0,336	0,486	0,549	0,574	0,585	0,589	0,591	0,592	0,593	0,593	0,593	0,593	0,593
$\overline{X}_9$	0,173	0,310	0,393	0,436	0,457	0,467	0,471	0,473	0,474	0,474	0,475	0,475	0,475
$\overline{X}_{10}$	0,000	0,214	0,439	0,578	0,643	0,670	0,681	0,685	0,687	0,688	0,688	0,688	0,688

Как видно из таблиц 2.3 и 2.4 значения состояния концептов НСКК $\underline{X}_i$ и $\overline{X}_i$ достигают своего установившегося значения за k = 13-14 итераций.

На рисунке 2.16 приведены изменения параметров состояний концептов НСКК (а)«серость» и б) «белизна» оценки состояния).



а) б)

Рисунок 2.16 – Изменение во времени состояний концептов НСКК (а) стабилизация «белого» значения концепта б) стабилизация «серости» концепта)

Серый вектор НСКК сходится к установившемуся значению: $X(k)$ = ([0,8; 1], [0,8;1], [0,8;1], [0,04;0,374], [0,269;0,751], [0,231;0,593], [0,365;0,669], [0,231;0,593], [0,152;0,475], [0,127;0,688]).

Искомое значение оценки риска нарушения целостности данных телеметрии вследствие комплексной атаки на АСУ ТП ПСП определяется серым числом [0,127; 0,688].

2.6 Выводы по главе

Комплекс моделей АСУ ТП как объекта защиты обеспечивает проведение количественной оценки рисков ИБ распределенных и гетерогенных промышленных систем с большим количеством узлов и уязвимостей как в отдельных выделенных зонах объекта, так и всей системы в целом, что позволяет выявить наиболее уязвимые группы активов и обосновать эффективный выбор

контрмер, обеспечив тем самым необходимый уровень защищенности АСУ ТП промышленного объекта.

Использование НСКК позволяет перейти от «точечных» оценок экспертного мнения к интервальным оценкам и к получению более достоверных интервальных оценок конечных результатов. Интервальные оценки весов НСКК могут отражать разброс мнений экспертной группы, что позволяет более полно учесть доступные для анализа рисков ИБ данные. Когнитивное моделирование оценки рисков ИБ с использованием НСКК позволяет учитывать фактор неопределенности, возникающий в процессе оценки вероятности эксплуатации уязвимости каждого из узлов объекта защиты.

Специфика АСУ ТП создает дополнительные сложности при анализе и управлении рисками ИБ, что обуславливает необходимость использования методов, которые будут эффективны, несмотря на невысокую формализованность объекта исследования с точки зрения моделирования сценариев атак. Особую роль при этом играет применение НСКК, которые обеспечивают наглядность, интерпретируемость и способность к обучению на реальных данных, а результаты в виде интервальных оценок более достоверны и дают экспертам больше материала для принятия решения.

Декомпозиция укрупненных НСКК позволяет экспертам раскрыть неопределенности на более развернутых уровнях НСКК с детализацией последствий от рассматриваемых факторов рисков ИБ. Это дает более точный результат количественной оценки рисков ИБ АСУ ТП за счет того, что есть возможность рассмотреть процесс реализации атак внутри каждой выделенной зоны промышленного объекта защиты. Это впоследствии поможет экспертам при подборе контрмер для каждой выделенной зоны безопасности и для объекта в целом.

Глава 3. Разработка метода сценарного моделирования атак на АСУ ТП промышленного объекта в нечетком когнитивном базисе

Предлагается метод сценарного моделирования атак, выполняющий заключительные этапы Методики ФСТЭК и основанный на построении и анализе комплекса моделей объекта и действий нарушителя, что позволит декомпозировать и формализовать возможные сценарии атак на целевые активы в выделенной зоне АСУ ТП с количественной оценкой рисков ИБ.

3.1 Разработка метода сценарного моделирования атак

По результатам анализа исследований в области моделирования сценариев атак (Приложение Г, Таблица Г.3) предложен метод сценарного моделирования многошаговых целенаправленных атак на основе Методики ФСТЭК и открытых баз данных угроз, уязвимостей и компьютерных атак.

Иерархия разработанного комплекса моделей [32, 38, 40, 43, 50, 176], являющихся основой для моделирования сценариев атак, представлена на рисунке 3.1.

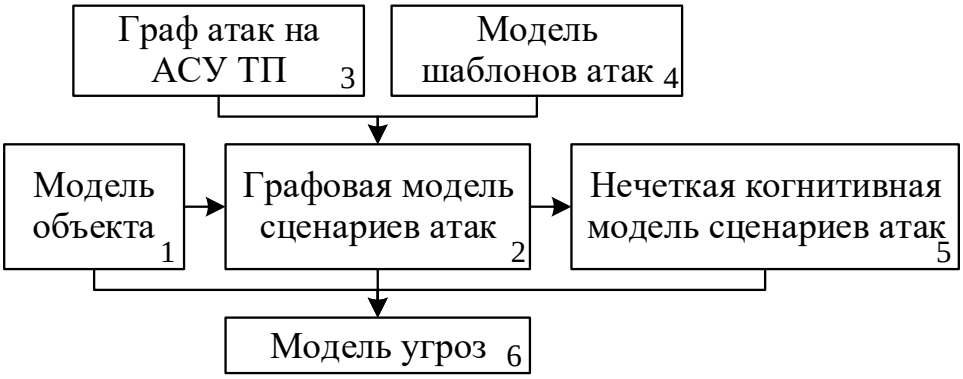


Рисунок 3.1 – Иерархия моделей построения сценариев атак

На основе зональной модели базовой архитектуры АСУ ТП промышленного объекта (1) строится ряд графовых моделей, раскрывающих детали реализации атаки. Графовые модели сценариев атак (2) формируются на основе графа атак на

промышленную сеть (3) (рисунок 3.3), перекрестных ссылок и матрицы переходов между выделенными идентификаторами баз данных.

На рисунке 3.2 представлена функциональная модель в нотации IDEF0, отображающая основные этапы процесса построения сценариев атак.

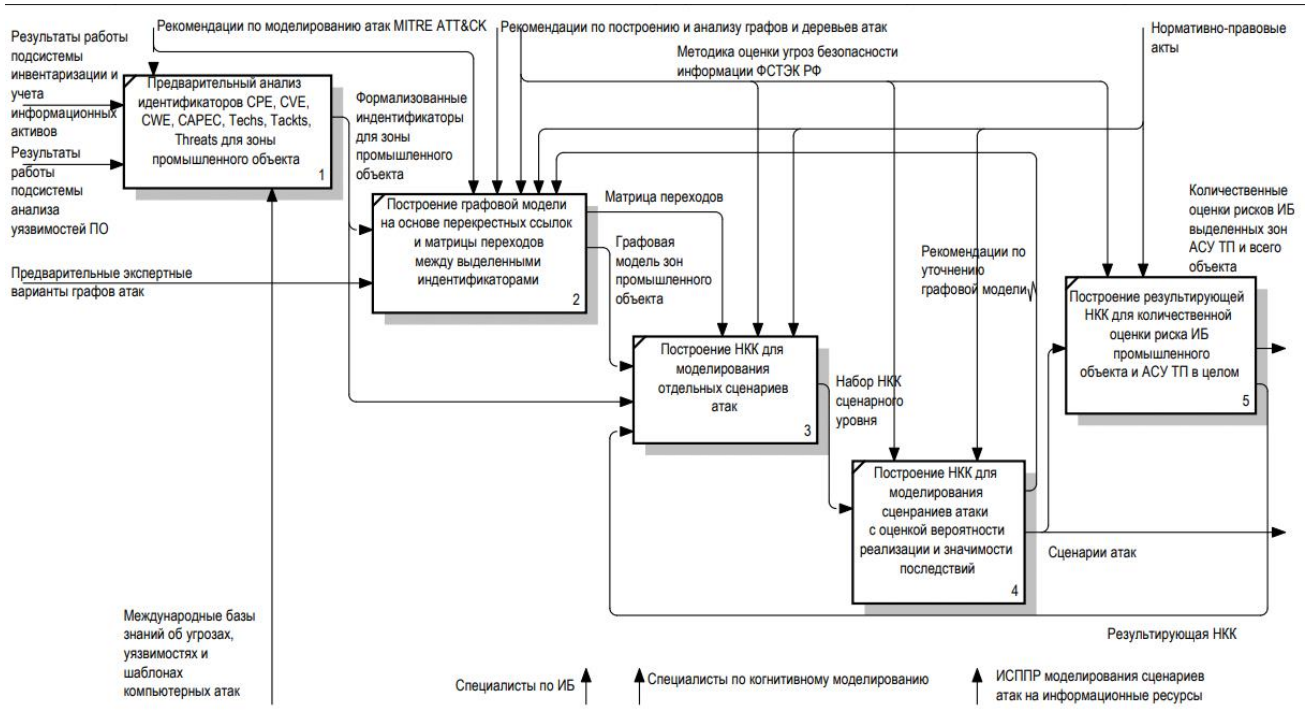


Рисунок 3.2 – Функциональная модель метода сценарного моделирования атак

По результатам работы подсистем инвентаризации и управления уязвимостями, а также на основе идентификаторов CPE, сведений из БДУ ФСТЭК (Threats) и баз данных шаблонов компьютерных атак (CPE, CVE, CWE, CAPEC), руководствуясь рекомендациями, приведенными в Методике ФСТЭК, и тактиками, техниками в матрице MITRE ATT&CK (Tackts, Techs), специалисты по ИБ выполняют формализацию множества выделенных идентификаторов для каждой из зон АСУ ТП промышленного объекта. Далее, на основе перекрестных ссылок и матрицы переходов между выделенными идентификаторами (CPE, CVE, CWE, CAPEC, ATT&CK, BDU) строится графовая модель выделенной зоны промышленного объекта с помощью специализированного ПО для управления графовыми БД – neo4j. Результирующая графовая модель с помощью алгоритма построения НКК представляется в виде укрупненного концепта и используется

далее для построения НКК, раскрывающей различные сценарии атак и итоговые количественные оценки риска ИБ.

Рисунок 3.3 иллюстрирует пример графа атак внешнего нарушителя ($ВЗ_1$) на АСУ ТП промышленного объекта. Перед построением графа атак анализируется модели нарушителя, наиболее вероятные атаки и наиболее уязвимые активы предприятия, после чего, исходя из экспертного анализа базовой архитектуры объекта защиты и возможных последствий от реализации атак ($П_1$, $П_2$), моделируется ряд возможных сценариев атак.

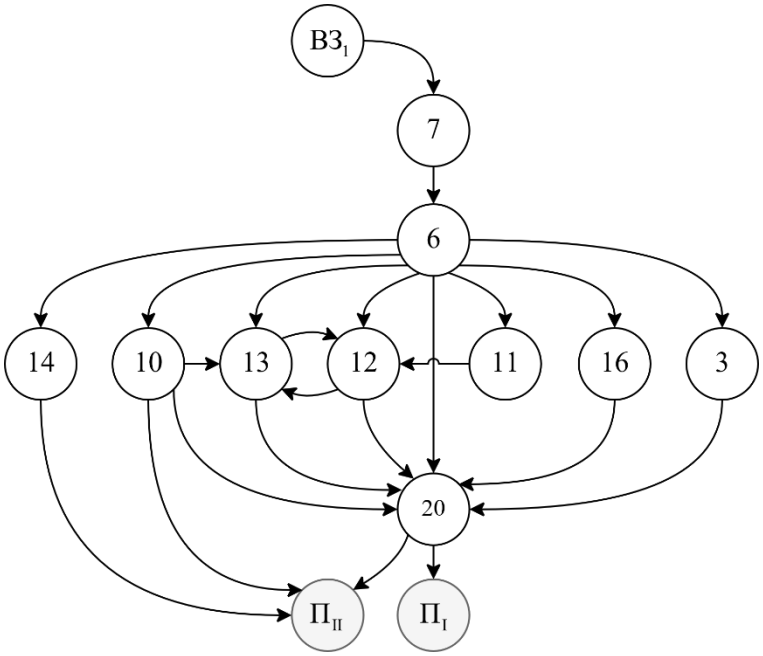


Рисунок 3.3 – Граф атак на АСУ ТП промышленного объекта

Возможные последовательности действий нарушителя (цепочки – эксплуатация последовательности уязвимостей компонентов АСУ ТП промышленного объекта) для реализации атаки (таблицы 3.1, 3.2) построены на основе экспертного анализа БДУ ФСТЭК и баз CAPEC, CVE, CWE, ATT&CK.

Таблица 3.1 – Эксплуатируемые уязвимости компонент АСУ ТП промышленного объекта

Компонент	Уязвимость
3	Уязвимость прикладного ПО управления версиями прошивок
6	Уязвимость ПО организации удаленного доступа в ЛВС
7	Уязвимость VPN-сервера

Компонент	Уязвимость
10	Уязвимость прикладного ПО сервера NTP
11	Уязвимость прикладного ПО SCADA клиента
12	Уязвимость прикладного ПО SCADA сервера
13	Уязвимость OPC-сервера
14	Уязвимость системного ПО сервера хранения исторических данных
16	Уязвимость коммутационного оборудования сети
20	Уязвимость механизмов авторизации ПЛК

Таблица 3.2 – Последовательность действий нарушителя для реализации атаки

Цепочка перемещений по уязвимым компонентам АСУ ТП	Результат реализации
7 → 6 → 13 → 20	Передача команды на ПЛК для отключения насоса через OPC-сервер
7 → 6 → 12 → 20	Передача команды на ПЛК для отключения насоса через SCADA сервер
7 → 6 → 16 → 20	Подмена сетевого трафика между 11 и 12, 12 и 13, 13 и 20
7 → 6 → 14	Нарушение целостности накопленных исторических данных на сервере 14 и искажение ТП
7 → 6 → 11 → 12 → 13	Нарушение корректной визуализации данных о ходе ТП на 11 и срабатывание защитного контура / команда оператора
7 → 6 → 10	Нарушение работы сервера NTP и нарушение целостности данных в 14
7 → 6 → 10 → 13 → 12	Задержка команд и сигналов из-за нарушения работы 10
7 → 6 → 3 → 20	Изменение работы сервера обновления прошивок ПЛК и технологического оборудования
7 → 6 → 20	Использование недостатков механизмов аутентификации и авторизации ПЛК (пароль и логин по умолчанию) для изменения режима работы ПЛК и искажения передаваемых данных

Графовые модели сценариев атак различной степени детализации строятся исходя из анализа модели объекта, модели нарушителя, наиболее вероятных атак и наиболее уязвимых ресурсов системы (рисунок 3.4):

– 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 промышленной системы;

– V_{CWE} – множество вершин, соответствующих идентификаторам CWE, представляющих недостатки программного и аппаратного обеспечения системы;

– V_{CAPEC} – множество вершин, соответствующих шаблонам атак CAPEC, описывающих известные типовые атаки;

– V_{Techs} – множество вершин, соответствующих техникам реализации атаки (из матрицы ATT&CK и Методики ФСТЭК), которые описывают инструменты и технологии, используемые нарушителем в процессе реализации атаки;

– V_{Tackts} – множество вершин, соответствующих тактикам (из матрицы ATT&CK и Методики ФСТЭК), т.е. действиям на различных этапах реализации атаки;

– $V_{Threats}$ – множество вершин, соответствующих УБИ из БДУ ФСТЭК.

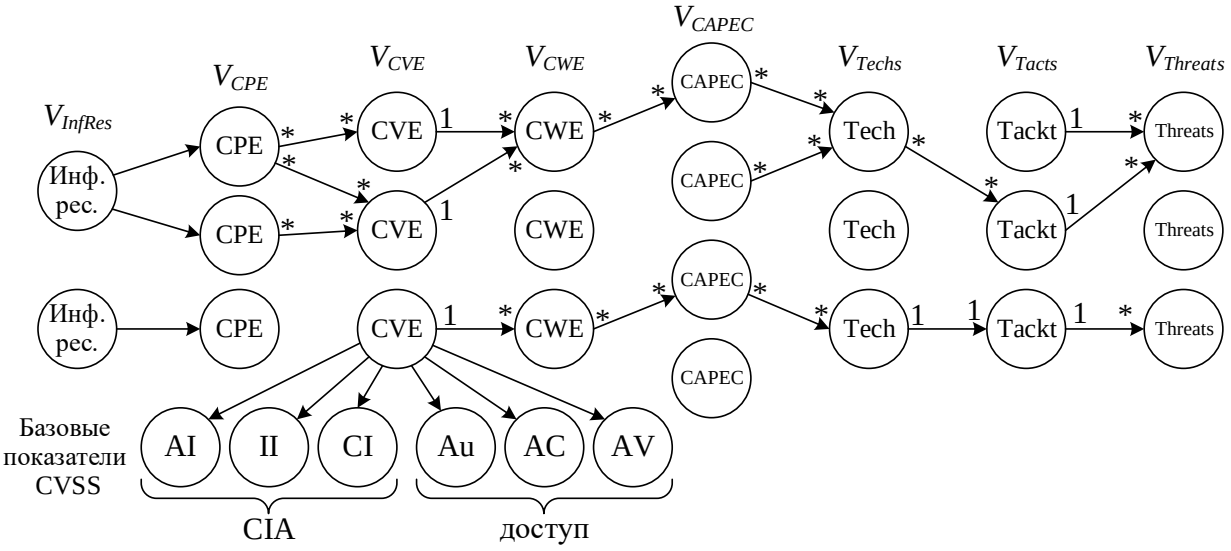


Рисунок 3.4 – Графовая модель сценариев атак, описывающая взаимосвязь CPE-CVE-CWE-CAPEC-ATT&CK

Модели шаблонов атак (4) (рисунки 3.5-3.8), построенные на основе открытой базы шаблонов атак CAPEC, используются для детализации графовой модели и анализа возможностей нарушителя, так как графовая модель проведения

атаки конструируется в виде цепочки вероятностных переходов между узлами CAPEC (рисунок 3.9) и представляет собой последовательности действий, совокупность методов и средств, при помощи которых нарушитель достигает поставленной цели воздействия на каждом этапе проведения атаки.

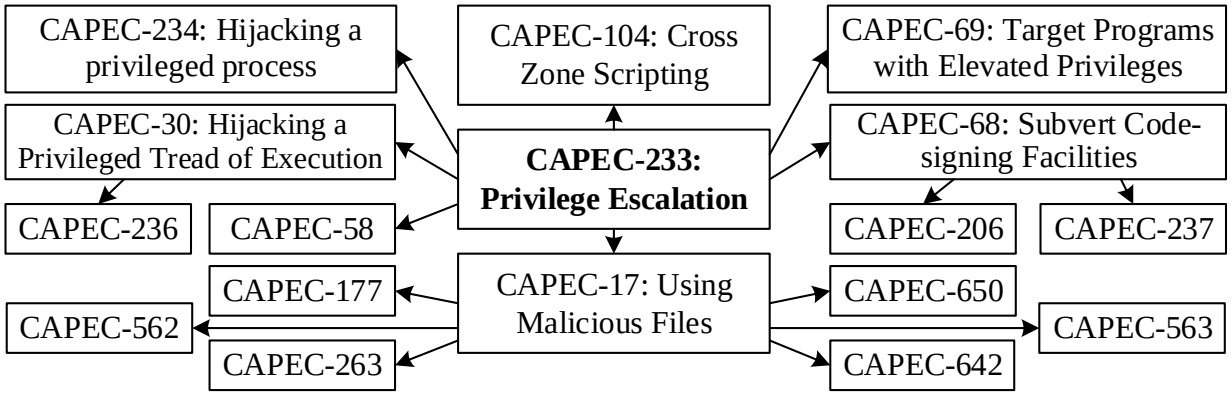


Рисунок 3.5 – Модель шаблонов атак для CAPEC-233

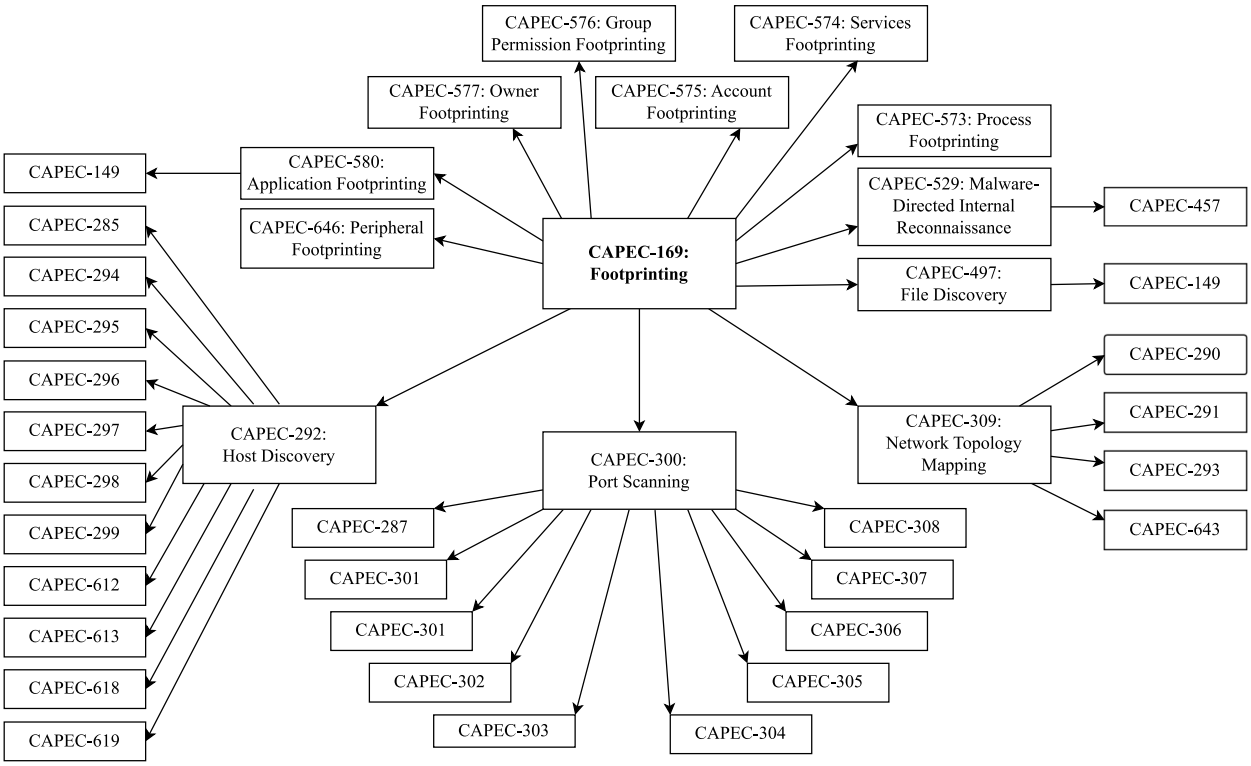


Рисунок 3.6 – Модель шаблонов атак для CAPEC-169

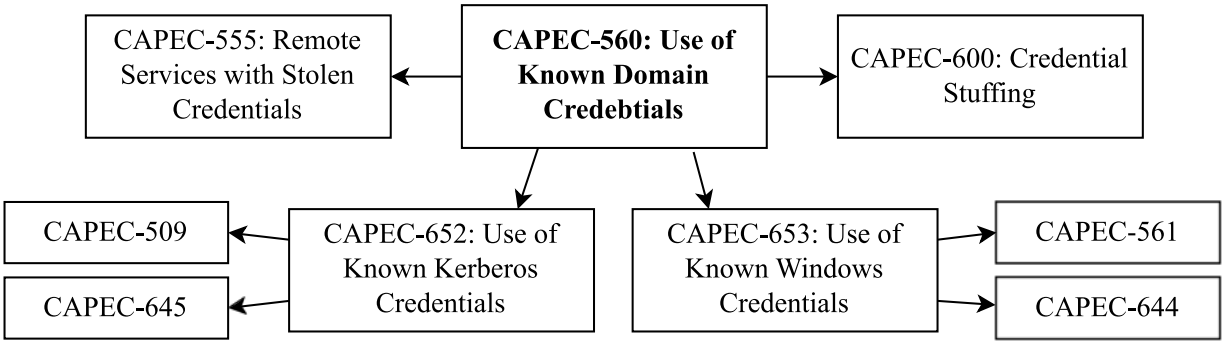


Рисунок 3.7 – Модель шаблонов атак для CAPEC-560

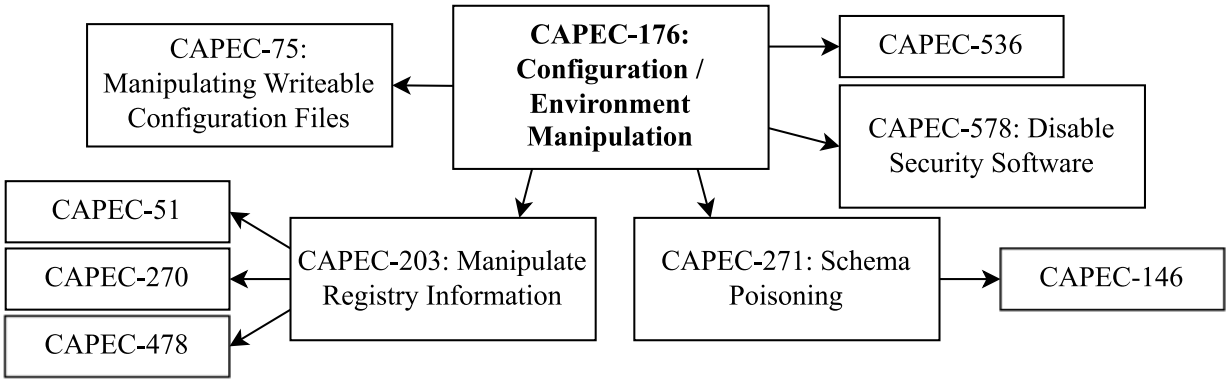


Рисунок 3.8 – Модель шаблонов атак для CAPEC-176

Для выстраивания правильной последовательности моделей шаблонов атак CAPEC и, соответственно, действий нарушителя, меташаблоны атак базы CAPEC сопоставлены с тактиками из Методики ФСТЭК, описывающими каждый шаг реализации атаки (Таблица 3.3).

Таблица 3.3 – Фрагмент сопоставления тактик Методики ФСТЭК и меташаблонов атак базы CAPEC

Тактики / Методика	Меташаблоны атак / CAPEC
1) сбор информации о системах и сетях	1) CAPEC-169: Footprinting. Включает в себя различные методы сбора информации для подготовки к атаке. Позволяет узнать о составе, конфигурации, механизмах безопасности системы и сети (рис. 3).
2) получение первоначального доступа к компонентам систем и сетей	2) CAPEC-560: Use of Known Domain Credentials. Злоумышленник угадывает или получает законные учетные данные для аутентификации и выполнения санкционированных действий под

Тактики / Методика	Металшаблоны атак / CAPEC
3) закрепление в системах и сетях	видом аутентифицированного пользователя (рис. 4).
4) повышение привилегий по доступу к компонентам систем и сетей	3) CAPEC233: Privilege Escalation. Злоумышленник использует уязвимость, позволяющую ему повысить свои привилегии и выполнить действия, которые ему не разрешено выполнять (рис. 5).
5) неправомерный доступ и воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям	4) CAPEC-176: Configuration / Environment Manipulation. Злоумышленник манипулирует файлами и настройками, которые влияют на поведение приложения (рис. 6).

Исходными данными для построения графовой модели проведения атак на основе моделей шаблонов атак являются результаты работы сканеров уязвимостей и базы данных БДУ ФСТЭК, CWE и CVE. Набор показателей системы оценки уязвимостей CVSS и базы CVE и CWE позволяют формализовать описание уязвимости и сценария ее эксплуатации, а также автоматизировать процесс построения цепочки возможных переходов внутри металшаблона атак.

В базах данных уязвимостей для каждой уязвимости определено значение уровня ее опасности на основе базовых метрик CVSS [125]. Однако для промышленных систем автоматизации базовые оценки могут не соответствовать реальной степени опасности последствий эксплуатации уязвимости. Для АСУ ТП целесообразнее использовать контекстные метрики CVSS [69, 175], то есть учитывать влияние уязвимости в среде функционирования ПО объекта защиты. С помощью контекстных метрик результирующая оценка CVSS дает более четкое представление о риске, который влечет за собой эксплуатация уязвимостей для конкретного предприятия.

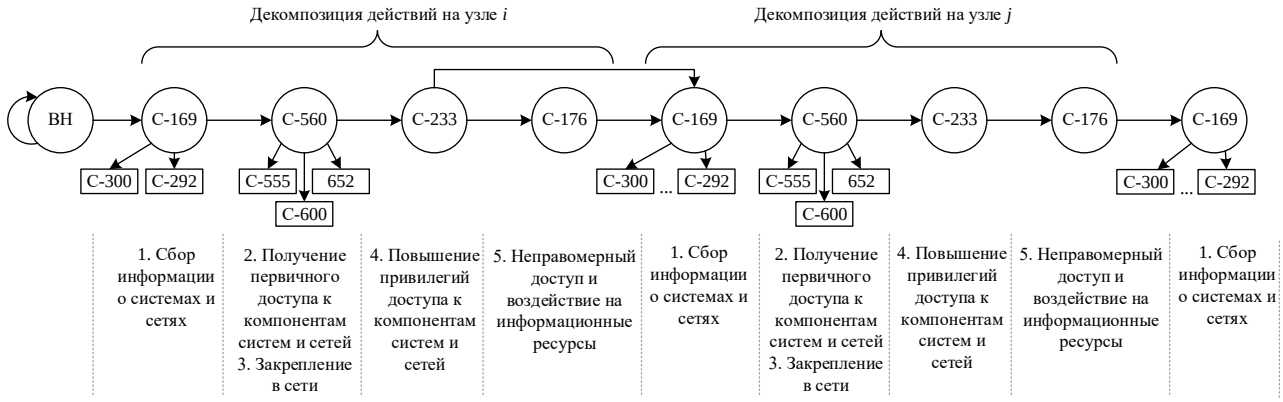


Рисунок 3.9 – Графовая модель проведения атаки на основе шаблонов атак CAPEC

Нечеткая когнитивная модель сценариев атаки (5) позволяет анализировать сценарии атак с требуемым уровнем детализации за счет механизмов декомпозиции и композиции действий нарушителя и формировать количественную 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 модели нарушителя, а также результаты применения предлагаемого метода сценарного моделирования (перечень актуальных угроз и сценарии их реализации, а также количественную оценку рисков ИБ АСУ ТП).

3.2 Разработка алгоритма построения сценариев атак в нечетком когнитивном базисе

Структура подсистемы анализа графовых моделей (рисунок 3.10) определяет организацию модулей и инструментов сбора данных, подготовки и построения моделей. Ключевыми являются модули импорта данных из внешних баз, поэтапного преобразования и формализации во внутреннюю графовую базу neo4j.

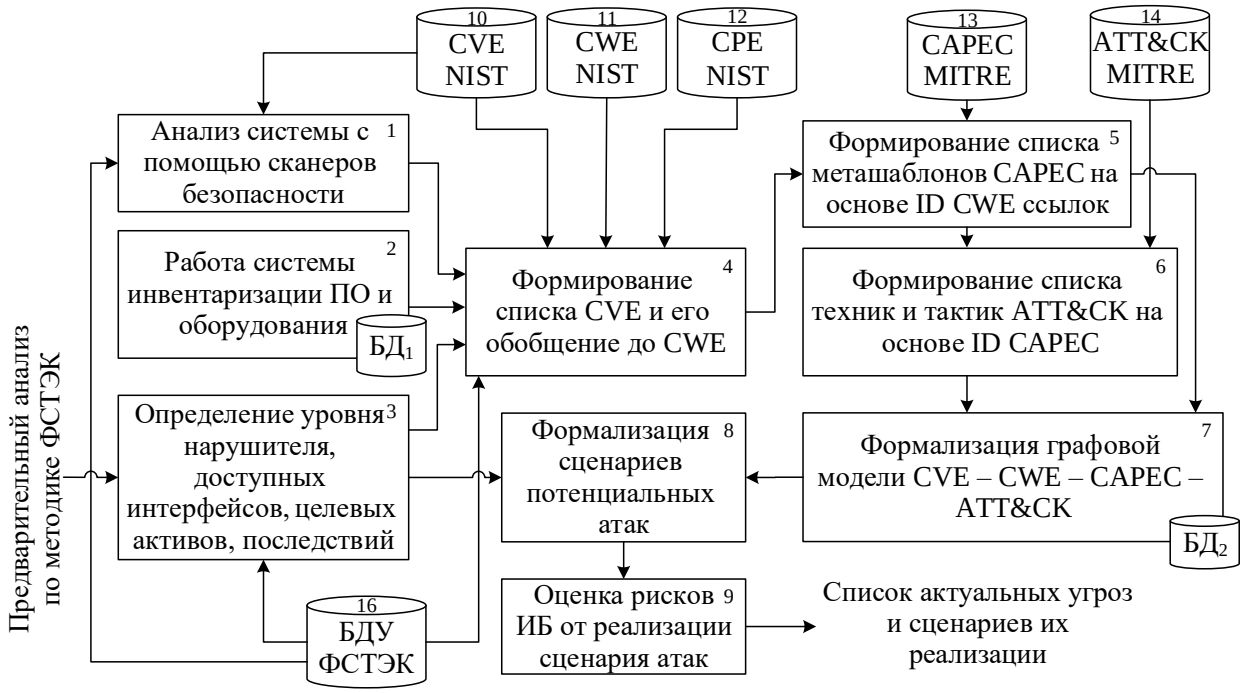


Рисунок 3.10 – Структура подсистемы построения и анализа графовых моделей

Алгоритм построения графовых моделей (рисунок 3.11) включает следующие основные шаги:

1) построение графа атак G_1 на основе модели объекта, нарушителя и последствий от реализации атаки;

2) построение графовой модели G_2 сценариев проведения атаки на основе графа атак $G1$ и множества вершин, сформированных на основе баз данных MITRE и банка данных угроз и уязвимостей ФСТЭК;

3) исключение недостижимых вершин графовой модели $G2$ на основе анализа перекрестных ссылок и детализация взаимосвязей компонентов баз данных CVE-CWE-CAPEC-ATT&CK;

4) строится фрагмент модели шаблонов атак на основе той графовой модели, которая получилась после исключения недостижимых вершин для каждого узла графа атак G_1.

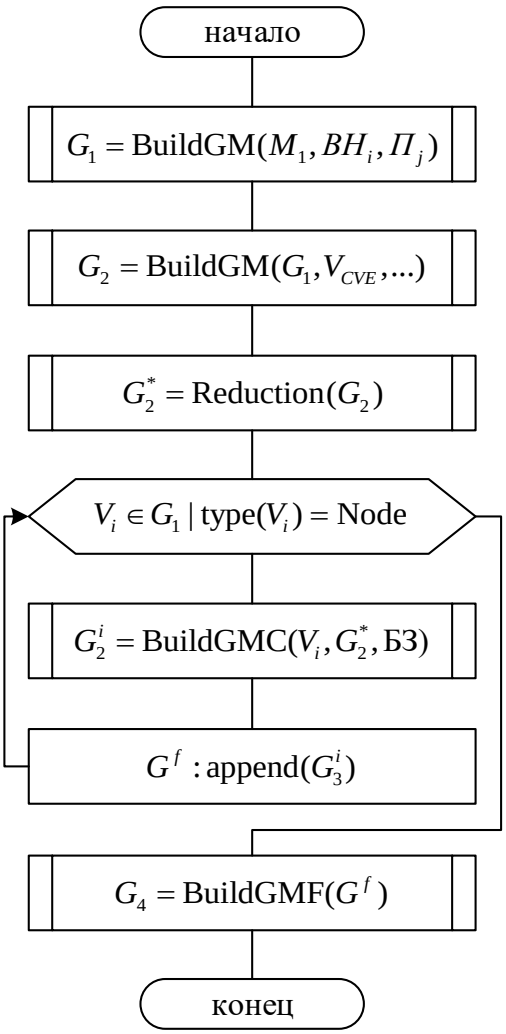


Рисунок 3.11 – Алгоритм построения графовой модели проведения атаки

Представленный алгоритм позволяет перейти к прореженной графовой модели и применению аппарата НКК к «сворачиванию» сценариев атак.

3.3 Разработка методики количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе метода сценарного моделирования

Разработана 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 (Приложение Е).

При анализе рисков ИБ АСУ ТП решается задача оптимизации параметров когнитивных моделей, отражающих оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений [32, 48, 70, 136, 177]. Возможна следующая формальная постановка задачи оптимизации:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = X_R \to min, \tag{2.6}$$

где $\Phi(\cdot)$ – целевая функция, X_R – установившееся значение переменной состояния концепта C_R, $W_{C_C^i,C_S^j}$ – настраиваемые параметры (веса), характеризующие распределение выделенных ресурсов контрмеры C_C^i для снижения вероятности реализации сценариев атак C_S^j.

На параметры $W_{C_C^i,C_S^j}$ накладывается ряд условий (2.7), связанных со спецификой определения весов в базисе «серых» чисел:

$$\forall W_{C_C^i,C_S^j}: \begin{cases} \overline{W}_{C_C^i,C_S^j}, \underline{W}_{C_C^i,C_S^j} \in [0,1]; \\ \overline{W}_{C_C^i,C_S^j} > \underline{W}_{C_C^i,C_S^j}; \\ \sum_i \left[\overline{W}_{C_C^i,C_S^j} + \underline{W}_{C_C^i,C_S^j}\right] < \theta. \end{cases} \tag{2.7}$$

Для применения классических реализаций алгоритмов оптимизации с ограничениями целевая функция представляется как норма вектора компонент серого числа X_R с дополнительным заданием штрафной компоненты (2.8), обеспечивающей корректное определение области значений $\overline{X}_R, \underline{X}_R \in [0,1]$:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = \left\|\overline{X}_R, \underline{X}_R\right\| + \alpha f\left(\overline{X}_R, \underline{X}_R\right), \quad f\left(\overline{X}_R, \underline{X}_R\right) = \begin{cases} 1, \overline{X}_R < 0, \underline{X}_R < 0; \\ 0, \text{otherwise.} \end{cases} \tag{2.8}$$

Для оптимизации весовых коэффициентов НСКК использован генетический алгоритм (ГА) [137, 143, 165] для поиска субоптимального решения с нелинейными ограничениями области задания и области значений целевой функции [158, 166].

Анализ соотношения полученных количественных оценок рисков ИБ выделенных зон АС ТП промышленного объекта и затрат на мероприятия по их снижению позволяет определить механизмы управления защищенностью целевых

активов системы и поддерживать ее необходимый уровень защищенности, а также оценивать требуемые при этом затраты на интеграцию и сопровождение контрмер.

Применение ГА позволяет формулировать задачу многокритериальной оптимизации в следующей постановке (2.9):

$$\Phi\left(W_{C_C^i, C_S^j}\right) = X_R \to min, \quad \sum X_R \to min,$$

$$\Phi\left(W_{C_C^i, C_S^j}\right) = \left\|\overline{X_R}, \underline{X_R}\right\| + \sum_i \left\|\overline{X_C^i}, \underline{X_C^i}\right\| + \alpha f\left(\overline{X_R}, \underline{X_R}\right) + \beta f\left(\overline{X_C^i}, \underline{X_C^i}\right), \qquad (2.9)$$

учитывающей одновременную минимизацию и оценки рисков, и суммарной оценки эффективности использования контрмер в различных сценариях моделирования.

Применение ГА оптимизации весовых коэффициентов НСКК позволяет определить оптимальные конфигурации контрмер в процессе оценки рисков ИБ АСУ ТП промышленного объекта в условиях реализации сложных многошаговых атак.

Принятие решения о выборе необходимых контрмер должно производиться при этом по критерию «эффективность – стоимость». Возможны следующие постановки задачи выбора управляющих факторов для снижения информационных рисков:

1) $S_\Sigma \to min$ при $R \le R_{\text{доп}}$ – минимизация затрат на мероприятия по защите информации при обеспечении допустимого уровня риска ИБ;

2) $R \to min$ при $S_\Sigma \le S_{\text{доп}}$ – минимизация риска ИБ при выделенных (допустимых) затратах на реализацию контрмер.

Здесь R и S_Σ – соответственно общий риск ИБ и суммарные затраты на мероприятия (контрмеры) по защите информации; $R_{\text{доп}}$ и $S_{\text{доп}}$ – допустимые значения риска ИБ и суммарных затрат.

3.4 Пример использования методики количественной оценки рисков ИБ АСУ ТП пункта приема-сдачи подготовленной нефти

Для детального моделирования сценариев атак и дальнейшей оценки рисков ИБ АСУ ТП ПСП (рисунок 2.6) воспользуемся предложенной методикой количественной оценки рисков.

Список уязвимостей, наиболее подходящих под модель рассматриваемого объекта, приведен в Таблице 3.4.

Таблица 3.4 – Список уязвимостей на основе анализа объекта защиты

Уязвимость	Описание
CVE-2019-6859	В контроллерах Modicon существует уязвимость CWE-798: использование жестко закодированных учетных данных, что может привести к раскрытию жестко закодированных учетных данных FTP при использовании веб-сервера контроллера в незащищенной сети.
CVE-2019-6812	Уязвимость CWE-798, связанная с использованием жестко закодированных учетных данных, существует в BMX-NOR-0200H с версиями прошивки до V1.7 IR 19, что может вызвать проблемы с конфиденциальностью при использовании протокола FTP.
CVE-2020-7507	В Easergy T300 (версия микропрограммы 1.5.2 и старше) существует уязвимость CWE-400: неконтролируемое потребление ресурсов, которая может позволить злоумышленнику войти в систему несколько раз, что приведет к отказу в обслуживании.
BDU:2020-01893	Уязвимость микропрограммного обеспечения оборудования Modicon Controllers, связана с наличием жестко закодированных учетных данных, используемых для передачи конфигурационных файлов оборудованию Modicon Controllers. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольную команду в отношении оборудования Modicon Controllers
BDU:2020-04014	Уязвимость микропрограммного обеспечения логического контроллера Modicon M218 Logic Controller связана с записью за границы буфера памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании
BDU:2019-03754	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Allen Bradley компании Rockwell Automation связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю,

Уязвимость	Описание
	действующему удалённо, выполнить произвольный код в результате использования модифицированного встроенного программного обеспечения
CVE-2018-19616	Проблема была обнаружена в Rockwell Automation Allen-Bradley PowerMonitor 1000. Неаутентифицированный пользователь может добавлять / редактировать / удалять администраторов, поскольку контроль доступа реализован на стороне клиента через атрибут disabled для элемента BUTTON.

Для списка уязвимостей выполняется подбор шаблонов атак, которые могут быть реализованы через выявленные уязвимости АСУ ТП ПСП.

На рисунке 3.12 приведен фрагмент графовой модели, отображающей взаимосвязь уязвимостей, недостатков ПО, совокупности методов и средств, позволяющих нарушителю реализовать атаку на АСУ ТП ПСП.

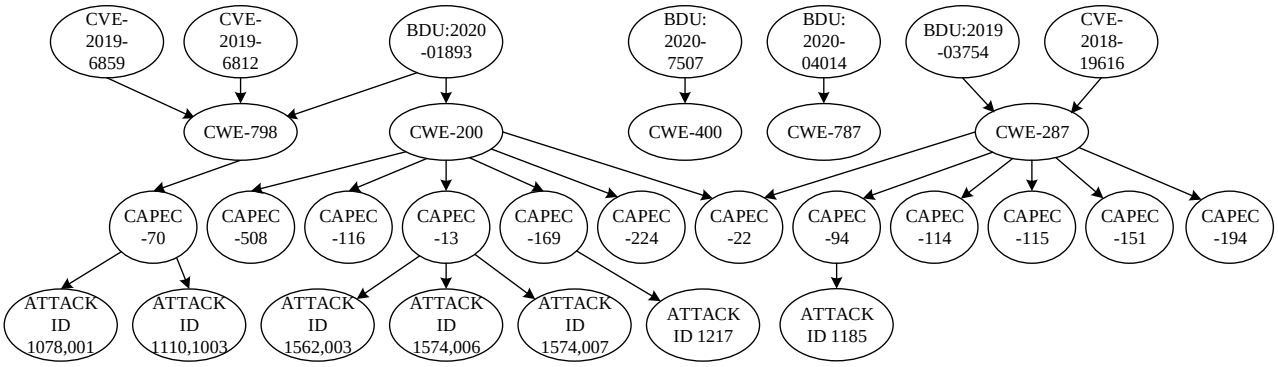


Рисунок 3.12 – Фрагмент графовой модели сценариев атак, описывающая взаимосвязь CPE-CVE-CWE-CAPEC-ATT&CK для АСУ ТП ПСП

С учетом построенной графовой модели реализации сценариев атак и модели угроз объекта, строятся актуальные способы эксплуатации уязвимостей и реализации угроз для зоны 5 АСУ ТП ПСП в виде НСКК. Итоговая цепочка действий нарушителя в виде укрупненной $НСКК_1$ представлена на Рисунке 3.13. Концепты для моделирования $НСКК_1$ приведены в Таблице 3.5.

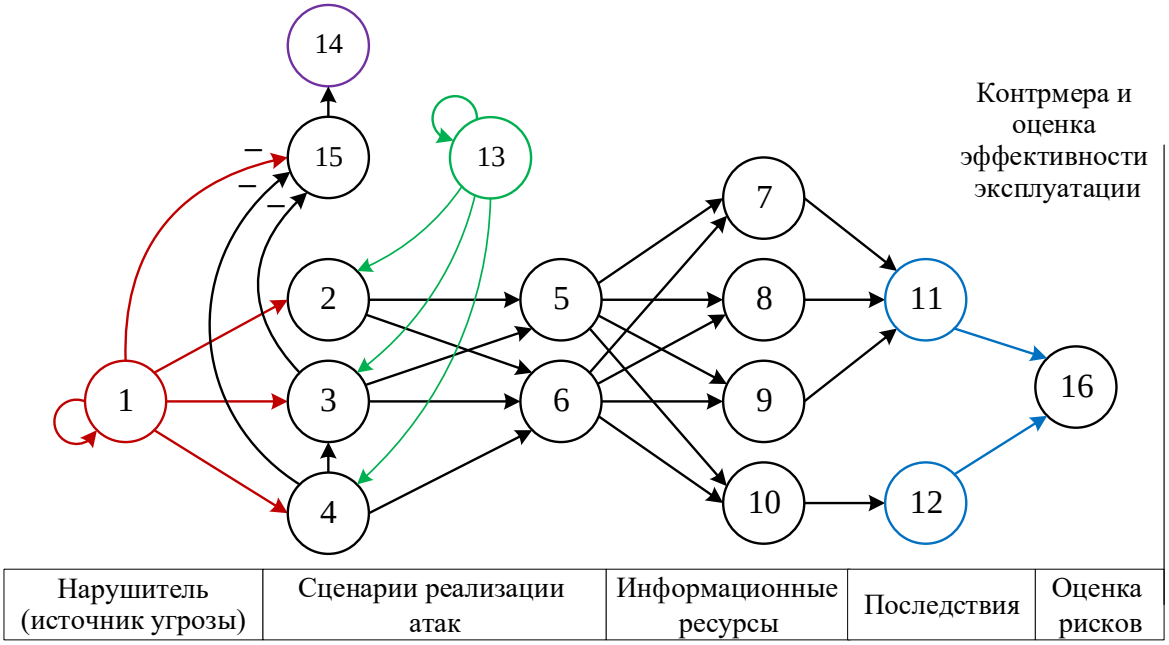


Рисунок 3.13 – Визуализация НСКК$_1$

Таблица 3.5 – Концепты НСКК$_1$ для моделирования актуальных способов реализации угроз

Концепт	Характеристика
C_1	Злоумышленник, реализующий сетевую атаку
C_2	Подмена ответа сервера FTP резервного копирования конфигураций ПЛК (УБИ.034)
C_3	Перехват учетной записи привилегированного пользователя на ПЛК (УБИ.034)
C_4	Учетная запись с параметрами по умолчанию на ПЛК (УБИ.030)
C_5	Модификация прошивки ПЛК (УБИ.188)
C_6	Перезапись проекта ПЛК в режиме online (УБИ.179)
C_7	Отказ в обслуживании оборудования
C_8	Потеря возможности мониторинга параметров СИКН
C_9	Перевод СИКН и управляемых объектов в аварийное состояние
C_{10}	Останов нефтетранспорта по магистральному нефтепроводу
C_{11}	Нарушение штатного режима функционирования АСУ ТП ПСП
C_{12}	Неспособность компании выполнить договорные обязательства
C_{13}	Система обнаружения аномалий сетевого трафика и мониторинга состояния компонент ИС и хода ТП
C_{14}	Оценка эффективности применения СЗИ
C_{15}	Оценка затрат на реализацию мер по снижению риска ИБ
C_{16}	Итоговая оценка рисков

Концепт C_1 выступает в качестве концепта-драйвера и представляет собой внешнего нарушителя, реализующего сетевую атаку, связанную с модификацией конфигураций ПЛК с целью нарушения ТП, создания аварийной ситуации на промышленном объекте или состояния аварийной остановки. Также в качестве концепта-драйвера установлен C_{13} – система обнаружения аномалий сетевого трафика и мониторинга состояния ресурсов АСУ ТП и хода ТП, то есть предлагаемая контрмера для минимизации рисков ИБ АСУ ТП. Фиксированным значением концепта-драйвера является оценка вероятности обнаружения аномалий состояния информационно-телекоммуникационной сети и наблюдаемого объекта, полученные в [179].

Целевыми установлены концепты-последствия C_{11} и C_{12}. Установившееся значение концепта C_{14} характеризует оценку эффективности применения контрмер. Нормированная в диапазон [0; 1] оценка затрат на реализацию мер по снижению рисков ИБ характеризуется состоянием концепта C_{15}.

Целевая функция для НСКК$_1$:

$$X_{11}, X_{12} \longrightarrow min;\ \Phi\left(W_{13,C_S^j}\right) = X_{11}, X_{12} \longrightarrow min,\ j = 2,3,4.$$

Применяемая контрмера обладает ограниченными возможностями оперативного анализа входящего сетевого трафика и трафика внутри промышленной сети без существенных задержек. Следовательно, необходимо распределение ресурсов ($W_{13,2}$, $W_{13,3}$, $W_{13,4}$, суммарное пороговое значение распределяемых ресурсов $\theta \leq 3$) контрмеры для анализа трафика между наиболее значимыми объектами АСУ ТП с целью минимизации итогового суммарного ущерба. Значение концепта-драйвера C_{13} задается оценкой эффективности обнаружения аномалий сетевого трафика и состояния объекта $X_{13} = [0{,}95;\ 0{,}98]$.

На область определения целевой функции $\Phi\left(W_{13,C_S^j}\right)$ наложены следующие ограничения:

$$\forall W_{13,i}: \begin{cases} \overline{W}_{13,i}, \underline{W}_{13,i} \in [0{,}05, 0{,}95], i = 2,3,4; \\ \overline{W}_{13,i} - \underline{W}_{13,i} \geq 0{,}05; \\ \sum_i \left[\overline{W}_{13,i} + \underline{W}_{13,i}\right] < 3. \end{cases}$$

Целевая функция с заданными ограничениями на область значений:

$$\Phi(W_{13,i}) = \left\|\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12}\right\| + \alpha f\left(\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12}\right);$$

$$f\left(\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12},\right) = \begin{cases} 1, \overline{X}_j < \varepsilon; \\ 0, \text{otherwise.} \end{cases} \qquad \varepsilon = 1e-4; \quad j = \overline{1,4}.$$

Определим перечень характеристик интеграции и последующего сопровождения контрмер для рассматриваемой промышленной системы (Таблица 3.6) и декомпозируем концепт C_{14} в соответствии с выделенными особенностями (Рисунок 3.14) для уточнения итоговой оценки эффективности решения.

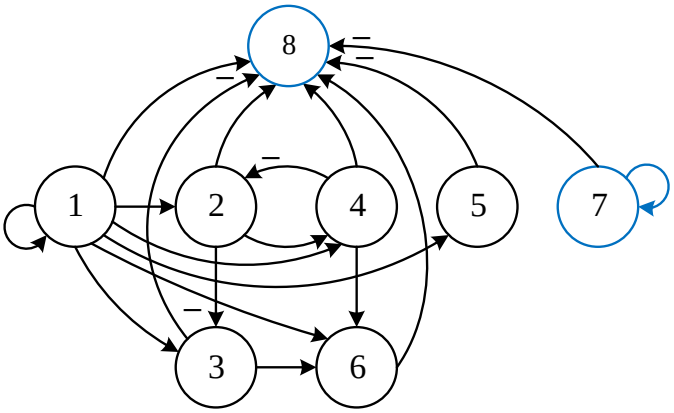


Рисунок 3.14 – Декомпозиция концепта C_{14}

Таблица 3.6 – Концепты НСКК$_2$ декомпозиции концепта C_{14} НСКК$_1$

Концепт	Характеристика
C_1	Стоимость контрмер (C)
C_2	Простота эксплуатации и сопровождения (S)
C_3	Стоимость сопровождения контрмер (CS)
C_4	Степень влияния на штатное функционирование (F)
C_5	Импортозамещение (Im)
C_6	Оперативность реагирования контрмер (R)
C_7	Концепт C_{15} от НСКК$_1$
C_8	Концепт C_{14} от НСКК$_1$

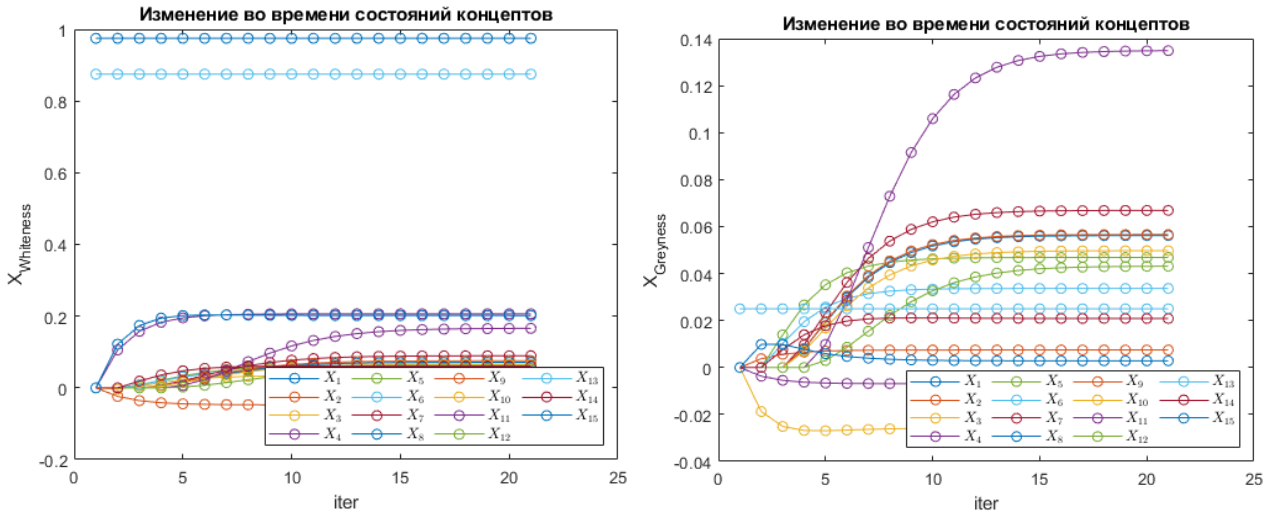
Оценка эффективности: $E = f(C, S, CS, F, Im, R)$.

Значение концептов вложенной НСКК$_2$ определяется после стабилизации состояния концептов НСКК$_1$ согласно схеме [32].

Для оценки рисков ИБ рассмотрим следующие сценарии моделирования.

Сценарий 1. Изменение во времени концептов НСКК$_1$ без оптимизации распределения весовых коэффициентов контрмеры C_{13}. Процесс изменения состояний концептов НСКК$_1$ во времени показан на Рисунке 3.15, где по оси ординат отмечены значения переменных состояния концептов НСКК$_1$, а по оси абсцисс – итерации сходимости НСКК$_1$.

Итоговый значения целевых концептов НСКК$_1$: $X_{11} = [0{,}03; 0{,}3]$ и $X_{12} = [0{,}01; 0{,}10]$, а также $X_{15} = [0{,}2; 0{,}2]$.

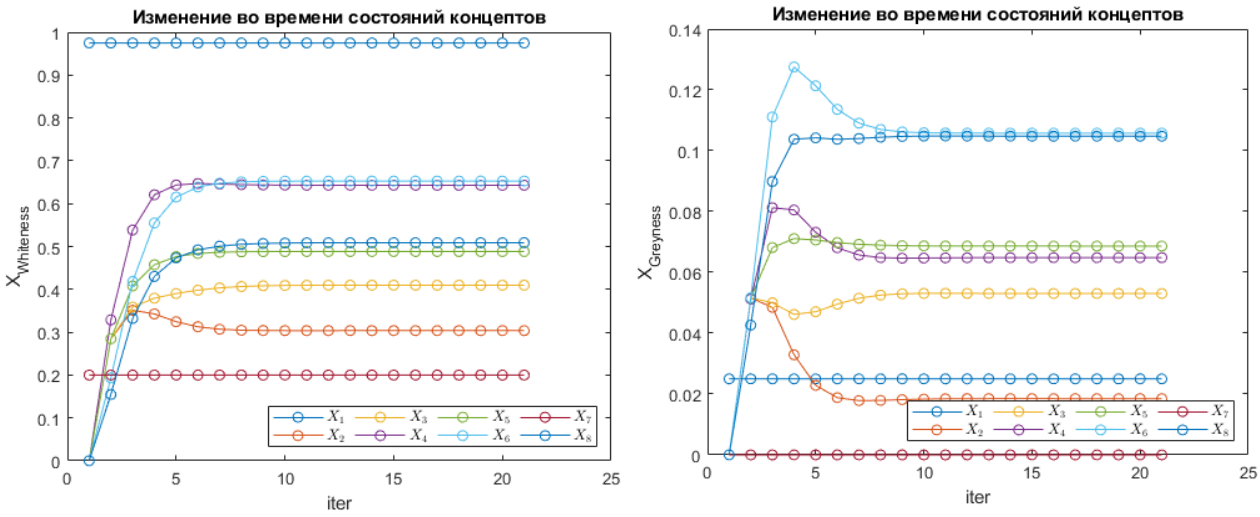


а) б)

Рисунок 3.15 – Стабилизация состояния концептов НСКК$_1$: а) «белизна» и б) «серость» оценок состояния концептов

Изменение во времени состояния концептов вложенной НСКК$_2$ без оптимизации распределения весовых коэффициентов контрмеры C_{13} представлено на Рисунке 3.16.

Итоговое значение целевого концепта НСКК$_2$ составило $X_8 = [0{,}4; 0{,}61]$.



а) б)

Рисунок 3.16 – Стабилизация состояния концептов НСКК$_2$: а) «белизна» и б) «серость» оценок состояния концептов

Сценарий 2. Рассмотрим применение ГА для оптимизации весовых коэффициентов $W_{13,2}$, $W_{13,3}$, $W_{13,4}$. Размер начальной популяции составляет 100 особей. Изменение среднего значения фитнес-функции по популяции и значения фитнес-функции для лучшей особи в популяции по итерациям ГА приведено на Рисунке 3.17.

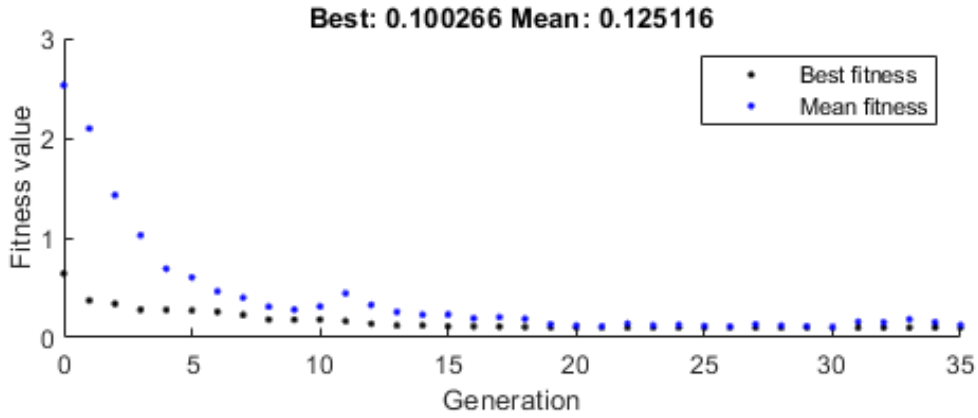
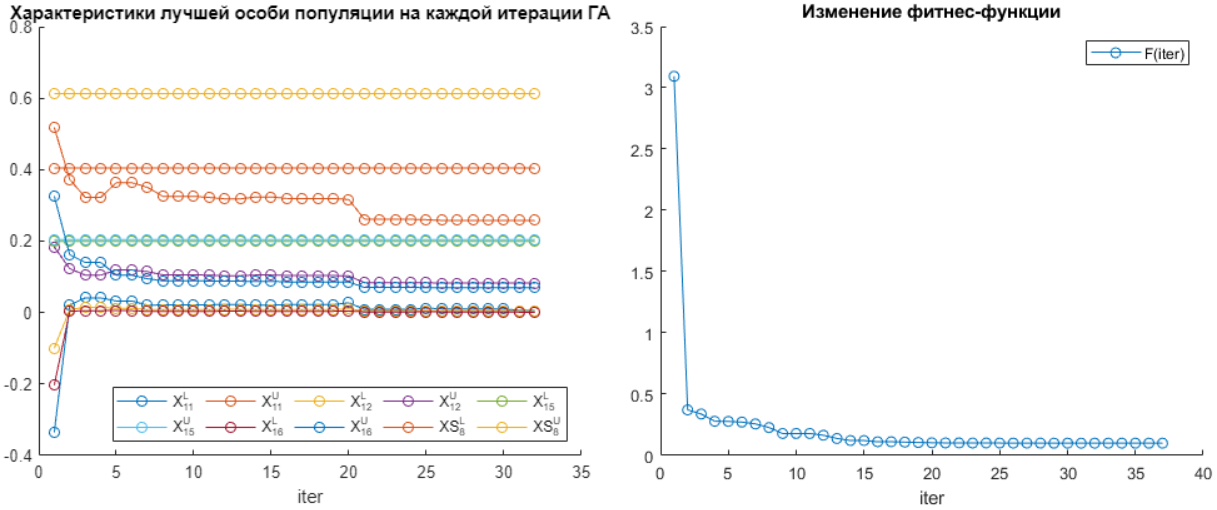


Рисунок 3.17 – Изменение среднего значения фитнес-функции по популяции и значения фитнес-функции для лучшей особи в популяции по итерациям ГА

Изменение во времени значений целевых концептов НСКК$_1$ – X_{11}, X_{12} и мониторинг состояния концепта X_8 для НСКК$_2$ по итерациям ГА показаны на Рисунке 3.18.

Значение параметров по результатам оптимизации для НСКК$_1$ – $X_{11} = [0{,}0153; 0{,}0947]$, $X_{12} = [0{,}0054; 0{,}0287]$, $X_{15} = [0{,}2175; 0{,}2486]$, для НСКК$_2$ – $X_8 = [0{,}4003; 0{,}6025]$. Значение фитнес-функции – 0,1003.



а) б)

Рисунок 3.18 – а) изменение во времени значений целевых концептов НСКК$_1$ – X_{11}, X_{12} и концепта X_8 для НСКК$_2$ по итерациям ГА; б) изменение фитнес-функции по итерациям ГА

Изменение подбираемых весовых коэффициентов, характеризующих распределение контрмер, по итерациям работы ГА показано на Рисунке 3.19.

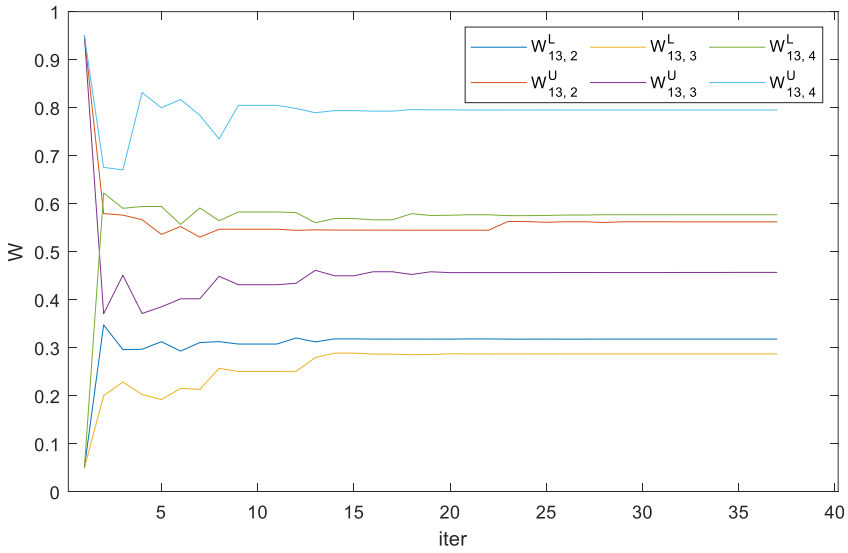


Рисунок 3.19 – Изменение подбираемых весовых коэффициентов по итерациям работы ГА

Итоговый значения целевых концептов НСКК$_1$ составили: $X_{11} = [0{,}03; 0{,}03]$ и $X_{12} = [0{,}01; 0{,}10]$, а также концепта $X_{15} = [0{,}2; 0{,}2]$.

Итоговая диаграмма состояний целевых концептов НСКК$_1$ и НСКК$_2$ приведена на Рисунке 3.20.

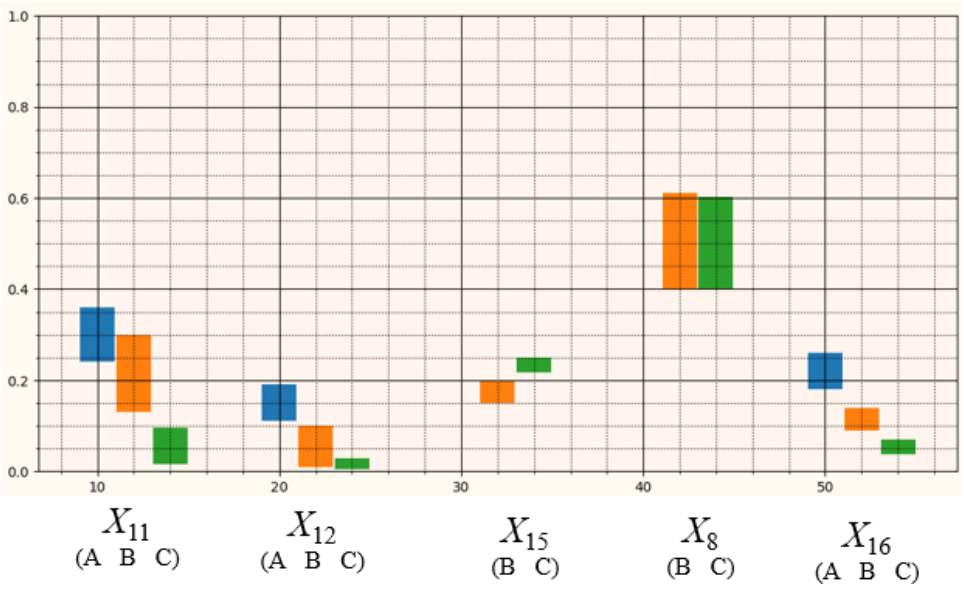


Рисунок 3.20 – Состояние целевых концептов НСКК$_1$ и НСКК$_2$ (по оси ординат – диапазон значения серых оценок состояния концептов)

Анализ диаграммы показывает, что оценки риска ИБ для целевых концептов C_{11} и C_{12} после оптимизации распределения ресурсов контрмеры уменьшились как в отношении разброса («серость»), так и в отношении центрального значения оценок («белизна») на 85-90%. Возросла оценка эффективности эксплуатации контрмеры (состояние концепта X_{14}) и уменьшилась оценка стоимости эксплуатации контрмеры несмотря на то, что в целевую функцию оптимизация этих параметров заложена не была. Следовательно, предложенный подход демонстрирует эффективность в выборе наиболее эффективных вариантов средств защиты при минимальных затратах и позволяет оптимизировать распределение ресурсов системы защиты информации для минимизации рисков ИБ.

В таблице 3.7 представлены результаты эксперимента по оценке рисков ИБ АСУ ТП ПСП. С помощью ГА получен набор весовых коэффициентов НСКК, отражающих оптимальное распределение затрат на реализацию мер по снижению риска ИБ АСУ ТП.

Таблица 3.7 – Результаты оценки рисков ИБ АСУ ТП ПСП с оптимизацией весов НСКК

Характеристика целевых концептов	Оценка рисков в диапазоне серых чисел		
	штатные контрмеры(A)	контрмеры выбраны на основе рекомендаций ИСППР сценарного уровня моделирования (B)	оптимизация ресурсов контрмер с помощью ГА (C)
Оценка риска ИБ для объекта в целом	[0,18; 0,26]	[0,09; 0,14]	[0,038; 0,070]
Оценка эффективности применения контрмер	[-; -]	[0,15; 0,20]	[0,218; 0,249]

Сравнение предложенной методики оценки рисков ИБ АСУ ТП с существующими аналогами показало, что применение существующих методик усложняется высокой степенью неопределенности и сложности процедуры формализации факторов, влияющих на уровень защищенности промышленной системы: появлением новых угроз, возможностью потери актуальности данных в ходе анализа рисков, что в значительной степени устраняется при использовании предложенной методики.

3.5 Выводы по главе

В главе 3 разработан метод сценарного моделирования атак на основе комплекса моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов, опирающийся на принципы когнитивного и предметно-ориентированного моделирования. Предложенный метод отличается формализованным описанием объекта защиты, угроз и уязвимостей в виде иерархии графовых моделей, что позволяет выявить структуру причинно-следственных связей между элементами АСУ ТП и компонентами открытых баз данных угроз, уязвимостей, шаблонов компьютерных атак, представить их в виде

последовательности действий, совокупности методов и средств, позволяющих нарушителю проводить атаку на АСУ ТП промышленного объекта.

Приведена формальная постановка задачи многокритериальной оптимизации, учитывающей возможность минимизации оценки риска ИБ выделенной зоны АСУ ТП промышленного объекта, и оценки эффективности использования контрмер в различных сценариях атак.

Разработана методика количественной оценки рисков ИБ АСУ ТП на основе иерархии моделей и алгоритма построения сценариев атак, отличающаяся нечетким когнитивным моделированием 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 функциональных ограничений.

Предложенные решения позволяют на 15 % повысить эффективность эксплуатации контрмер и в 2,5 раза ускорить процесс построения сценариев реализации актуальных угроз ИБ в ходе построения модели угроз объекта защиты.

Глава 4. Разработка архитектуры интеллектуальной системы поддержки принятия решений по оценки рисков ИБ АСУ ТП промышленных объектов

В данной главе разрабатываются инструментальные средства автоматизации моделирования сценариев атак в системе ИСППР с последующей количественной оценкой рисков ИБ АСУ ТП. Описываются возможности практического применения результатов работы, включающие анализ уязвимостей объекта и моделирование сценариев атак на основе открытых баз компьютерных атак, построение и визуализацию НКК, а также интеллектуальную оптимизацию весовых коэффициентов НКК.

4.1 Разработка структурно-функциональной организации ИСППР

Согласно стандарту ISO/IEC/IEEE 42010 [3] и рекомендациям SEI (Software Engineering Institute), архитектура системы – это «основные понятия и свойства системы в окружающей среде, воплощенные в его элементы, отношения и в принципах своей конструкции и эволюции».

Модели (информационная, функциональная, поведенческая), полученные в результате анализа требований к ИСППР, являются исходными данными для этапа детального проектирования архитектуры ИСППР. На выходе этапа проектирования должны быть сформированы модели данных, архитектуры и подсистем.

Общая схема разработки ИСППР представлена на рисунке 4.1.

Рисунок 4.1 – Общая схема разработки ИСППР

Структурно-функциональная организация разработанной ИСППР в задачах оценки рисков ИБ АСУ ТП [145, 146], реализующей предложенные модели и алгоритмы, представлена на рисунке 4.2. Руководствуясь основными принципами построения открытых систем (функциональная декомпозиция, модульность, открытость интерфейсов взаимодействия с внешними системами) выделены следующие подсистемы, направление на решение подзадач сбора, обработки и последующего анализа сведений, позволяющих сократить временные затраты на оценку рисков ИБ:

– подсистема ($ПС_1$) обработки и формализации сведений об уязвимостях, недостатках и составе программного и аппаратного обеспечения АСУ ТП (модули 2, 3);

– подсистема ($ПС_2$) построения и анализа графовой модели сценариев атак (модули 4, 5);

– подсистема ($ПС_3$) когнитивного моделирования и количественной оценки рисков ИБ (модули 6, 7);

– подсистема ($ПС_4$) построения фрагментов модели угроз ИБ АСУ ТП (модули 1, 8, 9).

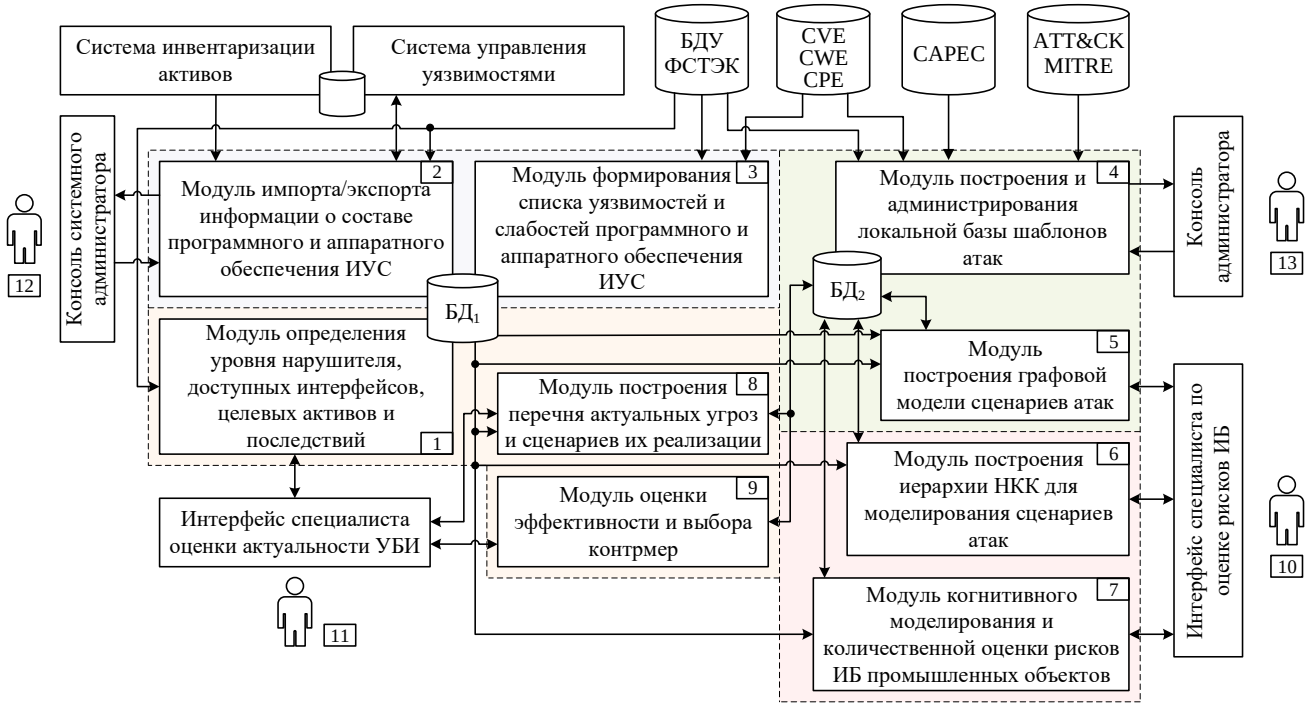


Рисунок 4.2 – Структурно-функциональная организация ИСППР в задачах оценки рисков ИБ АСУ ТП

Подсистема обработки и формализации сведений об уязвимостях, недостатках и составе программного и аппаратного обеспечения АСУ ТП. Модуль (2) импорта-экспорта информации о составе программного и аппаратного обеспечения обеспечивает взаимодействие с внешними системами инвентаризации и управления уязвимостями, позволяя в автоматизированном режиме обновлять в локальном хранилище (реляционная $БД_1$) информацию о составе, конфигурации, физической и логической топологии анализируемой АСУ ТП. Администрирование процесса импорта данных из внешних баз находится под контролем системного администратора (12).

Модуль (3) позволяет на основе накопленных данных о составе и организации АСУ ТП с учетом идентификаторов CPE и данных из внешних хранилищ NVD (CVE, CWE) и БДУ ФСТЭК России, сформировать список уязвимостей и слабостей программного и аппаратного обеспечения анализируемой системы. Информация из внешних баз импортируется через API интерфейсы в

установленных машинно-читаемых форматах (json и xml). Накопленные структурированные данные размещаются в хранилище $БД_1$.

Подсистема построения и анализа графовой модели сценариев атак. Модуль (5) обеспечивает возможность построения графовой модели сценариев атак на основе формализации цепочек CPE-CVE-CWE-CAPEC и построения графа связей указанных идентификаторов описаний в формате графовой $БД_2$ на основе технологий Neo4j и языка GraphQL. Вторая графовая модель, хранимая в $БД_2$, обеспечивает формализацию связей CAPEC-ATT&CK (Техники)-ATT&CK (Тактики)-Угрозы БДУ ФСТЭК. Множество связей между идентификаторами строится на основе перекрестных ссылок в их описаниях и дополняется ручной разметкой.

Модуль (4) обеспечивает возможность импорта данных из внешних хранилищ, трансляции их в схему данных $БД_2$ и администрирование процесса обработки накапливаемых данных. Администратор (13) подсистем обновления данных из внешних источников обеспечивает контроль процессов взаимодействия с внешними хранилищами и актуальность хранимых данных.

Подсистема когнитивного моделирования и количественной оценки рисков ИБ (Приложение Ж). Модуль (6) построения иерархии НКК позволяет выполнять моделирование сценариев атак на основе сворачивания графовой модели, формируемой на основе запросов к $БД_2$ для текущего набора выявленных уязвимостей с оценкой уровня их опасности. Модуль (7) предназначен для получения количественной оценки рисков ИБ для выделенных зон промышленного объекта по результатам когнитивного моделирования. Специалист (10) по оценке и моделированию рисков ИБ выполняет операции по подготовке и преобразования графовой модели в декомпозицию соответствующих концептов когнитивной карты текущего уровня анализа.

Подсистема построения фрагментов модели угроз ИБ АСУ ТП. Модуль (1) предназначен для формализации сведений об уровне нарушителя, доступных интерфейсах, целевых активах и возможных последствиях реализации угроз. Специалист (11) по оценке актуальных угроз, опираясь на Методику ФСТЭК

России и разработанные решения, определяет основные параметры, необходимые для расчета количественных оценок рисков ИБ, и дальнейшие действия по уточнению, корректировке и анализу сценариев атак. Модуль (8) на основе графовой модели позволяет сформировать сценарии реализации для актуальных угроз. Модуль (9) позволяет получить непосредственно количественные оценки рисков ИБ для выделенных зон АСУ ТП, а также сформировать перечень контрмер с возможностью количественной оценки эффективности их применения как для отдельных зон, так и для всей АСУ ТП в целом (на основе оценок рисков ИБ и затрат на их реализацию).

4.2 Разработка архитектуры и комплекса объектно-ориентированных моделей ИСППР оценки рисков ИБ АСУ ТП

Для выполнения анализа требований и дальнейшего проектирования ИСППР разработаны диаграммы вариантов использования (ДВИ) в нотации UML, раскрывающие типовой способ взаимодействия пользователей с установленными ролями с системой.

Выделенные роли пользователей:

– специалист по оценке актуальных угроз;

– системный администратор;

– администратор подсистемы обновления данных из внешних источников.

$ДВИ_1$ раскрывает процесс наполнения локальной $БД_1$ по результатам инвентаризации и импорта данных из внешних источников при взаимодействии пользователей с $ПС_1$ (рисунок 4.3, где 11 – специалист по оценке актуальных угроз; 12 – системный администратор; 13 – администратор подсистемы обновления данных из внешних источников).

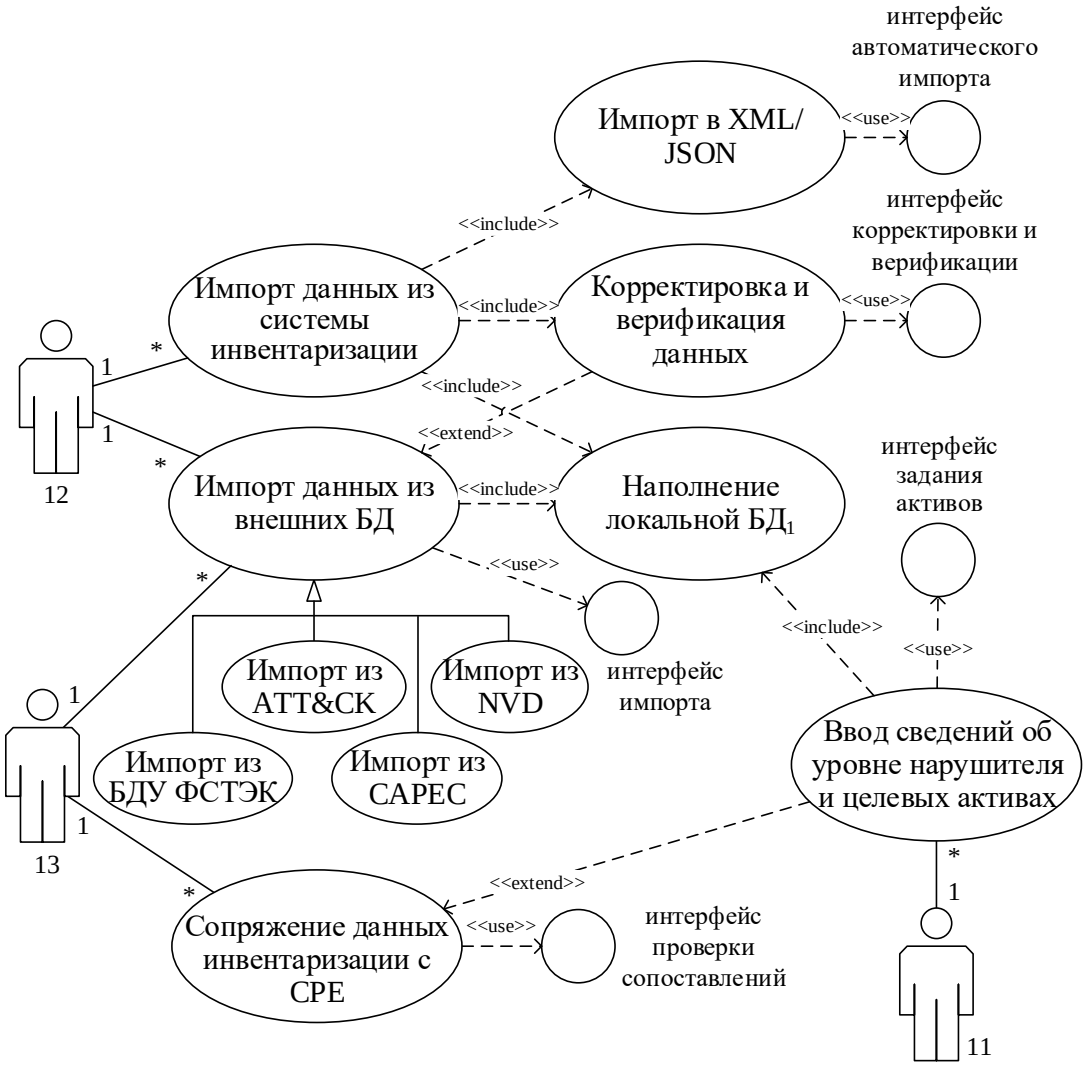


Рисунок 4.3 – ДВИ$_1$ наполнения локальной БД$_1$ по результатам инвентаризации и импорт данных из внешних источников при взаимодействии пользователей с ПС$_1$

ДВИ$_1$ включает базовые прецеденты импорта данных из внешних по отношению к проектируемой ИСППР систем с требуемым уровнем декомпозиции. Для каждого из акторов приведены типовые интерфейсы, посредствам которых осуществляется реализация прецедента.

ДВИ$_2$ (рисунок 4.4) раскрывает процесс взаимодействия пользователей с ПС$_2$ при построении и использовании графовой модели сценариев атак.

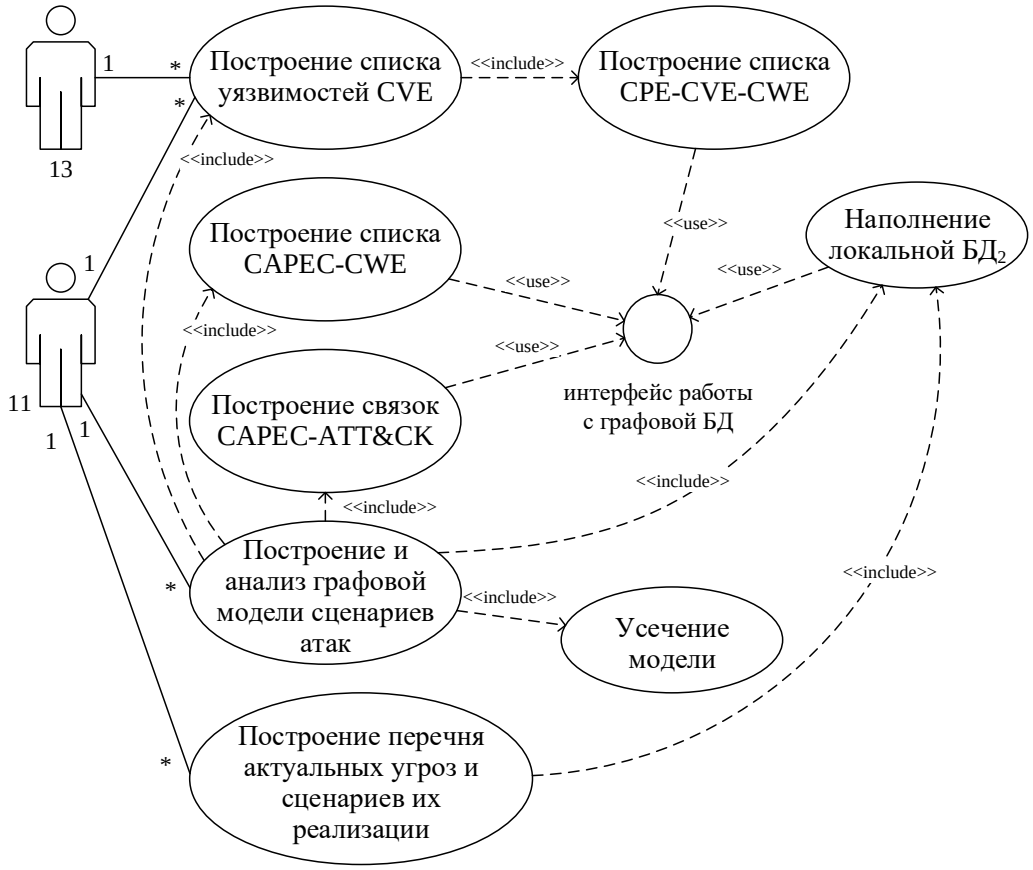


Рисунок 4.4 – ДВИ$_2$ взаимодействия пользователей с ПС$_2$ при построении и использовании графовой модели сценариев атак

Детализация прецедентов ДВИ$_2$ раскрывает основные этапы взаимодействия с внешними базами данных и знаний (NVD, MITRE ATT&CK и БДУ ФСТЭК) в ходе построения графовой модели сценариев атак на основе перекрестных связей между сущностями, описывающими как набор уязвимостей программного и аппаратного обеспечения, так и применимые нарушителями тактики и техники.

ДВИ$_3$ (рисунок 4.5, где 10 – специалист по оценке и моделированию рисков ИБ) раскрывает процесс количественной оценки рисков ИБ промышленного объекта и оценку эффективности выбора контрмер при взаимодействии пользователей с ПС$_3$ и ПС$_4$.

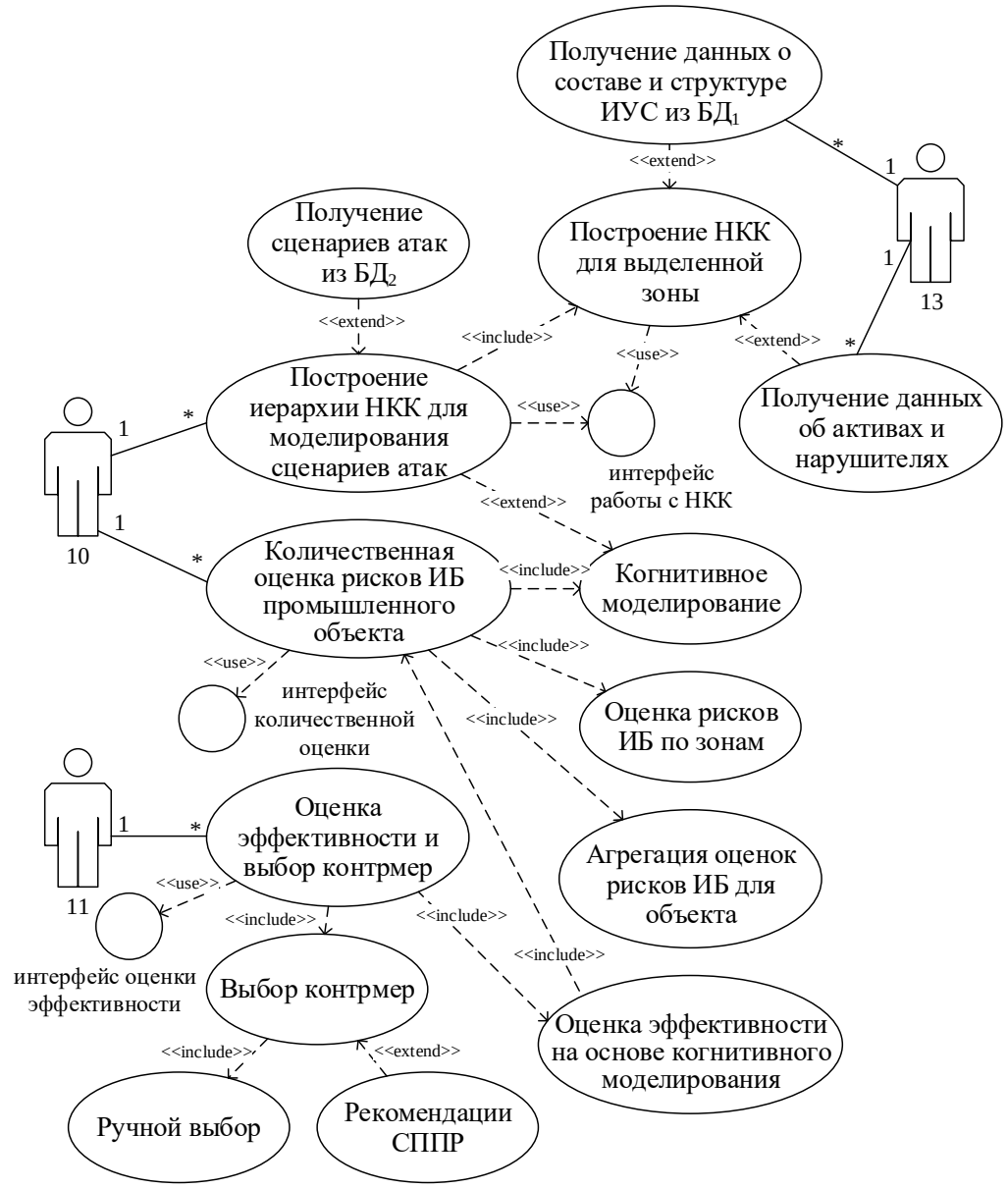


Рисунок 4.5 – ДВИ$_3$ количественной оценки рисков ИБ промышленного объекта при взаимодействии пользователей с ПС$_3$ и ПС$_4$

Разработанные ДВИ для выделенных пользовательских ролей являются основой для дальнейшей спецификации функциональных требований. Спецификация функциональных и нефункциональных требований является основой для последующего детального проектирования архитектуры ИСППР.

Одним из ключевых этапов детального проектирования архитектуры ИСППР является диаграмма классов, раскрывающая объектно-ориентированную декомпозицию ключевых подсистем. На рисунке 4.6 представлен фрагмент диаграммы классов ПС$_3$ в нотации UML.

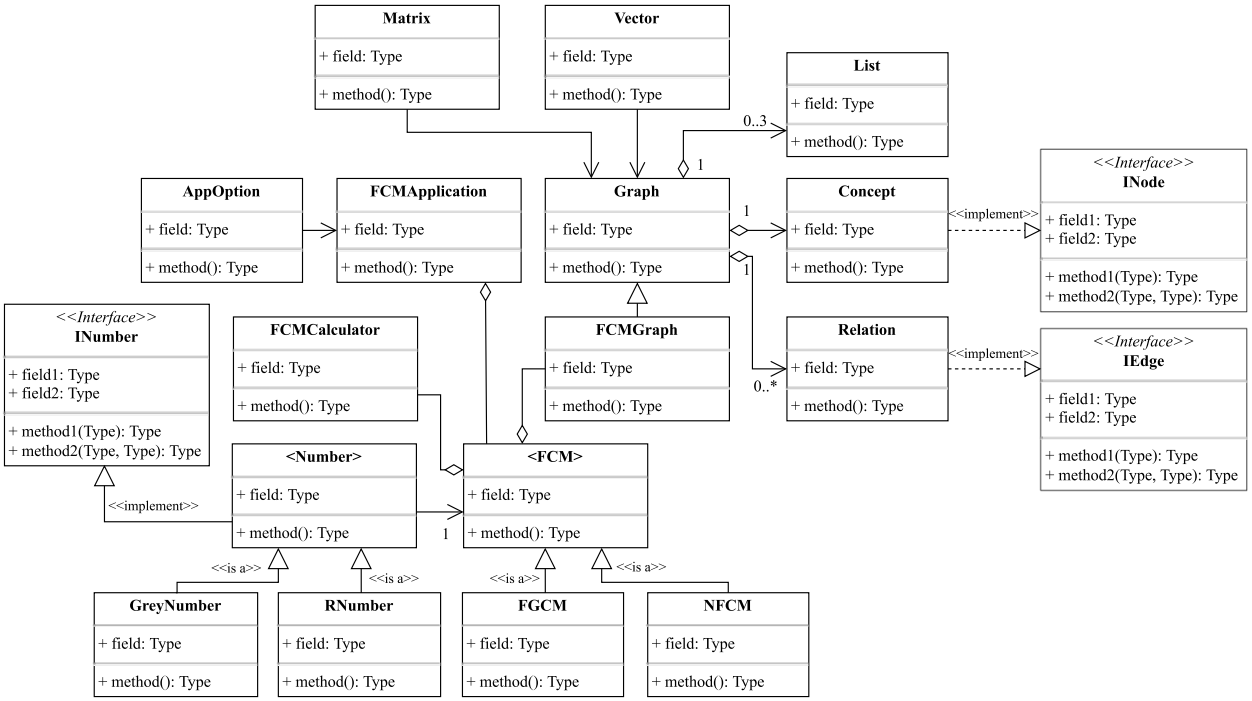


Рисунок 4.6 – Фрагмент диаграммы классов $ПС_3$ в нотации UML

Фрагмент диаграммы классов $ПС_3$ раскрывает статическую структурную иерархию ключевых сущностей, реализованных в процессе объектно-ориентированного анализа и проектирования в виде совокупности классов, интерфейсов и их взаимодействия (Таблица 4.1).

Таблица 4.1 – Описание классов и интерфейсов диаграммы классов $ПС_3$

№	Название класса (интерфейса)	Тип	Описание
1	GreyNumber	Класс	Реализация типа данных «Серое число»
2	RNumber	Класс	Реализация типа данных «Вещественное число»
3	Number	Абстрактный класс	Абстрактный класс, описывающие обобщенный тип данных «Число»
4	INumber	Интерфейс	Интерфейс, декларирующий операции над типом данных «Число»
5	FGCM	Класс	Реализация типа данных «Нечеткая серая когнитивная карта»
6	NFCM	Класс	Реализация типа данных «Нечеткая когнитивная карта» с веществennозначным типов весовых коэффициентов и состояний концептов
7	FCM	Абстрактный класс	Абстрактный класс, описывающий обобщенный тип «Нечеткая когнитивная карта» в виде графа связей
8	FCMCalculator	Класс	Реализация класса, описывающего механизм расчета состояний концептов когнитивной карты по итерациям

№	Название класса (интерфейса)	Тип	Описание
9	FCMApplication	Класс	Класс, описывающий основную сущность пользовательского приложения для создания и редактирования нечетких когнитивных моделей
10	AppOption	Класс	Класс, описывающий параметры настройки объекта пользовательского приложения
11	Graph	Класс	Базовый класс для описания типа данных «Граф» – ключевой АТД для моделирования НКК
12	Matrix	Класс	Класс для описания АТД «Матрица», определяющий создание и базовые операции над двумерными матрицами
13	Vector	Класс	Класс для описания АТД «Вектор», определяющий создание и базовые операции над одномерными массивами
14	List	Класс	Класс для описания АТД «Список», определяющий список вершин и ребер графа
15	Concept	Класс	Реализация класса для задания вершин ориентированного взвешенного графа НКК
16	INode	Интерфейс	Интерфейс, декларирующий основные операции над концептами графа НКК
17	Relation	Класс	Реализация класса для задания ребер ориентированного взвешенного графа НКК
18	IEdge	Интерфейс	Интерфейс, декларирующий основные операции для задания ребер (отношений) ориентированного взвешенного графа НКК

Представлен фрагмент логической модели данных $БД_1$, описывающей структуру и взаимосвязь основных сущностей предметной области, используемой для создания хранилища данных об угрозах, уязвимостях и сценариях их реализации $ПС_1$ и $ПС_4$ на основе взаимодействия с внешними базами знаний БДУ ФСТЭК, NVD и MITRE (Таблица 4.2, Рисунок 4.7).

Таблица 4.2 – Описание сущностей логической модели данных $ПС_1$ и $ПС_4$ в нотации ER-диаграмм

№	Название сущности	Группа	Описание
1	CAPEC	-	Описание одного шаблона CAPEC реализации атак
2	CAPEC2CVE	-	Реализация отношения «многие ко многим» между шаблонами CAPEC и описаниями уязвимостей CVE
3	Tech2CAPEC	-	Реализация отношения «многие ко многим» между шаблонами CAPEC и описаниями техник реализации атак M_Techs
4	CVE	NVD	Описание уязвимости CVE из международной базы NVD

№	Название сущности	Группа	Описание
5	CWE	NVD	Описание класса уязвимостей, характеризующих определенный недостаток программного обеспечения (CWE)
6	CVE2CWE	NVD	Реализация отношения «многие ко многим» между описаниями уязвимостей CVE и классами уязвимостей CWE
7	CVE2CPE	NVD	Реализация отношения «многие ко многим» между описаниями уязвимостей CVE и описанием программной (аппаратной) платформы CPE
8	CPE	-	Описание программной (аппаратной) платформы в формате языка шаблонов CPE
9	F_Techs	FSTEK	Описание техники реализации угрозы согласно методике ФСТЭК
10	F_Tackts	FSTEK	Описание тактики реализации угрозы согласно методике ФСТЭК
11	F_Threat2Tackt	FSTEK	Реализация отношения «многие ко многим» между описаниями угроз и тактик их реализации
12	F_Threats	FSTEK	Описание угроз безопасности информации согласно БДУ ФСТЭК
13	M_Tackt	ATT&CK	Описание тактик реализации атаки согласно базе MITRE ATT&CK ICS
14	Tack2Tech	ATT&CK	Реализация отношения «многие ко многим» между описаниями тактик и техник базы MITRE ATT&CK ICS
15	M_Techs	ATT&CK	Описание техники реализации атаки согласно базе MITRE ATT&CK ICS
16	F_Threat2M_TT	-	Реализация отношения «многие ко многим» между описаниями связок «тактика-техника» базы MITRE ATT&CK ICS и угроз безопасности информации ФСТЭК
17	Software	Inventory	Экземпляр программного обеспечения конечной системы
18	EndSystem	Inventory	Конечная систем
19	SystemObject	Inventory	Объект ИУС, для которого доступны описания в формате шаблонов CPE
20	ES2Soft	Inventory	Реализация отношения «многие ко многим» между экземплярами ПО и конечными системами, на которых они развернуты
21	SO2CPE	-	Реализация отношения «многие ко многим» между системными объектами и шаблонами описания CPE
22	Software	-	Реализация отношения «многие ко многим» между экземплярами ПО и шаблонами описания CPE

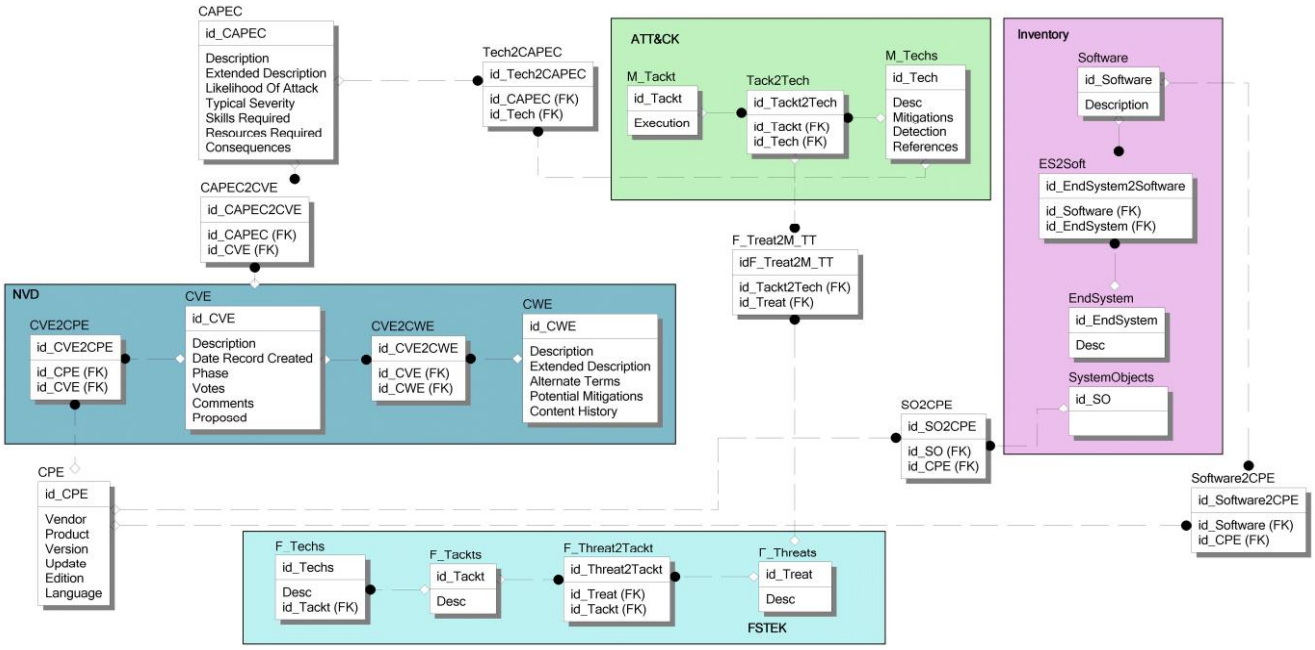


Рисунок 4.7 – Фрагмент логической модели данных $БД_1$ для $ПС_1$ и $ПС_4$

Информационная модель $БД_2$ включает два набора сущностей, связанных отношениями, что позволяет применить язык запросов Cypher для анализа иерархии сущностей, в том числе, с учетом непрямых связей, в виде ориентированного взвешенного графа. Использование специализированной графовой СУБД позволяет [14]:

– упростить анализ графовых структур в процессе перехода между смежными вершинами ориентированного графа за один шаг, исключая рекурсивный проход и операцию соединения (JOIN) для каждого уровня анализа данных в реляционных БД;

– предоставить интерфейс визуализации данных.

ATT&CK для ICS обеспечивает более полную и точную базу знаний при оценке и реализации мер защиты и противодействия. Использование ATT&CK обеспечивает понимание потенциальных угроз и действий нарушителя. Специалисты по ИБ могут принимать решения, сопоставляя действия и поведение нарушителя с конкретными контрмерами, которые могут быть развернуты в среде АСУ ТП (рисунок 4.8).

Исходные данные импортированы из внешнего хранилища ATT&CK (Enterprise, Mobile и ICS) в виде JSON файлов в формате STIX 2.1 (Structured Threat Information Expression) для описания CTI (Cyber Threat Intelligence).

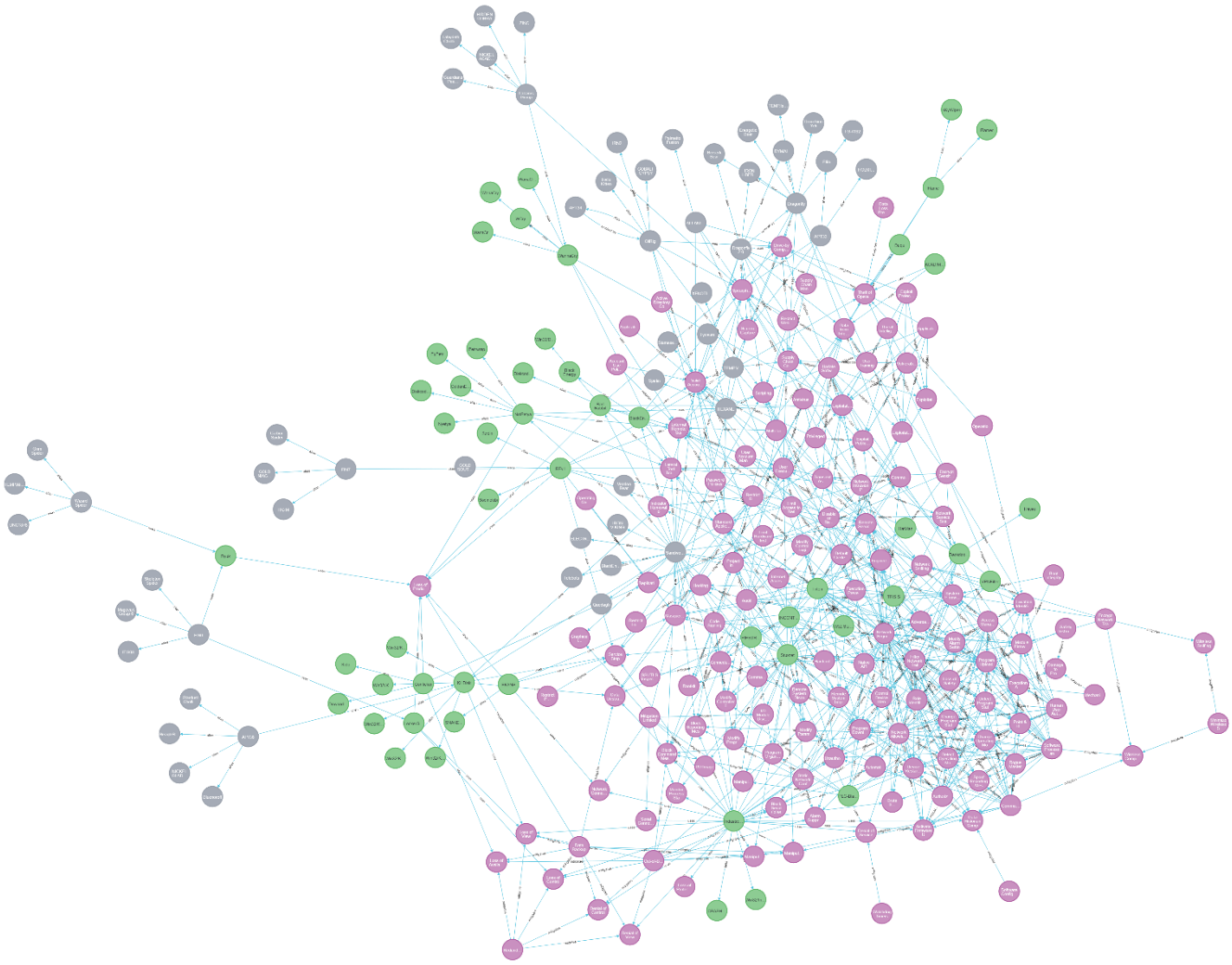


Рисунок 4.8 – Фрагмент графа, описывающего связи между сущностями тактиками, техниками и программным обеспечением, используемым нарушителями при реализации атаки

Первый набор сущностей (Таблица 4.3, Рисунок 4.9,) построен на основе [141, 169] и базы знаний MITRE ATT&CK для ICS о поведении нарушителей в технологической области промышленных систем управления, отражающая различные этапы жизненного цикла атаки, а также компоненты системы, на которые она нацелена. Раскрывается структура начальных этапов атак, затрагивающие ИТ-инфраструктуру с помощью тактик, техник и процедур, а также

действий, которые нарушители предпринимают против систем и функций промышленных систем управления.

Таблица 4.3 – Описание сущностей логической модели графовой БД$_2$ «Угрозы»

№	Сущность	Описание	Ключевые характеристики сущности
1	ICS Techniques ICS Subtechniques	Техники представляют собой то, «как» противник достигает тактической цели, выполняя действие.	ID Sub-techniques Tactic Platforms CAPEC ID Contributors Version Created Last Modified
2	ICS Tactics	Тактика представляет собой детализацию техники или подтехники ATT&CK. Это тактическая цель противника: причина совершения действия.	ID Created Last Modified
3	ICS Mitigations	Средства противодействия представляют концепции безопасности и классы технологий, которые можно использовать для предотвращения успешного выполнения техники.	ID Version Created Last Modified
4	ICS Data Sources	Источники данных представляют собой различные темы/темы информации, которые могут быть собраны датчиками/журналами. Источники данных также включают компоненты данных, которые идентифицируют определенные свойства/значения источника данных, относящиеся к обнаружению техник ATT&CK.	ID: Platforms Collection Layers Contributors Version Created Last Modified
5	ICS Groups	Кластеры действий, которые отслеживаются по общему имени в сообществе безопасности (возможны алиасы названий).	ID Contributors Version Created Last Modified
6	ICS Software	Пользовательский или коммерческий код, утилиты операционной системы, программное обеспечение с открытым исходным кодом или другие инструменты, используемые для поведения, смоделированного в ATT&CK (возможны алиасы названий)	ID Type Platforms Version Created Last Modified

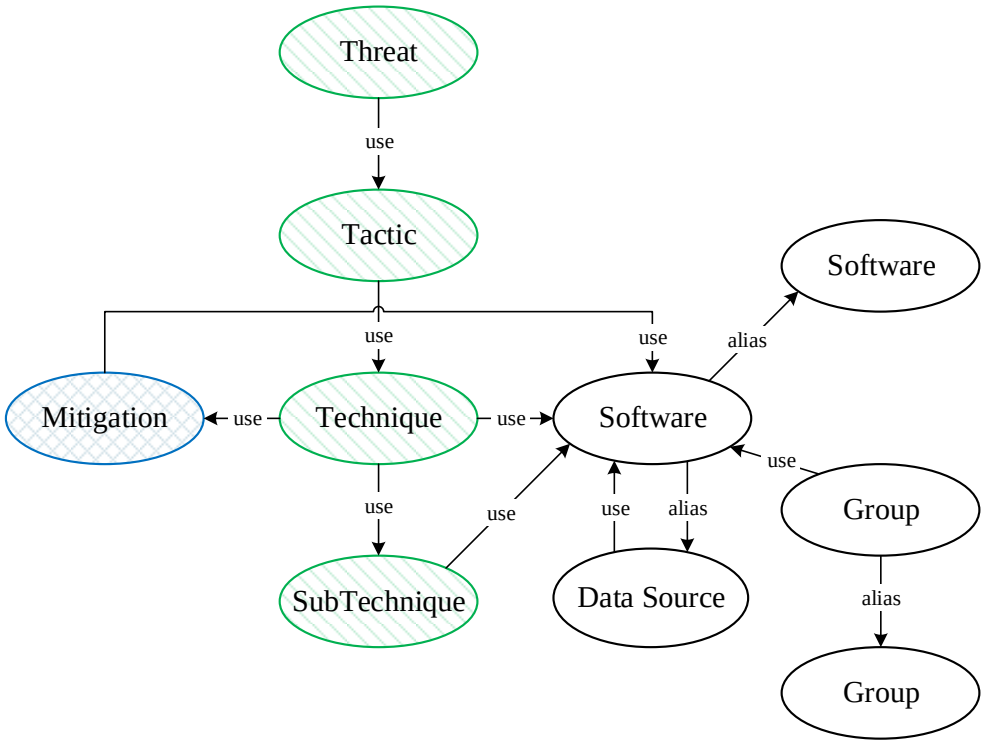


Рисунок 4.9 – Фрагмент логической модели данных графовой БД$_2$ «Угрозы»

Использовано два типа меток отношений между сущностями:

– «use» – «использует»;

– «alias» – «является синонимом».

Второй набор сущностей (Таблица 4.4, Рисунок 4.10) графовой БД$_2$ построен на основе GraphKer [157] и баз знаний NVD и MITRE ATT&CK для ICS и описывает «Сценарии» атак.

Таблица 4.4 – Описание сущностей логической модели графовой БД$_2$ «Сценарии» (фрагмент)

№	Сущность	Описание	Ключевые характеристики сущности
1	CPE	Шаблон описания платформы, содержащей уязвимость	ID
2	CVE	Описание уязвимости из БД NVD	ID
3	CWE	Описание класса уязвимостей – «слабостей» реализации программного и аппаратного обеспечения из БД NVD	Functional_Areas, Description, Affected_Resources, Submission_Name, Name
4	CAPEC	Описание шаблона CAPEC	Submission_Name, Description, Name, Skills_Required, Mitigations, Resources_Required, Likelihood_Of_Attack, Typical_Severity

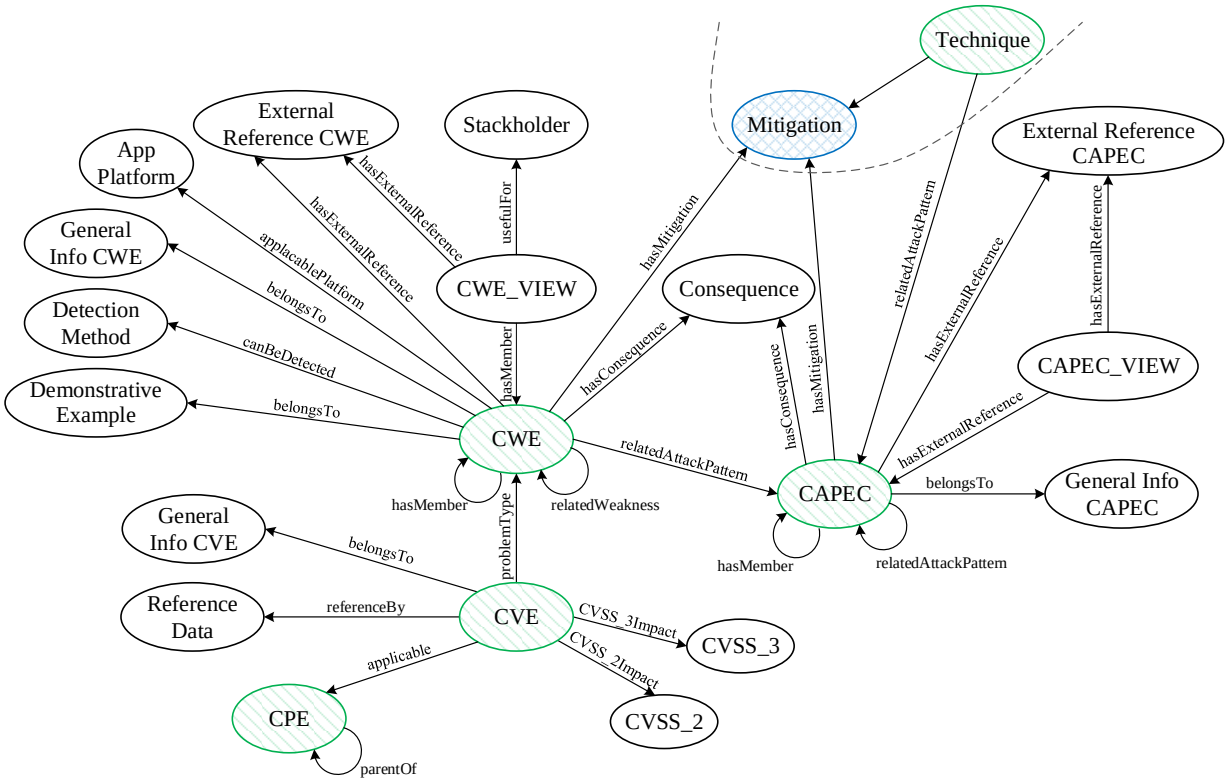


Рисунок 4.10 – Фрагмент логической модели данных БД$_2$ «Сценарии»

Ключевые отношения между выделенными сущностями позволяют отобразить многообразие типов связей и позволяет гибко настраивать сценарии поиска с применением языка запросов Cypher.

Разработка системы основана на широком использовании существующих архитектурных паттернов. На рисунке 4.11 представлен фрагмент диаграммы компонентов ПС$_3$-ПС$_4$ в нотации UML с реализацией паттерна «модель-представление-контроллер» (Model-View-Controller, MVC).

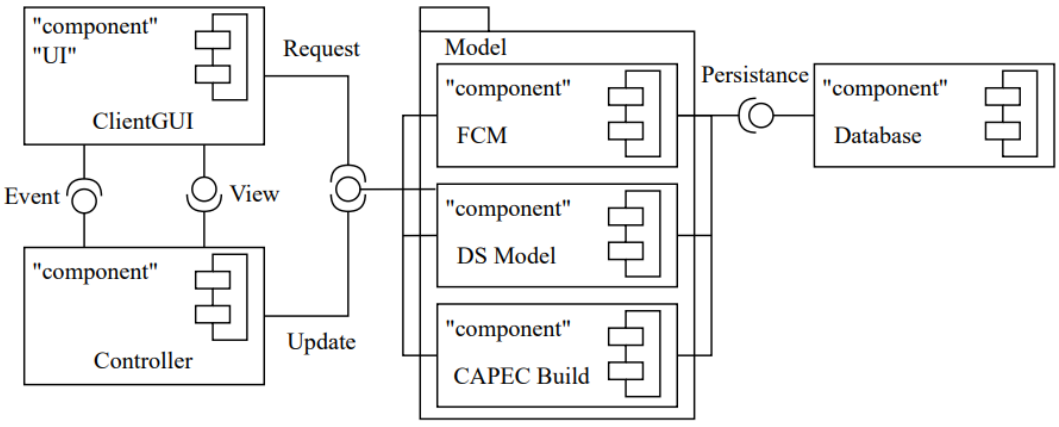


Рисунок 4.11 – Диаграммы компонентов ПС$_3$-ПС$_4$ в нотации UML с реализацией паттерна «модель-представление-контроллер»

Программная архитектура $ПС_3$-$ПС_4$ (Таблица 4.5) разделяется на три логических компонента:

– модель, управляющая системными данными и операциями над ними;

– компонент представление позволяет отображать данные для пользователя;

– компонент контроллер взаимодействует с пользователем, инициирует операции в модели и управляет работой компонента представления.

Таблица 4.5 – Описание пакетов и модулей диаграммы компонентов $ПС_3$-$ПС_4$

№	Название компонента / модуля	Тип	Описание
1	UI	Компонент	Компонент, обеспечивающий визуализацию и обслуживание очереди событий GUI (реализация представления) клиента для создания и редактирования НКК
2	Controller	Компонент	Компонент, обеспечивающий выполнение операций в модели (контроллер)
3	Model	Компонент	Компонент, содержащий модели управления системными данными и операциями над ними
4	FCM	Компонент	Компонент (входит в состав компонента Model) программной реализации НКК
5	DS Model	Компонент	Компонент (входит в состав компонента Model) программной реализации алгоритмов обучения НКК и оптимизации весовых коэффициентов с помощью генетических (эволюционных) алгоритмов
6	CAPEC Build	Компонент	Компонент (входит в состав компонента Model) программной реализации иерархического представления цепочек событий на основе графовой модели
7	Database	Компонент	Локальная база данных для хранения текущего состояния экземпляра приложения (обеспечение персистентности)

Таким образом, выполнен объектно-ориентированный анализ и проектирование подсистем в составе ИСППР [104-106].

4.3 Разработка инструментальных средств автоматизации моделирования сценариев атак в составе ИСППР

Проиллюстрируем типовой вариант применения разработанных средств автоматизации моделирования сценариев атак последовательностью действий и соответствующими экранными формами. Пусть в ходе анализа промышленного

объекта выявлены сущности АСУ ТП (промышленная сеть предприятия, промышленный коммутатор, ПЛК), для которых существуют актуальные уязвимости программного обеспечения: CVE-2019-6859, CVE-2019-6812, BDU:2020-7507, BDU:2020-01893, BDU:2020-04014, BDU:2019-03754, CVE-2018-19616, обобщаемые до CWE-798, CWE-287 и CWE-200.

После формирования списка актуальных уязвимостей выполняется построение графовой модели (рисунок 4.12).

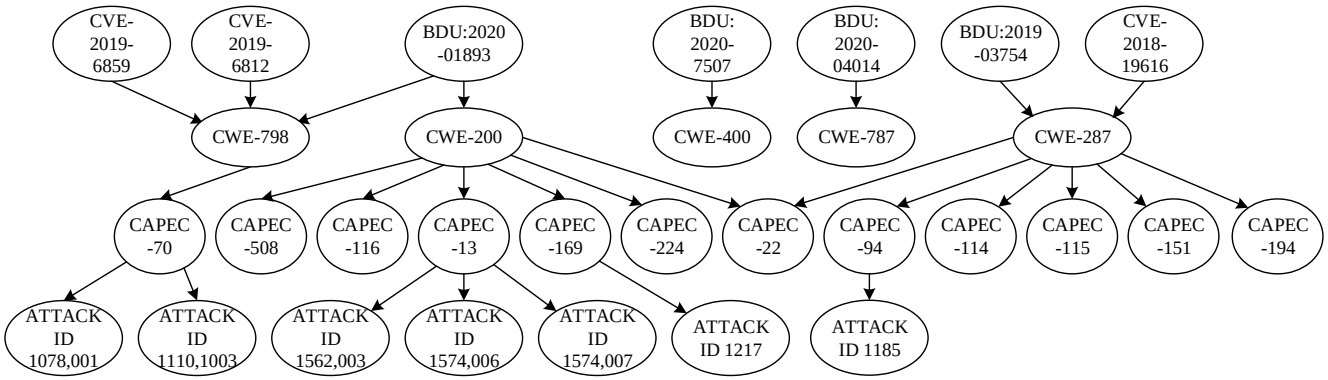


Рисунок 4.12 – Фрагмент сформированной графовой модели для заданного списка уязвимостей

Экранные формы, описывающие графовую модель в виде списка вершин и ребер, приведены на рисунке 4.13.

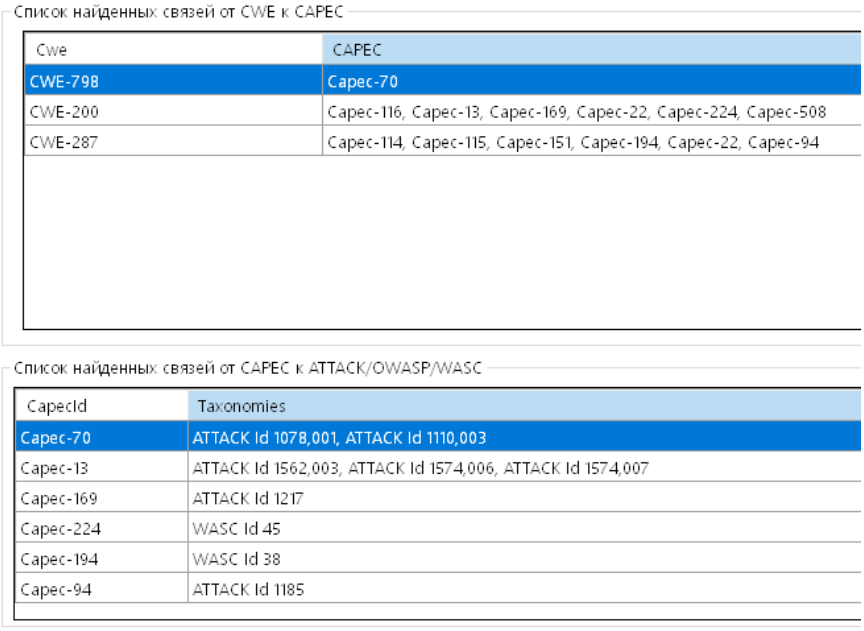


Рисунок 4.13 – Экранные формы списочного представления графовой модели

Далее выполняется формализация графовой модели в виде иерархической НКК позволяющей анализировать сценарии атак с требуемым уровнем детализации. Каждая атака укрупняется до концепта НКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность реализации атаки в каждом из возможных сценариев. Результирующая НКК позволяет оценить уровень рисков ИБ при реализации воздействия нарушителя на промышленную систему.

Для оценки риска ИБ используются определенные экспертами значения весов связей между концептами НКК. Так же необходимо выбрать целевые концепты, а также концепты-драйверы (Рисунок 4.14).

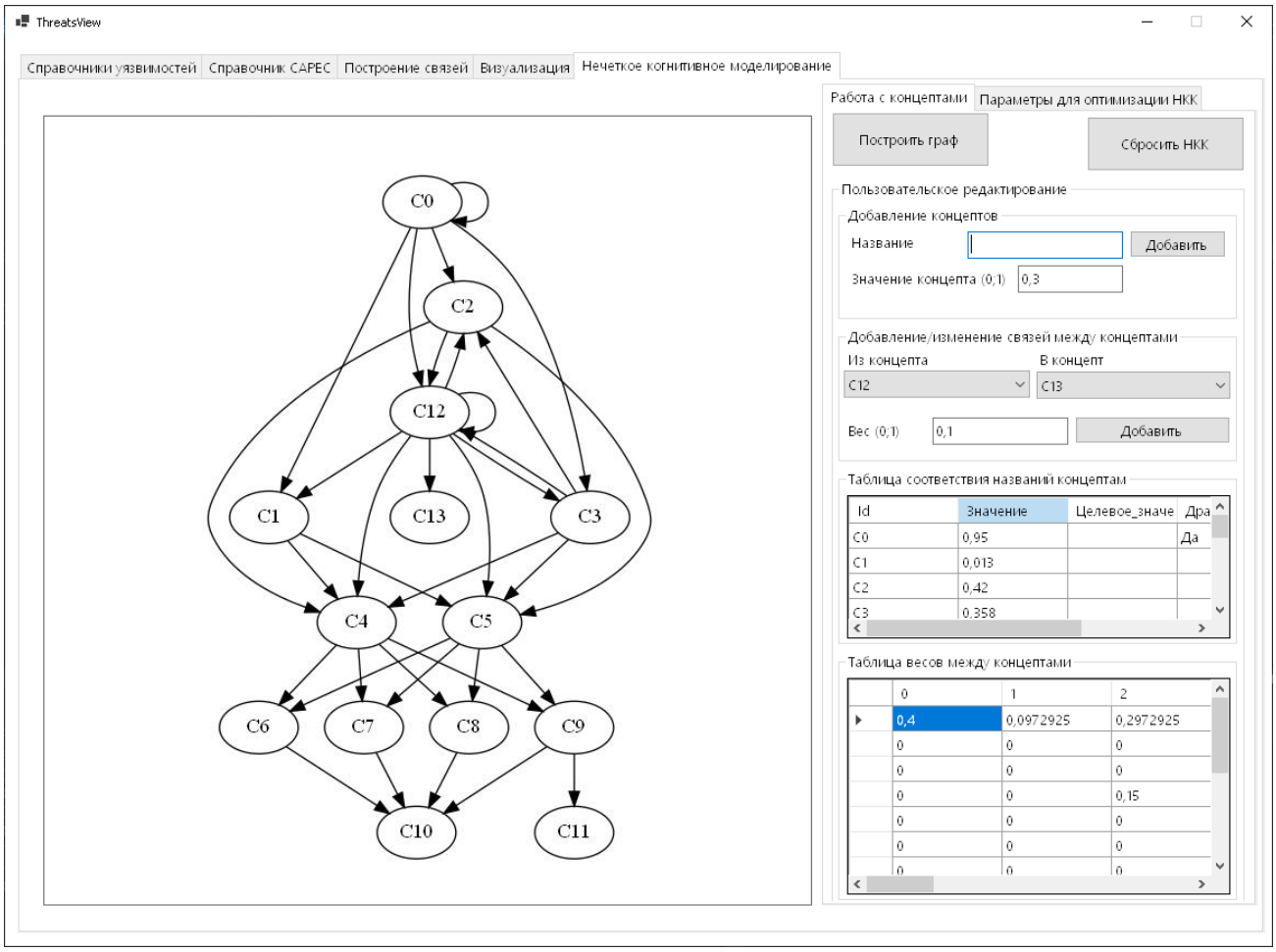


Рисунок 4.14 – Экранная форма графа НКК

Результирующая матрица весов НКК и векторы состояний концептов представляются в виде таблиц для последующего анализа экспертом.

Графический интерфейс для работы со списками уязвимостей и шаблонов атак представлен в виде экранных форм:

1. справочники уязвимостей (Рисунок 4.15):

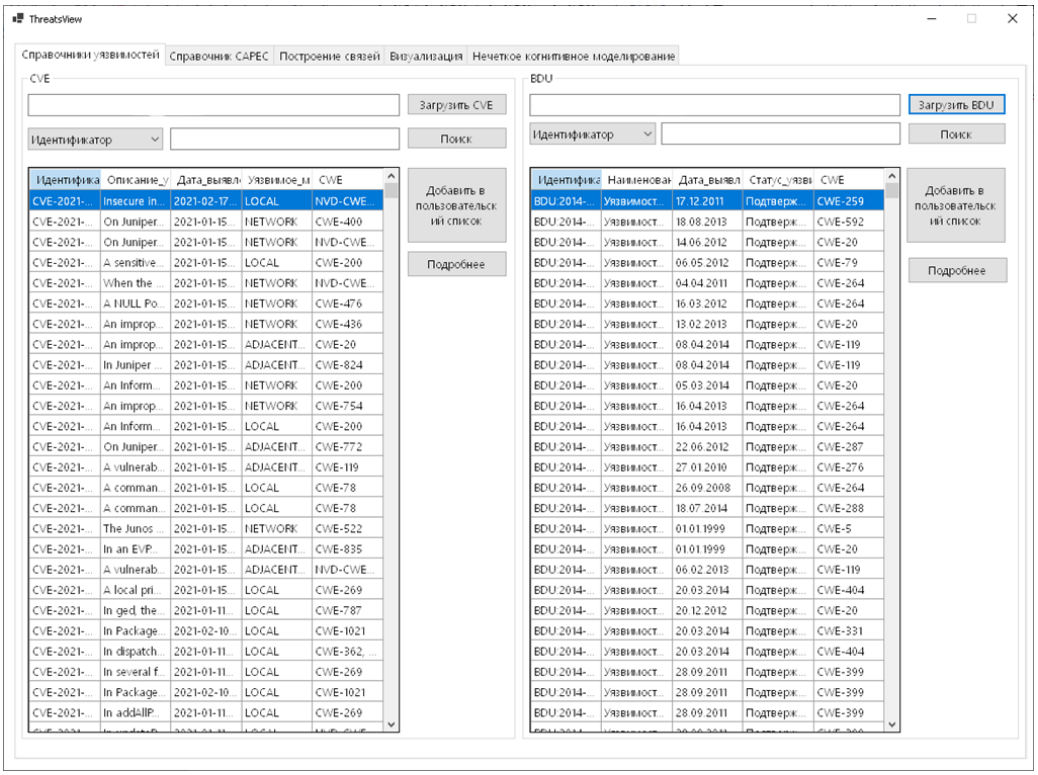


Рисунок 4.15 – Экранная форма навигации по справочникам уязвимостей

Форма позволяет пользователю:

1) загрузить справочники CVE, BDU;

2) произвести поиск по заданному полю и заданному тексту (Рисунок 4.16)

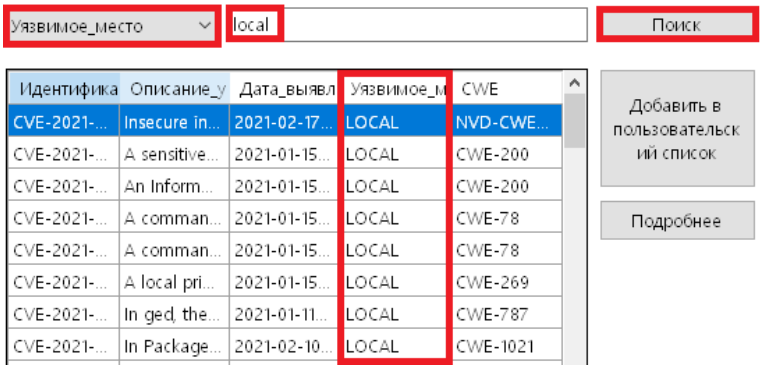


Рисунок 4.16 – Экранная форма результатов поиска уязвимости

3) получить подробную информацию об интересующей уязвимости;

4) добавить в пользовательский список интересующую уязвимость, нуждающуюся в дальнейшей обработке;

2. справочник CAPEC

3. построение связей (Рисунок 4.17);

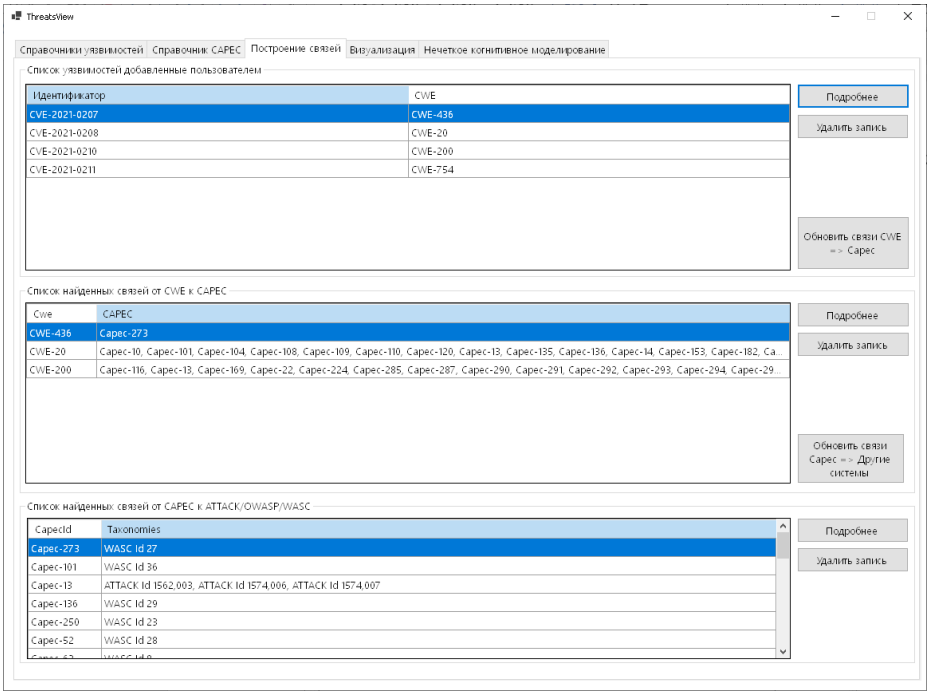


Рисунок 4.17 – Экранная форма «Построение связей»

Пользователю предоставляется возможность удаления выявленных связей, а также возможность повторного просмотра актуальной информации о CVE/BDU, CWE, CAPEC. Экранная форма «Визуализация» представлена на рисунке 4.18.

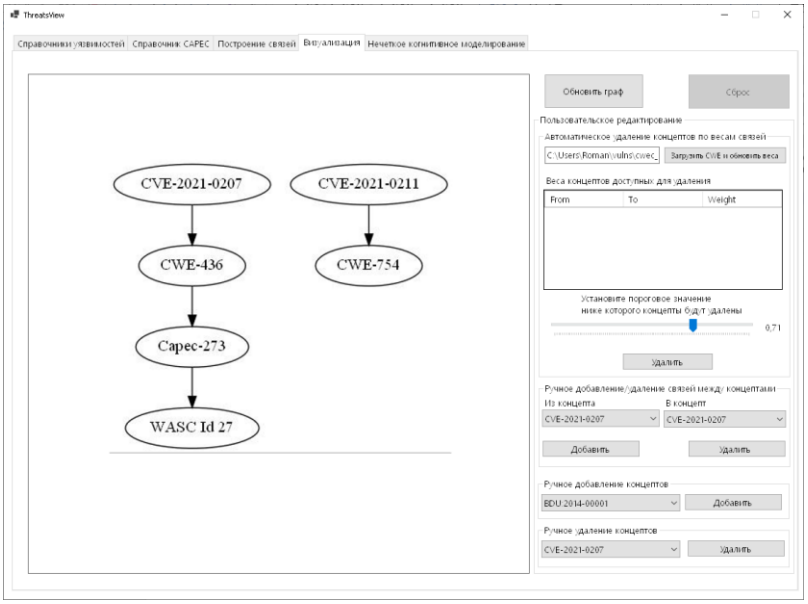


Рисунок 4.18 – Экранная форма «Визуализация»

Графический интерфейс подсистемы когнитивного моделирования состоит из окна визуализации графа и двух вкладок, позволяющим работать с построением НКК (Рисунок 4.19). Пользователю предоставляется возможность построения графа НКК

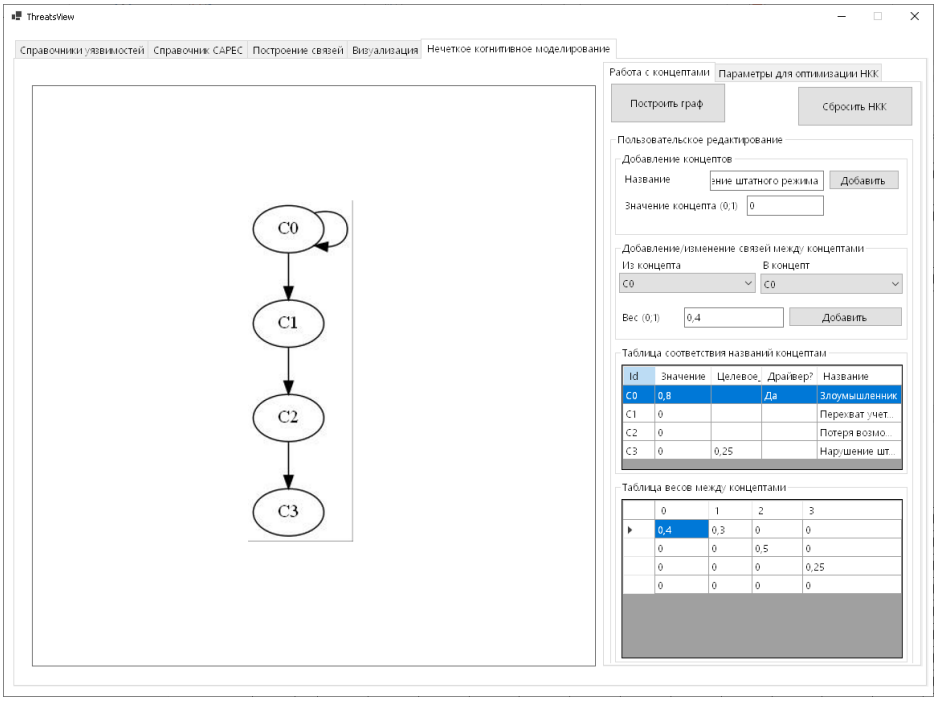


Рисунок 4.19 – Экранная форма «Нечеткое когнитивное моделирование»

Таким образом, разработанное программное обеспечение подсистем ИСППР позволяет выполнять:

– поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак, что позволяет специалистам, зная конкретные уязвимости объекта, получить наглядную графовую модель реализации атаки (свидетельство о регистрации ПО № 2021615069) [106];

– анализ сценариев атак с требуемым уровнем детализации и оптимизации весовых коэффициентов НКК при помощи методов машинного обучения для распределения ресурсов контрмер (свидетельство о регистрации ПО № 2021619894) [104].

4.4 Оценка эффективности применения инструментальных средств автоматизации моделирования сценариев реализации атак с последующей оценкой рисков ИБ на примере АСУ ТП пункта сдачи приема нефти

4.4.1. Обобщенная структурная схема территориально распределенной системы обустройства месторождения и транспорта товарной нефти

В качестве исследуемого объекта защиты рассматривается АСУ ТП нефтедобывающего предприятия, интегрированная в комплексную систему оперативного контроля и управления в реальном масштабе времени, и позволяющая передавать накапливаемые технологические данные в системы управления производственными процессами вышележащих уровней (Приложение З). Технологическая цепочка включает основные элементы: добыча нефти, сбор нефти, подготовка нефти, транспортировка товарной нефти [34, 112].

Обобщенная структурная схема территориально распределенной системы обустройства месторождения и транспорта товарной нефти (ТТН), представлена на рисунке 4.20, где: АГЗУ – автоматическая групповая замерная установка; ДНС – дожимная насосная станция; НПС – нефтеперекачивающая станция; ГСС – газосборная сеть; ПСП – приемо-сдаточный пункт; УПН – установка подготовки нефти; УПСВ – установка предварительного сбора воды; ЦПС – центральный пункт сбора; 1 – ВПТ – внутри промысловой трубопровод; ДС – добывающие скважины; НС – нагнетающая скважина; ВС – водозаборная скважина; КС – куст скважин; 2 – водовод; 3 – нефтесборный трубопровод; МН – магистральный нефтепровод; КНС – кустовая насосная станция.

Первой стадией анализа объекта защиты является создание базовой модели объекта защиты, позволяющей выделить основные виды деятельности, технологические цепочки и процессы, АСУ и прочие активы, распределенные по 5 логическим уровням.

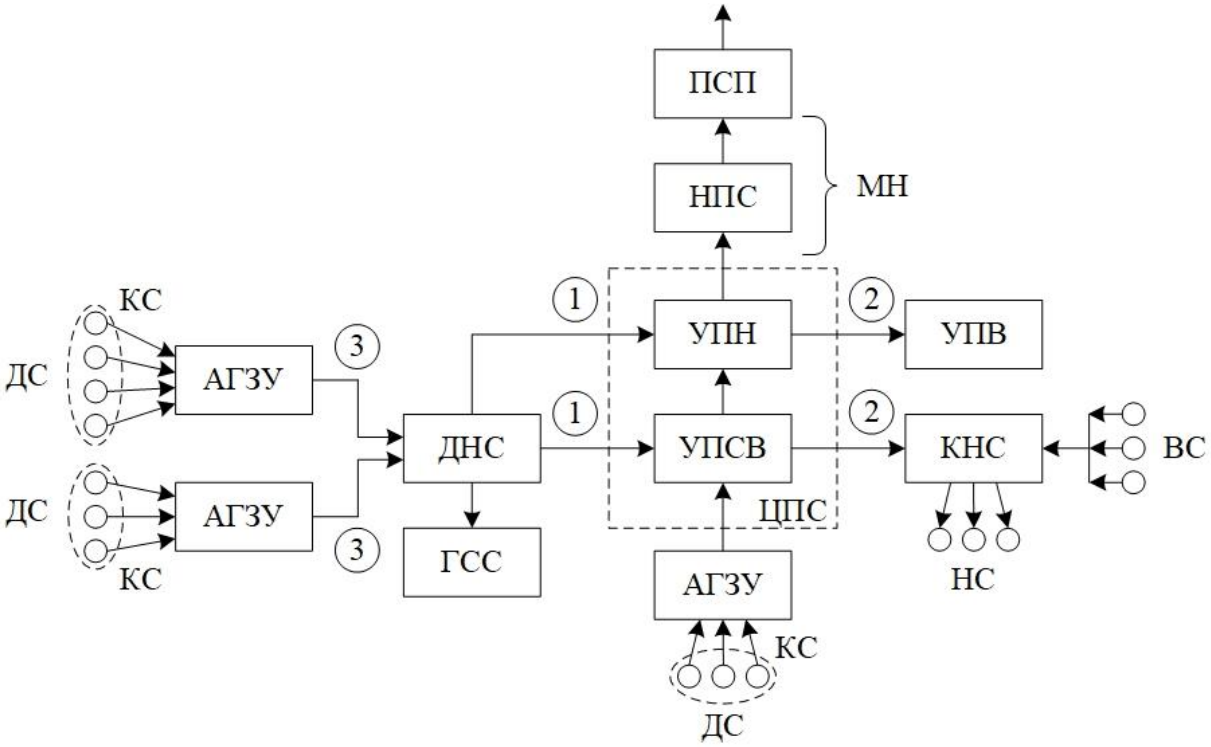


Рисунок 4.20 – Обобщенная структурная схема территориально-распределенной системы обустройства месторождения и транспорта товарной нефти

На рисунке 4.21 приведены основные ТП системы обустройства месторождения и системы ТТН.

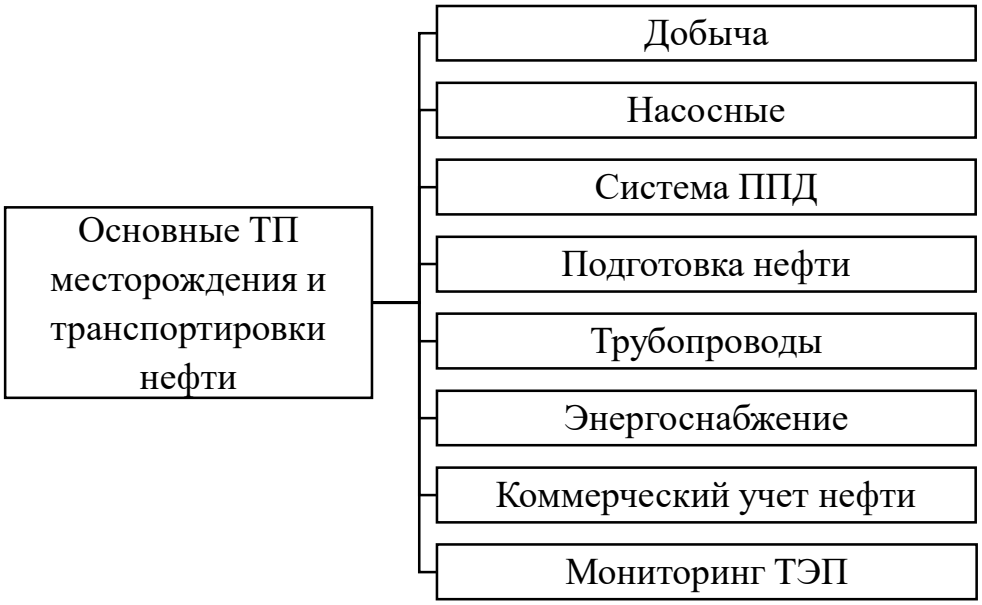


Рисунок 4.21 – Основные ТП системы обустройства месторождения и ТТН (ППД – поддержание пластового давления; ТЭП – технико-экономические показатели)

На рисунке 4.22 показана структура комплексной АСУ ТП обустройства месторождения и ТТН.

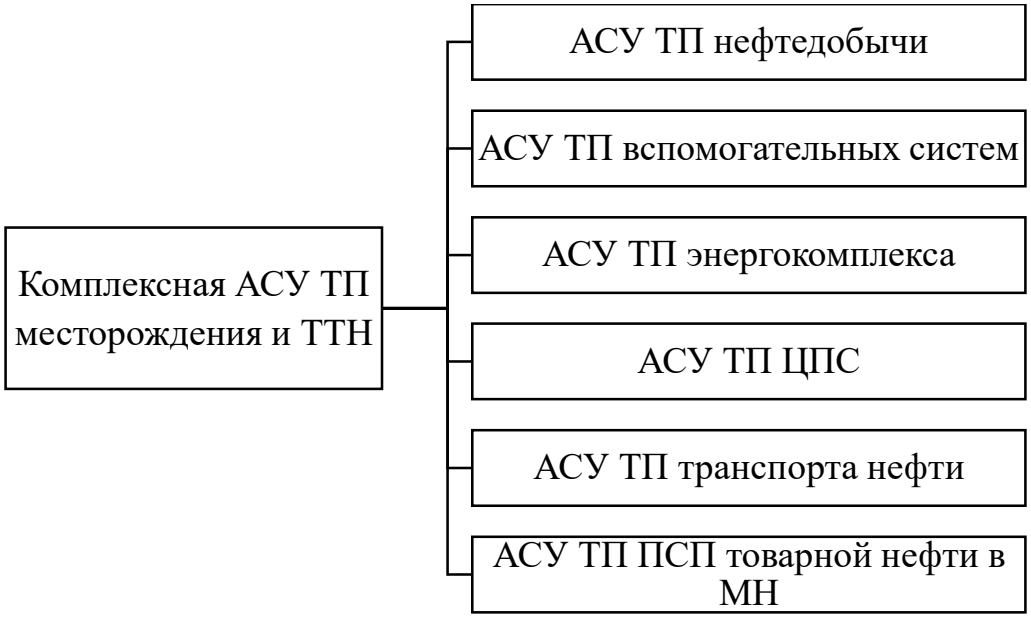


Рисунок 4.22 – Структура комплексной АСУ ТП обустройства месторождения и ТТН

На рисунке 4.23 приведена базовая модель АСУ ТП месторождения и ТТН, где КП – кустовая площадка; ПП – производственный процесс; БП – бизнес-процесс; УПГ – установка подготовки газа; ГТЭС – газовая ТЭС; ДП – диспетчерский пункт; ИМ – исполнительные механизмы; УДХ – установка дозировки химреагентов; ОУ – оперативное управление; ДОУ – диспетчерское оперативное управление

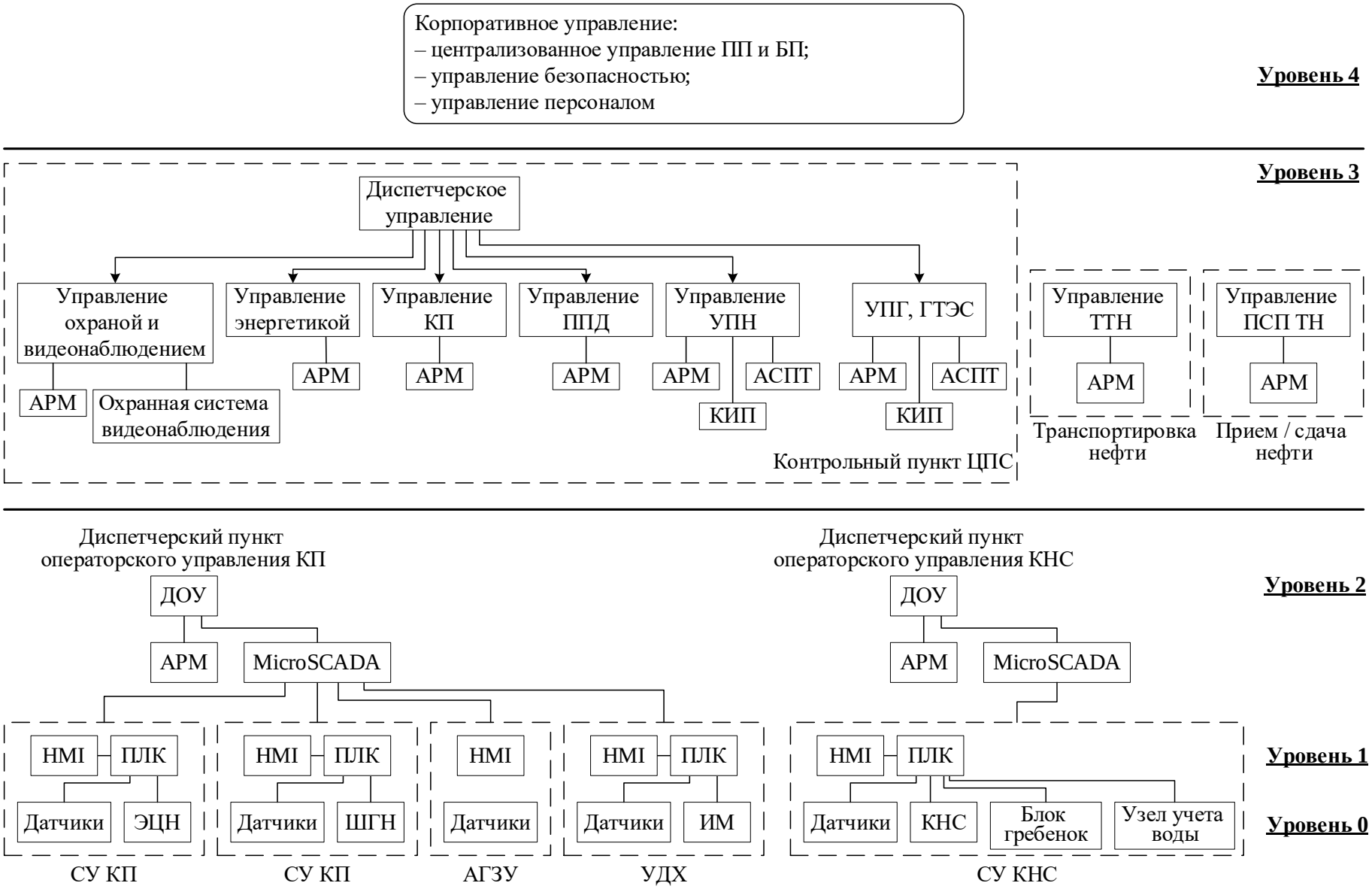


Рисунок 4.23 – Базовая модель АСУ ТП месторождения и ТТН

Подсистемы АСУ ТП месторождения можно рассматривать как отдельные зоны безопасности, объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации.

Модель архитектуры АСУ ТП месторождения и ТТН представлена на рисунке 4.24.

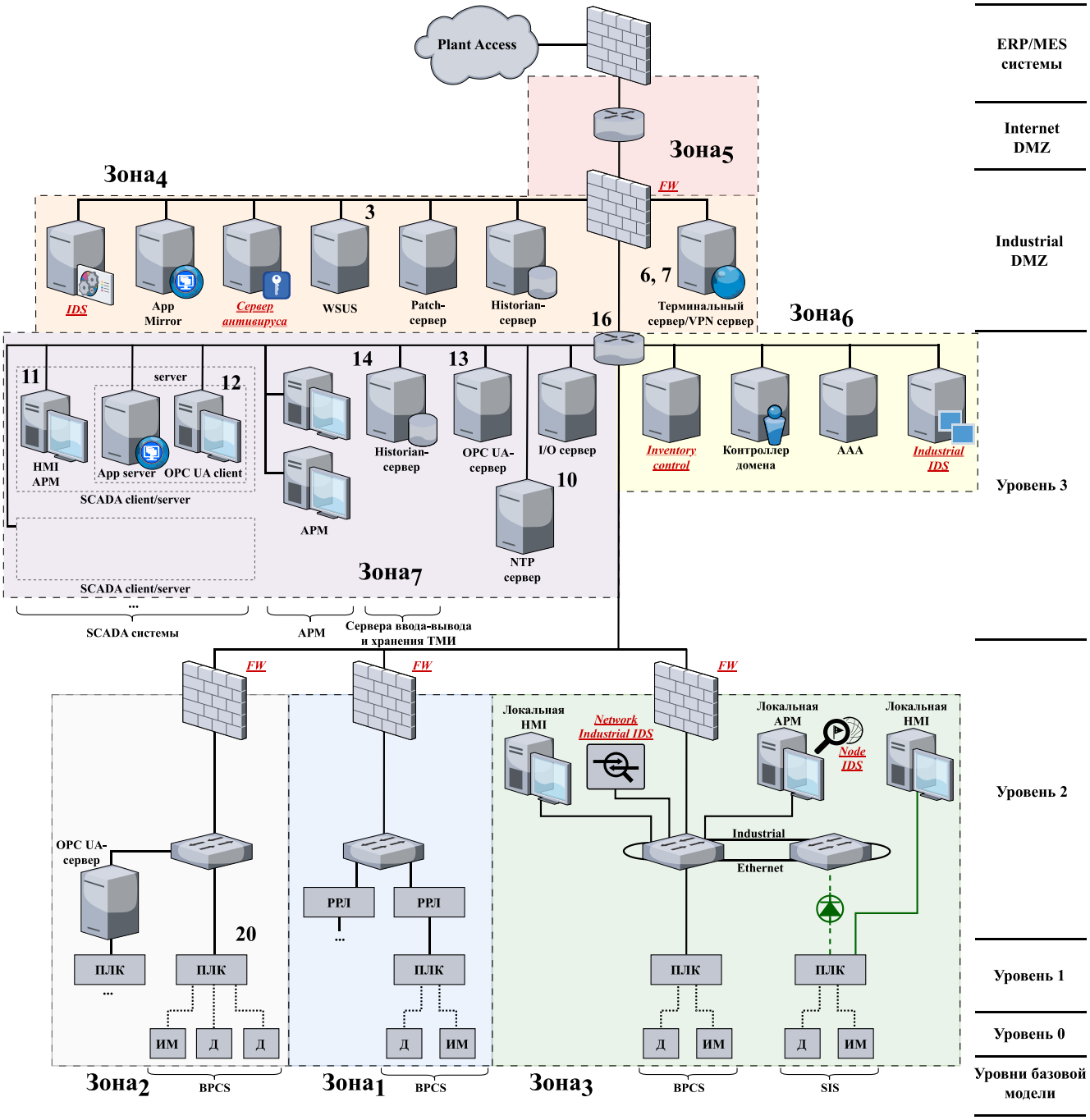


Рисунок 4.24 – Модель архитектуры АСУ ТП месторождения и ТТН (SIS – safety instrumented system – часть ICS; ICS – industrial control system; BPCS – basic process control system; BPCS + SIS = ICS)

4.4.2. АСУ ТП станции управления скважинным насосным оборудованием (Зона$_1$)

Процесс добычи нефти на площадке скважины заключается в подъеме нефти из скважины погружным насосным оборудованием (ЭЦН, ШГН). Продукция добывающей скважины поступает в автоматизированную групповую замерную установку (АГЗУ), расположенную на другой кустовой площадке.

На рисунке 4.25 и 4.26 представлена архитектура АСУ ТП станции управления скважинным насосным оборудованием, где РРЛ – радиорелейная линия связи; КП – кустовая площадка; ВОЛС – волоконно-оптическая линия связи; МХ – мультиплексор; КУЭ – коммерческий учет электроэнергии; БШД – беспроводной широкополосный доступ; СУ – станция управления; ЭЦН – электроцентробежный насос; ШГН – штанговый глубинный насос.

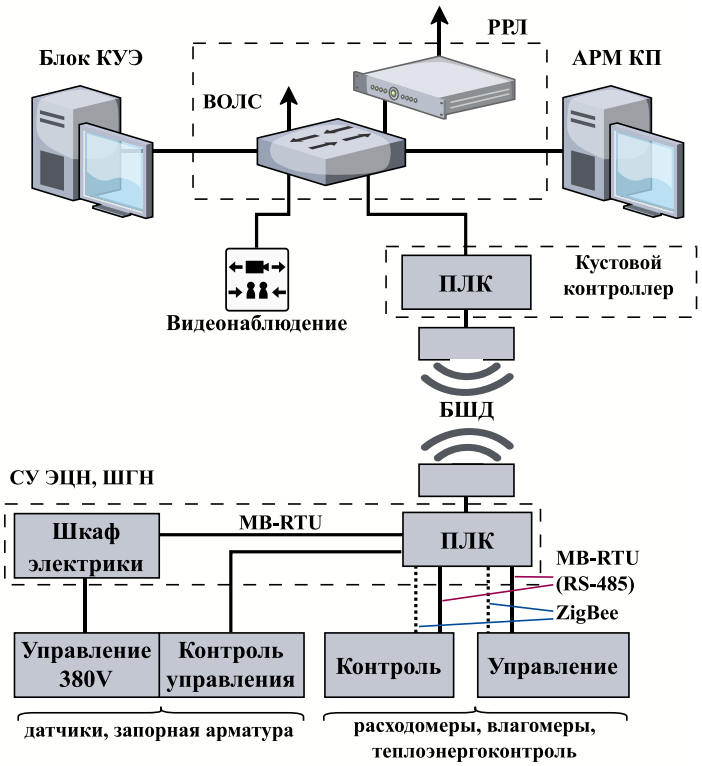


Рисунок 4.25 – АСУ ТП станции управления скважинным насосным оборудованием (Зона$_1$)

Оборудование нижнего уровня: датчик усилия; датчик угла поворота кривошипа; датчик уровня; расходомер; датчик протечек (группа датчиков); датчик давления; датчик температуры; датчик устьевого давления; датчик затрубного

давления; датчик угла поворота ротора электропривода; датчик-ваттметрографа; газоанализатор.

Оборудование среднего уровня: станция управления скважины: СУ «Электон-04» или «Борец-04»; кустовой контроллер телемеханики: СТМ-ZK2.91 («Интротест»); система широкополосного беспроводного доступа: Motorola Canopy T60-2400SMDD; коммутатор: EDS-G205A-4PoE («Моха») или Cisco WS-C3560C-8PC-S (Cisco); IP-камера Proline IP-WC2415PTZ4 POE производителя «Proline» или Hikvision DS-2CD4A26FWD-IZHS производителя «Hikvision».

Основные задачи АСУ ТП станции управления скважинным насосным оборудованием:

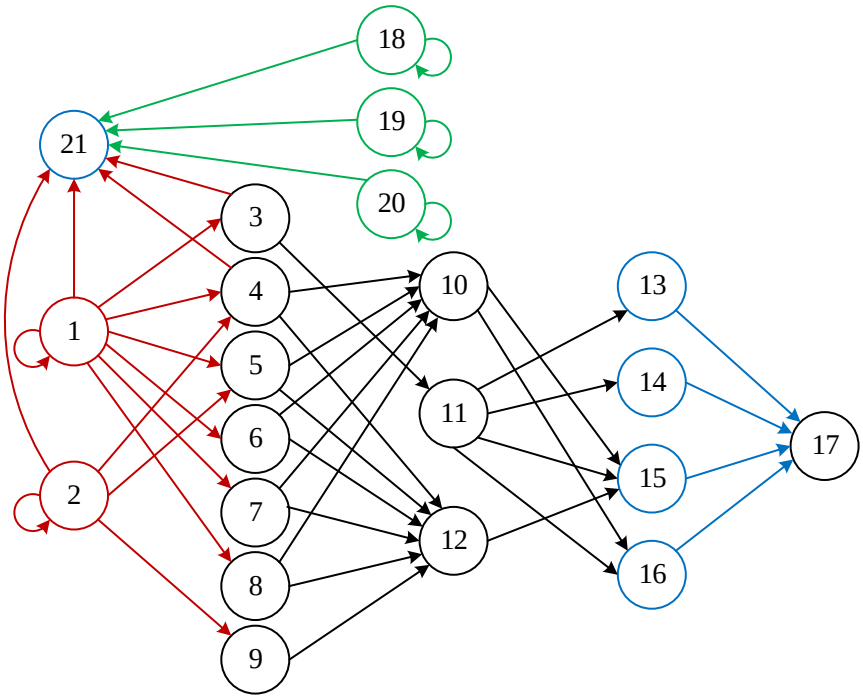
– управление насосным оборудованием;

– мониторинг работы оборудования;

– учет производственных показателей.

В процессе моделирования сценариев реализации атак на выделенную зону построена НСКК, приведенная на рисунке 4.26.

Выделенные концепты НСКК приведены в таблице 4.6.



Нарушитель (источник угрозы)	Сценарий атаки	Активы (целевые объекты атаки)	Последствия	Оценка рисков ИБ

Рисунок 4.26 – НКК СУ ЭЦН, ШГН

Таблица 4.6 – Описание концептов НКК СУ ЭЦН, ШГН

Концепт	Описание
C_1	Внешний нарушитель
C_2	Внутренний нарушитель
C_3	Сценарий реализации угрозы УБИ.204: Угроза несанкционированного изменения вредоносной программой значений параметров ПЛК. Реализует внешний нарушитель со средним потенциалом
C_4	Сценарий реализации угрозы УБИ.107: Угроза отключения контрольных датчиков. Реализует внешний нарушитель с высоким потенциалом и внутренний нарушитель с низким потенциалом
C_5	Сценарий реализации угрозы УБИ.011: Угроза деавторизации санкционированного клиента беспроводной сети. Реализует внешний и внутренний нарушители с низким потенциалом
C_6	Сценарий реализации угрозы УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам. Реализует внешний нарушитель с низким потенциалом
C_7	Сценарий реализации угрозы УБИ.125: Угроза подключения к беспроводной сети в обход процедуры аутентификации. Реализует внешний нарушитель с низким потенциалом
C_8	Сценарий реализации угрозы УБИ.126: Угроза подмены беспроводного клиента или точки доступа. Реализует внешний нарушитель с низким потенциалом
C_9	Сценарий реализации угрозы УБИ.184: Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства. Реализует внутренний нарушитель со средним потенциалом
C_{10}	Беспроводные датчики WSN
C_{11}	ПЛК
C_{12}	Устройство БШД
C_{13}	Блокировка системы противоаварийной защиты
C_{14}	Блокировка системы автоматического пожаротушения
C_{15}	Потеря возможности мониторинга
C_{16}	Перевод объекта в аварийный режим
C_{17}	Оценка рисков ИБ в Зоне$_1$[1]
C_{18}	Штатные / встроенные СЗИ (и принятые контрмеры)
C_{19}	Предлагаемые контрмеры (ручное распределение ресурсов СЗИ)
C_{20}	Предлагаемые контрмеры (автоматическое распределение ресурсов СЗИ с помощью ГА)
C_{21}	Оценка эффективности

Соответствующие весовые коэффициенты НКК описаны в таблице 4.7.

Таблица 4.7 – Веса связей концептов НКК СУ ЭЦН, ШГН

Вес связи	Диапазон	Вес связи	Диапазон
$W_{1\text{-}1}$	[;]	$W_{6\text{-}12}$	(0,85; 1]
$W_{1\text{-}3}$	(0,35; 0,6]	$W_{7\text{-}10}$	(0,85; 1]
$W_{1\text{-}4}$	(0,15; 0,35]	$W_{7\text{-}12}$	(0,85; 1]
$W_{1\text{-}5}$	(0,6; 0,85]	$W_{8\text{-}10}$	(0,6; 0,85]
$W_{1\text{-}6}$	(0,6; 0,85]	$W_{8\text{-}12}$	(0,6; 0,85]
$W_{1\text{-}7}$	(0,6; 0,85]	$W_{9\text{-}12}$	(0,15; 0,35]
$W_{1\text{-}8}$	(0,6; 0,85]	$W_{10\text{-}15}$	[;]
$W_{2\text{-}2}$	[;]	$W_{10\text{-}16}$	[;]
$W_{2\text{-}4}$	(0,85; 1]	$W_{11\text{-}13}$	[;]
$W_{2\text{-}5}$	(0,85; 1]	$W_{11\text{-}14}$	[;]
$W_{2\text{-}9}$	(0,6; 0,85]	$W_{11\text{-}15}$	[;]
$W_{3\text{-}11}$	(0,35; 0,6]	$W_{11\text{-}16}$	[;]
$W_{4\text{-}10}$	(0,85; 1]	$W_{12\text{-}15}$	[;]
$W_{4\text{-}12}$	(0,85; 1]	$W_{13\text{-}17}$	(0,35; 0,6]
$W_{5\text{-}10}$	(0,6; 0,85]	$W_{14\text{-}17}$	(0,35; 0,6]
$W_{5\text{-}12}$	(0,6; 0,85]	$W_{15\text{-}17}$	(0,35; 0,6]
$W_{6\text{-}10}$	(0,85; 1]	$W_{16\text{-}17}$	(0,6; 0,85]

На рисунке 4.27 и 4.28 представлена архитектура АСУ ТП СУ скважинным насосным оборудованием (уровень 2), соответствующая НСКК и таблицам 4.8 и 4.9 с описанием концептов и весовыми коэффициентами соответственно.

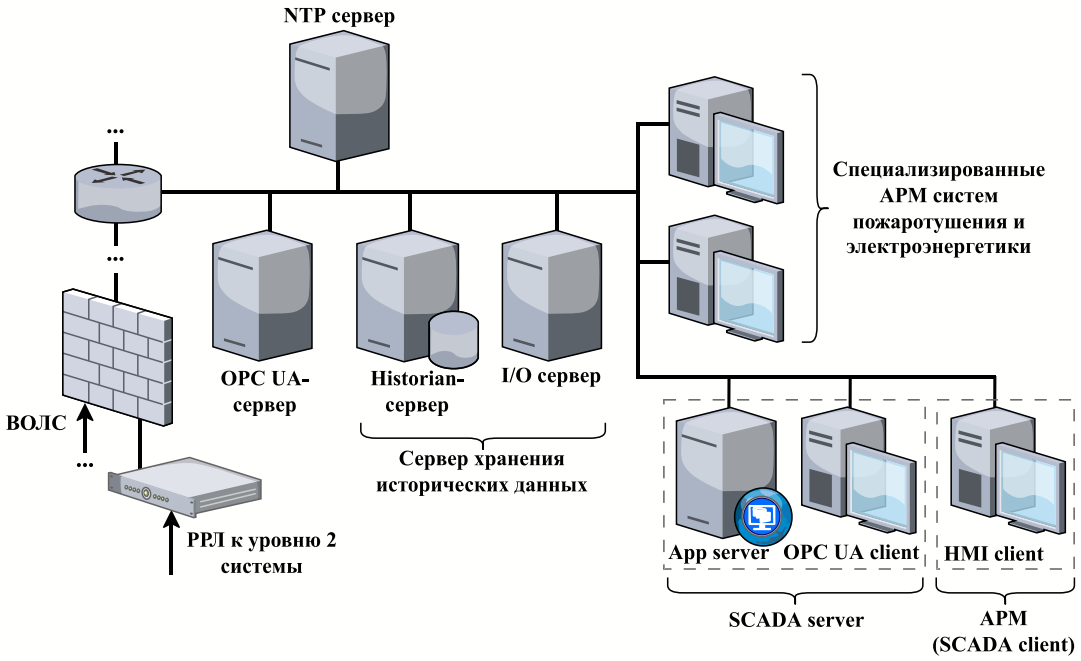


Рисунок 4.27 – Часть АСУ ТП СУ скважинным насосным оборудованием (уровень 2)

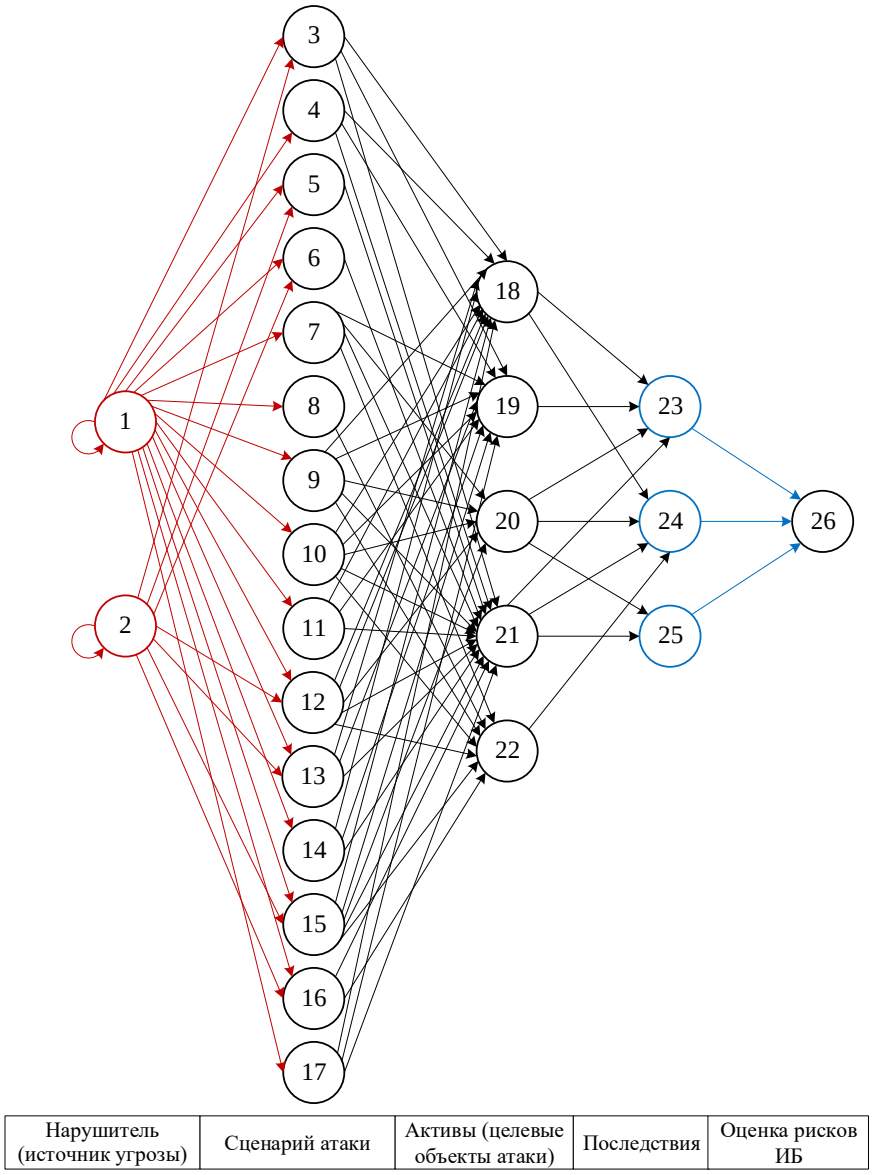


Рисунок 4.28 – НКК части АСУ ТП СУ скважинным насосным оборудованием (уровень 2)

Таблица 4.8 – Описание концептов части АСУ ТП СУ скважинным насосным оборудованием

Концепт	Описание
C_1	Внешний нарушитель
C_2	Внутренний нарушитель
C_3	Сценарий реализации угрозы УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными. Реализует внешний и внутренний нарушители с низким потенциалом

Концепт	Описание
C_4	Сценарий реализации угрозы УБИ.069: Угроза неправомерных действий в каналах связи. Реализует внешний нарушитель с низким потенциалом
C_5	Сценарий реализации угрозы УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети. Реализует внешний и внутренний нарушители со средним потенциалом
C_6	Сценарий реализации угрозы УБИ.080: Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети. Реализует внешний и внутренний нарушители со средним потенциалом
C_7	Сценарий реализации угрозы УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб. Реализует внешний нарушитель с низким потенциалом
C_8	Сценарий реализации угрозы УБИ.099: Угроза обнаружения хостов. Реализует внешний нарушитель с низким потенциалом
C_9	Сценарий реализации угрозы УБИ.103: Угроза определения типов объектов защиты. Реализует внешний нарушитель с низким потенциалом
C_{10}	Сценарий реализации угрозы УБИ.104: Угроза определения топологии вычислительной сети. Реализует внешний нарушитель с низким потенциалом
C_{11}	Сценарий реализации угрозы УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети. Реализует внешний нарушитель с низким потенциалом
C_{12}	Сценарий реализации угрозы УБИ.178: Угроза несанкционированного использования системных и сетевых утилит. Реализует внешний и внутренний нарушители с низким потенциалом
C_{13}	Сценарий реализации угрозы УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании». Реализует внешний и внутренний нарушители с низким потенциалом
C_{14}	Сценарий реализации угрозы УБИ.130: Угроза подмены содержимого сетевых ресурсов. Реализует внешний нарушитель с низким потенциалом
C_{15}	Сценарий реализации угрозы УБИ.145: Угроза пропуска проверки целостности программного обеспечения. Реализует внешний и внутренний нарушители с низким потенциалом
C_{16}	Сценарий реализации угрозы УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами. Реализует внешний нарушитель с

Концепт	Описание
	низким потенциалом и внутренний нарушитель со средним потенциалом
C_{17}	Сценарий реализации угрозы УБИ.193: Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика. Реализует внешний нарушитель со средним потенциалом
C_{18}	Сервер NTP
C_{19}	Historian-сервер
C_{20}	АРМ
C_{21}	App-сервер
C_{22}	АРМ SCADA client
C_{23}	Потеря возможности мониторинга
C_{24}	Перевод объекта в аварийный режим
C_{25}	Останов КП
C_{26}	Оценка рисков ИБ в Зоне$_3$[1]

Таблица 4.9 – Веса связей концептов НКК части АСУ ТП СУ скважинным насосным оборудованием

Вес связи	Диапазон	Вес связи	Диапазон
$W_{1\text{-}1}$	[;]	$W_{10\text{-}18}$	(0,15; 0,35]
$W_{1\text{-}3}$	(0,6; 0,85]	$W_{10\text{-}19}$	(0,15; 0,35]
$W_{1\text{-}4}$	(0,6; 0,85]	$W_{10\text{-}20}$	(0,15; 0,35]
$W_{1\text{-}5}$	(0,35; 0,6]	$W_{10\text{-}21}$	(0,15; 0,35]
$W_{1\text{-}6}$	(0,35; 0,6]	$W_{10\text{-}22}$	(0,15; 0,35]
$W_{1\text{-}7}$	(0,6; 0,85]	$W_{11\text{-}18}$	(0,15; 0,35]
$W_{1\text{-}8}$	(0,6; 0,85]	$W_{11\text{-}19}$	(0,15; 0,35]
$W_{1\text{-}9}$	(0,6; 0,85]	$W_{11\text{-}21}$	(0,15; 0,35]
$W_{1\text{-}10}$	(0,6; 0,85]	$W_{12\text{-}18}$	(0,85; 1]
$W_{1\text{-}11}$	(0,6; 0,85]	$W_{12\text{-}19}$	(0,85; 1]
$W_{1\text{-}12}$	(0,6; 0,85]	$W_{12\text{-}20}$	(0,85; 1]
$W_{1\text{-}13}$	(0,6; 0,85]	$W_{12\text{-}21}$	(0,85; 1]
$W_{1\text{-}14}$	(0,6; 0,85]	$W_{12\text{-}22}$	(0,85; 1]
$W_{1\text{-}15}$	(0,6; 0,85]	$W_{13\text{-}18}$	(0,6; 0,85]
$W_{1\text{-}16}$	(0,6; 0,85]	$W_{13\text{-}19}$	(0,6; 0,85]
$W_{1\text{-}17}$	(0,35; 0,6]	$W_{13\text{-}21}$	(0,6; 0,85]
$W_{2\text{-}2}$	[;]	$W_{14\text{-}18}$	(0,15; 0,35]
$W_{2\text{-}3}$	(0,85; 1]	$W_{14\text{-}19}$	(0,15; 0,35]
$W_{2\text{-}5}$	(0,6; 0,85]	$W_{14\text{-}21}$	(0,15; 0,35]
$W_{2\text{-}6}$	(0,6; 0,85]	$W_{15\text{-}18}$	(0,85; 1]
$W_{2\text{-}12}$	(0,85; 1]	$W_{15\text{-}19}$	(0,85; 1]
$W_{2\text{-}13}$	(0,85; 1]	$W_{15\text{-}20}$	(0,85; 1]

Вес связи	Диапазон	Вес связи	Диапазон
$W_{2\text{-}15}$	(0,85; 1]	$W_{15\text{-}21}$	(0,85; 1]
$W_{2\text{-}16}$	(0,6; 0,85]	$W_{15\text{-}22}$	(0,85; 1]
$W_{3\text{-}18}$	(0,85; 1]	$W_{16\text{-}21}$	(0,85; 1]
$W_{3\text{-}19}$	(0,85; 1]	$W_{16\text{-}22}$	(0,85; 1]
$W_{3\text{-}21}$	(0,85; 1]	$W_{17\text{-}18}$	(0,15; 0,35]
$W_{4\text{-}18}$	(0,35; 0,6]	$W_{17\text{-}19}$	(0,15; 0,35]
$W_{4\text{-}19}$	(0,35; 0,6]	$W_{17\text{-}21}$	(0,15; 0,35]
$W_{4\text{-}21}$	(0,35; 0,6]	$W_{18\text{-}23}$	[;]
$W_{5\text{-}21}$	(0,85; 1]	$W_{18\text{-}24}$	[;]
$W_{6\text{-}21}$	(0,85; 1]	$W_{19\text{-}23}$	[;]
$W_{7\text{-}19}$	(0,15; 0,35]	$W_{20\text{-}23}$	[;]
$W_{7\text{-}20}$	(0,15; 0,35]	$W_{20\text{-}24}$	[;]
$W_{7\text{-}21}$	(0,15; 0,35]	$W_{20\text{-}25}$	[;]
$W_{7\text{-}22}$	(0,15; 0,35]	$W_{21\text{-}23}$	[;]
$W_{8\text{-}22}$	(0,15; 0,35]	$W_{21\text{-}24}$	[;]
$W_{9\text{-}18}$	(0,15; 0,35]	$W_{21\text{-}25}$	[;]
$W_{9\text{-}19}$	(0,15; 0,35]	$W_{22\text{-}24}$	[;]
$W_{9\text{-}20}$	(0,15; 0,35]	$W_{23\text{-}26}$	(0,35; 0,6]
$W_{9\text{-}21}$	(0,15; 0,35]	$W_{24\text{-}26}$	(0,6; 0,85]
$W_{9\text{-}22}$	(0,15; 0,35]	$W_{25\text{-}26}$	(0,85; 1]

На рисунке 4.29 представлен фрагмент сценарного уровня, раскрывающий цепочку «уязвимость-слабость-шаблон» для одной выбранной уязвимости «CVE-2019-6812», сформированный с помощью запроса на языке Cypher:

```
MATCH (cve:CVE)-[:Problem_Type]-(cwe:CWE)-[:RelatedAttackPattern]-(capec:CAPEC)
MATCH (cve:CVE)-[:Problem_Type]-(cwe:CWE)-[:hasMitigation]-(mitigation:Mitigation)
WHERE (cve.Name starts with ("CVE-2019-6812"))
RETURN  cve, cwe, capec, mitigation
```

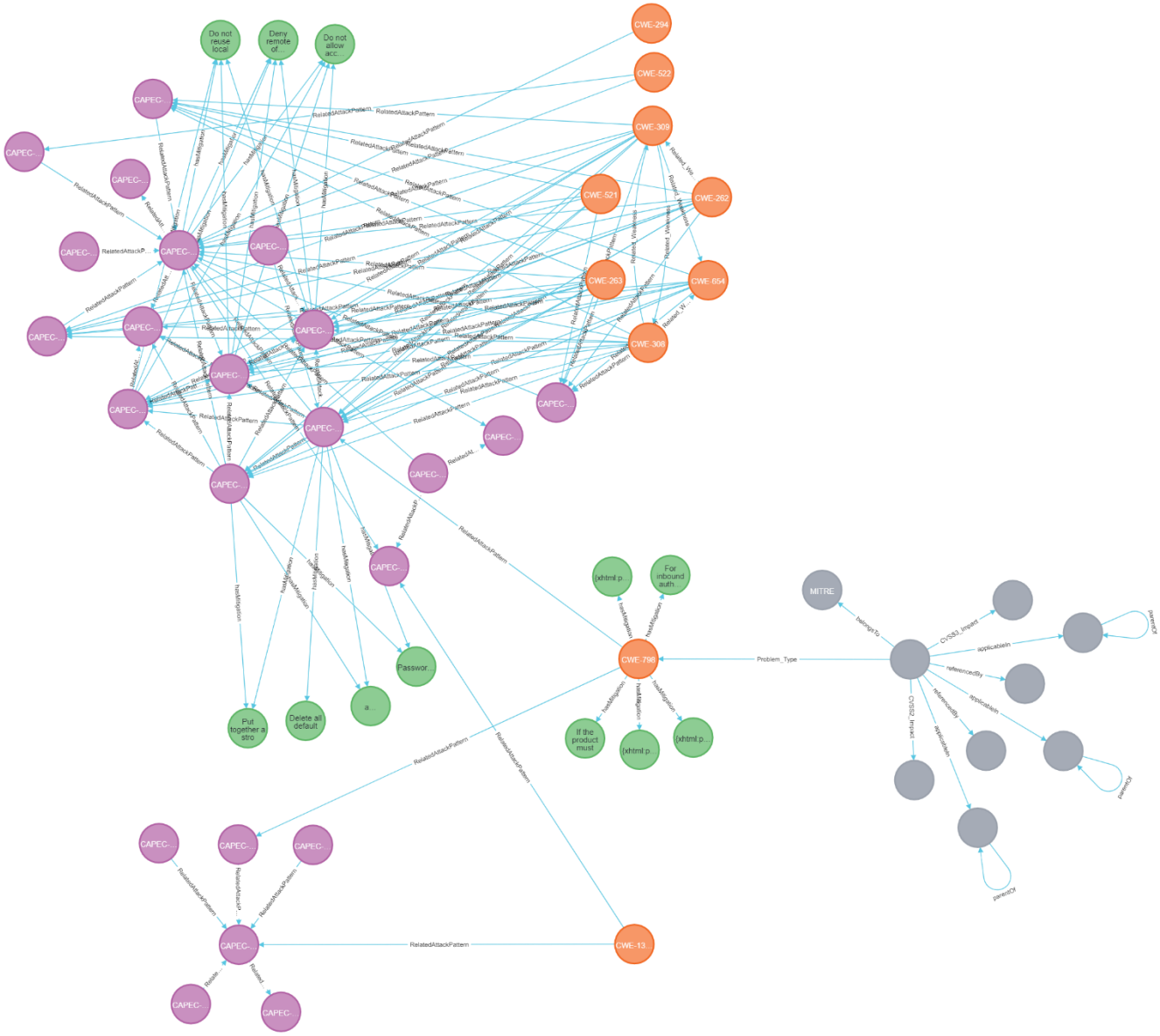


Рисунок 4.29 – Фрагмент сценарного уровня, раскрывающий цепочку «уязвимость-слабость-шаблон» для одной выбранной уязвимости «CVE-2019-6812»

С помощью описанных в главе 3 механизмов сворачивания НКК получена укрупнённая когнитивная модель оценки рисков ИБ на основе композиции зональных моделей для объекта защиты в целом (Рисунок 4.30), где: зона 1 – АСУ ТП станции управления скважинным насосным оборудованием; зона 2 – АСУ ТП установки подготовки нефти / сбора воды; зона 3 – АСУ ТП пункта сдачи-приема нефти; зона 4 – промышленная демилитаризованная зона; зона 5 – зона организации удаленного доступа к элементам и подсистемам АСУ ТП; зона 6 – зона

авторизации, аутентификации и учета сети уровня управления; зона 7 – АСУ ТП станции управления скважинным насосным оборудованием.

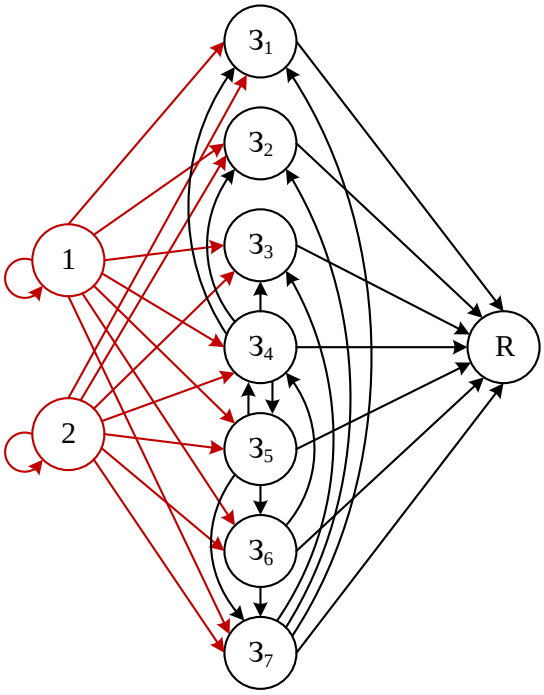


Рисунок 4.30 – Укрупненная когнитивная модель оценки рисков ИБ для АСУ ТП на основе композиции зональных моделей

Концепты C_1 и C_2 описывают, соответственно, внутреннего и внешнего нарушителей. Для каждой из зон с помощью соответствующей НСКК получена укрупненная до единственного концепта величина, характеризующая оценку риска ИБ. Итоговая количественная оценка риска ИБ для промышленного объекта рассматривается как значение концепта R с учетом взаимовлияния оценок, полученных для каждой из отдельных зон.

Установившееся значение концепта E для локальных НКК соответствующих зон характеризует оценку эффективности применения контрмер, раскрывающую нормированную в диапазон [0; 1] оценку затрат на реализацию мер по снижению рисков ИБ. Оценка затрат выполняется путем определения перечня характеристик интеграции и последующего сопровождения контрмер для рассматриваемой зоны:

– стоимость контрмер;

– простота эксплуатации и сопровождения;

– стоимость сопровождения контрмер

– степень влияния на штатное функционирование

– фактор импортозамещения;

– оперативность реагирования контрмер.

Проведено три сценария моделирования:

– **A**: применены штатные СЗИ, предусмотренные текущей архитектурой объекта защиты;

– **B**: дополнительные контрмеры выбраны на основе рекомендаций ИСППР сценарного уровня моделирования (концепты Mitigation для CWE, CAPEC, ATT&CK Tackt | Tech);

– **C**: выполнена оптимизация ресурсов выбранных контрмер с помощью ГА;

На рисунке 4.31 представлена сравнительная диаграмма оценки риска ИБ для объекта в целом в виде интервального серого числа для каждого из рассмотренных сценариев.

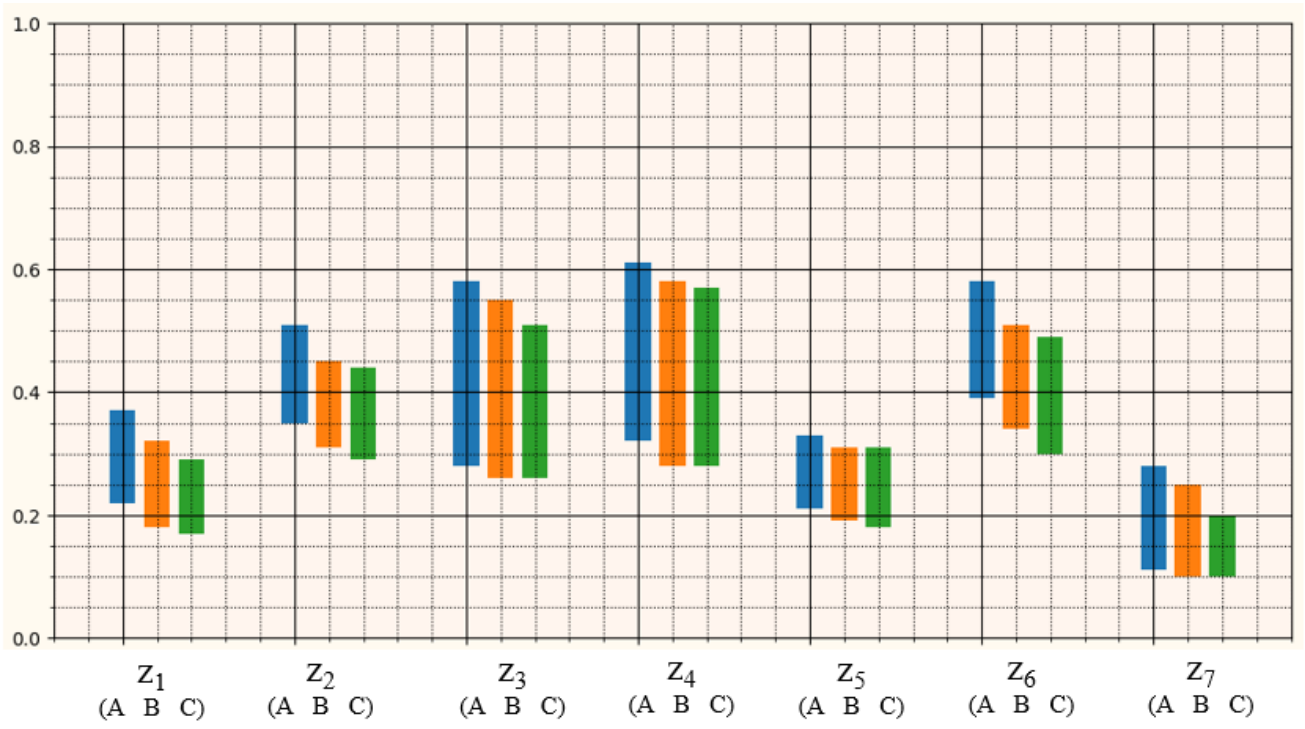


Рисунок 4.31 – Сравнительная диаграмма оценки риска ИБ для объекта в целом в виде серого числа для каждого из рассмотренных сценариев A, B, C (по оси абсцисс – номера зон, по оси ординат – оценка риска ИБ)

Оценка риска ИБ (R) для объекта в целом и оценка эффективности применения контрмер (E) в виде серых чисел для каждого из рассмотренных сценариев A, B, C представлена в таблице 4.10.

Таблица 4.10 – Оценка риска ИБ (R) для объекта в целом и оценка эффективности применения контрмер (E) в виде серых чисел для сценариев A, B, C

Сценарий	Концепт	Зона 1	Зона 2	Зона 3	Зона 4	Зона 5	Зона 6	Зона 7	ИТОГ
A	R_L	0,22	0,35	0,28	0,32	0,21	0,39	0,11	0,15
	R_U	0,37	0,51	0,58	0,61	0,33	0,58	0,28	0,63
	E_L	0,34	0,46	0,38	0,45	0,29	0,43	0,25	
	E_U	0,53	0,67	0,55	0,72	0,51	0,67	0,58	
B	R_L	0,18	0,31	0,26	0,28	0,19	0,34	0,1	0,16
	R_U	0,32	0,45	0,55	0,58	0,31	0,51	0,25	0,52
	E_L	0,4	0,51	0,45	0,52	0,33	0,5	0,31	
	E_U	0,58	0,71	0,61	0,78	0,57	0,72	0,64	
C	R_L	0,17	0,29	0,26	0,28	0,18	0,3	0,1	0,09
	R_U	0,29	0,44	0,51	0,57	0,31	0,49	0,2	0,5
	E_L	0,43	0,51	0,49	0,59	0,39	0,54	0,32	
	E_U	0,62	0,73	0,68	0,83	0,62	0,72	0,64	

На рисунке 4.32 представлена сравнительная диаграмма оценки эффективности применения контрмер для объекта в целом в виде серого числа для каждого из рассмотренных сценариев A, B, C.

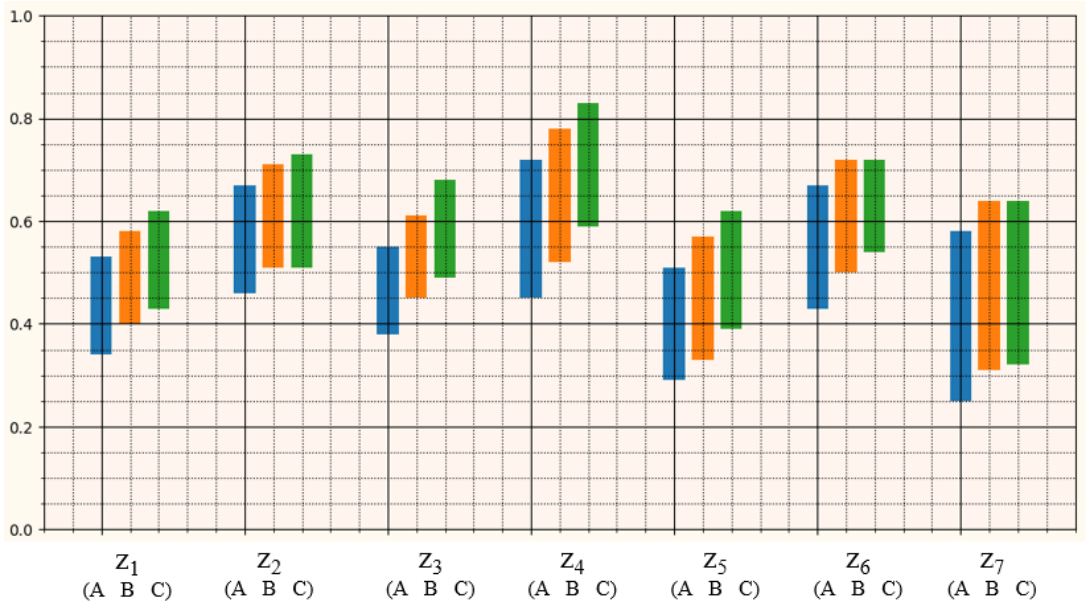


Рисунок 4.32 – Сравнительная диаграмма оценки эффективности применения контрмер для сценариев A, B, C (по оси абсцисс – номера зон, по оси ординат – оценка эффективности)

Предложенные решения позволяют:

– сформировать расширенный список контрмер на основе базы знаний ATT&CK, NVD для каждой из выделенных зон;

– на 15 % повысить эффективность эксплуатации контрмер за счет оптимизации распределения ресурсов их применения;

– на 10 % снизить количественную оценку риска ИБ;

– в 2,5 раза ускорить процесс построения сценариев реализации актуальных угроз ИБ в ходе построения модели угроз объекта защиты за счет автоматизации этапа сценарного моделирования.

4.5 Выводы по главе

Разработаны инструментальные средства автоматизации моделирования сценариев атак нарушения ИБ АСУ ТП в составе ИСППР на этапе количественной оценки рисков ИБ АСУ ТП. Автоматизация моделирования сценариев атак позволяет извлечь информацию о слабых местах инфраструктуры, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные сценарии атак и оценить их последствия для промышленного предприятия.

Разработаны практические рекомендации применения разработанных метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач. Проведенные эксперименты показали, что на этапах проектирования и внедрения контрмер временные затраты на моделирование сценариев 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 риска ИБ для объекта защиты в целом. Предложенные решения позволяют сформировать расширенный список контрмер на основе базы знаний ATT&CK, NVD для каждой из выделенных зон.

ЗАКЛЮЧЕНИЕ

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.

Список сокращений и условных обозначений

APT	–	Advanced Persistent Threats
ATT&CK	–	Adversarial Tactics, Techniques, and Common Knowledge
CAPEC	–	Common Attack Pattern Enumeration and Classification
CPE	–	Common Platform Enumeration
CPwE	–	Conwerged Plantwide Ethernet
CVE	–	Common Vulnerabilities and Exposures
CVSS	–	Common Vulnerability Scoring System
CWE	–	Common Weakness Enumeration
DCS	–	Distributed Control System
HMI	–	Human-machine interface
ICS	–	Industrial Control System
IIoT	–	Industrial Internet of Things
IOA	–	Indicator of Attack
IOC	–	Indicator of Compromise
SCADA	–	Supervisory Control and Data Acquisition
АРМ	–	Автоматизированное рабочее место
АСУ ТП	–	автоматизированная система управления технологическим процессом
БДУ ФСТЭК	–	банка данных угроз безопасности информации ФСТЭК России
ГА	–	генетический алгоритм
ДМЗ	–	демилитаризованная зона
ИБ	–	информационная безопасность
ИСППР	–	интеллектуальная система поддержки принятия решений
КИИ	–	критическая информационная инфраструктура
Методика ФСТЭК	–	Методика оценки угроз безопасности информации ФСТЭК России
ПЛК	–	программируемый логический контроллер
ПО	–	программное обеспечение
СЗИ	–	средство защиты информации
ТП	–	технологический процесс
УБИ	–	угроза безопасности информации
НКК	–	нечеткая когнитивная карта
НСКК	–	нечеткая серая когнитивная карта
ЛПР	–	лицо, принимающее решение

Словарь терминов

возможности нарушителя: Мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя. (Методика оценки угроз безопасности информации ФСТЭК)

компьютерная атака: Целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации. (ГОСТ Р 59709-2022)

контрмера: Действие, устройство, процедура или стратегия, которые ослабляют угрозу, уязвимость или противодействуют атаке путем ее отражения или предотвращения, или минимизации ущерба, который она способна нанести, или путем ее обнаружения и сообщения о ней, чтобы могло быть предпринято корректирующее действие. (ГОСТ Р 56205-2014)

меташаблон атаки: Абстрактная характеристика конкретной методологии или техники, используемой в атаке. (CAPEC)

модель угроз: Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации (ГОСТ Р 53114-2008).

оценка рисков: Процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения, и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации контрмер с целью минимизации общей уязвимости. (ГОСТ Р 56205-2014)

риск: Это сочетание вероятности события и его последствий. (ГОСТ Р ИСО/МЭК 27000-2012)

риск информационной безопасности: Это потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации. (ГОСТ Р ИСО/МЭК 27000-2012)

сценарий реализации угрозы: Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации. (Методика оценки угроз безопасности информации ФСТЭК)

тактика: Совокупность приемов и способов действий, используемых для проведения компьютерной атаки. (ГОСТ Р 59709-2022)

техника: Совокупность и порядок действий, используемых для проведения компьютерной атаки в рамках соответствующих тактик. (ГОСТ Р 59709-2022)

угроза: Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. (ГОСТ Р 56545-2015)

уязвимость: Недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации. (Методика оценки угроз безопасности информации ФСТЭК)

Список литературы

1. ГОСТ Р 56205-2014 IEC TS 62443-1-1 2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – М.: Стандартинформ, 2014.
2. ГОСТ Р 56498-2015/IEC/PAS 62443-3:2008 Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления. – М.: Стандартинформ, 2017.
3. ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры. – М.: Стандартинформ, 2019.
4. ГОСТ Р МЭК 61784-1-2016 Промышленные сети. – М.: Стандартинформ, 2017.
5. ГОСТ Р МЭК 62264-1-2010 Интеграция систем управления предприятием. Модели и терминология. – М.: Стандартинформ, 2014.
6. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа:https://fstec.ru/component/attachments/download/2919 (дата обращения 22.09.2022).
7. ОТТ-35.240.00-КТН-010-12 АСУ ТП и ПТС Компании. Информационная безопасность. Общие технические требования. – 2020.
8. Положение ПАО НК Роснефть № ПЗ-11 Р-0012 Информационная безопасность. Автоматизированные системы управления технологическими процессами. – 2020.
9. СТО Газпром 4.2-2-002 Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами. – 2009.
10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также

объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды (утверждены приказом ФСТЭК России от 14.03.2014 № 31). – М., 2014. [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 22.09.2022).

11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25.12.2017 г. № 239). – М.: 2017. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/1880 (дата обращения 22.09.2022).
12. Федеральный закон № 187-ФЗ «О безопасности критической ин-формационной инфраструктуры Российской Федерации» от 26.07.2017 г. – [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения 20.09.2022).
13. Абрамов, Е.С. Применение графов атак для моделирования вредоносных сетевых воздействий / Е.С. Абрамов, А.В. Андреев, Д. Мордвин // Известия Южного федерального университета. Технические науки. – 2012. – Т. 126. – № 1. – С. 165–174.
14. Абрамский, М.М. Сравнительный анализ использования реляционных и графовых баз данных в разработке цифровых образовательных систем / М.М. Абрамский, Т.И. Тимерханов // Вестник НГУ. Серия: Информационные технологии. – 2018. – Т. 16. – № 4. – С. 5–12.
15. Ажмухамедов, И.М. Динамическая нечеткая когнитивная модель оценки уровня информационной безопасности информационных активов вуза / И.М. Ажмухамедов // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. – Астрахань: Изд-во АГТУ, 2012. – № 2. – С. 137–141.
16. Ажмухамедов, И.М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности /

И.М. Ажмухамедов, О.М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – №. 3 (31). – С. 24–39.

17. Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения 26.09.2022).
18. Актуальные киберугрозы: II квартал 2022 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/#id5 (дата обращения 31.01.2023).
19. Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. – 2015. – Т. 13. – №. 2. – С. 215–221.
20. Абрамова, Т.В. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья / Т.В. Абрамова, Т.З. Аралбаев // Вестник УГАТУ. – 2020. – Т. 24, № 1 (87). – С. 76–84.
21. Атаки на технологические сети [Электронный ресурс]. – Режим доступа: https://www.akylkenes.kz/ru/p/ataki-na-tehnologicheskie-seti (дата обращения 28.10.2022).
22. Аубакирова, Г.М. Цифровизация промышленности Казахстана: факторы, тенденции, перспективы / Г.М. Аубакирова, Ф.М. Исатаева // Экономика, предпринимательство и право. – 2021. – Т. 11. – №. 1. – С. 51–68.
23. Байрс, Э. Использование стандартов ANSI/ISA-99 для обеспечения безопасности системы управления промышленным предприятием / Э. Байрс // Современные технологии автоматизации. – 2014. – №. 1 – С. 6–15.
24. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/ (дата обращения 31.01.2023).
25. Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – №. 1 (9). – С. 73–79.

26. Баранова, Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 / Е.К. Баранова, А.С. Забродоцкий // Образовательные ресурсы и технологии. – 2015. – №. 2 (10). – С. 73–80.
27. Большаков, А.С. Программное обеспечение моделирования угроз безопасности информации в информационных системах / А.С. Большаков, Д.И. Раковский // Правовая информатика. – 2020. – №. 1 – С. 26–39.
28. Борисов, В.В. Нечеткие модели и сети. Монография / В.В. Борисов, В.В. Круглов, А.С. Федулов. – Москва: Горячая линия - Телеком, 2012. – 284 с.
29. Братченко, А.И. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления / А.И. Братченко, И.В. Бутусов, А.М. Кобелян, А.А. Романов // Вопросы кибербезопасности. –2019. – № 1 (29). – С. 18–24.
30. Булдакова, Т.И. Методика анализа информационных рисков с применением нейро-нечеткой сети / Т.И. Булдакова, Д.А. Миков // НТИ. Сер. 2. Информационные процессы и системы. – 2015. – № 4. – С. 13–17.
31. Васильев, В.И. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования / В.И. Васильев, А.М. Вульфин, Р.Т. Кудрявцева // Доклады ТУСУР, Томск. – 2017. – Т. 20. – № 4. – С. 61–66.
32. Васильев, В.И. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – №. 2 (37). – С. 1–18.
33. Васильев, В.И. Анализ рисков инновационных проектов с использованием технологии многослойных не четких когнитивных карт / В.И. Васильев, А.М. Вульфин, Л.Р. Черняховская // Программная инженерия. – 2020. – № 3 (11). – С. 142–151.

34. Васильев, В.И. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт / В.И. Васильев, А.М. Вульфин, И.Б. Герасимова, В.М. Картак // Вопросы кибербезопасности. – 2020. – №. 2 (36). – С. 11–21.
35. Васильев, В.И. 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 Уфимского государственного авиационного технического университета. – 2019. – Т. 23. – №. 4 (86). – С. 122–131.
36. Васильев, В.И. 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.
37. Васильев, В.И. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) / В.И. Васильев, А.Д. Кириллова, С.Н. Кухарев // Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 4 (30). – С. 66–74.
38. Васильев, В.И. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова // Вопросы кибербезопасности. – 2021. – № 2 (42). – С. 2–16.
39. Васильев, В.И. 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.
40. Васильев, В.И. 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.
41. Васильев, В.И. Методика оценки рисков кибербезопасности АСУ ТП промышленного объекта / В.И. Васильев, А.М. Вульфин, К.И. Муслимова//

Информационные технологии интеллектуальной поддержки принятия решений. – 2019. – С. 197–201.

42. Васильев, В.И. Методы управления рисками кибербезопасности АСУ ТП промышленных объектов / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин // Труды Восьмой всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений». – Уфа-Ставрополь, Ханты-Мансийск, 6-9 октября 2020. – Т. 1. – С. 185–191.
43. Васильев, В.И. Моделирование кибератак на объекты АСУ ТП с помощью нечетких когнитивных карт / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин // 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.
44. Васильев, В.И. 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.
45. Васильев, В.И. Об эволюции понятия «Профиль защиты» в сфере информационной безопасности / В.И. Васильев, А.Д. Кириллова, В.В. Сагитова // Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 2 (28). – С. 53–59.
46. Васильев, В.И. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров // Информационные технологии. – 2018. – Т. 24. – №. 4. – С. 266–273.
47. Васильев, В.И. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, В.М. Картак, Л.Р. Черняховская // Информационные технологии. – 2020. – Т. 26. – №. 4. – С. 213–221.
48. Васильев, В.И. 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 Института системного анализа Российской академии наук. – 2019. – Т. 69. – №. 4. – С. 70–78.

49. Васильев, В.И. 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.
50. Васильев, В.И. Система проактивной защиты промышленного объекта на основе алгоритмов машинного обучения / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин, А.И. Фрид // FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых). – Ставрополь: Северо-Кавказский федеральный университет, 30 ноября, 2021. – С. 24–30.
51. Гарбук, С.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты / С.В. Гарбук, Д.И. Правиков, А.В. Полянский, И.В. Самарин // Вопросы кибербезопасности. – 2019. – № 3 (31). – С. 63–71.
52. Гаськова, Д.А. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры / Д.А. Гаськова, А.Г. Массель // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 42–49.
53. Глушенко, С.А. Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации / С.А. Глушенко, А.И. Долженко // Информационные технологии. – 2015. – Т. 21. – № 1. – С. 68–74.
54. Голубев, С. В. Информационная безопасность в автоматизированных системах управления / С.В. Голубев, С.А. Голубева, Е.А. Голубева // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения. – 2017. – С. 31–34.

55. Горбачев, И.Е. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / И.Е. Горбачёв, А.П. Глухов // Информатика и автоматизация. – 2015. – Т. 38. – С. 112–135.
56. Гузаиров, М.Б. 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 Уфимского государственного авиационного технического университета. – 2019. – Т. 23. – №. 4 (86). – С. 132–146.
57. Гузаиров, М.Б. Системный анализ информационных рисков вуза с применением нечетких когнитивных карт / М.Б. Гузаиров, В.И. Васильев, Р.Т. Кудрявцева // Инфокоммуникационные технологии. – 2007. – Т. 5. – №. 4. – С. 96–101.
58. Гузаиров, М.Б. 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 Института системного анализа Российской академии наук. – 2019. – Т. 69. – №. 4. – С. 62–69.
59. Гузаиров, М.Б. Управление защитой информации на основе интеллектуальных технологий / М.Б. Гузаиров, И.В. Машкина // Машиностроение. – 2013. – С. 241.
60. Гупта, А. FOUNDATION FIELDBUS или PROFIBUS-PA: выбор промышленной сети для автоматизации технологических процессов / А. Гупта, Р. Каро // Обзор. Промышленные сети. – 1999. – С. 16–22.
61. Данилушкин, И.А. Аппаратные средства и программное обеспечение систем промышленной автоматизаци: учебное пособие / И.А. Данилушкин. – Самара: Самарский государственный технический университет, 2005. – 168 с.
62. Дроботун, Е.Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя / Е.Б. Дроботун, О.В. Цветков // Программные продукты и системы. – 2016. – №. 3 (115). – С. 42–50.

63. Захарченко, В.Е. Опыт виртуальной пусконаладки АСУ ТП в нефтяной отрасли / В.Е. Захарченко, Н.А. Зарубин, Я.А. Ледаков // Деловой журнал Neftegaz.RU. – 2020. – № 6(102). – С. 46–49.
64. Ильченко, Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия / Л.М. Ильченко, Е.К. Брагина, И.Е. Егоров, С.Ю. Зайцев // Открытое образование. – 2018. – V. 22. – №. 2. – С. 61-70.
65. Исследования. Аналитики Positive Technologies [Электронный ресурс]. –Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения 18.01.2023).
66. Каменских, А.Н. Анализ рекомендаций по защите автоматизированных систем управления с целью выявления типичных уязвимостей / А.Н. Каменских, Д.А. Бортник // Электротехника, информационные технологии, системы управления. – 2016. – №. 17. – С. 48–60.
67. Кирилина, Т.Ю. Нормативно-правовое регулирование информационной безопасности автоматизированных систем управления технологическими процессами / Т.Ю. Кирилина, Е.Н. Горбанева, А.В. Познякевич // Информационно-технологический вестник. – 2018. – №. 2 (16). – С. 78–85.
68. Кириллова, А.Д. Анализ проекта методики моделирования угроз безопасности информации ФСТЭК России / А.Д. Кириллова // Материалы XIV Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: РИК УГАТУ. – 2020. – С. 20.
69. Кириллова, А.Д. Моделирования вектора атаки в базисе нечетких когнитивных карт с учетом оценок CVSS / А.Д. Кириллова // Мавлютовские чтения: Материалы XV Всероссийской молодежной научной конференции. В 7-ми томах, Уфа, 26–28 октября 2021 года. – Уфа: Уфимский государственный авиационный технический университет, 2021. – С. 229–235.
70. Кириллова, А.Д. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП / А.Д. Кириллова, В.И. Васильев // Проблемы информационной безопасности: материалы VII Всероссийской

заочной Интернет-конференции. – Ростов-на-Дону: Издательство ООО «АзовПринт», 20-21 февраля, 2018. – С. 138–142.

71. Кириллова, А.Д. Применение экспертной системы поддержки принятия решений в аудите информационной безопасности АСУ ТП / А.Д. Кириллова // Информационные технологии и системы: труды Шестой Международной научной конференции. – 2017. – С. 129–131.
72. Кириллова, А.Д. Экспертная система аудита информационной безопасности АСУ ТП / А.Д. Кириллова // Информационные технологии интеллектуальной поддержки принятия решений: материалы V Всероссийской конференции. – Уфа, 16-19 мая, 2017. – Т. 2. – С. 172–175.
73. Кирсанов, С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли / С.В. Кирсанов // Доклады ТУСУР. – 2013. – №. 2 (28). – С. 112–115.
74. Колосок, И.Н. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы / И.Н. Колосок, Л.А. Александровна // Информационные и математические технологии в науке и управлении. – 2019. – №. 2 (14). – С. 40–51.
75. Костогрызов, А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии / А.И. Костогрызов // Вопросы кибербезопасности. – 2022. – № 6. (52). – С. 71–82.
76. Котенко, Д.И. Методика итерационного моделирования атак в больших компьютерных сетях / Д.И. Котенко, И.В. Котенко, И.Б. Саенко // Информатика и автоматизация. – 2012. – Т. 23. – С. 50–79.
77. Котенко, И.В. Аналитическое моделирование атак для управления информацией и событиями безопасности / И. В. Котенко, А. А. Чечулин // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT 2012»: в 4 томах. – Дивноморское, 02–09 сентября, 2012. – Том 2. – С. 385–391.

78. Котенко, И.В. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения / И.В. Котенко, Е.В. Дойникова, А.А. Чечулин // Защита информации. Инсайд. – 2012. – №. 4 (46). – С. 54–66.
79. Котенко, И.В. Оценка рисков в компьютерных сетях критических инфраструктур / И.В. Котенко, И.Б. Саенко, Е.В. Дойникова // Инновации в науке. – 2013. – №. 16-1. – С. 84–88.
80. Лабутин, Н.Г. Моделирование действий специалиста при оценке угроз безопасности информации в информационных системах и сетях в соответствии с новой методикой ФСТЭК России / Н.Г. Лабутин, П.В. Костин // Труды НГТУ им. Р. Е. Алексеева. – 2022. – №. 3 (138). – С. 22–31.
81. Ландшафт угроз для систем промышленной автоматизации в России. Ответы, которые мы знаем доступа: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/ (дата обращения 20.09.2022).
82. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2022 [Электронный ресурс]. Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2023/03/06/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2022/ (дата обращения 08.03.2023).
83. Левцов, В. Анатомия таргетированной атаки [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения 20.09.2022).
84. Лившиц, И.И. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры / И.И. Лившиц, А.С. Бакшеев // Вопросы кибербезопасности. – 2022. – №. 6. (52). – С. 40–52.
85. Лившиц, И.И. Методика оценки рисков безопасности информационных технологий для сложных промышленных объектов в распределенных киберфизических системах / И.И. Лившец, А.А. Зайцева // Информационно-измерительные и управляющие системы. – 2019. – Т. 17. – №. 5. – С. 51–59.

86. Лившиц, И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингово типа / И.И. Лившиц // Вопросы кибербезопасности. – 2020. – №. 1 (35). – С. 42–51.

87. Лукацкий, А. Применимость стандартов NERC CIP в России / А. Лукацкий // Безопасность инфраструктуры энергоснабжения [Электронный ресурс]. Режим доступа: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (дата обращения 26.07.2022)

88. Максименко, В.Н. Основные подходы к анализу и оценке рисков информационной безопасности / В.Н. Максименко, Е.В. Ясюк // Экономика и качество систем связи. – 2017. – №. 2 (4). – С. 42–48.

89. Малюк, А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. / А.А. Малюк. – 2019. – 314 с.

90. Массель, А.Г. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов / А.Г. Массель, Д.А. Гаськова // Онтология проектирования. – 2019. – №. 2 (32). – С. 225–238.

91. Машкина, И.В. Анализ риска объекта информатизации / И.В. Машкина, Е.С. Степанова, Т.О. Вишнякова: Учебное пособие. – Уфа: УГАТУ, 2011. – 112 с.

92. Новохрестов, А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2016. – Т. 19. – №. 3. – С. 111–114.

93. Обзор Kaspersky Industrial CyberSecurity for Nodes [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/Kaspersky-Industrial-CyberSecurity-for-Nodes (дата обращения 26.09.2022).

94. Общие сведения об архитектуре сети OT Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/azure/defender-for-iot/organizations/best-practices/understand-network-architecture (дата обращения 26.09.2022).

95. Оптимальные решения для цифровизации электрических сетей // Энергетика и промышленность России. – 2018. – № 22 (354). – С. 28–29.

96. Оценка рисков информационной безопасности по методике Facilitated Risk Analysis Process [Электронный ресурс]. Режим доступа: https://www.ussc.ru/news/novosti/otsenka-riskov-ib-po-metodike-facilitated-risk-analysis-process (дата обращения 26.09.2022).

97. Петухов, А. Информационная безопасность промышленных систем в перспективе 3–5 лет / А. Петухов [Электронный ресурс]. – Режим доступа: https://www.itsec.ru/articles/informacionnaya-bezopasnost-promyshlennyh-sistem-v-perspektive-3-5-let (дата обращения 20.09.2022).

98. Пищик Б. Н. Безопасность АСУ ТП //Вычислительные технологии. – 2013. – Т. 18. – С. 170–175.

99. Правиков, Д.И.П. Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов / Д.И.П. Правиков, В. Г. Карантаев // Безопасность информационных технологий. – 2020. – Т. 27. – №. 4. – С. 37–52.

100. Пугин, В.В. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В.В. Пугин, О.Ю. Губарева // T-Comm-Телекоммуникации и Транспорт. – 2012. – №. 6. – С. 54–57.

101. Разумников, С.В. Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков ИТ для облачных сервисов / С.В. Разумников // Современные проблемы науки и образования. – 2014. – №. 1. – С. 247–247.

102. Решения Cisco по защите автоматизированных систем управления технологическими процессами [Электронный ресурс]. Режим доступа: https://technon.ru/upload/pdf/Podhod-Cisco-po-bezopasnosti-ASU-TP.pdf (дата обращения 26.09.2022).

103. Римша, А.С. Программно-алгоритмическое решение для оценки и учета рисков АСУ ТП газодобывающего предприятия / А.С. Римша, К.С. Римша //

Печатается по решению совета математического факультета Челябинского государственного университета. – 2018. – Т. 29. – С. 165.

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

105. Свидетельство о государственной регистрации программы для ЭВМ № 2021615080 Российская Федерация. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка: заявл. 26.03.2021; зарег. 02.04.2021. / А.М. Вульфин, А.В. Никонов, Д.Н. Габбасова и др.

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

107. Силов, В.Б. Принятие стратегических решений в нечеткой обстановке / В.Б. Силов // – М.: Инпро-Рес, 1995. – 228 с.

108. Системы автоматизации. Издание 1. – 2022 [Электронный ресурс]. – Режим доступа: https://ekra.ru/catalogs/docs/EKRA_%D0%90%D0%A1%D0%A3%20%D0% A2%D0%9F.pdf (дата обращения 26.09.2022).

109. Смирнов, Р.А. Исследование методик оценки угроз безопасности информации / Р.А. Смирнов, С.Н. Новиков // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 250–257.

110. Смотрим на технологическую сеть глазами злоумышленников [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/pt/blog/671656/#_ftnref1 (дата обращения 20.09.2022).

111. Степанова, Е.С. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности / Е.С. Степанова, И.В. Машкина, В.И. Васильев // Известия ЮФУ.

Технические науки/Тематич. выпуск «Информационная безопасность». – 2010. – №. 11 (112). – С. 31–40.

112. Филимонова, И.В. Принципиальные подходы к геолого-экономической оценке разномасштабных нефтегазовых объектов / И.В. Филимонова, Л.В. Эдер, М.В. Мишенин, И.В. Проворная //Геология нефти и газа. – 2014. – №. 1. – С. 15–23.

113. Чертков, А.А. Кибербезопасность в промышленной автоматизации / А.А. Чертков // Промышленные АСУ и контроллеры. – 2017. – №. 5. – С. 68–72.

114. Шинкаренко, А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов / А.Ф. Шинкаренко // Интеллектуальные технологии на транспорте. – 2016. – №. 1. – С. 16–20.

115. Эндрю, П. Активное выявление угроз с Elastic Stack: Построение надежного стека безопасности: предотвращение, обнаружение и оповещение / П. Эндрю, пер. с англ. В. С. Яценкова. // – М.: ДМК Пресс, 2022. – 326 с.

116. Ярушевский, Д. Обеспечение безопасности АСУ ТП – краткий обзор семейства стандартов IEC 62443 / Д. Ярушевский // Information Security/Информационная безопасность. – 2014. – №. 3. [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystvastandartov-iec-62443 (дата обращения 26.09.2022).

117. Abdo, H., A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis / H. Abdo, M. Kaouk, J. M. Flaus, F. Masse // Computers & security. – 2018. – Vol. 72. – pp. 175–195.

118. Aguilar, J. A survey about fuzzy cognitive maps papers / J. Aguilar // International journal of computational cognition. – 2005. – Vol. 3. – No. 2. – pp. 27–33.

119. Asghar, M.R. Cybersecurity in industrial control systems: Issues, technologies, and challenges / M.R. Asghar, Q. Hu, S. Zeadally // Computer Networks. – 2019. – Vol. 165. – pp. 106946.

120. Assante, M. J. The industrial control system cyber kill chain / M.J. Assante, R.M. Lee // SANS Institute InfoSec Reading Room. – 2015. – Vol. 1. – pp. 24.

121. Barankova, I.I. Analysis of the problems of industrial enterprises information security audit / I.I. Barankova, U.V. Mikhailova, O.B. Kalugina // Advances in Automation: Proceedings of the International Russian Automation Conference, RusAutoCon 2019, September 8-14, 2019, Sochi, Russia. – Springer International Publishing, 2020. – pp. 976–985.

122. Bhamare, D. Cybersecurity for industrial control systems: A survey / D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin // Computers & security. – 2020. – Vol. 89. – pp. 101677.

123. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021 [Электронный ресурс]. – Режим доступа: https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf (дата обращения 26.09.2022).

124. Common Attack Pattern Enumeration and Classification (CAPEC) [Электронный ресурс]. – Режим доступа: https://capec.mitre.org/index.html (дата обращения 26.09.2022).

125. Common Vulnerability Scoring System v3.0: Specification Document. [Электронный ресурс]. Режим доступа: https://www.first.org/cvss/v3.0/specification-document (дата обращения 26.09.2022)

126. Converged Plantwide Ethernet (CPwE) Design and Implementation Guide [Электронный ресурс]. – Режим доступа: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf (дата обращения 26.09.2022).

127. CRAMM Version 5.1 User Guide; Insight Consulting: 2005. [Электронный ресурс]. – Режим доступа: https://pdfcoffee.com/cramm-version-51-user-guide-pdf-free.html (дата обращения 26.09.2022).

128. DATAPK [Электронный ресурс]. – Режим доступа: https://datapk.ru/ (дата обращения 26.09.2022)

129. Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry [Электронный ресурс]. – Режим доступа: https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf (дата обращения 26.09.2022).

130. Efimov, B.I. Analysis of the impact of threats to change and block responses of experts in online survey systems / B.I. Efimov, P.S. Lozhnikov // Journal of Physics: Conference Series. – IOP Publishing, 2020. – Vol. 1546. – No. 1. – pp. 012079.

131. Espinosa, M.L. Fuzzy Cognitive Maps with Rough Concepts. / M.L. Espinosa, B. Depaire, K. Vanhoof // In Proceeding of the 9th IFIP WG 12.5 International Conference, AIAI 2013: Artificial Intelligence Applications and Innovations. – Paphos (Cyprus), September 30 – October 2, 2013. – pp. 527–536.

132. George, G. A graph-based security framework for securing industrial iot networks from vulnerability exploitations / G. George, S.M. Thampi // IEEE Access. – 2018. – Vol. 6. – pp. 43586–43601.

133. Gore, R. Markov chain modeling of cyber threats / R. Gore, J. Padilla, S. Diallo // The Journal of Defense Modeling and Simulation. – 2017. – Vol. 14. – No. 3. – pp. 233–244.

134. Hajeck, P. Interval-valued fuzzy cognitive maps for supporting business decisions. / P. Hajeck, O. Prochazka // Proceedings of IEEE International Conference on Fuzzy Systems. – Vancouver (Canada), July 2016. – pp. 531–536.

135. Hajek, P. Intuitionistic Fuzzy Grey Cognitive Maps for Forecasting Interval-Valued Time Series / P. Hajek, W. Froelich, O. Prochazka // Neurocomputing. – 2020. – pp. 173–185.

136. Hajrullin E., Secure Data Exchange in the Industrial Internet of Things Network of the Fuel and Energy Complex / E. Hajrullin, A. Vulfin, K. Mironov, A. Frid, M. Guzairov, A. Kirillova // Proceedings ICOECS 2020 International Conference on Electrotechnical Complexes and Systems. – Ufa, State Aviation Technical University Ufa, Russia, October 27-30, 2020. – pp. 353–358.

137. Haritha, K. Fuzzy cognitive map-based genetic algorithm for community detection / K. Haritha, M.V. Judy // Progress in Advanced Computing and Intelligent

Engineering: Proceedings of ICACIE 2019, Volume 1. – Springer Singapore, 2021. – pp. 412-426.

138. Hashim, N.A. Risk assessment method for insider threats in cyber security: A review / N.A. Hashim, Z. Zainal, P.A. Perumal, N.A. Zakaria // International Journal of Advanced Computer Science and Applications. – 2018. – Vol. 9. – No. 11. – pp. 1–5.

139. Homer, J. Aggregating vulnerability metrics in enterprise networks using attack graphs / J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S.R. Rajagopalan, A. Singhal // Journal of Computer Security. – 2013. – Vol. 21. – No. 4. – pp. 561–597.

140. Hu, J. I-hmm-based multidimensional network security risk assessment / J. Hu, S. Guo, X. Kuang, F. Meng, D. Hu, Z. Shi, // IEEE Access. – 2020. – Vol. 8. – pp. 1431–1442.

141. Import Mitre Att&ck into Neo4j database [Электронный ресурс]. Режим доступа: https://github.com/vmapps/attack2neo (дата обращения 31.01.2023)

142. International Society of Automation [Электронный ресурс]. – Режим доступа: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (дата обращения 26.09.2022).

143. Jamshidi, A. Dynamic risk assessment of complex systems using FCM / A. Jamshidi, D. Ait-Kadi, A. Ruiz, M.L. Rebaiaia // International Journal of Production Research. – 2018. – Vol. 56. – No. 3. – pp. 1070–1088.

144. Kaspersky Industrial CyberSecurity [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity (дата обращения 26.09.2022)

145. Kirillova, A.D. 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»: сборник трудов ИТНТ-2019. – Самара, 21-24 мая 2019. – 4 т. Науки о данных. – С. 391–398.

146. Kirillova, A.D. 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 Technology and Nanotechnology. – 2019. – С. 477–486.

147. Kosko, B. Fuzzy Cognitive Maps / B. Kosko // Intern. Journal of Man-Machine Studies. – 1986. – Vol. 1. – pp. 65–75.

148. Kuzminykh, I. Information Security Risk Assessment / I. Kuzminykh, B.V. Ghita, V. Sokolov, T. Bakhshi // Encyclopedia. – 2021. – Vol. 1. – No. 3. – pp. 602–617.

149. Maksimova, E.A. Predicting Destructive Malicious Impacts on the Subject of Critical Information Infrastructure / E.A. Maksimova, V.V. Baranov // In book: Futuristic Trends in Network and Communication Technologies. – 2021. – pp. 88–99.

150. Manzhosov, A.V. Method of Constructing a Graphic Model of the Regulatory and Legal Framework in the Sphere of Information Security / A.V. Manzhosov, I.P Bolodurina //Advanced Network Technologies and Intelligent Computing: First International Conference, ANTIC 2021, Varanasi, India, December 17-18, 2021. Springer International Publishing, 2022. – pp. 48–62.

151. MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения 26.09.2022).

152. Mohagheghi, S. Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems. [Электронный ресурс]. – Режим доступа: https://www.intechopen.com/books/ (дата обращения 17.08.2022).

153. Mohr, S. Modelling Approaches for Multilayer Fuzzy Cognitive Maps. [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/332158518_Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (дата обращения 17.08.2022).

154. Motlagh, O. Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map / O. Motlagh, E.I. Papageorgiou, S.H. Tang, Z. Jamaludin // Sains Malaysiana. – 2014. – Vol. 43(11). – pp. 1781–1790.

155. Munoz-Gonzalez, L.D Exact` inference techniques for the analysis of bayesian attack graphs / .X. Guo, D. Sgandurra, M. Barrere, E.C. Lupu, // IEEE Transactions on Dependable and Secure Computing. 2019. – vol. 16. – no. 2. – pp. 231–244.

156. Noel, S. CyGraph: graph-based analytics and visualization for cybersecurity / S. Noel, E. Harley, K.H. Tam, M. Limiero // Handbook of Statistics. – Elsevier, 2016. – Vol. 35. – pp. 117–167.

157. Open Source Tool - Cybersecurity Graph Database in Neo4j. GraphKer [Электронный ресурс]. – Режим доступа: https://github.com/amberzovitis/GraphKer (дата обращения 17.08.2022).

158. Padmalatha, E. Feature Selection Optimization Using a Hybrid Genetic Algorithm / E. Padmalatha, S. Sailekhya, S.A. Athyaab, J. Harsh Raj // ICT Analysis and Applications: Proceedings of ICT4SD 2020, Volume 2. – Springer Singapore, 2021. – pp. 411–421.

159. Papageorgiou, E.I. Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms / E.I. Papageorgiou // Intelligent Systems Reference Library 54, Springer Science & Business Media. – 2013. – Vol. 54. – 411 p.

160. Papageorgiou, E.I. Review of Fuzzy Cognitive Maps Research During the Last Decade / E.I. Papageorgiou // IEEE Trans. on Fuzzy Systems. – 2013. – Vol. 21. – No. 1. – pp. 66–79.

161. Peltier, T.R. Facilitated risk analysis process (FRAP) / T.R. Peltier // Auerbach Publication, CRC Press LLC. – 2000.

162. Poolsappasit, N. Dynamic security risk management using bayesian attack graphs / N. Poolsappasit, R. Dewri, I. Ray // IEEE Transactions on Dependable and Secure Computing. – 2012. – Vol. 9. – No. 1. – pp. 61–74.

163. PT Industrial Cybersecurity Suite [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/solutions/pt-ics/PT-ICS_brief.pdf (дата обращения 26.09.2022)

164. Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems [Электронный ресурс]. – Режим доступа: https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (дата обращения 26.09.2022)

165. Salmeron, J.L. Learning fuzzy cognitive maps with modified asexual reproduction optimisation algorithm / J.L. Salmeron, T. Mansouri, M.R.S. Moghadam, A. Mardani // Knowledge-Based Systems. – 2019. – Vol. 163. – pp. 723–735.

166. Salmeron, J.L. Uncertainty propagation in fuzzy grey cognitive maps with Hebbian-like learning algorithms / J.L. Salmeron, P.R. Palos-Sanchez // IEEE transactions on cybernetics. – 2017. – Vol. 49. – No. 1. – pp. 211–220.

167. Sivanandam, S.N. Genetic algorithm optimization problems / S.N. Sivanandam, S.N. Deepa // Introduction to genetic algorithms. – 2008. – pp. 165–209. (Sivanandam)

168. Spring, J. Time to Change the CVSS? / J. Spring, E. Hatleback, A. Householder, A. Manion, D. Shick // IEEE Security & Privacy. – 2021. – Vol. 19. – No. 2. – pp. 74–78.

169. STIX data representing MITRE ATT&CK [Электронный ресурс]. Режим доступа: https://github.com/mitre-attack/attack-stix-data (дата обращения 31.01.2023)

170. Stylios, C.D. Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems / C.D. Stylios, P.P. Groumpos // IFAC Large Scale Systems: Theory and Applications. Bucharest, Romania, 2001. – P. 61–66.

171. Stylios, C.D. Introducing the theory of fuzzy cognitive maps in distributed systems / C.D. Stylios, V.C. Georgopoulos, P.P. Groumpos // Proc. of the Twelfth IEEE Intern. Symposium on Intelligent Control. – Istanbul (Turkey), July 16-18, 1997. – pp. 55–60.

172. Tatam, M. A review of threat modelling approaches for APT-style attacks / M. Tatam, B. Shanmugam, S. Azam, K. Kannoorpatti // Heliyon. – 2021. – Vol. 7. – No. 1. – e05969 p.

173. Vasilyev, V.I. Algorithms for proactive security of industrial systems based on machine learning technologies / V.I. Vasilyev, A.M. Vulfin, A.D. Kirillova // VIII Международная конференция и молодёжная школа «Информационные технологии и нанотехнологии» (ИТНТ-2022). – Самара, 23-27 мая 2022. – Т. 4. Искусственный интеллект. – С. 042412

174. Vasilyev, V.I. 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 // Информационные технологии и системы: труды седьмой всероссийской научной конференции с международным участием. – Ханты-Мансийск, 12-16 марта, 2019. – С. 193–197.

175. Vasilyev, V.I. 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.

176. Vasilyev, V.I. Modeling the cyber attacks vector based on fuzzy cognitive maps / V.I. Vasilyev, A.D. Kirillova, A.M. Vulfin, A.V. Nikonov // Информационные технологии и нанотехнологии (ИТНТ-2021): сб. тр. по материалам VII Междунар. конф. и молодеж. шк., Самара, 20-24 сентября, 2021. – Т. 3. – С. 031372.

177. Vulfin, A.M. 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). – Moscow (Russia), July 1, 2021. Journal of Physics: Conference Series, 2021. – Vol. 2001. – pp. 012004.

178. Xiong J., Wu J. Construction of information network vulnerability threat assessment model for CPS risk assessment // Computer communications. – 2020. – Vol. 155. – pp. 197–204.

179. Xu, D. Automated security test generation with formal threat models / D. Xu, M. Tu, M. Sanford, L. Thomas // IEEE transactions on dependable and secure computing. – 2012. – Vol. 9. – No. 4. – pp. 526–540.

180. Yebiah-Bouteng, E.O. Using fuzzy cognitive maps (FCMs) to evaluate the vulnerabilities with ICT assets disposal policies / E.O. Yebiah-Bouteng // Intern.

Journal on Electrical & Computer Science (IJECS-IJENS). – 2012. – Vol. 12. – No. 05. – pp. 20–31.

181. Yeboah-Ofori, A. Cyber security threat modeling for supply chain organizational environments / A. Yeboah-Ofori // Future internet. – 2019. – Vol. 11. – No. 3. – pp. 63.

182. Zarreh, A. Risk assessment for cyber security of manufacturing systems: A game theory approach / A. Zarreh, H. Wan, Y. Lee, C. Saygin // Procedia Manufacturing. – 2019. – Vol. 38. – pp. 605–612.

183. Zhang, J.Y. Quotient FCMs-a decomposition theory for fuzzy cognitive maps / J.Y. Zhang, Z.Q. Liu, S. Zhou // IEEE transactions on fuzzy systems. – 2003. – Vol. 11. – No. 5. – pp. 593–604.

184. Zografopoulos, I. Cyberphysical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies / I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou // IEEE Access. – 2021. – Vol. 9. – pp. 29775–29818.

Приложение А – Акты о внедрении научных результатов

«УТВЕРЖДАЮ»
Проректор по учебной работе
ФГБОУ ВО «Уфимский университет науки и технологий»
_____ Ю.В. Рахманова
«__» 05 2023 г.

АКТ

о внедрении результатов диссертационной работы
Кирилловой Анастасии Дмитриевны на тему
«Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования»,
представленной на соискание ученой степени кандидата технических наук

Комиссия в составе: заведующий кафедрой вычислительной техники и защиты информации (ВТиЗИ), д.ф.-м.н., профессор Картак В.М.; профессор кафедры ВТиЗИ, д.т.н., профессор Фрид А.И.; начальник Учебного управления, к.э.н., доцент Гумерова З.Ж., составила настоящий акт о том, что следующие результаты диссертационной работы Кирилловой А.Д. используются в учебном процессе кафедры вычислительной техники и защиты информации:

– когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных нечетких когнитивных карт;

– метод и алгоритмы количественной оценки рисков информационной безопасности (ИБ) с использованием технологий сценарного моделирования атак и методов машинного обучения.

Материалы диссертационной работы используются в лекционных курсах, а также при проведении практических и лабораторных занятий по дисциплинам «Искусственный интеллект в системах защиты информации», «Экспертные системы комплексной оценки безопасности информационно-телекоммуникационных систем» для обучающихся по направлениям подготовки специалистов 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», магистров 10.04.01 «Информационная

безопасность», 09.04.01 «Информатика и вычислительная техника» (профиль «Безопасность и защиты информации»).

Результаты диссертационного исследования активно используются в учебном процессе при выполнении разделов курсовых проектов, научно-исследовательских и выпускных квалификационных работ, связанных с анализом и оценкой рисков ИБ объектов критической информационной инфраструктуры.

Заведующий кафедрой ВТиЗИ,
д.ф.-м.н., профессор _____ В.М. Картак

Профессор кафедры ВТиЗИ
д.т.н., профессор _____ А.И. Фрид

Начальник Учебного управления
к.э.н., доцент _____ З.Ж. Гумерова

«УТВЕРЖДАЮ»
Директор ООО «Инженерный центр систем безопасности»
_____ А.И. Луцкович
«02» 03 2023 г.

АКТ

о внедрении результатов диссертационной работы
Кирилловой Анастасии Дмитриевны на тему
«Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования»

Комиссия в составе: Луцкович Альберт Иванович, директор ООО «Инженерный центр систем безопасности (ИЦСБ)», Андреева Екатерина Юрьевна, заместитель директора по информационной безопасности ООО «ИЦСБ»; Башмаков Наиль Маратович, руководитель отдела развития сервисов мониторинга ИБ, составила настоящий акт о том, что следующие результаты диссертационной работы Кирилловой А.Д. используются в нашей организации при выполнении работ, связанных с исследованием и оценкой информационных рисков объектов КИИ:

– алгоритмы, методика и инструментальные средства количественной оценки рисков информационной безопасности (ИБ) АСУ ТП на основе моделирования сценариев атак.

Использование предложенных в работе алгоритмов, методики и инструментальных средств позволяет анализировать возможные сценарии компьютерных атак с требуемым уровнем детализации действий нарушителя и на основе этого формировать оценку вероятности успешной реализации атаки и ее последствий.

Практическая ценность полученных результатов заключается в повышении оперативности и достоверности результатов комплексной оценки

рисков ИБ объектов КИИ, оптимизации распределения затрат на реализацию, внедрение и сопровождение необходимых мер защиты с учетом их функциональных ограничений.

Директор _____ / А.И. Луцкович /

Заместитель директора по ИБ _____ / Е.Ю. Андреева /

Руководитель отдела _____ / Н.М. Башмаков /

«УТВЕРЖДАЮ»

Директор ЗАО «Республиканский центр защиты информации»

_____ С.Н. Зарипов

«24» 03 2023 г.

АКТ

о внедрении результатов диссертационной работы
Кирилловой Анастасии Дмитриевны на тему
«Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования»

Комиссия в составе главного инженера ЗАО «Республиканский центр защиты информации (РЦЗИ)», к.т.н. Бакирова А.А., заместителя директора РЦЗИ Хисамутдинова Т.З., ведущего специалиста РЦЗИ Федотова Д.Б. составила настоящий акт о том, что следующие результаты диссертационной работы Кирилловой А.Д. «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования», представленной на соискание ученой степени кандидата технических наук, прошли апробацию и были использованы в ЗАО «Республиканский центр защиты информации» на этапе комплексной оценки рисков информационной безопасности (ИБ) инфраструктуры АСУ ТП:

– методика количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с применением технологий когнитивного моделирования и методов машинного обучения.

Использование разработанной в диссертации методики анализа рисков ИБ АСУ ТП позволяет получить перечень актуальных угроз и количественную оценку рисков ИБ, а также существенно повышает обоснованность и полноту сценарного моделирования атак за счет формирования детализированного

перечня тактик и техник, которые может использовать возможный злоумышленник в ходе реализации целенаправленных атак.

Главный инженер, к.т.н. / А.А. Бакиров

Заместитель директора / Т.З. Хисамутдинов

Ведущий специалист / Д.Б. Федотов

УТВЕРЖДАЮ
Генеральный директор
ООО “НПП ОЗНА-Инжиниринг”
Кравцов М.В.
«04» 04 2023 г.

АКТ

о внедрении результатов диссертационной работы
Кирилловой Анастасии Дмитриевны на тему
«Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования»

Комиссия в составе:

1) Зориков Юрий Николаевич (директор по техническому развитию);

2) Албурин Ильшат Ахатович (начальник УИТ и ИБ);

3) Радченко Ольга Анатольевна (руководитель направления HR)

составила настоящий акт о том, что следующие результаты диссертационной работы Кирилловой А.Д. «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования», представленной на соискание ученой степени кандидата технических наук, прошли апробацию и были использованы в ООО “НПП ОЗНА-Инжиниринг” для анализа существующей промышленной инфраструктуры АСУ ТП на этапе идентификации актуальных угроз безопасности информации и количественной оценки рисков информационной безопасности АСУ ТП:

– исследовательский прототип интеллектуальной системы поддержки принятия решений (ИСППР) и программная реализация средств автоматизации моделирования сценариев атак.

Использование разработанного программного обеспечения ИСППР позволяет собрать информацию о слабых местах инфраструктуры АСУ ТП, наиболее опасных уязвимостях и потенциальных слабостях компонентов

системы, выявить потенциально наиболее вероятные (или опасные) сценарии атак и количественно оценить их последствия.

Практическая ценность полученных результатов заключается в сокращении более чем в 2,5 раза временных затрат на моделирование сценариев атак, а также повышении достоверности получаемой оценки рисков информационной безопасности промышленных объектов на основе Методики оценки угроз безопасности ФСТЭК России за счет использования технологий когнитивного моделирования и методов машинного обучения и ее снижении на 10 % при повышении на 15 % эффективности эксплуатации контрмер за счет оптимизации распределения ресурсов их применения.

Директор по техническому развитию _____ / Ю.Н. Зориков /

Начальник УИТ и ИБ _____ / И.А. Албурин /

Руководитель направления HR _____ / О.А. Радченко /

Приложение Б – Архитектура Conwerged Plantwide Ethernet (CPwE)

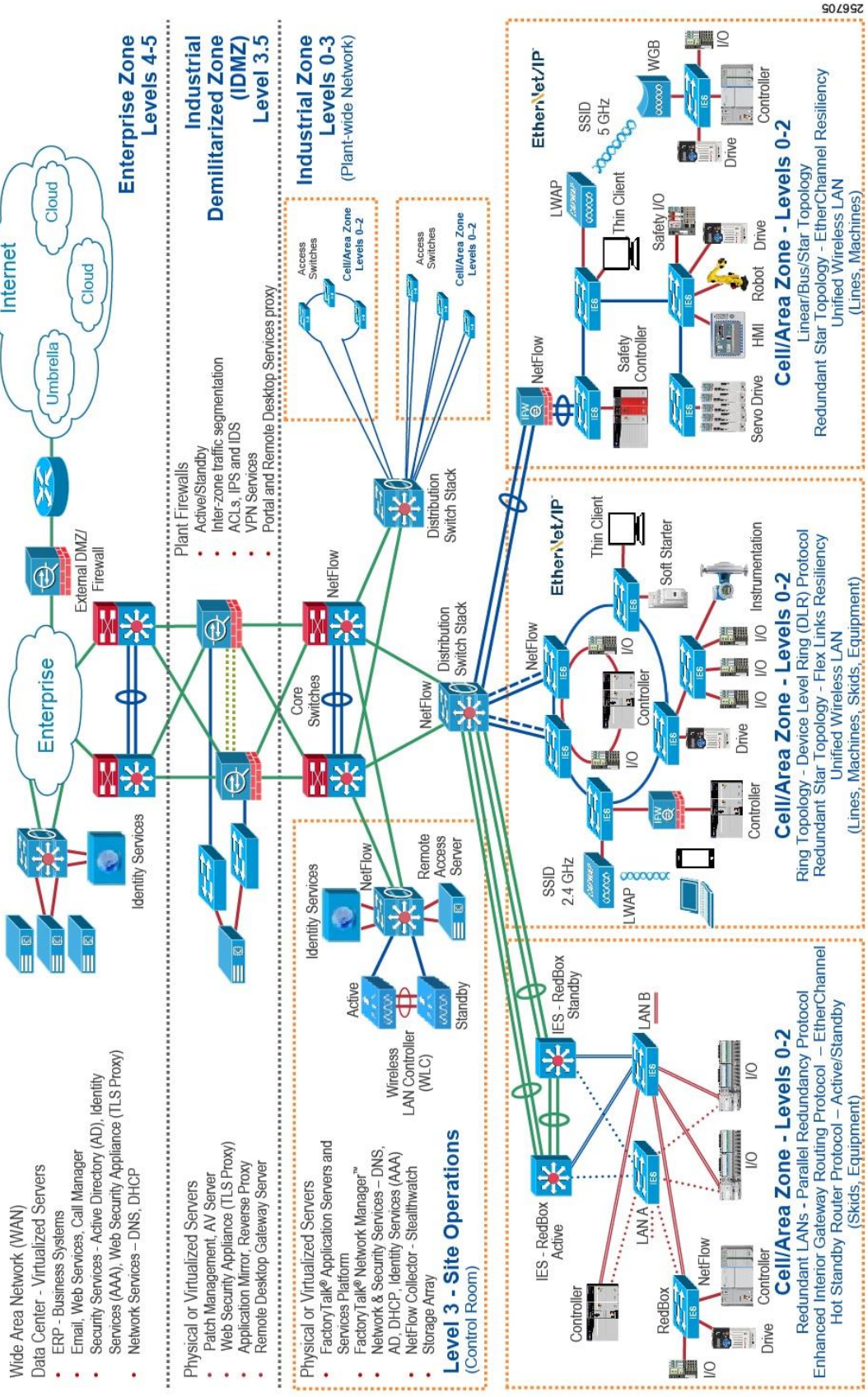


Рисунок Б.1 – Уровни архитектуры CPwE [126]

Приложение В – Нормативные документы в области обеспечения ИБ АСУ ТП

Таблица В.1 – Перечень нормативных стандартов в области обеспечения ИБ АСУ ТП промышленных объектов

Номер		Наименование
NIST SP 800-82		«Guide to Industrial Control Systems (ICS) Security» («Рекомендации по обеспечению безопасности промышленных систем автоматизации»)
Отраслевые стандарты NERC-CIP (Critical Infrastructure Protection)		
NERC CIP-002		Cyber Security – Critical Cyber Asset Identification (Кибербезопасность – Идентификация критически важных киберактивов)
NERC CIP-003		Cyber Security – Security Management Controls (Кибербезопасность – Средства управления безопасностью)
NERC CIP-005		Cyber Security – Electronic Security Perimeter(s) (Кибербезопасность – Электронный периметр безопасности)
NERC CIP-007		Cyber Security – Systems Security Management (Кибербезопасность – Управление безопасностью систем)
NERC CIP-013-1		Cyber Security – Supply Chain Risk Management (Кибербезопасность – Управление рисками цепочки поставок)
Серия международных стандартов ISA/IEC 62443		
General (Общие положения)	IEC/TS 62443-1-1:2009	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models (Терминология, концепции и модели)
	IEC/TR 62443-1-2	Master glossary of terms and abbreviations (Мастер-глоссарий терминов и аббревиатур)
	IEC/TS 62443-1-3	Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics (Системы показателей соответствия безопасности системы)
	IEC/TR 62443-1-4	IACS security life-cycle and use-case (Жизненный цикл безопасности и сценарий использования IACS)
Policies and Procedures (Политики и процедуры)	IEC 62443-2-1:2010	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program (Требования к системе управления безопасностью IACS)
	IEC/TR 62443-2-2	Implementation guidance for an IACS security management system (Руководство по внедрению системы управления безопасностью)
	IEC/TR 62443-2-3:2015	Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment (Управление патчами в среде IACS)
	IEC 62443-2-4:2015	Security program requirements for IACS service providers (Требования к установке и техническому обслуживанию для поставщиков IACS)

Номер		Наименование
System Requirements (Системные требования)	IEC/TR 62443-3-1:2009	Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems (Технологии безопасности IACS)
	IEC 62443-3-2:2020	Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design (Оценка рисков безопасности для проектирования системы)
	IEC 62443-3-3:2013	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (Системные требования безопасности и уровни безопасности)
Component Requirements (Требования к компонентам)	IEC 62443-4-1:2018	Security for industrial automation and control systems – Part 4-1: Product development requirements (Требования разработчиков продукции)
	IEC 62443-4-2:2019	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (Технические требования к безопасности компонентов IACS)
Серия стандартов ГОСТ Р МЭК 62443		
ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009		«Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»
ГОСТ Р МЭК 62443-2-1-2015		«Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Состояние проблемы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»
ГОСТ Р МЭК 62443-3-3-2016		«Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности»
Приказ ФСТЭК России от 14 марта 2014 г. № 31		«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды»
Федеральный закон от 26 июля 2017 г. № 187-ФЗ		«О безопасности критической информационной инфраструктуры Российской Федерации»
Приказ ФСТЭК России от 25 декабря 2017 г. № 239		«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Приложение Г – Анализ исследований в области обеспечения ИБ АСУ ТП

Таблица Г.1 – Анализ методов и подходов к решению задачи оценки рисков ИБ

Источник	Описание подхода к оценке рисков ИБ
Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли [73]	Для составления перечня возможных угроз ИБ АСУ ТП используется каталог угроз стандарта CRAMM. Для оценки рисков ИБ используется адаптированный для АСУ ТП стандарт CVSS.
Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов [114]	Предлагается многоуровневый подход к оценке уровня ИБ, основанный на деревьях атак и зависимостях сервисов. Методика объединяет качественный и количественный подходы к оценке уровня ИБ, опираясь на стандарт CVSS и методику FRAP.
Ильченко Л.М. и др. Расчет рисков информационной безопасности телекоммуникационного предприятия [64]	Предлагается метод оценки рисков ИБ на основе стандарта ГОСТ Р ИСО/МЭК 27005-2010, делается акцент на минимизацию ущерба от угроз безопасности из БДУ ФСТЭК, направленных на целостность и доступность распределенной информационной системы, однако качественные оценки в целом снижают эффективность.
Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры [52]	Подход к анализу и оценке рисков ИБ включает в себя методику анализа рисков энергетической инфраструктуры в соответствии с ИСО/МЭК 27005-2011, методику формирования сценариев экстремальных ситуаций в энергетике, методику качественной и количественной оценки рисков ИБ. Не дано описание алгоритма оценивания риска ИБ.
Котенко И.В., Саенко И.Б., Дойникова Е.В. Оценка рисков в компьютерных сетях критических инфраструктур [79]	Предложена методика оценки рисков ИБ в сетях критической инфраструктуры, которая позволяет проводить эту оценку в online-режиме в 3 этапа: 1) рассматриваются метрики для объектов графов атак; 2) рассчитывается количественный уровень для всех возможных угроз; 3) на основе уровней угроз определяется итоговый уровень ИБ.
Лившиц И.И., Зайцева А.А. Методика оценки рисков безопасности информационных технологий для сложных промышленных объектов в распределенных киберфизических системах [85]	Рассмотрена методика, основанная на современных риск-ориентированных стандартах ISO/IEC серии 27001 и 15408. Предложенная методика позволяет получить расчетные результаты оценки рисков ИБ технологий в ограничениях размещения и состава компонент сложных промышленных объектов.
Abdo H. et al. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie analysis [117]	Представлен подход, основанный на: определении сценариев атак с применением метода галстук-бабочка и деревья атак, что позволяет выявить причины и последствия нарушения ИБ; определении вероятности сценариев атак; оценке последствий. Данный подход достаточно трудоемкий.
Xiong J., Wu J. Construction of information network vulnerability threat assessment	Рассматриваются факторы, влияющие на сетевые атаки, и строится модель оценки рисков ИБ киберфизических систем на основе анализа и моделирования атак. Модель оценки

Источник	Описание подхода к оценке рисков ИБ
model for CPS risk assessment [178]	рисков ИБ предложена на базе методологии теории игр. Данные для расчетов определяются экспертным путем.
Zarreh A. et al. Risk assessment for cyber security of manufacturing systems: A game theory approach [182]	Предложен количественный подход оценки рисков ИБ в производственных системах с использованием теории игр. Рассматривается минимизация ущерба при минимальных затратах. Данные для расчетов определяются экспертным путем.
Homer J. et al. Aggregating vulnerability metrics in enterprise networks using attack graphs [139]	Разработана количественная модель оценки, позволяющая агрегировать показатели уязвимостей компонентов сети с применением графов атак. При заданных метриках CVSS, характеризующих вероятность эксплуатации уязвимости, модель вычисляет значение, представляющее совокупную вероятность того, что нарушитель реализует атаку в сети, то есть принимается во внимание влияние всех возможных взаимодействий между уязвимостями. Но использование модели предполагает, что нарушитель владеет всей информацией об объекте.
George G., Thampi S.M. A graph-based security framework for securing industrial IoT networks from vulnerability exploitations [132]	Отношения между компонентами сети Промышленного Интернета вещей (IIoT) и уязвимостями представлены в виде графовой модели, которая выступает в качестве основы для оценки рисков ИБ, а также визуализирует уровни угроз. Недостатком является то, что каждый узел графа атак представляет собой уязвимость, а не компонент сети, что приводит к потере информации при анализе, так как невозможно восстановить связь компонент – уязвимость.
Zografopoulos I. et al. Cyberphysical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies [184]	Продемонстрирована методология моделирования угроз для компонентов киберфизических систем, их взаимозависимостей, возможных точек входа для реализации атак и уязвимостей системы. Оценка рисков позволяет определить приоритет уязвимостей, учитывая их влияние на работу системы. Однако модель не интегрирует внутреннюю структуру объекта оценки.

Таблица Г.2 – Анализ методов интеллектуального анализа и моделирования в задаче оценки рисков ИБ

Источник	Описание применяемых интеллектуальных методов
Аникин И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях [20]	Предложен метод количественной оценки и управления рисками ИБ, основанный на оценке эффективности реализуемых мер защиты. Для решения задач оптимизации на этапе управления рисками ИБ используется генетический алгоритм. Представленный метод позволяет эффективно решать оптимизационные задачи по управлению рискам ИБ на основе метода нечеткой количественной оценки рисков ИБ в условиях нечеткости и неопределенности исходной информации.
Глушенко С.А., Долженко А.И. Система поддержки принятия решений нечеткого моделирования рисков	Предложена нечеткая продукционная модель, позволяющая снять ограничения на число учитываемых входных переменных и интегрировать как качественные, так и количественные подходы к оценке рисков ИБ. Система поддержки принятия решений позволяет строить многоуровневые нечеткие продукционные

Источник	Описание применяемых интеллектуальных методов
информационной безопасности организации [53]	модели, а используемый механизм нечеткого вывода на основе алгоритма Мамдани позволяет получить числовое значение риска, лингвистическое описание уровня риска, а также степень уверенности эксперта в возникновении неблагоприятного события. Полученная информация позволит лицу, принимающему решение, выявить приоритеты рисков и выработать план мероприятий по снижению влияния наиболее опасных угроз для проекта. Механизм анализа риска на основе нечеткой логики обладает широкими возможностями и позволяет адаптировать его к имеющимся моделям управления рисками. Недостатками данного подхода являются субъективность в выборе функций принадлежности и формировании правил нечеткого ввода.
Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечеткой сети [30]	Рассмотрена методика оценки рисков ИБ на основе нейронной сети, которая позволяет расширить возможности метода моделирования, адекватно использовать качественные и количественные оценки входных параметров, полученные от экспертов. Методика позволяет учитывать качество входной информации и степень доверия источников информации, а также обладает широкими возможностями, позволяющими адаптировать ее к разнообразным профилям прикладных систем и встраивать в состав разработок систем управления рисками ИБ.
Васильев В.И., Вульфин А.М., Кудрявцева Р.Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования [31]	Рассматривается применение технологии когнитивного моделирования для решения задач анализа и управления рисками ИБ и основные этапы когнитивного анализа. Полученные качественные модели в виде НКК полезны на этапе предварительной оценки рисков ИБ, при отсутствии достоверных статистических данных. Когнитивные модели обладают большей интерпретируемостью и предоставляют больше степеней свободы лицу, принимающему решение на основании результатов моделирования. Однако изучение реального сложного объекта встречается с рядом труднопреодолимых фактором (высокая размерность пространства состояний, неоднозначность выбора состава базовых концептов и выявления наиболее значимых связей между ними, неопределенность в оценке силы этих связи)
Степанова Е.С., Машкина И.В., Васильев В.И. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности [111]	Проводится количественная оценка рисков нарушения ИБ методом построения модели угроз на основе НКК, отражающей пути распространения угроз от источников до объектов атаки с учетом информационной инфраструктуры. На основе полученных значений полного относительного риска проводится модернизация системы защиты информации, после чего расчетное значение риска уменьшилось в 5,2 раз.
Ажмухамедов И. М., Князева О. М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз	Предложена методика на основе нечеткой когнитивной модели, состоящей из шести иерархических уровней (механизмы и средства защиты; угрозы и уязвимости; атаки; повреждения ресурсов и средств защиты; свойства информации, характеризующие ее защищенность, интегральный показатель уровня ИБ). Входными данными являются лингвистические

Источник	Описание применяемых интеллектуальных методов
информационной безопасности [15]	оценки текущего (или планируемого) состояния средств защиты информации, на основе которых рассчитываются значения концептов на вышестоящих уровнях. Методика позволяет адекватно оценивать уровень ИБ, а также вырабатывать практические рекомендации по его повышению. Но применение данного метода к сложным масштабируемым системам достаточно трудоемко.
Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesian attack graphs [164]	Описана структура управления рисками ИБ с использованием байесовских сетей, которая позволяет количественно оценивать вероятность реализации атаки на различных уровнях сети. Предлагается моделирование атак на сеть с использованием информации об уязвимостях (численные показатели метрик CVSS), что дает менее субъективные результаты оценки рисков. Также обеспечивается динамический анализ модели в процессе развертывания сети. Однако метод имеет и существенный недостаток, связанный с проблемами масштабируемости, принятие решения в больших моделях требует больших вычислительных затрат.
Munoz-Gonzalez L. et al. Exact Inference Techniques for the Analysis of Bayesian Attack Graphs [155]	Предлагается осуществлять статическую и динамическую оценку рисков ИБ с использованием байесовских графов атак. Модель позволяет оценить риски ИБ от реализации атаки путем расчета вероятности того, что нарушитель скомпрометирует каждый узел с учетом уже скомпрометированных узлов. Несмотря на то, что эта модель направлена на изучение возможных атак, она не связана со стандартами шаблонов атак (например, CAPEC) и иными базами данных.

Таблица Г.3 – Подходы к моделированию сценариев атак

Источник	Описание подхода к моделированию сценариев атак
Большаков А.С., Раковский Д.И. Программное обеспечение моделирования угроз безопасности информации в информационных системах [27]	Разработано ПО для моделирования УБИ в инфосистемах различного назначения с учетом БДУ ФСТЭК. Проводится группировка и ранжирование угроз БДУ ФСТЭК по объектам их воздействия на информационные ресурсы, что имеет практическую ценность с точки зрения выработки мер по обеспечению ИБ. Однако за основу взят устаревший методический документ ФСТЭК России.
Абрамов Е.С., Андреев А.В., Мордвин Д.В. Применение графов атак для моделирования вредоносных сетевых воздействий [13]	Описывается процесс расчета графа атак, анализ полученных результатов и оценка эффективности существующих контрмер. Рассматриваются все фазы функционирования ПО, предназначенного для проведения оценки защищенности: автоматизация построения модели сети, расчета графа атак, анализа полученных результатов и эффективности существующих контрмер, автоматизация процесса совершенствования и выработки новых контрмер. Использование графов атак при проведении анализа защищенности позволяет учесть взаимосвязь отдельных узлов и их параметры

Источник	Описание подхода к моделированию сценариев атак
	защищенности, что дает более точные данные для оценки защищенности всей системы в целом.
Горбачев И.Е., Глухов А.П. Моделирование процессов нарушения информационной безопасности критической инфраструктуры [55]	Представлен комплекс моделирования процессов нарушения ИБ. Исследованы неопределенности процесса моделирования нарушителя и пути их устранения. Для моделирования действий нарушителя, адекватного отображения его структуры, требуется разработать типовую онтологическую модель для представления знаний о нарушителях, после чего, в ходе проведения аудита, насыщать ее экспертными данными о нарушителе с привязкой к конкретной АСУ ТП, тем самым формируя базу знаний о нарушителе. Отмечаются прогностические возможности операционного комплекса, позволяющие генерировать с опережением новые модели нарушителя, исследовать их возможности и предлагать различные варианты защиты.
Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя [62]	Предлагается методика построения угроз для АСУ ТП, основанная на моделировании возможных сценариев действий нарушителя безопасности информации. Предложенная методика учитывает многоуровневую структуру объекта защиты и возможность реализации угрозы ИБ с помощью различных сценариев. По каждой возможной угрозе и нарушителю строится свое дерево атак, где вершина дерева – реализация угрозы. Количество уровней при построении дерева атак определяется исходя из требуемого уровня детализации сценария реализации угрозы. Основной проблемой построения деревьев атак является масштабируемость.
Котенко Д.И., Котенко И.В., Саенко И.Б. Методика итерационного моделирования атак в больших компьютерных сетях [76]	Разработана методика итерационного моделирования атак в больших компьютерных сетях, основанная на формальной модели, где процесс моделирования реализуется в виде следующих друг за другом итераций, которые последователь уточняют параметры объекта исследования и предъявляемые к нему требования. Формальная модель итерационного моделирования атак включает модели процессов определения задач моделирования, построения моделей атак, запуска моделей и анализа результатов моделирования атак. Процессы построения моделей атак могут быть декомпозированы различным образом в зависимости от предпочтительных классификаций атак, классификаций методов и средств моделирования атак.
Котенко И.В., Чечулин А.А. Аналитическое моделирование атак для управления информацией и событиями безопасности [77]	Рассматривается аналитическое моделирование атак, позволяющее строить многоуровневые модели сценариев атак на основе уязвимостей, а также использовать графы атак и зависимости сервисов для обнаружения атак и расчета метрик ИБ.
Новохрестов А.К. и др. Модель угроз безопасности автоматизированной	Подход к построению модели предполагает разделение системы на уровни сетей, операционных систем и ПО. Для описания угроз безопасности автоматизированной системы коммерческого учета энергоресурсов используется многоуровневая модель, построенная с помощью атрибутивного метаграфа вложенности, что позволяет получить полный перечень УБИ.

Источник	Описание подхода к моделированию сценариев атак
системы коммерческого учета энергоресурсов [92]	
Tatam M. et al. A review of threat modelling approaches for APT-style attacks [172]	Рассматриваются подходы к моделированию целевых угроз, их достоинства и недостатки. Подходы специфичны для каждого уровня организации, связанного с ним проекта и требований. Показано, что сложность современных объектов защиты требует гибридного подхода к моделированию угроз. Понимая нарушителей, их мотивацию и навыки можно выявить актуальность угрозы. Видимость этих угроз всем заинтересованным сторонам, помогает выявить все сценарии реализации угроз на всех этапах и уровнях.
Xu D. et al. Automated security test generation with formal threat models [179]	STRIDE помогает устранять угрозы конфиденциальности, целостности, доступности, аутентификации, авторизации и неотказуемости. Однако он не определяет конкретные сценарии атак, а в первую очередь классифицирует общие типы угроз, поэтому необходимо также исследовать и учитывать дополнительные сценарии из известных библиотек атак. Категория STRIDE может иметь несколько угроз, и альтернативно угроза может иметь несколько категорий STRIDE.
Gore R., Padilla J., Diallo S. Markov chain modeling of cyber threats [133]	Рассматриваются подходы к моделированию угроз на основе стохастической модели, преобразующей действия атаки и связанные с ними атрибуты в цепи Маркова и анализирующей их с помощью матриц перехода состояний, т. е. следующее состояние системы полностью зависит от текущего состояния. Этот аспект позволяет цепям Маркова идентифицировать цепочки сценариев атаки, которые требуют соблюдения предшествующего и текущего состояний системы, прежде чем атака сможет продолжить свой путь.
Yeboah-Ofori A., Islam S. Cyber cyber threats environments [181]	Рассматривается моделирование атак с использованием инструмента STIXviz. В основе моделирования лежат тактики, техники и процедуры матрицы ATT&CK, позвляющие проанализировать поведение нарушителя в наборах инцидентов. Собранная в процессе моделирования атак информация дает представление о модели поведения нарушителя, о его возможностях, действиях и намерениях. Моделирование атак и анализ моделей поведения на основе наборов сценариев, использующих в своем составе компоненты матрицы ATT&CK, позволяют определить и понять риски ИБ.
Noel S. et al. CyGraph: graph-based analytics and visualization for cybersecurity [156]	Рассматривается CyGraph, который объединяет отдельные данные и события в общую картинку для поддержки принятия решений и ситуационной осведомленности. Он сопоставляет предупреждения о вторжении с известными путями эксплуатации уязвимостей и предлагает наилучший способ реагирования на атаки. CyGraph включает модель графа атак, которая отображает потенциальные пути атак через сеть. Сюда входят сетевые атрибуты, которые потенциально способствуют успеху атаки, такие как топология сети, правила межсетевого экрана, конфигурации узлов и уязвимости. Результирующий граф знаний фиксирует сложные отношения между сущностями в области ИБ.

Приложение Д – Базы данных угроз, уязвимостей и шаблонов компьютерных атак

На сегодняшний день основными инструментами для моделирования сценариев атак являются международные базы данных компании MITRE и российская БДУ ФСТЭК.

Стандарт CPE (Common Platform Enumeration) представляет собой структурирование информации о всех возможных продуктах, операционных систем и аппаратных устройств, их версиях, вендорах и прочем с возможностью получения соответствия CPE и CVE (т.е. необходимо для определения применимости уязвимости). Данное решение компании MITRE было призвано стандартизировать все существующие платформы и создать методы их определения, однако производители ПО проигнорировали призыв к систематизации информации о своих продуктах и такой перспективны инструмент все еще остается малораспространенным, хотя его использование позволило бы решить проблему сопоставления результатов инвентаризации системы и данных уязвимостей.

Стандарт CVE (Common Vulnerabilities and Exposures) является на сегодняшний день основным стандартом в области унифицированного именования и регистрации обнаруженных уязвимостей ПО. Каждая обнаруженная уязвимость записывается в базу и содержит краткое описание типа и причин уязвимости, уязвимые версии ПО, оценку критичности уязвимости в соответствии со стандартом CVSS (Common Vulnerability Scoring System), ссылки на внешние источники с информацией об уязвимости, при этом происходит периодическое обновление информации. Сильной стороной стандарта CVE является его повсеместная поддержка в современном ПО и сервисах, направленных на обеспечение ИБ (базы данных и реестры уязвимостей, системы обнаружения атак, антивирусные средства, сканеры безопасности и средства мониторинга и др.).

Стандарт CWE (Common Weakness Enumeration) – классификация недостатков ПО, т.е. ошибок, которые могут привести к возникновению

уязвимостей. Для классификации недостатков используется многоуровневая структура, которая описывает древовидное устройство CWE: конечные недостатки объединяются в типы, типы – в категории, категории – в представления. Каждое представление – особый способ классификации записей CWE, предназначенный для упрощения решения конкретной задачи.

MITRE ATT&CK [151] – это серия тактических матриц, которые используются для описания действий нарушителя. Существует три основные матрицы: Enterprise, Mobile и ICS. Начальные этапы атак, затрагивающие ИТ-инфраструктуру, возможно описать с помощью тактик и техник, представленных в базе знаний ATT&CK для Enterprise. Однако поведение нарушителя на более поздних стадиях атак, если они затрагивают технологический сегмент, выходит за рамки ATT&CK для Enterprise. Ключевое отличие в структуре ATT&CK для ICS – наличие дополнительных тактик, которые были определены для более точного описания целей нарушителя в области технологий АСУ ТП. В ATT&CK для ICS уделяется основное внимание действиям, которые нарушители предпринимают против систем и функций промышленных систем управления. Этапы развития атак и тактики их реализации – это то, какие цели нарушитель преследует на данный момент. В свою очередь, тактики делятся на техники, т.е. на уточнение способов – как нарушите добивается этих целей. В отличие от тактик и техник из Методики ФСТЭК, приведенные в матрице ATT&CK тактики подробно описывают возможные варианты поведения нарушителя, для каждой техники представлено подробное описание и известные случаи применения, а также методы обнаружения и меры по нейтрализации атаки. Таким образом, база данных ATT&CK позволяет детально проанализировать действия нарушителя при моделировании атак.

Стандарт CAPEC (Common Attack Pattern Enumeration and Classification) [124], включает в себя перечень и классификатор шаблонов типовых атак с описанием целей, целевых уязвимостей и общих методов, используемых при атаках на компоненты информационной системы.

CAPEC позволяет:

– стандартизировать получение и описание шаблонов атак;

– собирать известные шаблоны атак в общий перечень для последующего эффективного использования;

– классифицировать шаблоны атак для легкого определения во всем перечне необходимого подмножества;

– с помощью явных ссылок связывать шаблоны атак и перечни общеизвестных слабых мест CWE.

Каталог в базе CAPEC представляет собой набор меташаблонов атак, сгруппированных по некоторым общим критериям и включающим в себя наборы стандартных шаблонов атак. Меташаблон атаки представляет собой абстрактную характеристику конкретной методологии или техники, используемой при проведении атаки. Стандартные шаблоны атак ориентированы на конкретную методологию или технику, используемую для осуществления атаки.

БДУ ФСТЭК [24] (Банк данных угроз безопасности информации ФСТЭК России) содержит сведения об основных УБИ и уязвимостях, характерных для государственных информационных систем, информационных систем персональных данных и АСУ ТП. БДУ ФСТЭК содержит, помимо названия и кода угрозы, её краткое описание, вероятные источники, объекты воздействия и последствия, которые повлечет за собой реализация угрозы. Эти сведения не структурированы, угрозы классифицированы по нарушителям, которые могут ими воспользоваться, а также последствиям, которые использование этих угроз может повлечь. Содержание БДУ ФСТЭК не является исчерпывающим и может дополняться по результатам исследования объекта защиты.

При использовании БДУ ФСТЭК в процессе моделирования сценариев атак и оценки рисков ИБ нет возможности перейти от общетеоретического и высокоуровневого описания угрозы на уровень оценки конкретных действий нарушителя при ее реализации

Приложение Е – Методика количественной оценки рисков ИБ АСУ ТП промышленных объектов

Методика количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе нечеткого когнитивного моделирования сценариев проведения 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, представлена в виде функциональной модели в нотации IDEF0. Данная модель позволяет рассмотреть процесс количественной оценки рисков как набор взаимосвязанных действий с последующей их детализацией и представлением в виде иерархической структуры дочерних моделей в соответствии с методом и алгоритмами, предложенными в диссертации.

Основные этапы проведения оценки рисков ИБ выделенных зон АСУ ТП и промышленной системы в целом отображены в виде декомпозиции первого уровня функциональной модели (Рисунок 2.2). Дальнейшая декомпозиция второго уровня блоков функциональной модели отображает последовательность действий на каждом этапе проведения оценки рисков ИБ АСУ ТП.

На рисунке Е.1 представлена диаграмма декомпозиции второго уровня блока функциональной модели A0-1 и отображает процесс построения модели объекта защиты на основе ГОСТ 62443, включающий в себя построение базовой, объектной и зональной модели АСУ ТП, рассмотренные в диссертации в разделе 2.2.

На рисунке Е.2 представлена диаграмма декомпозиции второго уровня блока функциональной модели A0-2 и отображает процесс построения графа атак, графовой модели сценариев атак и модели шаблонов атак на основе полученной иерархии моделей объекта. Подробно эти этапы рассматривались в разделе 3.1 данной диссертации.

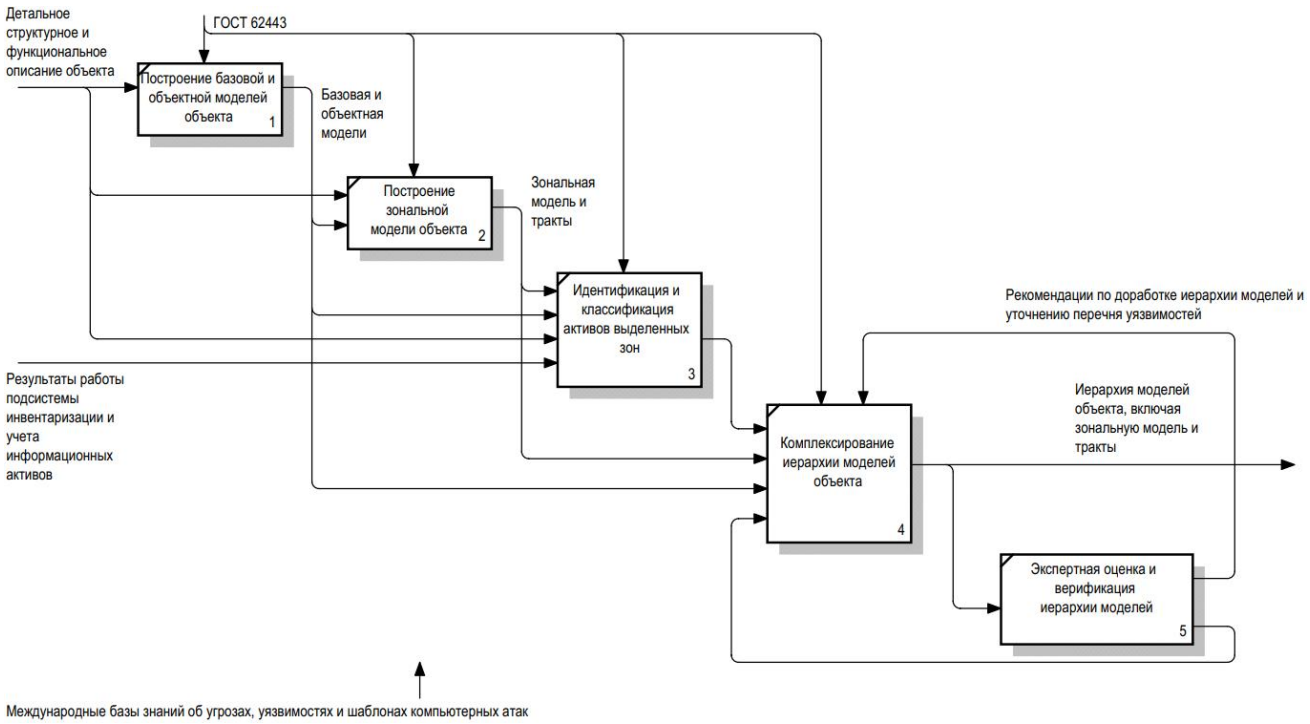


Рисунок Е.1 – Декомпозиция блока А0-1 «Построение моделей объекта на основе ГОСТ 62443»

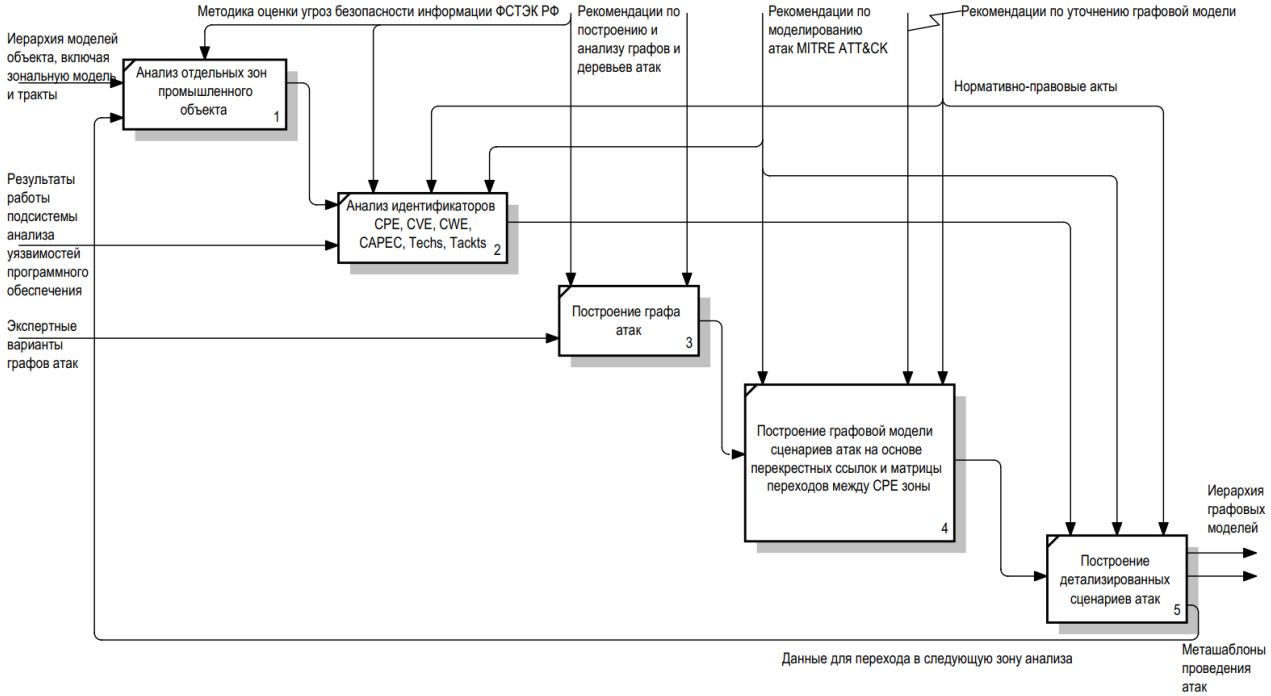


Рисунок Е.2 – Декомпозиция блока А0-2 «Построение графа атак, графовой модели сценариев атак и модели шаблонов атак»

На рисунке Е.3 представлена диаграмма декомпозиции второго уровня блока функциональной модели А0-3 и отображает процесс построения нечеткой

когнитивной модели сценариев атак (раздел 3.2) на основе полученной иерархии моделей объекта и иерархии графовых моделей.

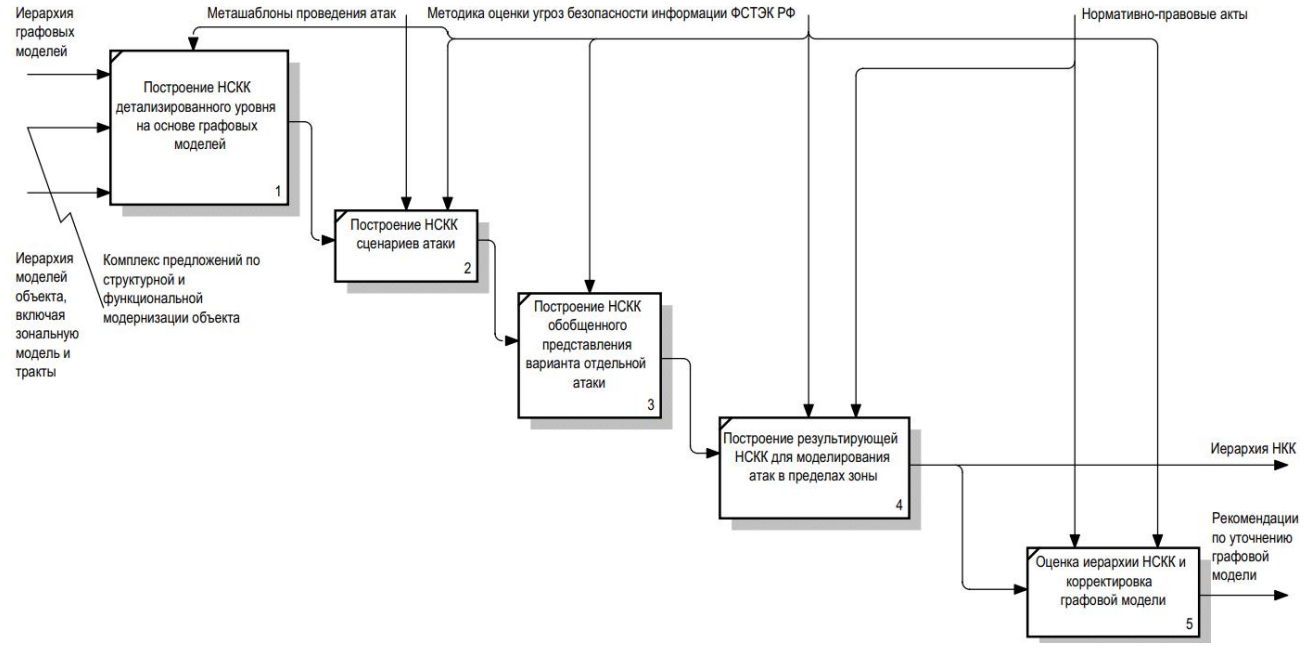


Рисунок Е.3 – Декомпозиция блока А0-3 «Построение нечеткой когнитивной модели сценариев атак»

На рисунке Е.4 представлена диаграмма декомпозиции второго уровня блока функциональной модели А0-4 и отображает процесс построения модели угроз ИБ АСУ ТП, представляющий собой формализацию описания объекта, нарушителя, возможных последствий реализации угроз и возможных способов их реализации.

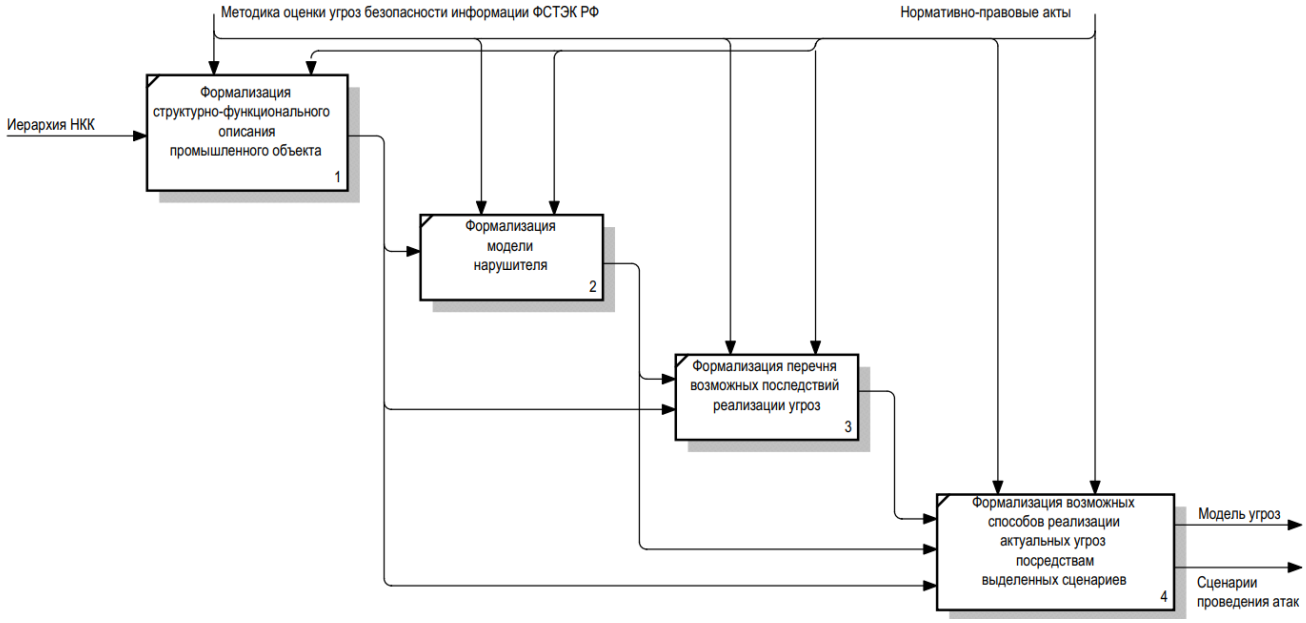


Рисунок Е.4 – Декомпозиция блока А0-4 «Построение модели угроз ИБ АСУ ТП»

Завершающий этап предложенной методики (Рисунок Е.5) проводится на основе сценариев атак и модели угроз и включает в себя количественную оценку рисков ИБ АСУ ТП, выбор контрмер с распределением их функциональных ресурсов в соответствии с наиболее уязвимыми элементами промышленной системы, оценку эффективности выбранных мер защиты и выработку практических рекомендаций и предложений по повышению уровня защищенности ИБ АСУ ТП промышленного объекта.

Применение разработанной методики на АСУ ТП промышленного объекта, позволяет получить:

– количественную оценку рисков ИБ выделенных зон АСУ ТП и всего объекта в целом;

– практические рекомендации по повышению уровня защищенности АСУ ТП промышленного объекта;

– комплекс предложений по структурной и функциональной модернизации АСУ ТП.

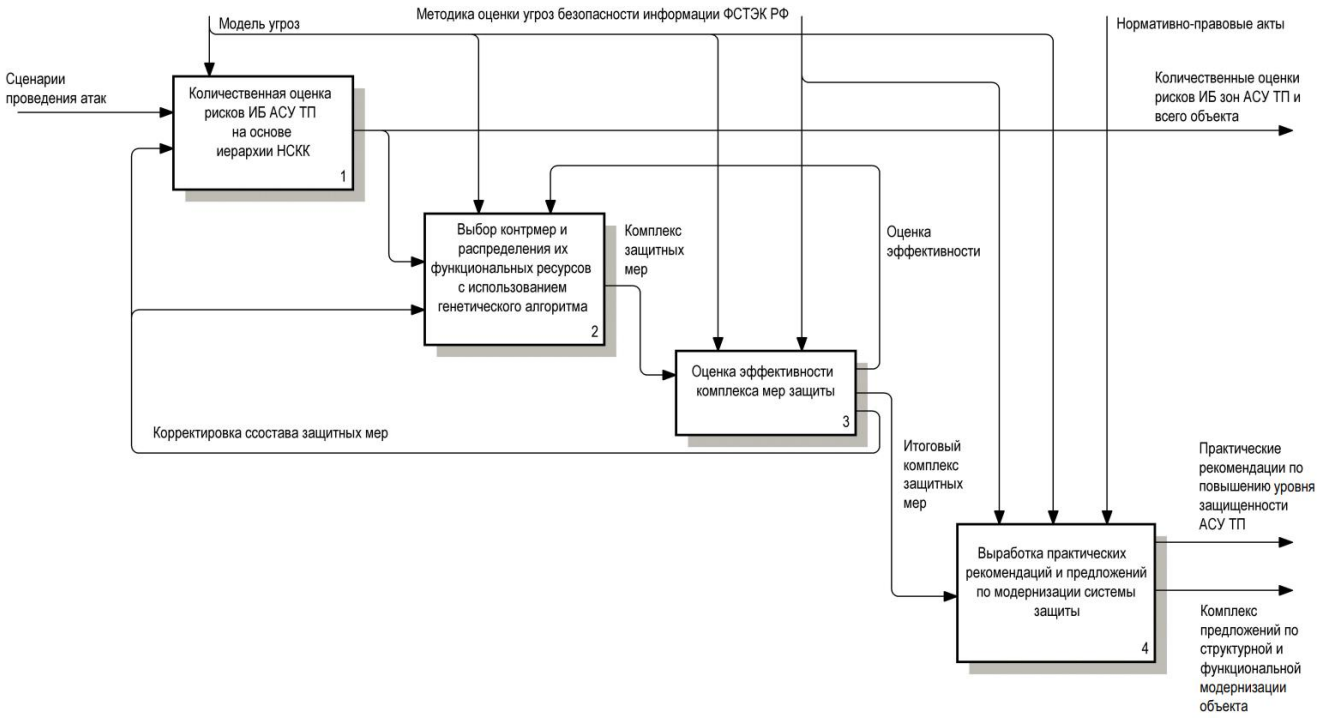


Рисунок Е.5 – Декомпозиция блока А0-5 «Количественная оценка рисков ИБ АСУ ТП и выработка практических рекомендаций по повышению уровня защищенности объекта защиты»

Приложение Ж – Фрагменты листинга программного кода реализации подсистемы когнитивного моделирования

```
classdef FGCM

    properties (Access = public)
        n           % количество вершин
        X           % начальные состояния концептов
        G           % ориентированный граф НКК
        FGCM_name   % имя карты
    end

    methods (Access = public)
        %% конструктор
        function self = FGCM(num_vertexes, ...
                             s, ...
                             t, ...
                             W, ...
                             type, ...
                             FGCM_name)

            self.FGCM_name = FGCM_name;

            self.n = num_vertexes;

            % начальные состояния концептов
            X(num_vertexes) = GreyNumber();
            self.X = X';

            % создание таблицы ребер графа
            EdgeTable = table(  [s t], ...
                                type, ...
                                W, ...
                                'VariableNames', {'EndNodes' 'type' 'W'});

            % задание списка вершин графа
            names = {};
            for k = 1:num_vertexes
                names{k} = sprintf('C_%d', k);
            end

            % создание таблицы вершин графа
            X_s(num_vertexes) = GreyNumber();
            NodeTable = table(names', X_s', 'VariableNames', {'Name' 'States'});

            % задание графа
            self.G = digraph(EdgeTable, NodeTable);
        end

        %% сохранение FGCM в csv файл
        function writeToFile(obj, file_name)
            pathToFIS = fullfile('.', 'dataSets', file_name);

            s = [];
            t = [];

            W_L = [];
            W_U = [];
            for k = 1:size(obj.G.Edges.EndNodes)
                source = split(obj.G.Edges.EndNodes{k, 1}, '_');
                s = [s; str2double(source{2})];

                target = split(obj.G.Edges.EndNodes{k, 2}, '_');
                t = [t; str2double(target{2})];

                W_L = [W_L; obj.G.Edges.W(k).W_L];
                W_U = [W_U; obj.G.Edges.W(k).W_U];
```

```
65.             end
66.
67.             varNames = {'source'; 'target'; 'type'; 'weight_L'; 'weight_U'};
68.             T = table(s, t, obj.G.Edges.type, W_L, W_U, 'VariableNames', varNames);
69.             writetable(T, pathToFIS, 'Delimiter', '\t')
70.
71.         end
72.
73.         %% расчет карты
74.         function obj = calc_FGCM(obj, num_iterations)
75.
76.             for k = 1:num_iterations
77.                 % добавляем новое состояние в матрицу изменения состояний
78.                 addX(obj.n) = GreyNumber();
79.                 obj.X = [obj.X addX'];
80.
81.                 for i = 1:obj.n
82.                     % находим список ребер и узлов графа - прецессоров
83.                     [eid, nid] = inedges(obj.G, i);
84.
85.                     hasLoop = 0;
86.                     num_precessors_node = length(nid);
87.
88.                     % цикл по всем узлам прецессорам
89.                     for j = 1:num_precessors_node
90.                         prev_node_id = nid(j);
91.                         prev_edge_id = eid(j);
92.         %                 fprintf(1, "\t\t\tp_node = %d[%d, %d]\n", prev_node_id,
    G.Edges.W(prev_edge_id).W_L, G.Edges.W(prev_edge_id).W_U);
93.
94.                         if (prev_node_id == i)
95.                             hasLoop = 1;
96.                             continue;
97.                         end
98.
99.                         % отличие в выносе отрицательного веса связи за скобки
100.                          % умножения. Подразумевает наличие скобок (X * W)
101.                          obj.X(i, k + 1) = obj.X(i, k + 1) + ...
102.                                            obj.G.Edges.type(prev_edge_id) .* ...
103.                                                (   obj.X(prev_node_id, k) * ...
104.                                                    obj.G.Edges.W(prev_edge_id));
105.                    end
106.
107.                    if (hasLoop == 1)
108.                        obj.X(i, k + 1) = obj.X(i, k);
109.                        hasLoop = 0;
110.                    else
111.                        obj.X(i, k + 1) = FGCM.func_activ(obj.X(i, k) + obj.X(i, k
    + 1));
112.                    end
113.
114.                end
115.            end
116.        end % of function
117.
118.        %% Расчет эффективности карты
119.        function res = rate_FGCM(obj)
120.            num_iterations = size(obj.X, 2) - 1;
121.            res = ...
122.                (   obj.X(obj.n - 1, num_iterations + 1).getWhiteness() + ...
123.                    obj.X(obj.n, num_iterations + 1).getWhiteness() ...
124.                );
125.
126.        end % of function
127.
128.
129.        %% печать лога работы FGCM
130.        function print_log(obj)
131.
132.            % печать состояния концептов
133.            [num_vertexes, num_iterations] = size(obj.X);
```

```
134.             fprintf(1, "\n\n\n%d\n\n\n", num_iterations);
135.             X_Greyness = zeros(num_vertexes, num_iterations);
136.             X_Whiteness = zeros(num_vertexes, num_iterations);
137.             for i = 1:num_vertexes
138.                 for j = 1:num_iterations
139.                     fprintf(1, "\t%5.2f, %5.2f", obj.X(i, j).W_L, obj.X(i, j).W_U);
140.                     X_Greyness(i, j) = obj.X(i, j).getGreyness();
141.                     X_Whiteness(i, j) = obj.X(i, j).getWhiteness();
142.                 end
143.                 fprintf(1, "\n");
144.             end
145.
146.             % график стабилизации состояний концептов ("белизна")
147.             figure();
148.             plot(X_Whiteness', '-o');
149.             title('Изменение во времени состояний концептов', 'Interpreter',
    'latex');
150.             xlabel('iter');
151.             ylabel('X_{Whiteness}');
152.
153.             leg = {};
154.             for i = 1:num_vertexes
155.                 leg{i} = sprintf('$X_{%d}$', i);
156.             end
157.             legend(leg, 'Interpreter', 'latex', 'Location', 'southeast',
    'NumColumns', 4);
158.             ylim([0 1])
159.
160.             pathToFig = fullfile('.', 'pics', strcat(obj.FGCM_name, '_XW.png'));
161.             exportgraphics(gca, pathToFig, 'Resolution', 300)
162.
163.             % график стабилизации состояний концептов ("серость")
164.             figure();
165.             plot(X_Greyness', '-o');
166.             title('Изменение во времени состояний концептов', 'Interpreter',
    'latex');
167.             xlabel('iter');
168.             ylabel('X_{Greyness}');
169.
170.             leg = {};
171.             for i = 1:num_vertexes
172.                 leg{i} = sprintf('$X_{%d}$', i);
173.             end
174.             legend(leg, 'Interpreter', 'latex', 'Location', 'southeast',
    'NumColumns', 4);
175.
176.             pathToFig = fullfile('.', 'pics', strcat(obj.FGCM_name, '_XG.png'));
177.             exportgraphics(gca, pathToFig, 'Resolution', 300)
178.
179.             % отрисовка таблицы весовых коэффициентов
180.             num_weights = length(obj.G.Edges.W);
181.             weights_table = zeros(num_weights, 3);
182.             for i = 1:num_weights
183.                 weights_table(i, 1) = obj.G.Edges.W(i).W_L;
184.                 weights_table(i, 2) = obj.G.Edges.W(i).W_U;
185.                 weights_table(i, 3) = obj.G.Edges.W(i).getGreyness();
186.             end
187.             fig = figure('Name', 'W');
188.             uit = uitable(fig, 'ColumnName', {'W_L'; 'W_U'; 'Greyness'}, 'Data',
    weights_table);
189.
190.             data = get(uit, 'Data');
191.             pathToTable = fullfile('.', 'pics', strcat(obj.FGCM_name,
    '_W_L_U_G.xlsx'));
192.             writematrix(data, pathToTable)
193.
194.             % отрисовка таблицы состояния концептов
195.             X_L = zeros(num_vertexes, num_iterations);
196.             for i = 1:num_vertexes
197.                 for j = 1:num_iterations
198.                     X_L(i, j) = obj.X(i, j).W_L;
```

```
199.                 end
200.             end
201.             fig = figure('Name', 'X_L');
202.             uit = uitable(fig, 'Data', X_L);
203.
204.             data = get(uit, 'Data');
205.             pathToTable = fullfile('.', 'pics', strcat(obj.FGCM_name,
    '_X_L.xlsx'));
206.             writematrix(data, pathToTable)
207.
208.             X_U = zeros(num_vertexes, num_iterations);
209.             for i = 1:num_vertexes
210.                 for j = 1:num_iterations
211.                     X_U(i, j) = obj.X(i, j).W_U;
212.                 end
213.             end
214.             fig = figure('Name', 'X_U');
215.             uit = uitable(fig, 'Data', X_U);
216.
217.             data = get(uit, 'Data');
218.             pathToTable = fullfile('.', 'pics', strcat(obj.FGCM_name,
    '_X_U.xlsx'));
219.             writematrix(data, pathToTable)
220.
221.         end % of function
222.     end
223.
224.         methods (Static)
225.         %% чтение FGCM из файла
226.         function [n, s, t, W, type] = readFromFile(file_name)
227.             pathToFIS = fullfile('.', 'dataSets', file_name);
228.
229.             % параметры чтения CSV файла - для проверки
230.             opts = detectImportOptions(pathToFIS);
231.
232.             % чтение файла
233.             fis = readtable(pathToFIS, ...
234.                             'Format', '%f%f%f%f%f'); % source, target, type,
    weight(L U)
235.
236.             s = fis.source;
237.             t = fis.target;
238.             type = fis.type;
239.
240.             num_edges = length(s);
241.             W(num_edges) = GreyNumber();
242.             for k = 1:num_edges
243.                 W(k) = GreyNumber(fis.weight_L(k), fis.weight_U(k));
244.             end
245.             W = W';
246.
247.             % количество вершин
248.             n = max(max(s), max(t));
249.         end % of function
250.
251.         %% чтение FGCM из файла с нечетким заданием весов
252.         function [n, s, t, W, type] = readFromFileFL(file_name)
253.             pathToFIS = fullfile('.', 'dataSets', file_name);
254.
255.             % параметры чтения CSV файла - для проверки
256.             opts = detectImportOptions(pathToFIS);
257.
258.             % чтение файла
259.             fis = readtable(pathToFIS, ...
260.                             'Format', '%f%f%f%s'); % source, target, type, weight
261.
262.             s = fis.source;
263.             t = fis.target;
264.             type = fis.type;
265.
```

```
266.             f_value = [GreyNumber(0, 0) GreyNumber(0, 0.15) GreyNumber(0.15, 0.35)
   GreyNumber(0.35, 0.6) GreyNumber(0.6, 0.85) GreyNumber(0.85, 1.0)];
267.             f_key = ["Z" "VL" "L" "M" "H" "VH"];
268.             d = dictionary(f_key, f_value);
269.
270.             num_edges = length(s);
271.             W(num_edges) = GreyNumber();
272.             for k = 1:num_edges
273.                 key = fis.weight(k);
274.                 W(k) = d(key);
275.             end
276.             W = W';
277.
278.             % количество вершин
279.             n = max(max(s), max(t));
280.         end % of function
281.
282.         %% функция активации
283.         function res = func_activ(val)
284.             res = GreyNumber();
285.             res.W_L = tanh(val.W_L / 2);
286.             res.W_U = tanh(val.W_U / 2);
287.         end
288.
289.
290.          end
291. end
```

Приложение З – Комплекс когнитивных моделей для оценки риска ИБ территориально распределенной АСУ ТП нефтедобывающего месторождения

На рисунке 3.1 представлена архитектура АСУ ТП установки подготовки нефти / сбора воды (УПН / УПСВ), где ПАЗ – противоаварийная защита; КНС – кустовая насосная станция; МН – магистральный нефтепровод; АСТПиКЗ – автоматическая система пожаротушения и контроля загазованности.

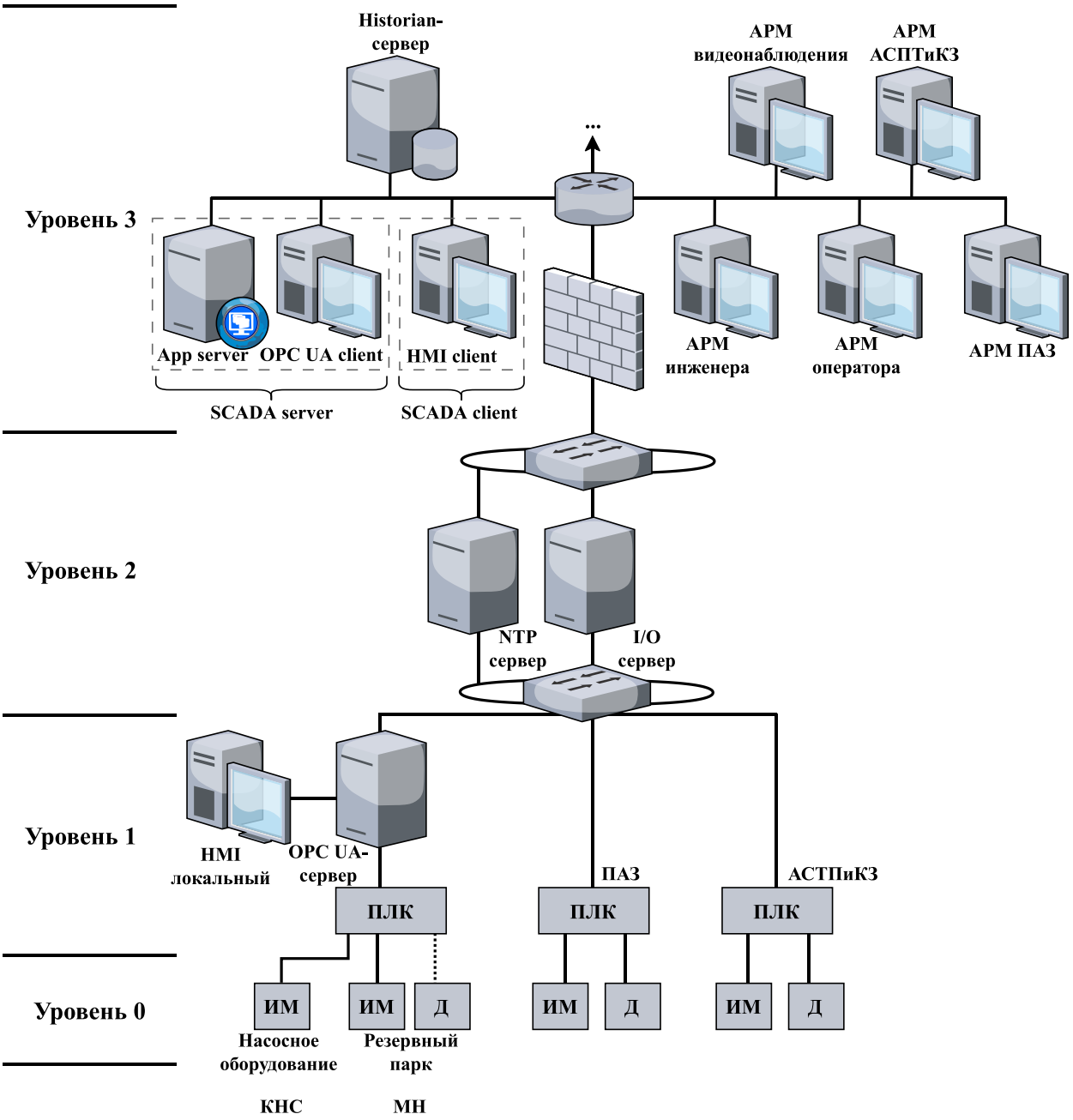


Рисунок 3.1 – АСУ ТП установки подготовки нефти / сбора воды (УПН / УПСВ)

Основные задачи: отделение нефти от воды и газа; подача воды на КНС; предварительная очистка нефти.

На рисунке 3.2 представлена архитектура АСУ ТП Пункта сдачи-приема нефти.

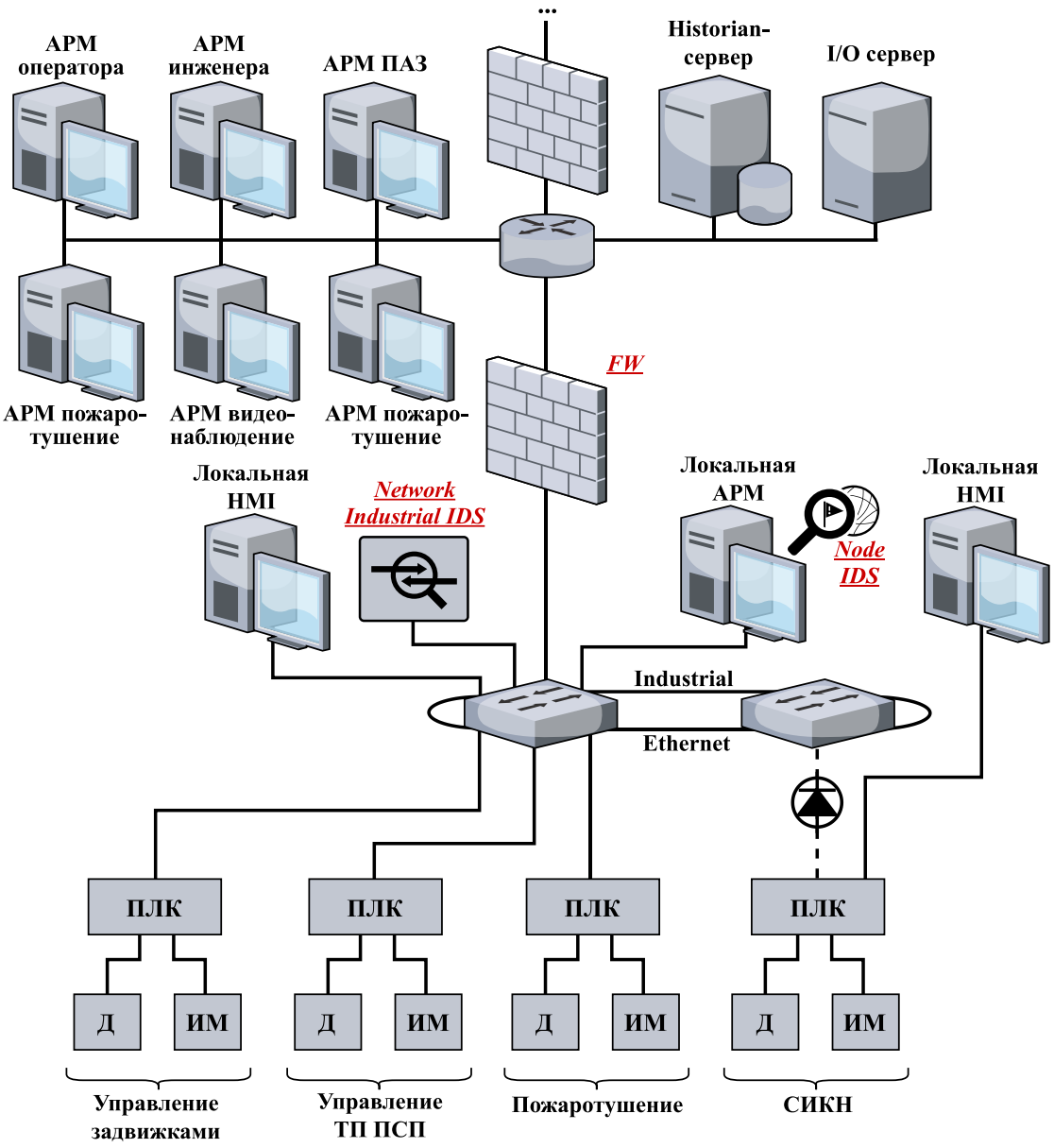


Рисунок 3.2 – АСУ ТП Пункта сдачи-приема нефти

Основные функции: оперативный круглосуточный учет; инвентаризация нефти в резервуарах; определение качественных показателей.

На рисунке 3.3 приведена НКК АСУ ТП пункта сдачи-приема нефти.

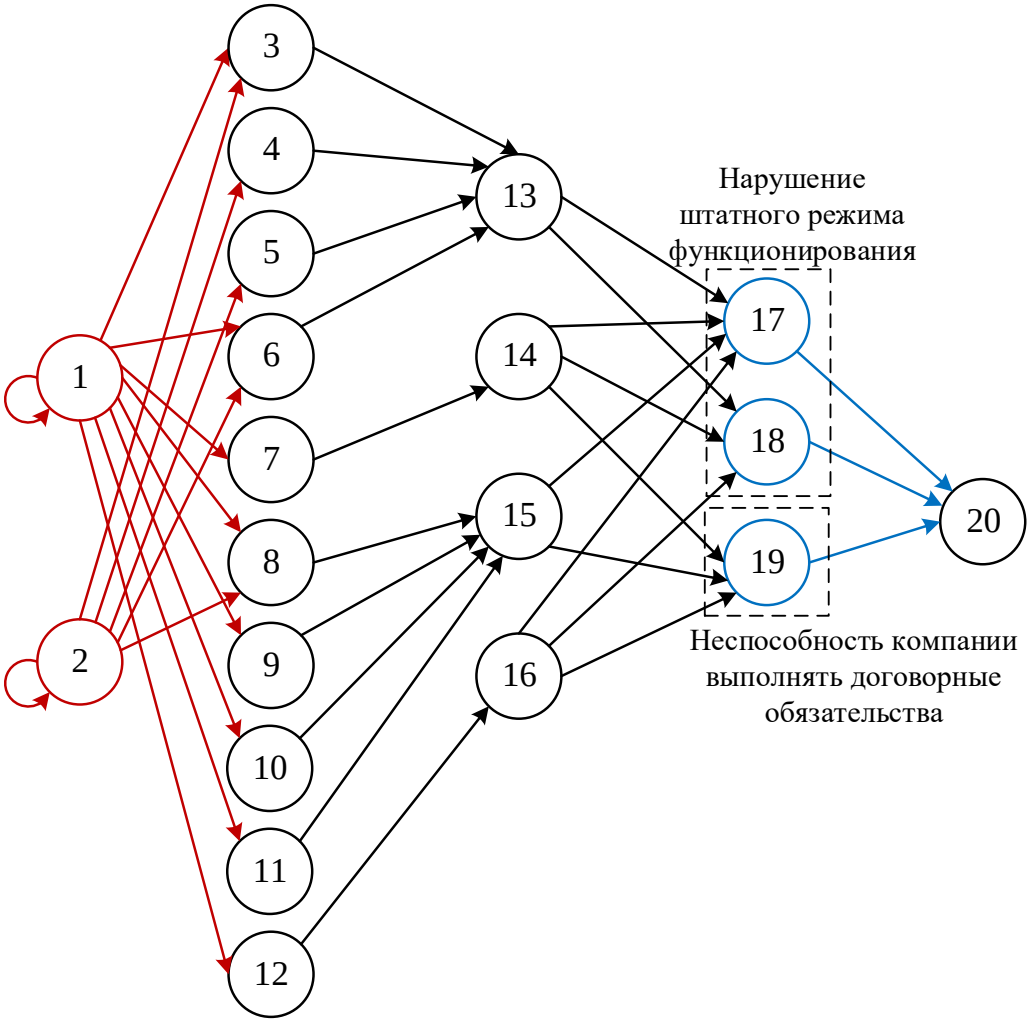


Рисунок 3.3 – НКК АСУ ТП пункта сдачи-приема нефти

В таблице 3.1 приведено описание концептов части АСУ ТП пункта сдачи-приема нефти.

Таблица 3.1 – Описание концептов части АСУ ТП Пункта сдачи-приема нефти

Концепт	Описание
C_1	Внешний нарушитель
C_2	Внутренний нарушитель
C_3	Сценарий реализации угрозы УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации. Реализует внешний нарушитель с высоким потенциалом и внутренний нарушитель с низким потенциалом
C_4	Сценарий реализации угрозы УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы.

Концепт	Описание
	Реализует внутренний нарушитель с низким потенциалом
C_5	Сценарий реализации угрозы УБИ.177: Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью. Реализует внутренний нарушитель с низким потенциалом
C_6	Сценарий реализации угрозы УБИ.179: Угроза несанкционированной модификации защищаемой информации. Реализует внешний и внутренний нарушители с низким потенциалом
C_7	Сценарий реализации угрозы УБИ.204: Угроза несанкционированного изменения вредоносной программой значений параметров ПЛК. Реализует внешний нарушитель со средним потенциалом
C_8	Сценарий реализации угрозы УБИ.011: Угроза деавторизации санкционированного клиента беспроводной сети. Реализует внешний и внутренний нарушители с низким потенциалом
C_9	Сценарий реализации угрозы УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам. Реализует внешний нарушитель с низким потенциалом
C_{10}	Сценарий реализации угрозы УБИ.125: Угроза подключения к беспроводной сети в обход процедуры аутентификации. Реализует внешний нарушитель с низким потенциалом
C_{11}	Сценарий реализации угрозы УБИ.126: Угроза подмены беспроводного клиента или точки доступа. Реализует внешний нарушитель с низким потенциалом
C_{12}	Сценарий реализации угрозы УБИ.069: Угроза неправомерных действий в каналах связи. Реализует внешний нарушитель с низким потенциалом
C_{13}	АРМ КП
C_{14}	ПЛК
C_{15}	Устройство БШД
C_{16}	Сетевое оборудование
C_{17}	Потеря возможности мониторинга
C_{18}	Перевод объекта в аварийный режим
C_{19}	Остановка КП
C_{20}	Оценка рисков ИБ в $Зоне_1^2$

Соответствующие весовые коэффициенты НКК описаны в таблице 3.2.

Таблица 3.2 – Веса связей концептов НКК АСУ ТП пункта сдачи-приема нефти

Вес связи	Диапазон	Вес связи	Диапазон
$W_{1\text{-}1}$	[;]	$W_{7\text{-}14}$	(0,35; 0,6]
$W_{1\text{-}3}$	(0,15; 0,35]	$W_{8\text{-}15}$	(0,6; 0,85]

Вес связи	Диапазон	Вес связи	Диапазон
$W_{1\text{-}6}$	(0,6; 0,85]	$W_{9\text{-}15}$	(0,85; 1]
$W_{1\text{-}7}$	(0,35; 0,6]	$W_{10\text{-}15}$	(0,85; 1]
$W_{1\text{-}8}$	(0,6; 0,85]	$W_{11\text{-}15}$	(0,6; 0,85]
$W_{1\text{-}9}$	(0,6; 0,85]	$W_{12\text{-}16}$	(0,35; 0,6]
$W_{1\text{-}10}$	(0,6; 0,85]	$W_{13\text{-}17}$	[;]
$W_{1\text{-}11}$	(0,6; 0,85]	$W_{13\text{-}18}$	[;]
$W_{1\text{-}12}$	(0,6; 0,85]	$W_{14\text{-}17}$	[;]
$W_{2\text{-}2}$	[;]	$W_{14\text{-}18}$	[;]
$W_{2\text{-}3}$	(0,85; 1]	$W_{14\text{-}19}$	[;]
$W_{2\text{-}4}$	(0,85; 1]	$W_{15\text{-}17}$	[;]
$W_{2\text{-}5}$	(0,85; 1]	$W_{15\text{-}19}$	[;]
$W_{2\text{-}6}$	(0,85; 1]	$W_{16\text{-}17}$	[;]
$W_{2\text{-}8}$	(0,85; 1]	$W_{16\text{-}18}$	[;]
$W_{3\text{-}13}$	(0,35; 0,6]	$W_{16\text{-}19}$	[;]
$W_{4\text{-}13}$	(0,85; 1]	$W_{17\text{-}20}$	(0,35; 0,6]
$W_{5\text{-}13}$	(0,85; 1]	$W_{18\text{-}20}$	(0,6; 0,85]
$W_{6\text{-}13}$	(0,35; 0,6]	$W_{19\text{-}20}$	(0,85; 1]

НКК части АСУ ТП СУ скважинным насосным оборудованием (Уровень2) приведена на рисунке 3.4. В таблице 3.3 приведено описание концептов НКК части АСУ ТП СУ скважинным насосным оборудованием, а соответствующие весовые коэффициенты НКК описаны в таблице 3.4.

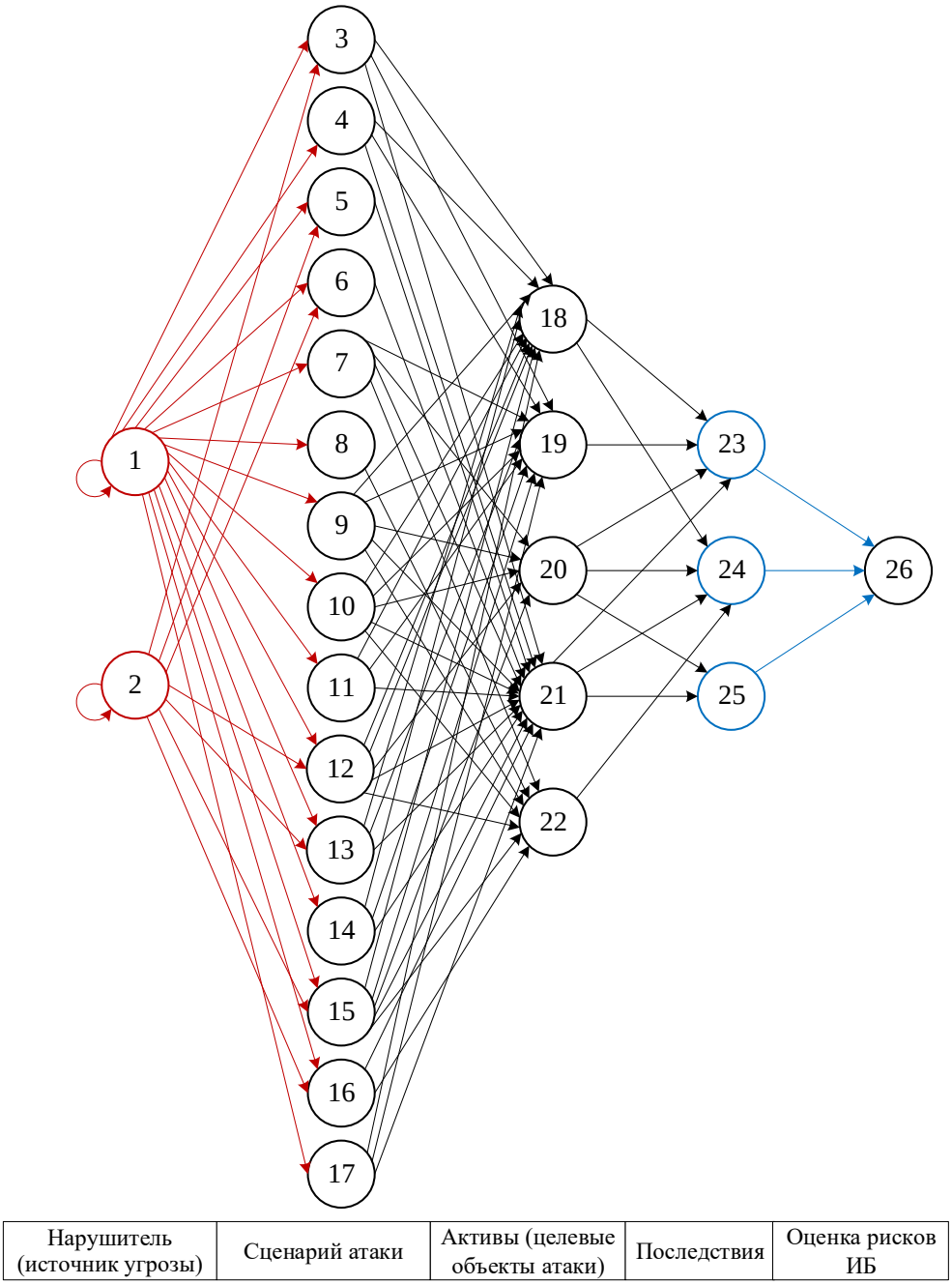


Рисунок 3.4 – НКК АСУ ТП СУ скважинным насосным оборудованием (Уровень2)

Таблица 3.3 – Описание концептов НКК АСУ ТП СУ скважинным насосным оборудованием (Уровень2)

Концепт	Описание
C_1	Внешний нарушитель
C_2	Внутренний нарушитель
C_3	Сценарий реализации угрозы УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными. Реализует внешний и внутренний нарушители с низким потенциалом

Концепт	Описание
C_4	Сценарий реализации угрозы УБИ.069: Угроза неправомерных действий в каналах связи. Реализует внешний нарушитель с низким потенциалом
C_5	Сценарий реализации угрозы УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети. Реализует внешний и внутренний нарушители со средним потенциалом
C_6	Сценарий реализации угрозы УБИ.080: Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети. Реализует внешний и внутренний нарушители со средним потенциалом
C_7	Сценарий реализации угрозы УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб. Реализует внешний нарушитель с низким потенциалом
C_8	Сценарий реализации угрозы УБИ.099: Угроза обнаружения хостов. Реализует внешний нарушитель с низким потенциалом
C_9	Сценарий реализации угрозы УБИ.103: Угроза определения типов объектов защиты. Реализует внешний нарушитель с низким потенциалом
C_{10}	Сценарий реализации угрозы УБИ.104: Угроза определения топологии вычислительной сети. Реализует внешний нарушитель с низким потенциалом
C_{11}	Сценарий реализации угрозы УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети. Реализует внешний нарушитель с низким потенциалом
C_{12}	Сценарий реализации угрозы УБИ.178: Угроза несанкционированного использования системных и сетевых утилит. Реализует внешний и внутренний нарушители с низким потенциалом
C_{13}	Сценарий реализации угрозы УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании». Реализует внешний и внутренний нарушители с низким потенциалом
C_{14}	Сценарий реализации угрозы УБИ.130: Угроза подмены содержимого сетевых ресурсов. Реализует внешний нарушитель с низким потенциалом
C_{15}	Сценарий реализации угрозы УБИ.145: Угроза пропуска проверки целостности программного обеспечения. Реализует внешний и внутренний нарушители с низким потенциалом
C_{16}	Сценарий реализации угрозы УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами. Реализует внешний нарушитель с низким потенциалом и внутренний нарушитель со средним потенциалом

Концепт	Описание
C_{17}	Сценарий реализации угрозы УБИ.193: Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика. Реализует внешний нарушитель со средним потенциалом
C_{18}	Сервер NTP
C_{19}	Historian-сервер
C_{20}	АРМ
C_{21}	App-сервер
C_{22}	АРМ SCADA client
C_{23}	Потеря возможности мониторинга
C_{24}	Перевод объекта в аварийный режим
C_{25}	Останов КП
C_{26}	Оценка рисков ИБ в Зоне$_3$[1]

Таблица 3.4 – Веса связей концептов НКК НКК АСУ ТП СУ скважинным насосным оборудованием (Уровень2)

Вес связи	Диапазон	Вес связи	Диапазон
$W_{1\text{-}1}$	[;]	$W_{10\text{-}18}$	(0,15; 0,35]
$W_{1\text{-}3}$	(0,6; 0,85]	$W_{10\text{-}19}$	(0,15; 0,35]
$W_{1\text{-}4}$	(0,6; 0,85]	$W_{10\text{-}20}$	(0,15; 0,35]
$W_{1\text{-}5}$	(0,35; 0,6]	$W_{10\text{-}21}$	(0,15; 0,35]
$W_{1\text{-}6}$	(0,35; 0,6]	$W_{10\text{-}22}$	(0,15; 0,35]
$W_{1\text{-}7}$	(0,6; 0,85]	$W_{11\text{-}18}$	(0,15; 0,35]
$W_{1\text{-}8}$	(0,6; 0,85]	$W_{11\text{-}19}$	(0,15; 0,35]
$W_{1\text{-}9}$	(0,6; 0,85]	$W_{11\text{-}21}$	(0,15; 0,35]
$W_{1\text{-}10}$	(0,6; 0,85]	$W_{12\text{-}18}$	(0,85; 1]
$W_{1\text{-}11}$	(0,6; 0,85]	$W_{12\text{-}19}$	(0,85; 1]
$W_{1\text{-}12}$	(0,6; 0,85]	$W_{12\text{-}20}$	(0,85; 1]
$W_{1\text{-}13}$	(0,6; 0,85]	$W_{12\text{-}21}$	(0,85; 1]
$W_{1\text{-}14}$	(0,6; 0,85]	$W_{12\text{-}22}$	(0,85; 1]
$W_{1\text{-}15}$	(0,6; 0,85]	$W_{13\text{-}18}$	(0,6; 0,85]
$W_{1\text{-}16}$	(0,6; 0,85]	$W_{13\text{-}19}$	(0,6; 0,85]
$W_{1\text{-}17}$	(0,35; 0,6]	$W_{13\text{-}21}$	(0,6; 0,85]
$W_{2\text{-}2}$	[;]	$W_{14\text{-}18}$	(0,15; 0,35]
$W_{2\text{-}3}$	(0,85; 1]	$W_{14\text{-}19}$	(0,15; 0,35]
$W_{2\text{-}5}$	(0,6; 0,85]	$W_{14\text{-}21}$	(0,15; 0,35]
$W_{2\text{-}6}$	(0,6; 0,85]	$W_{15\text{-}18}$	(0,85; 1]
$W_{2\text{-}12}$	(0,85; 1]	$W_{15\text{-}19}$	(0,85; 1]
$W_{2\text{-}13}$	(0,85; 1]	$W_{15\text{-}20}$	(0,85; 1]
$W_{2\text{-}15}$	(0,85; 1]	$W_{15\text{-}21}$	(0,85; 1]
$W_{2\text{-}16}$	(0,6; 0,85]	$W_{15\text{-}22}$	(0,85; 1]

Вес связи	Диапазон	Вес связи	Диапазон
$W_{3\text{-}18}$	(0,85; 1]	$W_{16\text{-}21}$	(0,85; 1]
$W_{3\text{-}19}$	(0,85; 1]	$W_{16\text{-}22}$	(0,85; 1]
$W_{3\text{-}21}$	(0,85; 1]	$W_{17\text{-}18}$	(0,15; 0,35]
$W_{4\text{-}18}$	(0,35; 0,6]	$W_{17\text{-}19}$	(0,15; 0,35]
$W_{4\text{-}19}$	(0,35; 0,6]	$W_{17\text{-}21}$	(0,15; 0,35]
$W_{4\text{-}21}$	(0,35; 0,6]	$W_{18\text{-}23}$	[;]
$W_{5\text{-}21}$	(0,85; 1]	$W_{18\text{-}24}$	[;]
$W_{6\text{-}21}$	(0,85; 1]	$W_{19\text{-}23}$	[;]
$W_{7\text{-}19}$	(0,15; 0,35]	$W_{20\text{-}23}$	[;]
$W_{7\text{-}20}$	(0,15; 0,35]	$W_{20\text{-}24}$	[;]
$W_{7\text{-}21}$	(0,15; 0,35]	$W_{20\text{-}25}$	[;]
$W_{7\text{-}22}$	(0,15; 0,35]	$W_{21\text{-}23}$	[;]
$W_{8\text{-}22}$	(0,15; 0,35]	$W_{21\text{-}24}$	[;]
$W_{9\text{-}18}$	(0,15; 0,35]	$W_{21\text{-}25}$	[;]
$W_{9\text{-}19}$	(0,15; 0,35]	$W_{22\text{-}24}$	[;]
$W_{9\text{-}20}$	(0,15; 0,35]	$W_{23\text{-}26}$	(0,35; 0,6]
$W_{9\text{-}21}$	(0,15; 0,35]	$W_{24\text{-}26}$	(0,6; 0,85]
$W_{9\text{-}22}$	(0,15; 0,35]	$W_{25\text{-}26}$	(0,85; 1]