Федеральное государственное бюджетное учреждение науки
Институт систем энергетики им. Л.А. Мелентьева
Сибирского отделения Российской академии наук

На правах рукописи

Гаськова Дарья Александровна

МЕТОДЫ, МОДЕЛИ И КОМПЛЕКС ПРОГРАММ АНАЛИЗА КИБЕРСИТУАЦИОННОЙ ОСВЕДОМЛЕННОСТИ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Специальность 05.13.18 – Математическое моделирование,
численные методы и комплексы программ

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
Кандидат технических наук
Массель Алексей Геннадьевич

ИРКУТСК – 2020

Оглавление

Введение

Актуальность диссертационной работы определяется двумя основными факторами. Первый фактор обусловлен необходимостью рассмотрения энергетики как критической инфраструктуры (КИ), нарушение функционирования или разрушение которой приводит к экстремальным ситуациям (ЭкС) и губительным последствиям и нарушению национальной безопасности (НБ) страны.

Вторым фактором является возрастание значимости проблемы кибербезопасности цифровой экономики в целом и цифровой энергетики [1] в частности.

Проблема обеспечения кибербезопасности в энергетическом секторе, как одной из важнейших критических инфраструктур, осложняется тесной связью энергетики со всеми сферами жизнедеятельности современного общества. Это подтверждается, с одной стороны, высокой значимостью обеспечения энергетической безопасности (ЭБ) России, а с другой, вступлением в силу Федерального закона № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной структуры Российской Федерации» [2] и принятием в 2019 году Доктрины энергетической безопасности Российской Федерации [3]. Несмотря на то, что Концепция стратегии кибербезопасности Российской Федерации [4] до сих пор не принята, противодействие киберугрозам является одним из приоритетных направлений Государственной программы «Научно-технологическое развитие Российской Федерации» на 2019-2030 годы [5].

Развитие и внедрение новых информационно-коммуникационных технологий, а также продвижение концепции цифровой трансформации энергетики, в совокупности со спецификой энергетического сектора обусловили необходимость включения киберугроз в список стратегических угроз ЭБ [6].

С одной стороны, использование технологий искусственного интеллекта (ИИ), а также перспективных технологий, таких, как промышленный интернет вещей, большие данные, машинное обучение, облачные технологии,

распределенные реестры повышает риски кибератак на энергетические объекты. С другой стороны, применение методов ИИ в области кибербезопасности активно развивается в рамках подхода, называемого киберситуационной осведомленностью. Киберситуационная осведомленность (КСО) - область исследований, связанная с применением методов искусственного интеллекта в области кибербезопасности, направленная на повышение осведомленности о возможных ситуациях нарушений кибербезопасности и автоматическое обнаружение киберугроз [7]. В исследованиях киберситуационной осведомленности, в том числе, используют такие методы искусственного интеллекта, как семантическое моделирование, байесовские сети доверия (БСД), технология экспертных систем, когнитивная графика.

Под термином «Киберситуационная осведомленность энергетических объектов» будем понимать осведомленность о состоянии киберсреды энергетических объектов, включающую информацию о: критических уязвимостях энергетических объектов с точки зрения кибербезопасности; киберугрозах, инициирующих эти критические уязвимости, а также о техногенных угрозах энергетической безопасности, вызванных киберугрозами.

Проблема киберситуационной осведомленности связана как с обработкой и анализом большого количества данных, поступающих в реальном времени с узлов локальной вычислительной сети (ЛВС) предприятия, в том числе анализом данных с интеллектуальных датчиков, для выявления киберугроз и отслеживания рисков их реализации, так и с предоставлением аналитику-эксперту больших объемов информации с учетом когнитивной составляющей восприятия.

Процесс «цифровизации» энергетических объектов (ЭО) может вызывать возникновение киберугроз, связанных с внедрением новых решений, применением новых бизнес-моделей, которые могут сопровождаться отсутствием или недостаточностью информации для оперативного принятия решений по обеспечению кибернетической безопасности объекта. Необходима разработка методов, моделей и комплекса программ анализа киберситуационной осведомленности и поддержки деятельности аналитика-эксперта. Необходима

разработка методов, моделей и комплекса программ анализа киберситуационной осведомленности и поддержки деятельности аналитика-эксперта.

Степень изученности проблемы. Исследования критических инфраструктур [8] являются достаточно молодым направлением, но уже стали приоритетными во многих странах мира, и в первую очередь в США. Исследования критических инфраструктур представлены в работах Калашникова А.О., Rybnicek M., Poisel R., Ouyang M. и др. Научные исследования и прикладные разработки по комплексным проблемам обеспечения безопасности населения, объектов инфраструктуры и среды жизнедеятельности рассматривались в работах Кондратьева А., Махутова Н.А., Тимашева С.А. и др.

Проблемы обеспечения энергетической безопасности рассматриваются национальными органами власти и международными организациями, такими, как Международное энергетическое агентство (МЭА, International Energy Agency), Организация по безопасности и сотрудничеству в Европе (ОБСЕ, Organization for Security and Co-operation in Europe), Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС, Asia-Pacific Economic Cooperation), Council of the European Union – один из основных директивных органов Европейского Союза, и др. В ИСЭМ СО РАН проблемы обеспечения энергетической безопасности рассматривались в работах Воропая Н.И., Еделева А.В., Клименко С.М., Кононова Ю.Д., Массель Л.В., Пятковой Н.И., Сендерова С.М., Славина Г.Б., Чельцова М.Б., и др.

Обеспечение информационной и кибернетической безопасности критической инфраструктуры, как правило, является приоритетным на высшем уровне власти. Вопросами кибербезопасности в энергетике занимались: AlMajali A., Govindarasu M., Manimaran G., Neuman C., Hanh A., Sridhar S., Ten C.-W., Wadhawan Y., Васильев В.И., Гурина Л.А., Колосок И.Н., Коркина Е.С., Краковский Ю.М., Массель А.Г., Мохор В.В., Б.В. Папков и др.

Органами стандартизации в области киберситуационной осведомленности в энергетике являются National Institute of Standards and Technology (NIST) совместно с National Cybersecurity Center of Excellence (NCCoE). Вопросами

киберситуационной осведомленности и мониторинга киберсреды занимаются Brynielsson J., Davies M., Ekelhart A., Eckhart M., Erbacher R., Frank U., Graf R., Joo M., Kott A., McDonald T.J., Mills R.F., Okolica J.S., Patel M., Seo J., Skopik F., Wang C., Котенко И.В., и другие. В нашей стране это направление является малоисследованным.

Объектом исследования является критическая информационная инфраструктура (КИИ) энергетической инфраструктуры.

Предметом исследования являются методы анализа киберситуационной осведомленности, семантические методы анализа киберугроз и методы построения интеллектуальных программных комплексов для поддержки предлагаемых методов на примере энергетических объектов.

Цель диссертационной работы: разработка методов, моделей и интеллектуального программного комплекса для анализа киберситуационной осведомленности энергетических объектов.

Поставлены и решены следующие задачи:

1. Анализ существующих методов исследования критических инфраструктур, проблем кибербезопасности и киберситуационной осведомленности.

2. Разработка методического подхода к анализу киберситуационной осведомленности энергетических объектов, включающий:

- фрактальную стратифицированную модель (ФС-модель) структурирования знаний в области кибербезопасности энергетической инфраструктуры;
- систему онтологий киберситуационной осведомленности энергетических объектов;
- вероятностную модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, с использованием байесовских сетей доверия (БСД-модели);
- численный метод определения уровня киберситуационной осведомленности энергетического объекта;

- методику анализа киберситуационной осведомленности энергетических объектов.

3. Разработка архитектуры интеллектуального программного комплекса для анализа киберситуационной осведомленности, реализующего предложенные методы, модели и алгоритмы.

4. Разработка технологии анализа киберситуационной осведомленности энергетического объекта.

5. Реализация и апробация разработанных методов, моделей и интеллектуального программного комплекса для определения уровня КСО энергетических объектов.

Методами и средствами исследования являются: методы искусственного интеллекта, математический аппарат байесовских сетей доверия, методы теории графов, методы системного анализа, методы семантического моделирования и визуальной аналитики на основе методов когнитивной графики, методические основы построения интеллектуальных информационных систем в исследованиях энергетики, методы инженерии знаний, методы объектного подхода (анализ, проектирование, программирование), методы проектирования информационных систем, экспертных систем и программных комплексов.

Составляют предмет научной новизны и на защиту выносятся следующие положения:

1. Впервые предложен подход к анализу киберситуационной осведомленности энергетических объектов, как синтез исследований кибербезопасности и ситуационной осведомленности, отличающийся использованием семантического моделирования, технологии экспертных систем и методов визуализации.

2. Разработан оригинальный методический подход к анализу киберситуационной осведомленности энергетических объектов, включающий:

- ФС-модель структурирования знаний в области кибербезопасности энергетической инфраструктуры;
- систему онтологий КСО энергетических объектов;

- вероятностную модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз;
- численный метод определения уровня КСО энергетического объекта;
- методику анализа КСО энергетических объектов.

3. Разработана архитектура и выполнена реализация интеллектуального программного комплекса для анализа киберситуационной осведомленности, реализующего предложенные методы и модели, отличающегося интеграцией экспертной системы, компонента байесовских сетей доверия и компонента визуальной оценки рисков (когнитивной графики), разработанных на основе авторских алгоритмов.

Теоретическая значимость результатов заключается в разработке методического подхода к анализу киберситуационной осведомленности энергетических объектов, включающего вероятностную модель и численный метод, и подтверждается применением результатов диссертационной работы в проектах,, поддержанных грантами Российского фонда фундаментальных исследований (РФФИ): гранты РФФИ № 15-07-01284а (2015-2017), №16-07-004574 (2016-2018), № 17-07-01341а (2017-2019), №18-07-00714а (2018-2020), № 18-57-81001 ЕАПИ_а (2018-2020), № 19-07-00351а (2019-2020), № 19-57-04003 Бел_мол_а (2019-2020).

Под руководством автора был выполнен проект РФФИ № 18-37-00271 мол_а (2018-2020) «Методы и программные средства анализа угроз и оценки рисков нарушения кибербезопасности критических инфраструктур», в котором также применены результаты диссертационной работы.

Практическая значимость определяется реализацией интеллектуального программного комплекса и возможностью внедрения разработанных численного метода, вероятностной модели и интеллектуального программного комплекса при планировании технологических режимов работы энергетических объектов в условиях цифровой трансформации энергетики, при совершенствовании используемого программно-технического комплекса эксплуатируемых автоматизированных систем управления, разработке и внедрении новых моделей и

алгоритмов задач автоматизированного управления, при подготовке методических материалов, планов и программ проведения тренировок, деловых игр персонала. Результаты работы применены при выполнении:

- Проекта по госзаданию ИСЭМ СО РАН: IV.35.1.3 «Методы, технологии и инструментальные средства интеллектуализации поддержки принятия решений в интегрированных интеллектуальных энергетических системах», № госрегистрации 01201361373, тема (проект) № 0349-2014-0011 (2013-2016).
- Проекта по госзаданию ИСЭМ СО РАН: III.17.2.1 «Проблемы разработки, адаптации и применения интеллектуальных информационно-телекоммуникационных технологий в интегрированных интеллектуальных энергетических системах», № госрегистрации АААА-А17-117030310444-2, тема (проект) № 0349-2016-0005 (2017-2020).

В рамках выполнения проекта № 19-57-04003 Бел_мол_а (2019-2020) результаты диссертационной работы были переданы в Институт энергетики НАН Беларуси.

По результатам представления работы в 2018 году автору присуждена стипендия мэра г. Иркутска в области науки и техники.

Соответствие диссертации паспорту научной специальности.

Содержание диссертационной работы соответствует паспорту научной специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ:

п 3. Разработка, обоснование и тестирование эффективных вычислительных методов с применением современных компьютерных технологий (пп. 1, 2, 3 новизны).

п. 4. Реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента (пп. 2, 3 новизны).

п. 5. Комплексные исследования научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента (пп. 2, 3 новизны).

Апробация работы. Результаты работы докладывались на Международных конференциях «International Young Scientists Conference in Computational Science», 2019 г., Ираклион (Греция), «Computer Science and Information Technologies», Варна (Болгария), 2018 г., Баден-Баден (Германия), 2017 г.; Международном конгрессе по интеллектуальным системам и информационным технологиям, Дивноморское (Россия), 2018 г., Международной конференции «Computer Technology and Applications», Владивосток (Россия), 2017 г.; научных семинарах «Critical Infrastructures in the Digital World», 2017-2021 гг.; XXI-XXV Байкальских Всероссийских конференциях «Информационные и математические технологии в науке и управлении», г. Иркутск, 2016-2020 гг., Международной конференции «Физико-техническая информатика – СРТ-2020», 2020 г., конференциях молодых ученых ИСЭМ СО РАН, г. Иркутск, 2016-2019 гг., а также на семинарах и заседаниях секций Ученого совета и отдела систем искусственного интеллекта в энергетике ИСЭМ СО РАН.

Личный вклад. Результаты, составляющие новизну и выносимые на защиту, получены лично автором.

Публикации. По теме исследования опубликованы 21 статей, из них 3 – входят в перечень ВАК, 4 статьи проиндексированы в Scopus и WOS, 6 – в рецензируемых научных изданиях. Получены 3 свидетельства о государственной регистрации программы для ЭВМ.

Объем и структура работы. Диссертация объемом 172 стр. состоит из введения, трех глав, заключения, списка литературы из 162 наименований, 3 приложений, основной текст изложен на 132 страницах.

Глава 1. Анализ проблемы – кибербезопасность энергетических объектов критической инфраструктуры

Аннотация главы

Первая глава диссертационной работы посвящена анализу предметной области, которая находится на стыке таких направлений исследований, как критические инфраструктуры, энергетический сектор как составляющая КИ, а также цифровая трансформация энергетики и обостряющиеся в связи с этим вопросы нарушения кибербезопасности критической информационной инфраструктуры.

В главе выполнен анализ наиболее известных подходов и методов, применяемых в исследованиях кибернетической безопасности и составляющих её направлений безопасности, а также даны определения основных понятий, которых придерживается автор в своем исследовании.

Также приводятся статистические данные об инцидентах в области кибербезопасности в энергетическом секторе, критических инфраструктурах и автоматизированных системах управления технологическими процессами (АСУ ТП). Проанализированы тенденции возникновения уязвимостей в программно-аппаратной инфраструктуре технологических объектов, а также актуальные для таких объектов киберугрозы. Представлен обзор зарубежных и национальных нормативных правовых документов и руководств в области обеспечения кибербезопасности, применимых в энергетическом секторе.

Выделено направление исследований киберситуационной осведомленности, которая находится на стыке исследований ситуационной осведомленности и кибербезопасности. Приводятся определения этого термина и некоторых аспектов его исследований.

Дано описание используемых в диссертации методов искусственного интеллекта и интеллектуальных технологий исследования. Автором делается

акцент на важности анализа киберситуационной осведомленности энергетических объектов для достижения кибербезопасности КИИ.

1.1 Энергетический сектор как критическая инфраструктура

Изучение и анализ критической инфраструктуры - относительно молодое научное направление. Этот вопрос стал привлекать к себе пристальное внимание только в конце прошлого столетия. Так, в июле 1996 года административным указом Президента США № 13010 «О работе по исследованию уязвимости защиты критической инфраструктуры от кибернетических и физических угроз» была сформирована комиссия по защите критической инфраструктуры при Президенте США (President’s Commission on Critical Infrastructure Protection – PCCIP) [8, 9].

Инфраструктура (термин 1.1) называется критической, если ее выход из строя либо уничтожение оказывают значительное влияние на здравоохранение, безопасность, экономику и социальное благосостояние [10]. Отказ в такой инфраструктуре или ее выход из строя может нанести ущерб обществу и экономике, а также способен привести к каскаду аварий, приводящих к сбоям в многочисленных инфраструктурах с потенциальными катастрофическими последствиями [11].

В российских исследованиях критической инфраструктурой называют часть гражданской инфраструктуры, выход из строя либо уничтожение которой может привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации [8]. Энергетический сектор (термин 1.2) относят к одной из основных критических инфраструктур.

Основными подходами к изучению КИ являются исследования КИ как больших сложных систем стратегического масштаба (БСССМ) (термин 1.3) и исследования КИ как киберфизических систем (КФС) (термин 1.4).

При рассмотрении КИ как БСССМ ключевой особенностью критических инфраструктур является их сильная взаимозависимость. Обеспечение защиты и устойчивости критических инфраструктур являются национальным и

международным приоритетами [11]. На рисунке 1.1. представлена иерархия и взаимосвязанность 11 секторов в соответствии с их важностью, отраженной в «Национальной стратегии по физической защите критической инфраструктуры и ключевых объектов» (The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets) 2003 года [8].

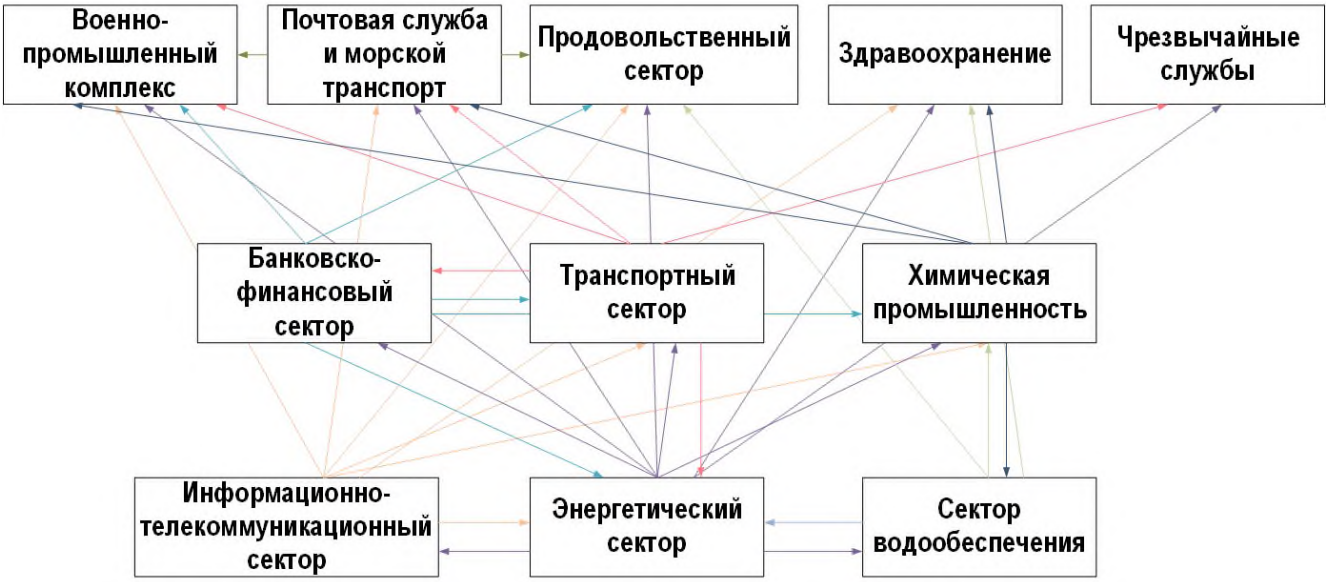

Рисунок 1.1 – Взаимосвязь критических инфраструктур

При таком подходе в первую очередь рассматриваются проблемы обеспечения защищенности населения и объектов техносферы, которые являются междисциплинарными, а их решение предполагает получение новых знаний на базе фундаментальных исследований, развиваемых в соответствующих областях [12].

В этом направлении исследований КИ основными подходами являются теория центров тяжести Клаузевица [13, 14], похожий подход Вардена [15, 16], теория самоорганизующихся сетей (Scale-Free Network) А. Барабаши [17, 18], а также имитационное моделирование [9]. Основные усилия в этой области направлены на создание моделей, имитирующих поведение КИ и позволяющих определять взаимосвязи между ее объектами и выявлять наиболее уязвимые из них. В имитационных моделях могут применяться различные методы (агентное моделирование, дискретно-событийное, динамическое), а выбор какого-либо из них зависит от специфики изучаемой инфраструктуры и задач исследования.

При рассмотрении КИ как КФС большое внимание уделяется вопросам безопасности. Новизна и принципиальное отличие КФС от существующих встроенных систем или АСУ ТП, на которые они похожи внешне, состоит в том, что КФС интегрируют в себе кибернетическое начало, компьютерные аппаратные и программные технологии, а также качественно новые исполнительные механизмы, встроенные в окружающую их среду и способные воспринимать ее изменения, реагировать на них, самообучаться и адаптироваться [19]. Одним из основных требований к КФС, помимо функциональной эффективности, является безопасность взаимодействия ее компонентов с учетом комплексного влияния на управляемые объекты. Обеспечение безопасности КФС связано с двумя ключевыми свойствами КФС. Первым является безопасность, нацеленная на обеспечение защиты системы от случайных отказов, а вторым является защищенность, нацеленная на защиту системы от преднамеренных атак. Практическая реализация КФС [20] связана с технологиями «Интернета вещей» (термин 1.5) и беспроводных сенсорных сетей (термин 1.6). Множество исследований КФС связанны именно с этими двумя практическими направлениями.

Критические инфраструктуры рассчитаны на работу в течение длительных периодов времени (несколько десятков лет), их функционирование обеспечивается за счет технического обслуживания, обновления и интеграции новых технологий. С практической стороны вопрос заключается в том, что в критических инфраструктурах наблюдается все больше и больше системных нарушений, возникающих из-за небольших возмущений, которые каскадируются до масштабных последствий [11].

Ведущим направлением решения проблем обеспечения безопасности являются теории, основанные на концепции риска [21], которая, как правило, включает определение текущих состояний элементов системы, условий, при которых возможно возникновение и развитие аварийных, чрезвычайных и катастрофических ситуаций, а также качественное и количественное описание

сценариев и последствий при достижении предельных состояний с возникновением аварий и катастроф.

1.2 Существующие подходы к обеспечению кибернетической безопасности

В диссертационной работе кибернетическая безопасность рассматривается как важный аспект цифровой трансформации энергетики в Российской Федерации, которая является быстроразвивающимся и междисциплинарным направлением исследований. В октябре 2017 года прошла конференция «Совещание главных инженеров-энергетиков 2017 (СГИЭ)» [22], на которой впервые были широко освещены вопросы цифровой трансформации электроэнергетики России в рамках взаимодействия представителей государственной власти, частных компаний и научного сообщества. В настоящее время приняты стратегии цифровой трансформации в компаниях «Россети» [23] и «Газпром нефть» [24], ведется работа в рамках проектов по созданию «Интернета энергии», по снижению потерь электроэнергии электрических сетей, по развитию искусственного интеллекта межотраслевым Альянсом, по запуску цифровых подстанций, цифровых линий электропередач, развитию цифровых технологий в области обеспечения устойчивости энергосистемы и др. [25].

В диссертационном исследовании понятие «кибербезопасность» (термин 2.1) рассматривается вместе с понятием «кибернетическая среда» (термин 2.2), в свою очередь, тесно связанной с понятием «ресурса организации или пользователя» (термин 2.3) в соответствии с рекомендацией МСЭ-Т X.1205 «Обзор кибербезопасности» 2008 год [26]. Кибернетическая безопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в кибернетической среде [26].

В соответствии с международным стандартом ISO/IEC 27032:2012 «Information technology – Security techniques – Guidelines for cybersecurity» [27]

кибербезопасность базируется на безопасности приложений (термин 2.4), информационной безопасности (термин 2.5), сетевой безопасности (термин 2.6), безопасности Интернет (термин 2.7) и защите ключевых информационных систем объектов критических инфраструктур (термин 2.8), но не является синонимом ни одного из них [28]. Определения вышеперечисленных сфер безопасности изложены в переводе [28]. На рисунке 1.2 отражено положение кибербезопасности относительно других сфер безопасности [29].

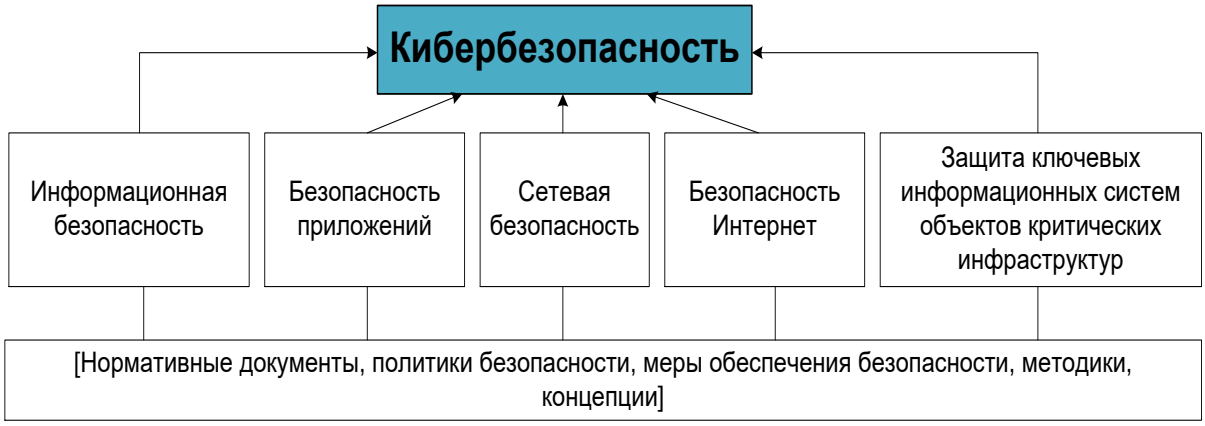

Рисунок 1.2 – Положение кибербезопасности относительно других сфер безопасности

Обеспечение кибербезопасности подразумевает управление рисками [26]. В этом контексте далее приведем основные понятия, рассматриваемые в области кибербезопасности.

Активом (asset) называется некоторая сущность, ценная для личности, организации или государства [28]. Активы рассматриваются как источники уязвимостей.

Уязвимость (vulnerability) – слабость, слабое звено актива или системы управления, которое может быть использовано для реализации угрозы [28].

Угроза (threat) – потенциально нежелательное воздействие, в результате которого может быть причинен вред системе, личности или организации. Угрозы, существующие в киберпространстве, имеют смысл лишь в контексте их привязки к активам [28]. Угрозы рассматриваются и как источники риска, и как предполагаемое намерение совершить атаку [26].

Атака (attack) – 1) попытка уничтожения, раскрытия, внесения изменений, вывода из строя, хищения или получения несанкционированного доступа к активу [30]; 2) намеренная попытка изменить, нарушить или остановить функционирование компьютерных систем или сетей, а также программ или информации, которые они содержат или передают [31].

Вектор атаки (attack vector) – 1) путь и способ действий, следуя которым нарушитель стремится получить доступ к компьютеру или сетевому серверу для реализации своего умысла [28]; 2) последовательность действий нарушителя, приводящая к получению несанкционированного доступа к целевой системе. Атака на одну целевую систему может быть реализована с помощью разных векторов [32].

Вектор проникновения – способ преодоления сетевого периметра в результате эксплуатации недостатков защищенности [33].

Ранее в исследованиях кибербезопасности энергетических комплексов было введено понятие киберхалатности, которое также рассматривается в исследовании. Киберхалатность [31] – неумышленные действия сотрудников организации, которые могут причинить вред, обусловленные неосторожностью, низкой компьютерной грамотностью или пренебрежением мерами, обеспечивающими кибербезопасность, которые по причиняемому ущербу сравнимы с кибератаками [35].

Традиционно обеспечение безопасности информационно-телекоммуникационного оборудования в организациях рассматривалось с позиции информационной безопасности.

В настоящее время кибербезопасность рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности (National Cyber Security Strategy – NCSS) служит средством усиления безопасности и надежности информационных систем государства. Первые стратегии кибербезопасности начали появляться в начале предыдущего десятилетия. Одной из первых стран, которая стала воспринимать кибербезопасность как вопрос государственной важности, были

Соединенные Штаты Америки. В 2003 году в США была опубликована Национальная стратегия безопасности в киберпространстве (National Strategy to Secure Cyberspace). В 2005–2011 гг. еще двенадцать стран – членов Евросоюза опубликовали свои государственные стратегии кибербезопасности. О признании значимости кибербезопасности свидетельствует значительное количество национальных стратегий. Однако в этих документах также проявляются значительные различия в определении кибербезопасности и других ключевых терминов [36].

В России велась работа над проектом Концепции Стратегии Кибербезопасности Российской Федерации [4], но документ не получил конечную версию, не прошел стадию промульгации. К сожалению, в России до сих пор нет однозначного понимания кибербезопасности [37], как правило, ее пытаются идентифицировать с информационной безопасностью.

В настоящее время в России начались подвижки в области обеспечения безопасности критической информационной инфраструктуры (термин 2.9). В июле 2017 года был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2]. Согласно этому закону к объектам критической информационной инфраструктуры относят информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие, в том числе, в сфере энергетики. Определение объектов КИИ устанавливается на основе значимости объекта, путем осуществления категорирования, исходя из социальной, политической, экономической, экологической значимости, а также значимости с точки зрения обороны страны, безопасности государства и правопорядка. В Российской Федерации основным регулятором информационной безопасности КИИ является Федеральная служба по техническому и экспортному контролю (ФСТЭК), кроме которой также можно назвать ФСБ, СВР, МинОбороны, ФСО, Минкомсвязь, Роскомнадзор, МВД, Банк России, Совет Безопасности, Минэнерго, Минэкономразвития, Администрация Президента, Ростехрегулирование, Минтруд и др.

Кроме того, перечислим сопутствующие нормативные документы по обеспечению безопасности КИИ в РФ:

- Постановление Правительства Российской Федерации от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [38].
- Приказ ФСТЭК России от 6 декабря 2017 года № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [39].
- Приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [40].
- Приказ ФСТЭК России от 22 декабря 2017 года № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [41].
- Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [42].

В энергетическом секторе основными документами по безопасности являются:

- Федеральный закон от 21 июля 1997 года № 116-ФЗ «О безопасности объектов топливно-энергетического комплекса» [43].
- Приказ ФСТЭК от 14 марта 2014 года № 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 природной среды» [44].

Наиболее известными зарубежными и международными являются группы стандартов NERC-CIP (США и Азия), CPNI (Великобритания), BDEW White Paper (Германия, Европа), ISA-62443 (International Society of Automation), IEC 62351, NIST Special Publications 800 series (США), ISO 27000 series (международные), Ausgrid (корпоративный, Австралия).

Подходы к обеспечению безопасности имеют общую структуру и состоят из четырех основных этапов [44]:

- выявление критических ресурсов системы и их уязвимостей;
- определение угроз, реализация которых может привести к нарушению функционирования критических ресурсов и/или всей системы;
- анализ рисков и определение ущербов от реализации угроз;
- выбор и применение мер по снижению риска и принятие остаточных рисков.

Для выявления критических ресурсов системы и их потенциальных уязвимостей осуществляется описание архитектуры системы (схемы, планы расположения физических компонентов). Для этого строятся UML-диаграммы, применяются нотации бизнес-моделирования, такие как IDEF0, BPMN, EPC и др. Осуществляется категорирование ресурсов и их уязвимостей по значимости, а также анализ существующих мер безопасности. Например, степень риска уязвимостей компонентов АСУ ТП определяют на основе значения «Common Vulnerability Scoring System» (CVSS) [45].

Для определения угроз, как правило, строятся модели нарушителя, например, для оценки уязвимостей используются деревья атак и сети Петри [46, 47]. Далее составляются частные модели угроз с описанием возможностей нарушителей [48], потенциальных уязвимостей системы, способов реализации угроз безопасности и последствий от их реализации.

Анализ рисков и определение ущербов от реализации угроз осуществляется с применением качественных, количественных или гибридных методов [49-51]. Качественные оценки осуществляются с применением лингвистических или балльных шкал [52], для количественных оценок используют вероятностные модели и балльные шкалы, гибридные методы сочетают в себе два вышеперечисленных метода и являются наиболее полными [53].

Как правило, риск рассчитывается как продукт угрозы, уязвимости и последствий, что называют общей моделью риска (R) (1.1) [54]:

$$R = \{T, V, C\}, \quad (1.1)$$

где T – угрозы, V – уязвимости, C – ущерб.

Такой подход к оценке риска в информационной безопасности называют трехфакторным [49]. При использовании трехфакторного подхода уровень риска информационной безопасности определяется через возможность использования уязвимости V, возможность реализации угрозы T, используя заданную уязвимость V, и ущерб C от реализации угрозы T [49].

Выбор мер обеспечения безопасности осуществляется в первую очередь для рисков с высокой вероятностью наступления и большим ущербом [55]. При этом безопасность должна обеспечиваться на всех этапах жизненного цикла системы: создание, внедрение, эксплуатация, модификация и вывод из эксплуатации – с учетом класса защищенности объекта [44].

Переход от информационной безопасности к кибернетической безопасности обусловлен бурным развитием техники, экономики и общества, характерным в последние десятилетия. Развитие современных технологий, увеличение численности населения планеты, истощение углеводородных энергетических ресурсов и другие факторы требуют изменения и ресурсной базы, в том числе топливно-энергетического комплекса (ТЭК), к которому современное общество предъявляет все более жесткие требования к качеству ресурсов, а также требует постоянного увеличения производимого объема ресурса.

Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р утверждена программа «Цифровая экономика Российской Федерации»

[1]. Цифровая энергетика развивается с учётом федеральных стратегий и отраслевых программ. Целями программы являются создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности.

Основными цифровыми технологиями, которые планируют развивать в рамках программы, являются большие данные, нейротехнологии и искусственный интеллект, системы распределенного реестра, квантовые технологии, новые производственные технологии, промышленный интернет, компоненты робототехники, технологии беспроводной связи, технологии виртуальной и дополненной реальностей.

Программа цифровой экономики, в том числе, ориентируется на стратегию научно-технологического развития Российской Федерации, утвержденную Указом Президента Российской Федерации от 1 декабря 2016 года № 642 [56]. В области энергетики данная стратегия направлена на качественное изменение характера глобальных и локальных энергетических систем, рост значимости энерговооруженности экономики и наращивание объема выработки и сохранения энергии, ее передачи и использования. При этом приоритетами научно-технологического развития Российской Федерации на ближайшие 10-15 лет названы следующие направления:

- переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта;
- переход к экологически чистой и ресурсосберегающей энергетике, повышение эффективности добычи и глубокой переработки углеводородного сырья, формирование новых источников, способов транспортировки и хранения энергии;

- противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства.

Процесс «цифровизации» энергетических объектов может вызывать возникновение киберугроз, связанных с внедрением новых решений, применением новых бизнес-моделей, которые могут сопровождаться отсутствием или недостаточностью информации для оперативного принятия решений по обеспечению кибернетической безопасности объекта. В связи с этим необходимо расширять область знаний об объектах, рассматривать взаимосвязи технологических процессов ЭО и их влияние на состояние кибернетической безопасности объекта и взаимосвязанных инфраструктур.

1.2.2 Кибернетическая безопасность энергетической инфраструктуры

Энергетическая безопасность (термин 1.7) рассматривается как состояние защищенности от угроз энергетической безопасности, а также нарушений стабильности и бесперебойности. Эти угрозы определяются как внешними (геополитическими, макроэкономическими, конъюнктурными) факторами, так и собственно состоянием и функционированием энергетического сектора страны [57]. Угрозы энергетической безопасности традиционно объединяются в пять основных групп [57]. В последнее время список угроз был расширен угрозами кибербезопасности, реализация которых может спровоцировать серьезнейшие экстремальные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей. Киберугрозы рассматриваются как один из важнейших современных видов угроз энергетической безопасности [6].

Нештатные ситуации в энергетическом секторе такие, как критические или чрезвычайные, являются предметом исследований энергетической безопасности. Угрозами ЭБ являются дефицит потребностей в ресурсах приемлемого качества в

нормальных условиях и экстремальных ситуациях, нарушение стабильности и бесперебойности энергообеспечения [57].

С одной стороны, стремительное распространение компьютерной среды, развитие информационных технологий и тенденция перехода к интеллектуальной энергетике делают киберугрозы одной из важнейших тактических и стратегических угроз ЭБ. С другой стороны, на объектах КИ наблюдается недооценивание необходимости проведения систематических превентивных мероприятий по предотвращению киберугроз и постоянного обновления средств защиты, что, в свою очередь, может повлиять на возникновение значительного и длительного дефицита энергоресурсов в зависимости от масштаба и последствий кибератак [58].

Анализ инцидентов показывает, что КИИ могут быть уязвимы для кибератак, способных привести к разрушению физических систем и сетей [11]. Наблюдается увеличение злонамеренных атак на АСУ ТП [59]. Такие атаки уже не являются гипотетическими, и, соответственно, ЭО требуют эффективной защиты не только от случайных сбоев, но и подобного вида угроз и опасностей, которые являются более сложными для прогнозирования [11].

По данным исследований компании Positive Technologies [60] в автоматизированных системах управления технологическим процессом наблюдается тенденция роста обнаруженных уязвимостей (рисунок 1.3).

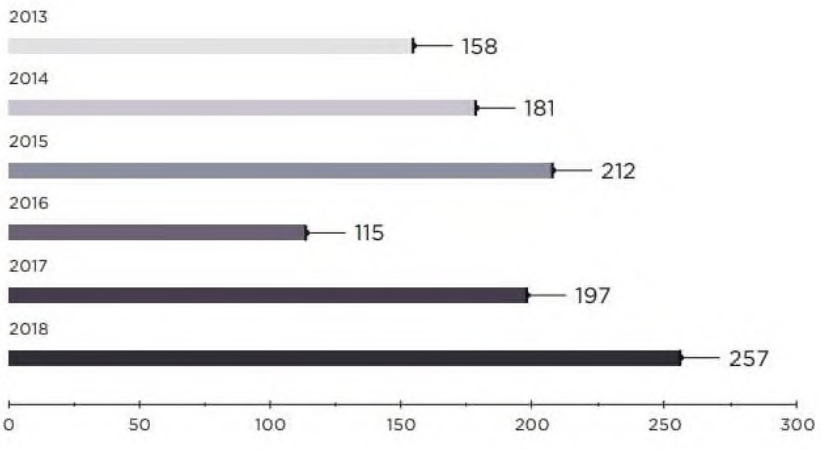

Рисунок 1.3 – Динамика обнаружения уязвимостей. Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

Процесс предупреждения компьютерных атак и реагирования на них – длительная и циклическая задача, которая состоит из нескольких этапов, в том числе, постановка цели защиты от тривиальных атак и атак низкой сложности (по статистике это примерно 75% атак). Только решив эту задачу, можно переходить к защите от более сложных атак, а затем - от незнакомых типов атак [61].

Исследования Лаборатории Касперского за 2017 года показали, что большая часть уязвимостей затрагивает автоматизированные системы, управляющие энергетикой (178), производственными процессами различных предприятий (164), водоснабжением (97) и транспортом (74) [62]. Результаты этого исследования и аналогичного за 2018 год представлены на рисунке 1.4.

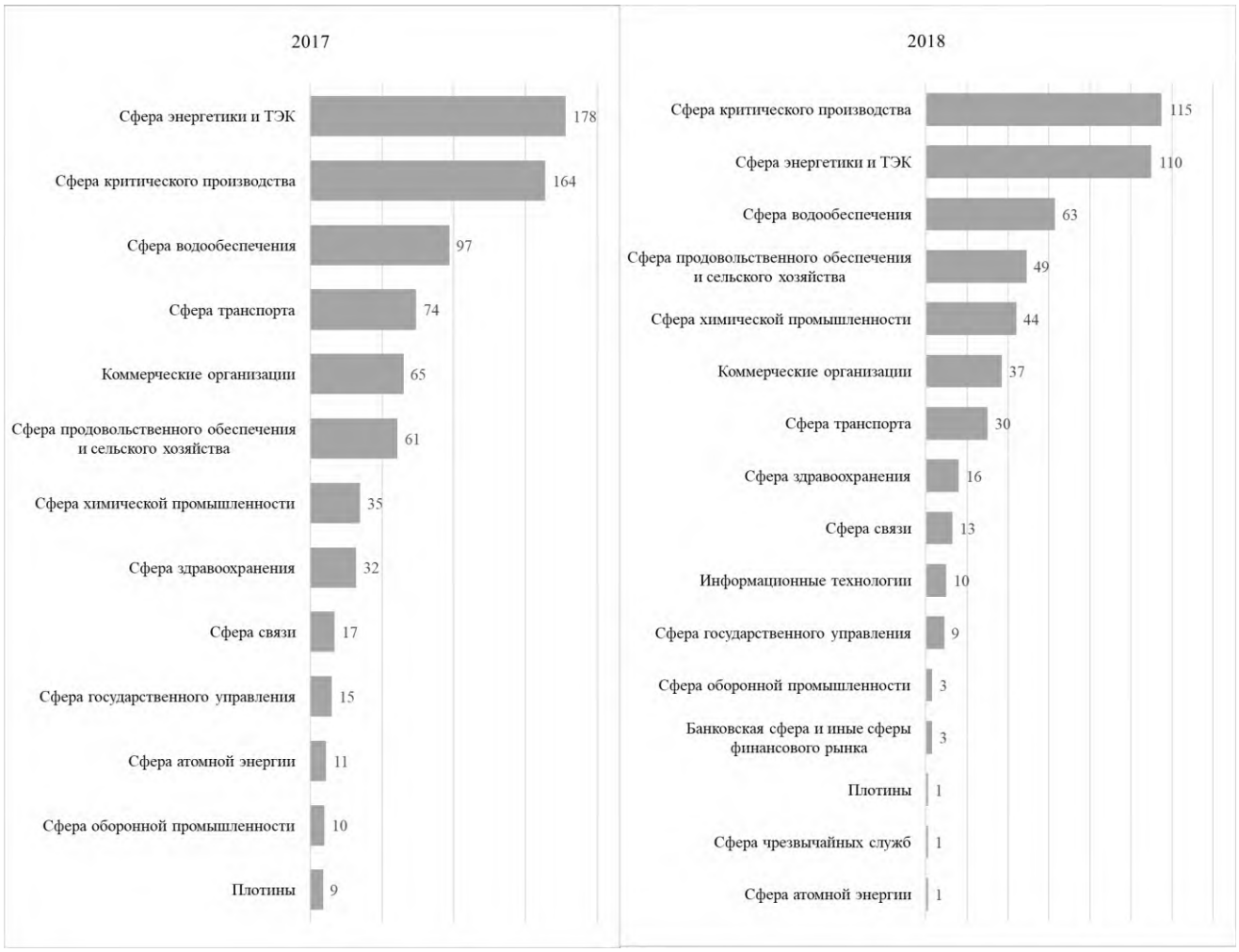

Рисунок 1.4 – Количество уязвимых продуктов, используемых в различных отраслях за 2017-2018 гг.

Согласно источнику [63], в подавляющем большинстве случаев наиболее успешные атаки хакеров, преступников и других злоумышленников направляются

на серверы и компьютеры конечных пользователей, подключенные к Интернету. Для атаки на компьютеры зачастую используются такие инструменты, как [61] вредоносное программное обеспечение (ПО), трояны, бот-сети, фишинг, распределенные атаки типа «отказ в обслуживании» (DDoS), а также атаки «человек посередине» (термины 2.10-2.15) (рис. 1.5).

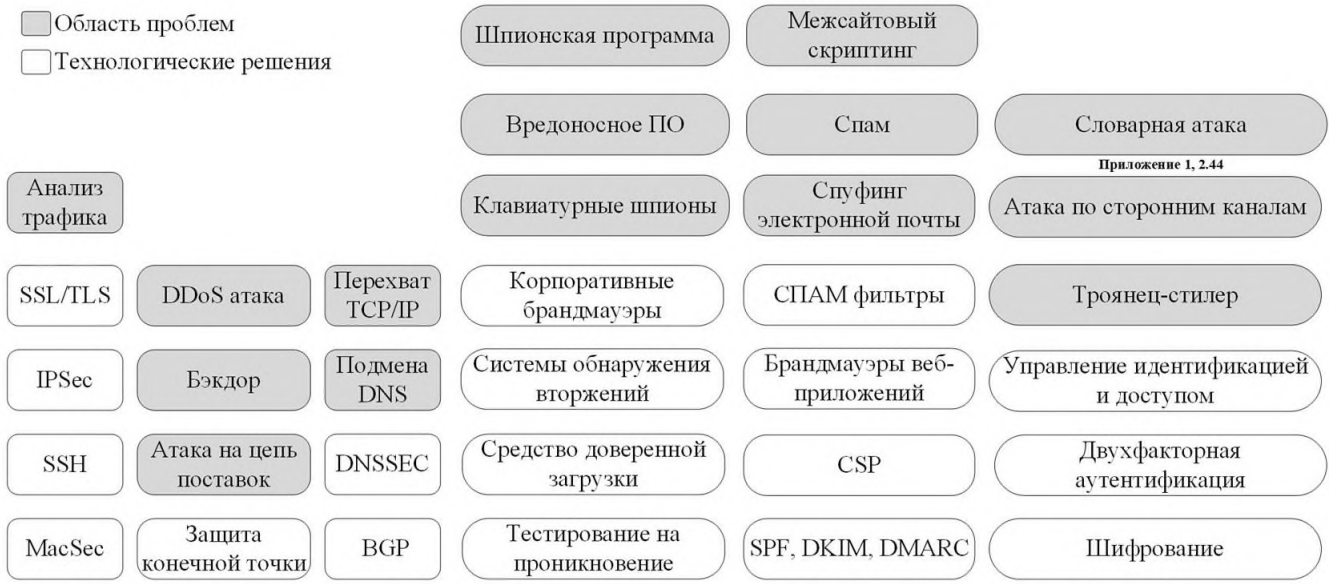

Рисунок 1.5 – Проблемы кибербезопасности и технологические решения (термины 2.1-2.45)

Разрушительное воздействие на инфраструктуру и промышленный шпионаж – это основные цели киберпреступников, атакующих ТЭК [64]. Подробное описание списка тактик и возможных техник для осуществления целевых атак представлено в базе знаний MITRE ATT&CK (Enterprise) [65], выполненной в виде таблицы.

Рост количества известных уязвимостей, а также доступных в интернете компонентов АСУ ТП дает злоумышленникам все больше возможностей для проведения атак, что может привести к серьезным последствиям [61].

Процесс «цифровизации» энергетических сетей [66, 67], использование интеллектуальных технологий, датчиков и сенсоров Интернета вещей в работе энергетических систем повышают риски в области кибербезопасности энергетических предприятий. При реализации концепций интеллектуальной и

цифровой энергетики необходимо учитывать следующие потенциальные риски использования современных информационных технологий [68]:

- повышенная сложность информационной сети повышает количество уязвимостей для потенциальных атак и непреднамеренных ошибок.
- сети, взаимосвязанные с другими сетями, которые также могут занимать несколько «умных» доменов сети, увеличивают вероятность каскадных аварий.
- большое количество взаимосвязей программных компонентов увеличивает уязвимость программного кода, что упрощает злоумышленникам внедрение в программный код вредоносного кода и уязвимостей.
- по мере увеличения узлов сети увеличивается и число точек входа в систему для злоумышленников.

При решении проблемы перехода к интеллектуальной энергетике выделяют две взаимосвязанные области – технологическая инфраструктура и информационно-телекоммуникационная инфраструктура. Успех создания ИЭС во многом зависит от успешного применения современных информационных технологий. В свою очередь, говорить о применении последних имеет смысл при наличии развитой современной технологической инфраструктуры. Решения по развитию технологической инфраструктуры, безусловно, относятся к классу стратегических решений. Для обоснования и поддержки принятия таких решений целесообразно привлечение интеллектуальных информационных технологий [69].

1.3 Киберситуационная осведомленность энергетических объектов

Термин «ситуационная осведомленность» возник из области пилотирования самолетов и многие определения этого термина в 80х тесно связаны с авиационной областью. В те годы, эта область исследований была направлена на помощь пилоту в понимании ситуации в любой момент времени, а также на оценку дизайнов дисплеев, кабин пилотного транспортного средства для быстрого отслеживания

пилотами меняющихся тактических ситуаций и способствования высокой выживаемости в боевой обстановке [70].

Термин «ситуационная осведомленность», или Situational Awareness, тесно связан в первую очередь с пионерными работами Мики Эндсли (Mica R. Endsley) [70, 71], в которых ситуационная осведомленность определена как «чувственное восприятие элементов обстановки в (едином) пространственно-временном континууме, осознанное восприятие их значения, а также проецирование их в ближайшее будущее». В своей работе [72] М. Эндсли отмечала, что проблемы нового класса технологий, заключающиеся в том числе в росте сложности систем и генерации в них огромного объема данных, являются одним из факторов роста интереса к ситуационной осведомленности. Развитие новых информационно-коммуникационных технологий добавило измерение «Cyber» к традиционным военным и деловым операциям ситуационной осведомленности, поскольку системы и сети, работающие в киберпространстве, имеют уязвимости, которые представляют значительные риски как для отдельных организаций, так и для национальной безопасности [73].

Применение методов искусственного интеллекта в области кибербезопасности направлено на повышение осведомленности о возможных ситуациях и автоматическом обнаружение угроз [7]. Такое направление исследований развивается в рамках подхода, называемого киберситуационной осведомленностью. Далее приведем некоторые определения киберситуационной осведомленности.

Frank U., Brynielsson J. в [74] определили киберситуационную осведомленность как часть ситуационной осведомленности, которая касается киберсреды. При этом авторы придерживаются традиционного понимания ситуационной осведомленности, предложенного Endsley (1988) [70] и раскрывают две точки зрения на ситуационную осведомлённость: техническую и когнитивную.

Техническая составляющая – сбор, обработка, объединение и визуализация данных для проведения технической оценки взаимосвязанных фрагментов информации

Когнитивная составляющая касается способности аналитика проводить когнитивный анализ представленных данных, понимать технические последствия и делать выводы, необходимые для принятия обоснованных решений и получения наилучшего результата

Pappaterra M.J. и Flammini F. в [7] придерживаются аналогичного определения киберситуационной осведомленности, включающей в себя не только сбор соответствующих данных, но и процесс интерпретации и объединения информации в устойчивое знание (solid knowledge) с целью дальнейшего прогнозирования [70]. Т.е. с одной стороны ситуационная осведомленность – это сбор, обработка и объединение данных для проведения технической оценки взаимосвязанных фрагментов информации. В качестве таких фрагментов информации выступают данные с датчиков и от персонала, систем мониторинга, различных метрик и экспертные знания. Данный собираются, обрабатываются соответствующими алгоритмами, визуализируются для дальнейшей интерпретации аналитиком. С другой стороны – деятельность аналитика, заключающаяся в когнитивном анализе представленных данных, целью которого является некоторый вывод, необходимый для принятия обоснованных решений для получения наилучшего результата [7].

Определение термина «ситуационная осведомленность» в контексте киберсреды приведено в глоссарии Национального института стандартов и технологий США (NIST) [75], в соответствии с которым ситуационная осведомленность – восприятие мер (стратегий, средств) обеспечения безопасности предприятия и его ландшафта угроз в единой пространственно-временной системе координат; понимание двух этих аспектов вместе (риск); прогноз их состояния на ближайшее будущее (перевод автора).

На основе определений, приведенных в [7, 74, 76], в контексте данных исследований под киберситуационной осведомленностью понимается область исследований, связанная с применением методов искусственного интеллекта в области кибербезопасности, направленная на повышение осведомленности о

возможных ситуациях нарушений кибербезопасности и автоматическое обнаружение киберугроз.

Самостоятельное понимание ситуационной осведомленности, полученное на основе анализа и оценки действий в сети, рассматривается как дополнительная информация и знания для получения общей ситуационной осведомленности путем их объединения с информацией и знаниями о параметрах, состояниях, характеристиках системы вне киберсреды [74].

Эта сравнительно новая концепция для нашей страны уже получила достаточно широкое распространение за рубежом [7, 74, 76-78]. Отмечается, что киберситуационная осведомленность не может рассматриваться изолированно, она взаимозависима и является частью ситуационной осведомленности, которая ограничена рамками киберсреды.

Современные решения для автоматизации технологического процесса на энергетических объектах становятся более сложными и используют передовые цифровые технологии [79], что приводит к увеличению рисков нарушения безопасности этих объектов, вплоть до возникновения экстремальных ситуаций.

Процессы выявления, количественного определения, анализа и оценки рисков, а также их обработки должны быть неотъемлемыми компонентами общего процесса принятия управленческих решений [21]. К этому процессу относится и управление рисками, которое включает процесс управления безопасностью информационных систем. Управление рисками – это все скоординированные действия по управлению и контролю организации в отношении риска. Две основные цели управления рисками состоят в том, чтобы обеспечить принятие адекватных мер для защиты людей, окружающей среды и активов от нежелательных последствий предпринимаемых действий, а также сбалансировать различные проблемы, такие, как безопасность и затраты. Управление рисками охватывает как меры по предотвращению возникновения опасностей и угроз, так и меры по снижению их потенциальных последствий.

Методы системного анализа рисков используются для анализа систем, в которых не хватает данных, для точного прогнозирования будущих характеристик

системы. При этом осуществляется декомпозиция системы на подсистемы и компоненты, для которых доступно больше информации. Общие вероятности и риск зависят от архитектуры системы и вероятностей на уровне подсистем и компонентов. Количественная оценка риска, часто называемая вероятностной оценкой, связана с методами системного анализа. Количественная оценка рисков систематизирует текущее состояние знаний, включая неопределенности относительно явлений, процессов, видов деятельности и анализируемых систем. Предназначена для определения возможных опасностей и угроз, а также для анализа их причины и последствии. Некоторыми из традиционных инструментов, используемых для анализа вероятностей и риска, являются теория статистической оценки, анализ дерева отказов и анализ дерева событий. Другие методы посвящены более детальному представлению и анализу риска и связанных с ним неопределенностей, включая задачи по принятию решений, которые должны поддерживаться результатами анализа. Примерами относительно недавно введенных методов являются байесовские сети доверия, двоичные диаграммы, анализ надежности в нескольких состояниях, сети Петри и современные инструменты моделирования Монте-Карло [80].

Анализ ИТ-рисков является ключевым элементом процесса управления безопасностью информационных систем. В контексте безопасности ИТ-систем риск ИТ-систем - это общая мера вероятности и серьезности ситуации, в которой данная угроза использует специфические слабости, вызывая потерю или повреждение активов системы, а, следовательно, косвенную или прямую потерю для организации [81].

Анализ ИТ-рисков состоит из следующих трех основных этапов:

1. Определение опасностей / угроз / возможностей (источников).
2. Анализ причин и следствий, включая анализ уязвимостей.
3. Описание риска с использованием вероятностей и ожидаемых значений [80].

1.4 Методы искусственного интеллекта и интеллектуальные технологии исследования

Развитие информационных технологий и их внедрение на предприятиях, с одной стороны, упростили работу с самими технологическими процессами, а с другой, усложнили информационно-коммуникационную инфраструктуру организации. В начале процесса цифровой трансформации энергетики важность обеспечения кибербезопасности не вполне осознавалась, в настоящий момент большое количество научных и прикладных исследований и работ рассматривают кибербезопасность как одно из ведущих направлений при проектировании, внедрении, эксплуатации и вывода из нее сложных технологических объектов. Влияние нарушения кибернетической безопасности на работу предприятия не всегда является очевидным и легко предсказуемым, поскольку череда небольших недочетов в КИИ может привести к большим негативным последствиям. В связи с этим, работа основывается на методах искусственного интеллекта и интеллектуальных технологиях. Далее представлены основные методы, используемые в работе.

1.4.1 Онтологический инжиниринг и фрактальный подход к структурированию знаний

Разработка систем, основанных на знаниях (knowledge based systems), является одним из основных направлений искусственного интеллекта. Оно связано с разработкой моделей представления знаний, созданием баз знаний, образующих ядро экспертных систем. В последнее время включает в себя модели и методы извлечения и структурирования знаний рассматривается как составляющая инженерии знаний [82]. Инженерия знаний (термин 3.1) является теоретической основой науки о методах разработки систем, основанных на знаниях, и посвящена теоретическим и практическим проблемам проектирования баз знаний, в том числе

получению и структурированию знаний специалистов для последующей разработки интеллектуальных систем или систем управления знаниями. При разработке систем, основанных на знаниях, выделяют три этапа домашинной обработки:

- Добыча (получение) знаний из источников (эксперты, Интернет, специальная литература). Результатом этапа является огромное количество гетерогенных противоречивых фрагментов знаний.
- Концептуализация (структурирование) разрозненных фрагментов в единую модель. Результат представляет собой слабо формализованное представление, называемое полем знаний.
- Формализация поля знаний при помощи специализированных языков представления знаний. В результате этапа формируется база знаний, описанная на языке представления знаний [82].

Основными языками инженерии знаний являются семантические сети, фреймы, системы правил-продукций, язык нечетких множеств и нечеткого вывода, нейронные сети, объектно-ориентированные представления, языки ситуационного управления и др. [83].

Онтологический инжиниринг развивает основные положения инженерии знаний и объединяет две основные технологии проектирования больших систем – объектно-ориентированный и структурный анализ [84]. Целями онтологического инжиниринга являются повышение уровня интеграции информации, необходимой для принятия управленческих решений, повышение эффективности информационного поиска, предоставление возможности совместной обработки знаний на основе единого семантического описания пространства знаний.

Алгоритм онтологического инжиниринга включает 5 этапов согласно [84]:

- выделение концептов – базовых понятий данной предметной области;
- определение «высоты дерева онтологий» – числа уровней абстракции;
- распределение концептов по уровням;
- построение связей между концептами – определение отношений и взаимодействий базовых понятий;

- консультации с различными специалистами для исключения противоречий и неточностей.

Онтология или концептуальная модель предметной области, состоит из иерархии понятий предметной области, связей между ними и законов, которые действуют в рамках этой модели.

Онтологии делятся на:

- «весомые» онтологии (Heavy-weighted), содержащие аксиомы (1.2);

$$O = \{C, R, A\}, \quad (1.2)$$

- «легкие» (Light-weighted), их не содержащие (1.3).

$$O = \{C, R\}, \quad (1.3)$$

где O – онтология, C – совокупность концептов предметной области, R – совокупность отношений между ними, A – набор аксиом (законов и правил, которые описывают принципы существования концептов) [85].

Применение онтологического инжиниринга для систематизации основных понятий предметной области может связать все виды угроз, их взаимовлияния друг на друга и на остальные концепты предметной области.

В энергетическом секторе применяется онтологический инжиниринг для поддержки принятия стратегических решений, обеспечивающий взаимосвязи и согласованность исследований при разработке систем онтологий. Система онтологий, включающая онтологии ситуационного управления, а также методика проведения исследований стратегий развития энергетики представлена в работе [86]. В работе [87] онтология ТЭК применяется при моделировании критических инфраструктур энергетики. Формальное описание отраслей энергетики и компонентов интеллектуальной системы поддержки принятия стратегических решений применяется в исследованиях энергетической безопасности [88, 89]. При разработке системы оперативного мониторинга технологической инфраструктуры нефтегазодобывающих предприятий применялся формат представления данных в виде объектов онтологии [90]. Исследование кибербезопасности и её основные понятия в соответствии с ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности»,

а также основные особенности кибербезопасности в энергетике изложены в работе [91].

Фрактальный подход предложен д.т.н. Л.В. Массель в девяностых годах прошлого века, как методический подход к структурированию знаний, и заключается в построении фрактальной стратифицированной модели знаний, которая основана на представлении разных форм (видов) знаний как информационных объектов расслоенного (стратифицированного) пространства [92].

Каждый уровень представления знаний представляет собой слой (страту) этого пространства, объединяющий однотипные информационные объекты, и соответствует своему информационному миру. Допускается отображение из любого слоя в каждый. Графически ФС-модель удобно изображать в виде совокупности вложенных сферических оболочек. Информационный объект на сферической оболочке условно обозначается точкой. При необходимости детально рассмотреть такой объект осуществляется его расслоение, причем другие объекты при этом могут быть также рассмотрены «точечно». Таким образом, организована возможность работы с разномасштабными объектами, используя одни и те же методы, сохраняя при отображении (переходе от слоя к слою) инвариант объекта – его существующие свойства.

Математическое описание ФС-модели приведено в [92, 93]. В рамках фрактального подхода знания исследователя в некоторой области могут быть представлены как «вырезка» из сферического информационного пространства, которая графически может быть представлена в виде конуса или пирамиды, включающих некоторые слои. Такой конус может представлять собой, например, дисциплину, подход или метод.

Применение фрактального подхода для семантического моделирования в энергетике описано в [94]. Удобство применения фрактального подхода для семантического моделирования заключается в возможности рассматривать интересующие аспекты, избегая моделей большой размерности (включающих большое количество концептов и связей), которые при полном их представлении

неудобны для восприятия. Применение фрактального подхода позволяет осуществлять расслоение (детализацию) и/или агрегирование концептов с сохранением внутренней структуры связей и смысла и обеспечивает возможность разномасштабного представления семантических моделей [94].

Применение фрактального подхода к построению информационных технологий рассмотрено в [95]. В соответствии с традиционной цепочкой решения задачи [96] (задача – модель – алгоритм – программа – решение задачи) в области информационных технологий можно выделить основные базовые слои: слой математических моделей, слой алгоритмов, слой программ, слой моделей данных, слой моделей знаний.

Использование фрактального подхода позволяет представить любую информационную технологию как совокупность информационных слоев и их отображений. Процесс построения информационной технологии в таком случае заключается в разработке способов описания информационных слоев (или объектов) и способов отображений из любого слоя в каждый, а реализация этих способов дает инструментальные средства поддержки конкретной информационной технологии [95].

Фрактальный подход к проектированию архитектуры информационных систем рассматривается в [97]. При этом подходе, типовым расслоением информационных систем является выделение трех уровней: уровня управления данными, уровня прикладной логики (бизнес-логики) и уровня управления интерфейсом.

Практическое применение фрактального подхода в этой работе рассмотрено в разделе 2.1.

1.4.2 Байесовские сети доверия

Байесовской сетью является графическая модель, отображающая вероятностные зависимости множества переменных, и позволяющая проводить вероятностный вывод с помощью этих переменных [98]. Иными словами,

байесовская сеть – это модель, отражающая события некоторой предметной области, и то, как эти состояния вероятностно связаны (термин 3.2). Как и любой другой граф, байесовская сеть состоит из вершин (событий) и ребер (однонаправленная связь). БСД представляет собой ациклический граф, каждой вершине которого соответствует случайная переменная, а дуги графа кодируют отношения условной независимости между этими переменными.

Если из вершины A выходит дуга в вершину B, то A называют родителем B (термин 3.3), а B называют потомком A. Если из вершины A существует ориентированный путь в вершину B, то A называется предком B, а B называется потомком A (термин 3.4).

Множество всех родителей вершины $X_i, 1, \dots, n$ обозначается $Parents_i$. Каждая вершина $X_i, 1, \dots, n$ характеризуется распределением условных вероятностей $P(X_i|Parents_i)$, которое количественно оценивает влияние родителей на эту переменную.

Условной вероятностью события A по отношению к событию B называется вероятность события A, найденная при условии, что событие B произошло и обозначается $P(A|B)$.

Вероятности, которые используются в байесовских сетях, могут быть байесовскими или частотными: при построении сети при помощи априорных знаний вероятности будут байесовскими, при обучении таких сетей на статистических данных, вероятность будет частотной.

Априорная вероятность – распределение вероятностей, которое выражает предположения до учёта экспериментальных данных

Апостериорная вероятность – условная вероятность случайного события при условии того, что известны апостериорные данные, т.е. полученные после опыта.

Формула полной вероятности позволяет вычислить вероятность интересующего события через условные вероятности этого события в предположении неких гипотез, а также вероятностей этих гипотез:

$$P(B) = \sum_{i=1}^{N} P(A_i)P(B|A_i), \quad (1.4)$$

Формула Байеса для двух событий A и B имеет вид:

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)} \quad (1.5)$$

где $P(A)$ – априорная вероятность гипотезы A, $P(A|B)$ – вероятность гипотезы A при наступлении события B (апостериорная вероятность), $P(B|A)$ – вероятность наступления события B при истинности гипотезы A. $P(B)$ – полная вероятность наступления события B.

Совместное распределение в теории вероятностей – это распределение совместных исходов, образованных из нескольких случайных величин. Каждый элемент в совместном распределении представлен в виде произведения соответствующих элементов в таблицах условных вероятностей (ТУВ) байесовской сети. Байесовские сети представляют собой декомпозированное представление совместного распределения. Вероятностный вывод требует совместного распределения вероятностей, вследствие чего возникает проблема экспоненциальной сложности с ростом количества переменных. Для решения подобной проблемы создаются модели байесовской сети доверия, разбивающие сложное распределение вероятностей на ряд простых узлов, что снижает проблематичность получения знаний и сложность вероятностного вывода [99].

В общем случае формула Байеса для полной группы несовместных событий $A_1, A_2, \dots, A_n$ при условии, что произошло событие B, имеет следующий вид:

$$P(A_j|B) = \frac{P(A_j)P(B|A_j)}{\sum_{i=1}^{n} P(A_i)\,P(B|A)} \quad (1.6)$$

Числовые значения в байесовских сетях могут быть также и субъективными, личностными, оценками ожиданий экспертов по поводу возможности осуществления событий.

Рассуждением в байесовской сети называют пропагацией свидетельств (апостериорный или байесовский вывод): в систему поступает информация о том, что события, соответствующие тем или иным ее узлам, произошли, после чего ставится задача определить, как изменились вероятности других узлов (вершин графа).

Сценарный подход изначально возник при изучении социальных систем. Специфика сценарного планирования заключается в одновременном рассмотрении нескольких вариантов развития, для каждого из которых определяются внутренние и внешние факторы, устанавливаются критерии и индикаторы, а также оцениваются риски [100]. Как правило, сценарии представляют собой вероятностное описание возможного или желательного варианта развития рассматриваемых явлений и процессов. На основе анализа сценариев выстраиваются планы развития и принимаются управленческие решения, как порядок действий, необходимых для достижения предпочтительных состояний и ситуаций [100].

Сценарий развития сложной системы включает модели, содержащие существенные факторы, которые могут быть формализованы с приемлемой степенью точности [101]. В случае экстремальных ситуаций в энергетике сценарий представляет собой пессимистические оценки основных количественных характеристик исследуемых энергетических объектов [102].

В [101] обоснована целесообразность применения аппарата знаковых ориентированных графов для генерации сценариев сложных систем, а также описаны требования к математическому аппарату для построения моделей в рамках сценарного подхода:

- возможность построения эффективных с вычислительной точки зрения алгоритмов анализа;
- низкая требовательность (чувствительность) к полноте и точности исходных данных;
- возможность относительно несложной программно-системной реализации.

Для построения таких моделей были выбраны Байесовские сети доверия. Ранее Байесовские сети применялись для анализа угроз энергетической безопасности [103]. Применение Байесовских сетей как инструмента реализации сценарного подхода, рассчитанного на стратегическое планирование, позволит строить модели экстремальных ситуаций с использованием байесовских

вероятностей при введении числовых значений на основе знаний и опыта эксперта или частотных вероятностей при наличии статистических данных, зачастую отсутствующих в свободном доступе.

Сценарный анализ рисков, присущих сложным системам, характеризуется отсутствием «массового» характера событий в сценарии, и направлен на изучение уникальных ситуаций и связей [100].

1.4.3 Технология экспертных систем

Экспертные системы (термин 3.5) являются наиболее распространенным классом интеллектуальных систем. Современные ЭС – это сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и распространяющие этот эмпирический опыт для консультаций менее квалифицированных пользователей. Разработка экспертных систем, как активно развивающаяся ветвь информатики, направлена на использование компьютеров для обработки информации в тех областях науки и техники, где малопригодны традиционные математические методы моделирования. В этих областях важны смысловая и логическая обработка информации, опыт экспертов. Экспертные системы делятся на 2 класса: ЭС тиражирования знаний и ЭС получения новых знаний. Как правило, преобладают ЭС первого класса. ЭС включает в себя четыре основных компонента [104].

База знаний – основа любой ЭС, содержит объекты и факты, утверждения в виде правил, связывающие объекты. Файлы и объекты описывают то, что известно в данной конкретной области в данный момент. Эти данные представляют краткосрочную информацию, т.е. они могут быть дополнены или изменены в процессе работы. Правила устанавливают ситуационные, концептуальные и причинные взаимосвязи между объектами, правила являются более долговременной информацией.

Машина вывода с механизмом логического вывода реализацией функции, а также синтаксис логических выводов. Машина вывода осуществляет поиск в базе

знаний соответствующих триплетов или пар по правилам рациональной логики, согласно введенным правилам для получения решения. Приводится в действие при получении запроса от пользователя и выполняет следующие задачи:

- сравнивает сведения, содержащуюся в запросе пользователя, с содержимым базы знаний;
- осуществляет поиск определенных целей или причинных связей;
- оценивает, относит определенность фактов или их достоверность, основываясь на соответствие коэффициентов доверия, связанных с каждым фактом.

Интерфейс разумных умозаключений организует обмен сведениями между пользователем и машиной вывода, т.е. осуществляет диалог. При этом решает следующие задачи:

- ввод новых знаний в базу знаний, т.е. ввод триплетов или пар, а также правил взаимосвязи объектов;
- корректировка базы знаний и правил между объектами;
- удаление ненужных пар или триплетов, правил;
- ввод или получение результата, решения.

Подсистема объяснений, предназначенная для вывода правил, на основе которых ЭС представила результат вывода.

Модель знаний определяет форму представления знаний в базе знаний. На рисунке 1.6 представлена условная классификация моделей представления знаний [104].

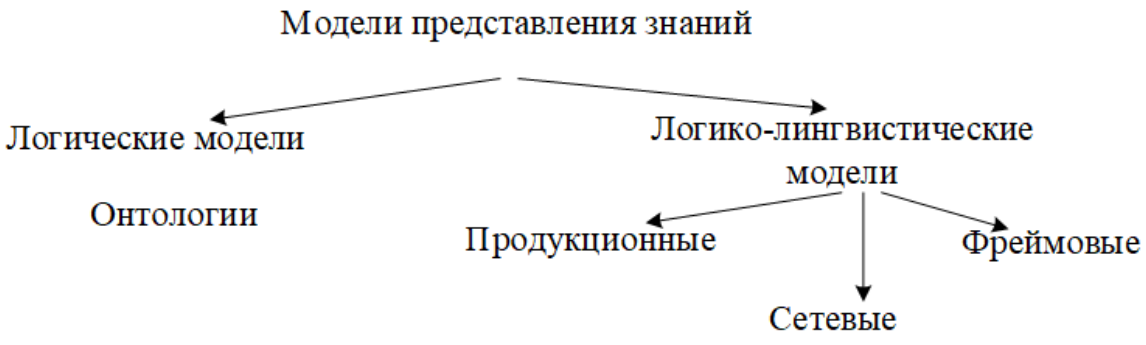

Рисунок 1.6 – Классификация моделей представления знаний

Логическая модель знаний – модель представления знаний, в основе которой лежит формальная система (например, исчисление предикатов).

Логико-лингвистическая модель знаний – модель, основанная на расширении формальной системы, в рамках которой вводятся процедуры изменения всех или части элементов в зависимости от решаемых задач.

Фреймовая модель знаний – модель представления знаний, в основе которой лежат фреймы. Фрейм состоит из конечного числа слотов (составных частей), каждый из которых имеет имя и значение (последнее может являться ссылкой на другие слоты).

Сетевая модель знаний – модель представления знаний, основанная на семантической сети, в вершинах которой находятся информационные единицы, а дуги характеризуют отношения и связи между ними.

Продукционная модель знаний – модель представления знаний, в основе которой лежат правила (продукции) вида «ЕСЛИ-ТО».

Модель представления знаний в виде онтологий была введена позже и лежит вне этой классификации, предназначена для представления декларативных знаний (подробнее в разделе 1.4.1).

ЭС эффективны лишь в специфических «экспертных» областях, где важен эмпирический опыт специалистов. Факторы, свидетельствующие о необходимости разработки и внедрения экспертных систем [82]:

- невозможность или неэффективность математического моделирования;
- нехватка специалистов, затрачивающих значительное время на оказание помощи другим;
- выполнение небольшой задачи требует многочисленного коллектива специалистов, поскольку ни один из них не обладает достаточными знаниями;
- сниженная производительность, поскольку задача требует полного анализа сложного набора условий, а обычный специалист не в состоянии просмотреть (за отведенное время) все эти условия;

- большое расхождение между решениями самых хороших и самых плохих исполнителей.

1.5 Выводы по главе

В первой главе выполнен анализ предметной области, в рамках которого рассмотрены определение и основные виды угроз энергетической безопасности, а также место киберугроз в исследованиях энергетической безопасности, существующие подходы к исследованию критических инфраструктур, подходы к обеспечению безопасности критической информационной инфраструктуры, в том числе кибербезопасности, национальные и зарубежные нормативные документы по обеспечению кибернетической, информационной и технической безопасности энергетических объектов и критических инфраструктур в целом.

Из анализа предметной области основным выводом является то, что в Российской Федерации нет четкого понимая понятия кибербезопасности, нормативно-правовая база, методические рекомендации и подходы находятся в стадии разработки, а существующие документы, ГОСТЫ и стандарты не объединены в единое нормативное пространство. Одновременно с этим, на государственном уровне устанавливаются требования по обеспечению безопасности, в том числе от киберугроз, объектов критической информационной инфраструктуры, к которым непременно относятся энергетические объекты. Нормативно-правовой документацией и крупными компаниями, занимающимися обеспечением безопасности сложных технологических объектов, подчеркивается необходимость привлечения научного сообщества к вопросам фундаментальных исследований и прикладного применения научных подходов и разработок в области обеспечения безопасности критической информационной инфраструктуры.

Критическая инфраструктура на примере энергетики является, с одной стороны, большой сложной системой стратегического масштаба, а с другой инфраструктура энергетического сектора приближается к киберфизической

системе в рамках концепции цифровой энергетики, как части цифровой экономики и «цифровизации» инфраструктур в целом.

В результате выполненного анализа в работе ставится проблема определения влияния киберугроз на энергетическую инфраструктуру, прогнозирования последствий такого влияния в условиях внедрения новых информационно-коммуникационных технологий и сопровождающих изменений бизнес-процессов на предприятии.

Внедрение новых информационно-телекоммуникационных технологий приносит новые риски, которые можно отнести к категории гипотетических и сложно прогнозируемых. Это связано с переходным периодом цифровой трансформации энергетики, сложностью, масштабностью, сильной взаимозависимостью и гетерогенностью систем. В условиях внедрения новых технологий риски кибернетической безопасности приобретают стратегический характер. Ранее для исследования стратегических угроз энергетической безопасности в коллективе, в котором работает автор, были предложены байесовские сети доверия [105], а с целью проведения анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов была предложена методика [106]. В связи с этим в исследовании ставятся задачи по адаптации существующего метода исследования стратегических угроз энергетической безопасности с использованием байесовских сетей доверия для более узкого направления исследований – киберугроз, а также задачи по развитию подхода к анализу киберситуационной осведомленности энергетических объектов. Хотя подход и является относительно новым для нашей страны, темпы роста внедрения интеллектуальных информационных технологий на предприятиях только увеличиваются. С одной стороны, это способствует повышению эффективности работы предприятия, уменьшению трудозатрат и повышению наблюдаемости работы объекта, а с другой, применение программных продуктов на основе искусственного интеллекта, не обеспечивающих однозначное понимание достигаемых прогнозов для экспертов (работа по принципу «черного ящика», злонамеренное вмешательство в алгоритмы и процессы) вызывает опасения

возникновения экстремальных ситуаций в энергетике из-за нарушения кибербезопасности.

Для решения проблемы анализа киберситуационной осведомленности энергетических объектов предлагается применение моделей структурирования знаний и семантического моделирования для анализа когнитивной составляющей КСО и анализ киберугроз для анализа технической составляющей КСО, как синтез подходов к исследованию ситуационной осведомленности и кибербезопасности энергетических объектов.

Глава 2. Методический подход к анализу киберситуационной осведомленности энергетических объектов

Аннотация главы

В главе представлен предлагаемый автором методический подход к анализу киберситуационной осведомленности энергетических объектов, включающий анализ киберугроз энергетического объекта, построение модели сценариев ЭкС в энергетике, вызванных реализацией киберугроз, и определение уровня киберситуационной осведомленности энергетического объекта.

При разработке методического подхода выполнено структурирование знаний с использованием онтологического инжиниринга и фрактального подхода.

Предлагаемый методический подход содержит указания по определению критических активов критической информационной инфраструктуры энергетического объекта, выявлению уязвимостей и соответствующих киберугроз, установлению взаимосвязей между угрозами кибернетической и энергетической безопасности, а также по идентификации и оценке рисков последствий нарушения кибернетической безопасности с учетом возможности наступления экстремальной ситуации в энергетике, вызванной реализацией киберугроз.

Методический подход к анализу киберситуационной осведомленности энергетических объектов включает:

- ФС-модель структурирования знаний в области кибербезопасности энергетической инфраструктуры;
- систему онтологий киберситуационной осведомленности энергетических объектов;
- вероятностную модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, с использованием байесовских сетей доверия (БСД-модели);
- численный метод определения уровня киберситуационной осведомленности энергетического объекта;

- методику анализа киберситуационной осведомленности энергетических объектов.

Далее каждый пункт будет рассмотрен подробнее.

2.1 Фрактальная стратифицированная модель структурирования знаний в области кибербезопасности энергетической инфраструктуры

Согласно фрактальному подходу к структурированию данных и знаний [93], можно выполнить расслоение пространства данных и знаний D и построить отображения из любого слоя в каждый. В таком случае можно представить информационное пространство данных и знаний для исследований кибербезопасности энергетической инфраструктуры как (2.1) [107]:

$$D = \{M, E, V, T, R\}, \quad (2.1)$$

где M – слой предлагаемых методов; E – слой энергетической инфраструктуры; V – слой уязвимостей активов энергетического объекта; T – слой угроз, R – слой рисков.

В результате структурирования знаний в области кибербезопасности энергетической инфраструктуры предложена ФС-модель, представленная на рисунке 2.1 в виде конуса [108].

Представленное графическое отображение ФС модели в виде конуса представляет собой совокупность данных и знаний об энергетической инфраструктуре, уязвимостях, угрозах, рисках и методах их исследования в диссертационной работе. Далее представлены логические зависимости выделенных слоев в виде отображений ФС модели.

В представленной модели могут использоваться 6 типов отображений F:

$F_M^E: E \to M$ – отображение из слоя энергетической инфраструктуры в слой методов;

$F_M^V: V \to M$ – отображение из слоя уязвимостей в слой методов;

$F_M^T: T \to M$ – отображение из слоя угроз в слой методов;

$F_V^E: E \to V$ – отображение из слоя энергетической инфраструктуры в слой уязвимостей;

$F_V^T: T \to V$ – отображение из слоя угроз в слой уязвимостей;

$F_T^R: R \to T$ – отображение из слоя рисков в слой угроз.

Отметим, что отображения могут быть как прямые, так и обратные.

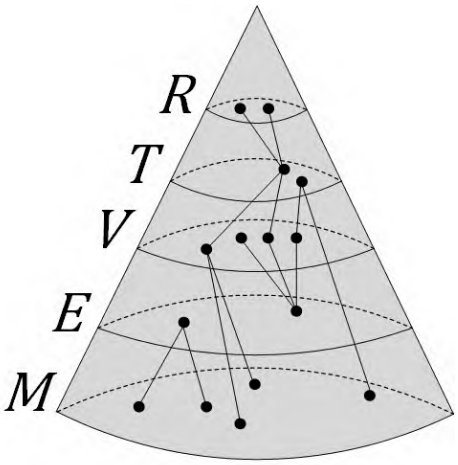

Рисунок 2.1 – Фрактальная стратифицированная модель структурирования знаний в области кибербезопасности энергетической инфраструктуры

Рассмотрим следующий уровень детализации исследования, в рамках диссертационной работы [109]. ФС-модель, описывающая взаимосвязь предлагаемых методов исследования, рисков наступления экстремальных ситуаций в энергетике, угроз, уязвимостей и объектов цифровой энергетики, представлена на рисунке 2.2, где E – слой энергетической инфраструктуры (показано расслоение в виде конуса), M – слой методов, R – слой рисков, T – слой киберугроз, V – слой уязвимостей. Диаграмма отображает следующий уровень детализации исследования, в которой каждому слою ФС модели, представленной на рисунке 2.1, соответствует конус на рисунке 2.2, включающий слои, соответствующие данным и знаниям в области кибербезопасности энергетической инфраструктуры.

В свою очередь, слой методов можно представить как (2.2):

$$M = \{O, ExS, B, Rv\}, \tag{2.2}$$

где O – слой методов онтологического инжиниринга; ExS – слой технологии экспертных систем; B – слой технологии байесовских сетей доверия; Rv – слой методов анализа рисков.

Слой уровня энергетической инфраструктуры имеет вид (2.3):

$$E = \{E_s, E_o, E_i\}, \tag{2.3}$$

где E_s – слой уровня энергетических систем; E_o – слой уровня энергетических объектов; E_i – слой уровня КИИ.

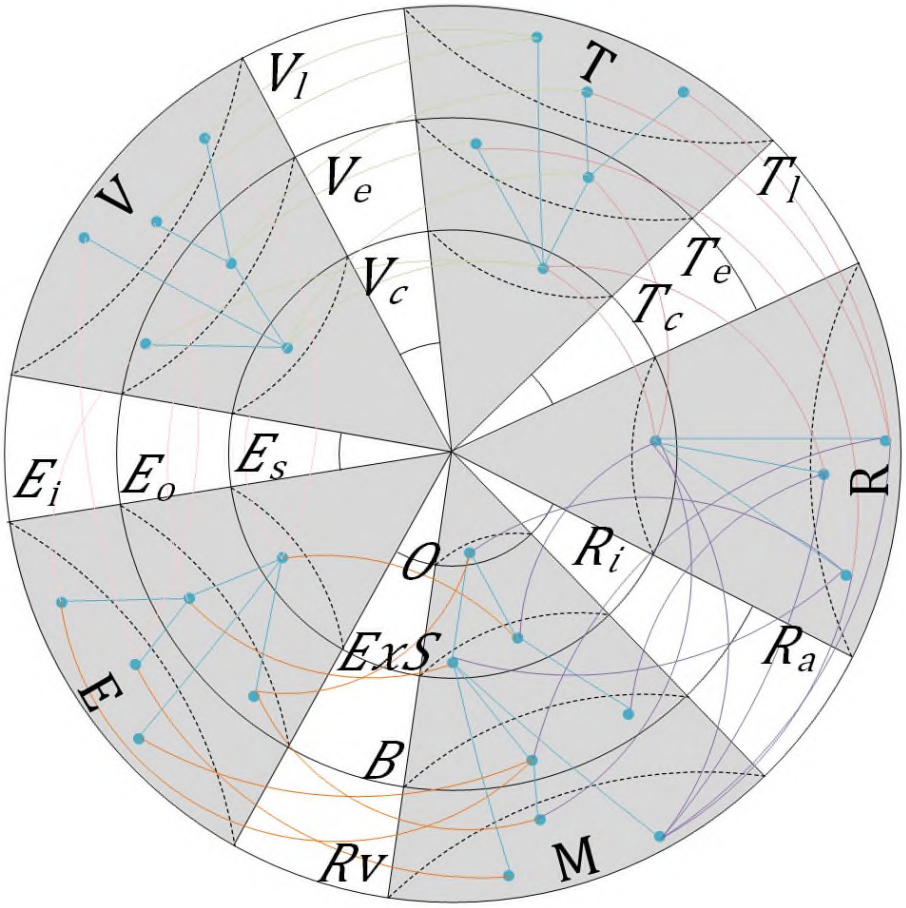

Рисунок 2.2 – Расширенная фрактальная стратифицированная модель энергетической инфраструктуры с позиции кибернетической и энергетической безопасности

Слой уязвимостей представлен как (2.4):

$$V = \{V_c, V_e, V_l\}, \tag{2.4}$$

где V_C – слой уязвимостей активов корпоративного сегмента ЛВС; V_e – слой уязвимостей активов технологического сегмента (ТС) ЛВС; V_l – слой уязвимостей активов технологической инфраструктуры.

Слой угроз состоит из (2.5):

$$T = \{T_c, T_e, T_l\}, \quad (2.5)$$

где T_C – слой киберугроз критических уязвимостей активов ЭО; T_e – слой техногенных угроз энергетической безопасности; T_{ex} – слой угроз энергетической безопасности.

Слой рисков представлен как (2.6):

$$R = \{R_i, R_a\}, \quad (2.6)$$

где R_i – слой рисков КИИ; R_a – слой рисков аварий и катастроф.

При построении ФС-модели определены этапы проведения исследования:

- анализ активов энергетического объекта;
- анализ уязвимостей активов энергетического объекта;
- анализ киберугроз и угроз энергетической безопасности на энергетическом объекте;
- оценка рисков наступления экстремальной ситуации, вызванной реализацией киберугроз.

Интерпретировать ФС-модель можно следующим образом. Анализу активов ЭО соответствует отображение F_M^E из слоя энергетической инфраструктуры в слой методов. Анализу уязвимостей активов ЭО соответствуют отображения F_M^V из слоя уязвимостей в слой методов и отображение F_V^E из слоя энергетической инфраструктуры в слой уязвимостей. Анализу киберугроз ЭО соответствуют отображения F_M^T из слоя угроз в слой методов и отображение F_V^T из слоя угроз в слой уязвимостей. Оценке рисков наступления экстремальной ситуации в энергетике, вызванной реализацией киберугроз, соответствует отображение F_T^R из слоя рисков в слой угроз.

Применение фрактального подход позволяет формально описать и представить предметную область как совокупность информационных слоев и их отображений из любого слоя в каждый. На основе фрактального подхода отображаются взаимосвязи основных понятий и разработана система онтологий, представленная далее.

2.2 Система онтологий киберситуационной осведомленности энергетических объектов

Для исследования киберситуационной осведомленности энергетических объектов, включающих критическую информационную инфраструктуру, с позиции энергетической и кибернетической безопасности выполнен онтологический инжиниринг с использованием фрактального подхода.

Рассмотрение энергетического сектора как критической инфраструктуры, включающей критическую информационную инфраструктуру, с позиции энергетической и кибернетической безопасности, является довольно трудоемкой задачей, для решения которой в три этапа выполнен онтологический инжиниринг.

На первом этапе извлечения знаний из источников были проанализированы национальные и международные стандарты, научно-исследовательские работы, аналитические и исследовательские статьи, а также отчеты частных компаний в областях:

- энергетический сектор и энергетическая безопасность;
- методы семантического моделирования и искусственного интеллекта;
- КИ и КИИ;
- киберфизические системы;
- кибернетическая, информационная и сетевая безопасность;
- сложные технологические объекты и АСУ ТП;
- управление ИТ-рисками.

В результате первого этапа найден материал в перечисленных областях в том числе статистического характера, определения и описания, алгоритмы и модели, методы, методики и программные продукты.

Разработана структура системы онтологий киберситуационной осведомленности энергетических объектов, представленная на рисунке 2.3 [110].

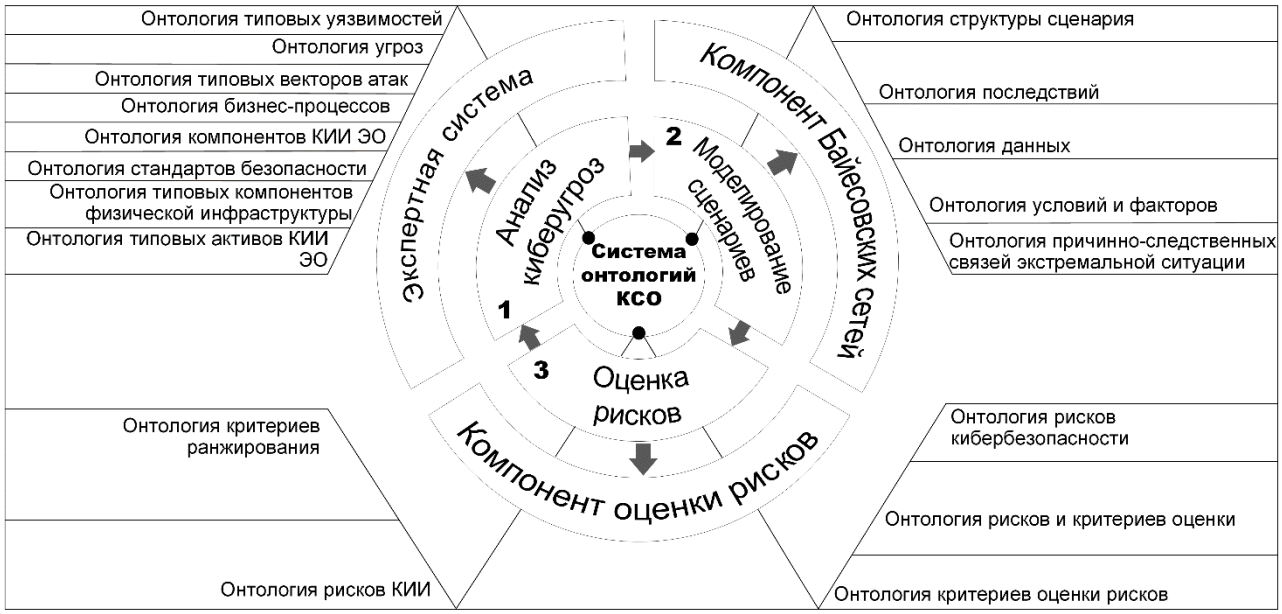

Рисунок 2.3 – Система онтологий киберситуационной осведомленности энергетической инфраструктуры

Основными группами задач [111] анализа киберситуационной осведомленности энергетических объектов являются:

1) анализ киберугроз энергетической инфраструктуры;
2) моделирование сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз;
3) оценка рисков наступления экстремальной ситуации в энергетике, вызванной реализацией киберугроз, ранжирование объектов и активов по уровню рисков и выработка рекомендаций.

Метаонтология КСО энергетической инфраструктуры представлена на рис. 2.4. Представлены основные понятия и их взаимосвязи.

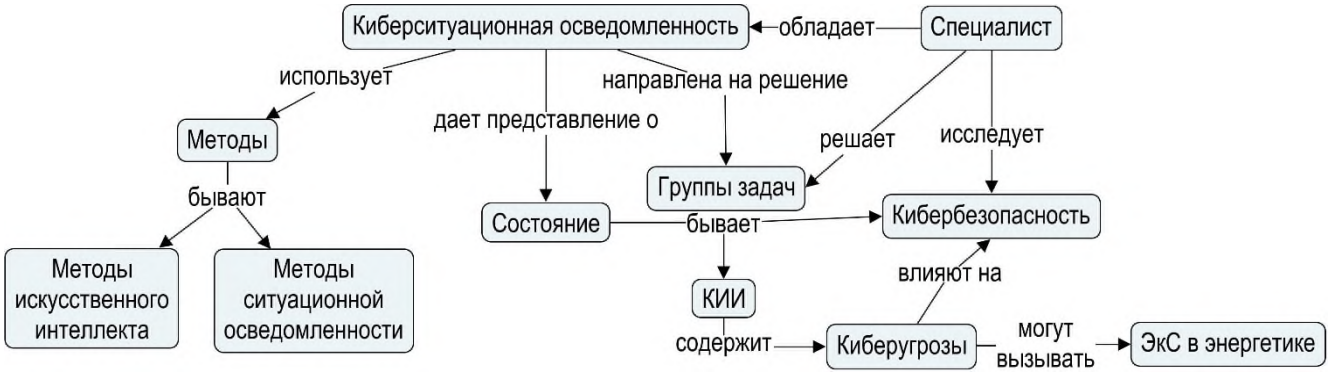

Рисунок 2.4 – Метаонтология КСО энергетической инфраструктуры

В центре системы онтологий находятся выявленные выше группы задач, выделенные в три блока. Для их решения предложено использовать методы искусственного интеллекта и интеллектуальные информационные технологии, применение которых отражено в трех компонентах интеллектуального программного комплекса. Для адаптации и развития предложенных методов, а также их реализации в каждом из компонентов необходимо построить онтологические модели, которые в соответствии с группами задач объединены в подсистемы. Подсистемы онтологий, которые детализируют рис. 2.3., далее рассмотрены подробнее.

На втором этапе концептуализации (структурирования) знаний построены подсистемы онтологий для каждой группы задач анализа КСО энергетических объектов, выделены основные понятия рассматриваемой области и их взаимосвязи.

Подсистема онтологий для решения задачи анализа киберугроз представлена на рисунке 2.5 (блок 1, рис. 2.3).

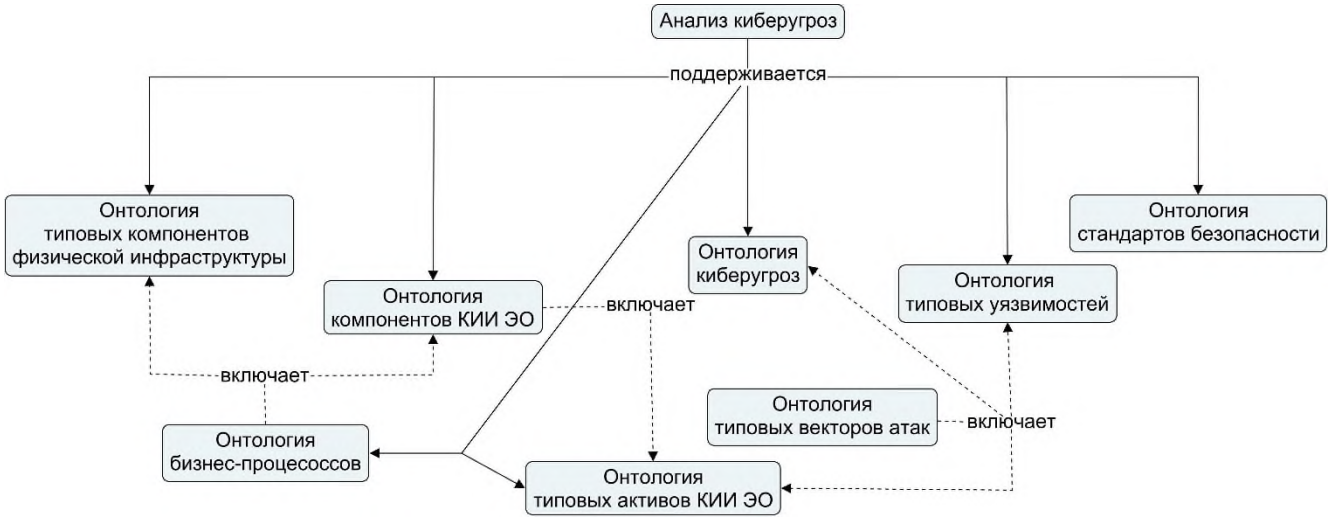

Рисунок 2.5 – Подсистема онтологий для анализа киберугроз

Подсистема онтологий для анализа киберугроз включает восемь взаимосвязанных онтологий. Анализ угроз до сих пор остаётся нетривиальной задачей. Наибольшая сложность заключается в сопоставлении уязвимостей активов автоматизированных информационных систем, используемых на предприятии, и возможных угроз безопасности, реализация которых повлечёт ощутимые потери для рассматриваемого объекта. В настоящее время не

существует единого нормативно-правового пространства, охватывающего вопросы обеспечения безопасности в области энергетики. Нормативные документы охватывают различные области безопасности и используют различную терминологию. Анализ нормативных документов, в том числе международных, отражен, например, в работах [112, 113]. Онтология стандартов безопасности разрабатывается с целью кластеризации знаний по методам проведения оценки безопасности, а также методам обеспечения безопасности для каждой из областей кибербезопасности: безопасности приложений, информационной безопасности, сетевой безопасности, безопасности Интернет и защите ключевых информационных систем объектов критических инфраструктур. Онтология стандартов безопасности будет применяться при разработке экспертной системы, являющейся компонентом интеллектуального программного комплекса анализа КСО энергетических объектов [114].

С целью определения основных угроз в энергетике, связанных с нарушением кибербезопасности на объектах, разработана онтология угроз, представленная в Приложении А на рисунке 4.1. Как правило, описание уязвимостей и угроз включает слабые места конкретного программного продукта. Основные задачи онтологического инжиниринга в данной области заключаются в установлении актуальных уязвимостей и угроз для энергетики и их классификации для типовых компонентов и активов КИИ. Соответствующие онтологии будут применяться для формирования структуры и дальнейшего наполнения базы знаний разрабатываемой ЭС [115] с целью построения векторов атак на целевые активы предприятия. Формирование векторов атак позволяет устанавливать связи между уязвимостями и угрозами. Типовые векторы атак на промышленные предприятия и корпоративные информационные системы (КИС) описаны в исследованиях ведущих компаний, таких как Лаборатория Касперского [116] и Positive Technologies [32, 117], типовые угрозы в энергетике описаны в [118].

В ходе анализа киберугроз исследуются активы КИИ рассматриваемого объекта и выявляются критически значимые и содержащие уязвимости. Онтологический инжиниринг в данной области проводился на трёх уровнях

автоматизированной системы управления технологическими процессами, особое внимание при этом уделялось верхнему уровню диспетчерского управления, поскольку характерной особенностью последствий реализации угроз на этом уровне является возможность получения административного доступа к системе управления предприятием.

Анализ киберугроз ведётся на основе онтологического инжиниринга основных бизнес-процессов (термин 3.6) КИИ ЭО, целью которого является обоснование полноты выявляемых уязвимостей. Для формирования базы знаний об ЭО выполняется онтологический инжиниринг типовых компонентов их технологической инфраструктуры, а также компонентов КИИ.

Онтологический инжиниринг в рамках анализа угроз позволил систематизировать разрозненную информацию о самих ЭО, их характеристиках и компонентах, бизнес-процессах, активах, связанных с ними уязвимостях и угрозах нарушения кибербезопасности, а также стандартах безопасности, применимых в энергетическом секторе.

Задачи по прогнозированию условий функционирования и развития систем энергетики и ТЭК, оценке состояния в этих условиях, выбор альтернатив и мер по предотвращению критических и чрезвычайных ситуаций в энергетике решаются в рамках модельных сценарных исследований [87]. При решении задачи прогнозирования поведения ЭО в условиях нарушения кибернетической безопасности, вызывающих реализацию угроз энергетической безопасности, которые могут приводить к значительным негативным последствиям как для самого объекта, так и для внешней среды, проводился онтологический инжиниринг, по результатам которого сформирована подсистема онтологий. Подсистема онтологий для решения задачи моделирования сценариев возникновения ЭкС в энергетике, вызванных реализацией кибеугроз, представлена на рисунке 2.6 (детализация блока 2, рис. 2.3).

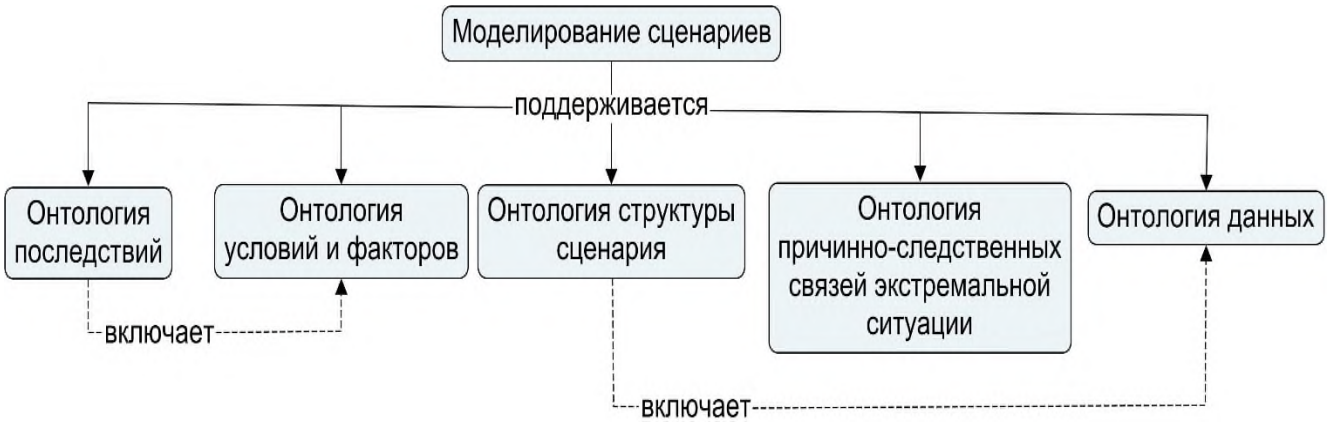

Рисунок 2.6 – Подсистема онтологий для моделирования сценариев экстремальных ситуаций в энергетике, вызванных киберугрозами

В диссертационной работе рассматриваются сценарии нарушения кибербезопасности энергетической инфраструктуры как часть сценариев нарушения энергетической безопасности. Количество инцидентов, связанных с реализацией киберугроз на промышленных предприятиях, растет [32], а возглавляет список энергетический сектор [116]. Онтология сценария экстремальной ситуации в энергетике, вызванной киберугрозами, представлена в Приложении А на рисунке 4.2. На основе представленной онтологии далее разрабатывалась модель построения сценариев в рамках моделирования БСД, которые хорошо зарекомендовали себя в качестве инструмента вероятностного моделирования для анализа как угроз энергетической безопасности [103], так и экономических рисков [119] и рисков информационных технологий [120].

Сценарий экстремальной ситуации в энергетике представляет собой вероятностные оценки возможных ситуаций, представленные последовательностью уязвимостей, киберугроз, угроз энергетической безопасности и угроз причинения ущерба рассматриваемому предприятию и/или территориально-приближенной внешней среде, либо энергосистеме в целом. При этом состояниями узлов байесовской сети доверия, как правило, являются пессимистические оценки основных количественных характеристик активов исследуемых ЭО в условиях нарушения кибербезопасности рассматриваемого объекта [121].

Помимо присутствия уязвимостей в активах КИИ или отсутствия средств защиты и методов обеспечения надежности активов КИИ, немаловажными при возникновении той или иной ситуации являются текущее состояние системы и влияющие на неё факторы, например, такие, как сезонность, экологическая значимость прилегаемой территории, социальные факторы и другие. Это направление онтологического инжиниринга основывается на исследованиях устойчивости энергетических систем [11, 122] и технологической безопасности [12] и рассматривается как перспектива дальнейшего исследования.

В процессе формирования графа экстремальной ситуации оценивается вероятность наступления вероятных негативных событий с точки зрения эксперта, таких, как снижение генерации, снижение нагрузки, отключение групп потребителей и др. В работах по исследованию энергетической безопасности разработаны индикаторы [57], по которым можно судить о наступлении той или иной экстремальной ситуации. В этом направлении разрабатывается онтология последствий с учетом исследований индикаторов энергетической безопасности на основе анализа описанных инцидентов, например, в [123, 124]. В Приложении А на рис. 4.3 представлена онтология причинно-следственных связей экстремальной ситуации, вызванной киберугрозами.

Подсистема онтологий для решения задачи оценки рисков нарушения кибербезопасности энергетических объектов представлена на рисунке 2.7 (детализация блока 3, рис. 2.3).

Процесс оценки рисков включает в себя три этапа: идентификация, анализ и оценивание рисков. Анализ рисков сопровождается идентификацией значимых угроз и уязвимостей, а также оценкой вероятности реализации угроз и уязвимостей [125]. В работе анализ рисков проводится в рамках решения задач по анализу киберугроз и моделированию сценариев экстремальных ситуаций в энергетике [126].

В работе риск рассматривается как сочетание последствий некоторого события (инцидента) и связанной с ним возможностью возникновения

(вероятностью возникновения), а оценка риска – как общий процесс идентификации рисков, анализа риска и оценивания рисков [53].

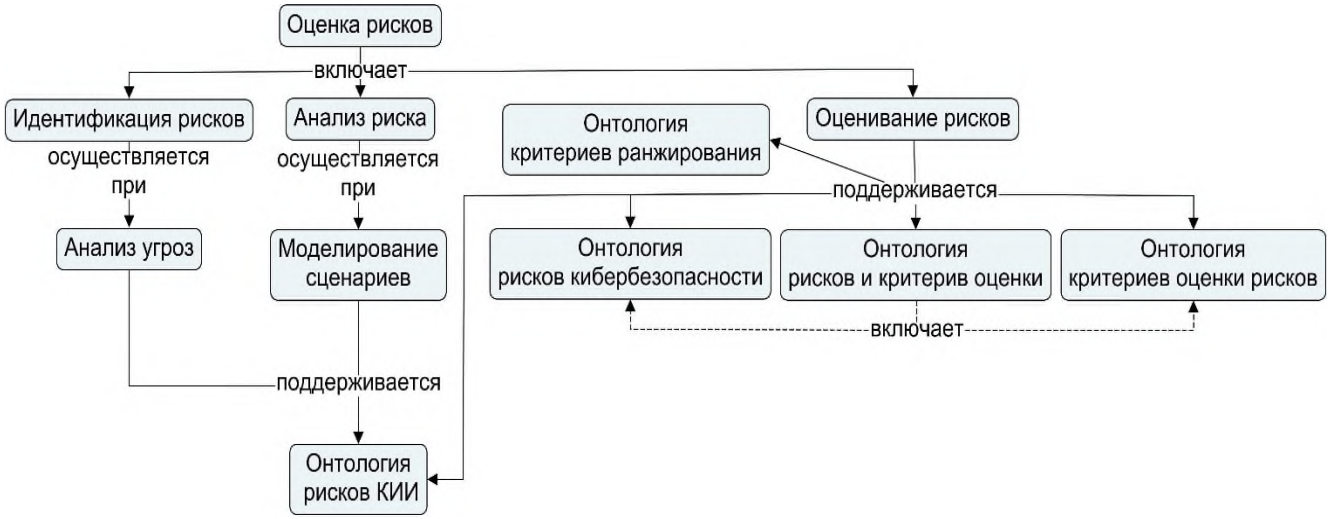

Рисунок 2.7 – Подсистема онтологий для оценки рисков нарушения кибербезопасности энергетической инфраструктуры

Риски кибербезопасности рассматриваются, с одной стороны, как риски киберсреды, а с другой, как вид рисков энергетической безопасности [127], связанных с нарушением функционирования технологической инфраструктуры ЭО, приводящим к негативным последствиям. Онтология рисков кибербезопасности представлена в Приложении А на рисунке 4.4. Шкала оценивания рисков должна учитывать масштаб последствий, и, в дальнейшем, уровень индикаторов энергетической безопасности объектов.

На основе метаонтологии КСО энергетической инфраструктуры и онтологий, построенных на втором этапе онтологического инжиниринга проблем кибербезопасности энергетической инфраструктуры, выполнен третий этап онтологического инжиниринга.

Третий этап – этап формализации поля знаний при помощи специализированных языков представления знаний выполнен для системы онтологий в рамках формализации модели ЭкС в энергетике, вызванных киберугрозами, и описания численного метода, полученные сущности использовались при проектировании интеллектуального программного комплекса, представленного в главе 3.

2.3 Вероятностная модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз

В рамках исследований киберситуационной осведомленности предлагается модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, на основе БСД. На основе модели осуществляется вероятностный вывод и определяются вероятности киберугроз на каждом этапе. Модель предлагается строить в соответствии с типовой схемой атаки на технологический сегмент сети [32], содержащей три основных этапа:

1. Проникновение в КИС.
2. Проникновение из КИС в технологический сегмент (ТС) локальной вычислительной сети (ЛВС).
3. Атака на целевой актив.

На основе структурирования знаний с использованием фрактального подхода и онтологического инжиниринга разработана модель сценариев ЭкС в энергетике, вызванных киберугрозами. В общем виде модель $\boldsymbol{M}$ описывается как:

$$\boldsymbol{M} = \{A, V, T, W, C, F\}, \tag{2.7}$$

где A – множество активов КИИ энергетического объекта (аппаратно-программные, программные, протоколы и пр.):

$$A = \{A^{\mathrm{E}}, A^{\mathrm{I}}\}, \tag{2.8}$$

где A^{E} – множество активов локальной вычислительной сети (ЛВС) (киберсреды), A^{I} – множество активов технологической инфраструктуры (ТехИ) (энергетические объекты);

V – множество всех обнаруженных критических уязвимостей рассматриваемой ЛВС, V_i – множество критических уязвимостей актива киберсреды, $i = \overline{1, |A^{\mathrm{E}}|}$:

$$V_i = \{v_{i1}, v_{i2} \ \ldots, v_{ih}\}, V_i \subset V; \tag{2.9}$$

T – множество киберугроз активов ЛВС:

$$T = \{T^V, T^W\}, \tag{2.10}$$

где T^V – множество киберугроз, инициирующих критические уязвимости V:

$$T_i^V = \{t_{i1}^V, t_{i2}^V, \dots, t_{iu}^V\}, T_i^V \subset T^V, \quad (2.11)$$

T^W – множество киберугроз, спровоцированных инициирующими киберугрозами T^V в рамках одного вектора угрозы:

$$T_i^W = \{t_{i1}^W, t_{i2}^W, \dots, t_{iq}^W\}, T_i^W \subset T^W; \quad (2.12)$$

W – множество техногенных угроз ЭБ, вызванных киберугрозами T:

$$W = \{w_1, w_2, \dots, w_m\}; \quad (2.13)$$

C – множество последствий реализации угроз:

$$C = \{c_1, c_2, \dots, c_z\}; \quad (2.14)$$

F – множество взаимосвязей между критическими активами, уязвимостями активов ЛВС, угрозами и последствиями реализации угроз):

$$F = \{F_A^V, F_V^T, F_W^T, F_W^C\}, \quad (2.15)$$

где $F_A^V: V \longrightarrow A$, $F_V^T: T \longrightarrow V$, $F_W^T: T \longrightarrow W$, $F_W^C: C \longrightarrow W$.

Вероятностной моделью сценариев ЭкС в энергетике, вызванных киберугрозами, будем называть ациклический, ориентированный, взвешенный граф G такой, что:

$$G = (N, U; q), \quad (2.16)$$

где N – множество вершин графа, U – множество дуг графа, q – функция на вершинах.

Каждой вершине N_i графа G соответствует единственная случайная величина X_i, такая, что:

$$X_i \in \{X^V \cup X^T \cup X^W \cup X^C\}, \quad (2.17)$$

где $i = \overline{1,n}$ и $n = |V| + |T| + |W| + |C|$, X^V – множество случайных величин, соответствующих V, X^T – множество случайных величин, соответствующих T, X^W – множество случайных величин, соответствующих W, X^C – множество случайных величин, соответствующих C.

На множество дуг U графа G наложены ограничения, в рамках которых отношение между X^V и X^T задается двумя типами дуг: (X^V, X^T) или (X^T, X^V); отношение между X^T и X^W задается как (X^T, X^W); между X^W и X^C как (X^W, X^C), а другие составляют пустые множества.

Зададим функцию q на вершинах графа G как:

$$q: N \to B, \tag{2.18}$$

где B_i – матрица весов вершины N_i. Для каждой вершины N_i элементами этой матрицы являются вероятности соответствующей случайной величины X_i(безусловные вероятности в случае, когда предков нет, условные вероятности в случае, когда есть набор предков $pa(X_i)$ вершины N_i), представленные в матричном виде в ТУВ).

2.4 Численный метод определения уровня КСО энергетического объекта

Определение уровня КСО энергетического объекта осуществляется по формуле:

$$L = \frac{\gamma}{2^n - 1}, \tag{2.19}$$

где L – уровень КСО энергетического объекта, γ – количество рассчитанных сценариев, $2^n - 1$ – общее количество сценариев, где $n = |V| + |T| + |W|$. Значения V, T, W введены ранее в формулах (2.9)-(2.13).

Численный метод описывается алгоритмом, представленным на рис 2.8 а. Блоки 4-7 представлены детализированным алгоритмом (рис. 2.8 б).

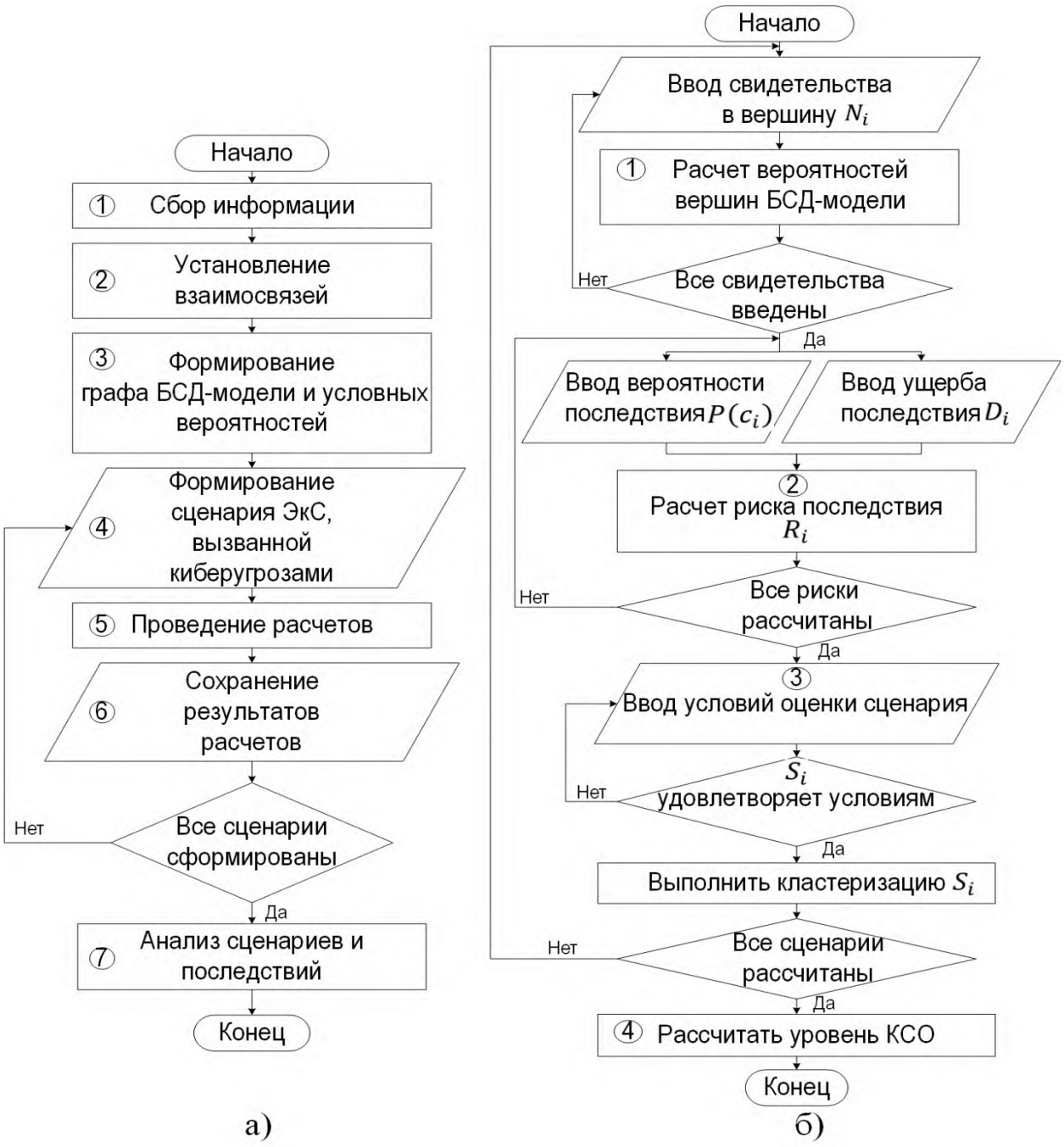

Рисунок 2.8 – а) алгоритм определения уровня КСО энергетического объекта, б) детализированный алгоритм определения уровня КСО (блоки 4-7)

Комментарий к рисунку 2.8 а. Блоки 1-2 соответствуют сбору информации, который заключается в определении множеств активов A по формуле (2.8), критических уязвимостей V (2.9), киберугроз T (2.10-2.12), W – техногенных угроз ЭБ (2.13), C – последствий реализации угроз (2.14), установление взаимосвязей F (2.15).

Блок 3 соответствует формированию графа G и заполнению матриц весов B_i для вершин N_i, в данном случае $i = \overline{1, |N|}$. При этом совместное распределение вероятностей на множестве вершин, соответствующих X графа G называют:

$$P(X) = (P_1(X), P_2(X), \dots, P_n(X)), \quad (2.20)$$
$$P_i(X) = P(X_i | pa(X_i))$$

где X_i введено в (2.17), $pa(X_i)$ – множество предков вершины, соответствующей X_i, в данном случае $n = |N|$.

Проведение расчетов (блоки 4-6) выполняется с целью ответа на вопрос «Как изменится вероятность последствий, если принять, что некоторое множество уязвимостей и/или угроз реализовано?». Такое множество будем называть множеством свидетельств, каждое из которых можно описать утверждением вида «Определенные уязвимости из V и/или угрозы из T, W реализованы». При наличии такого множества свидетельств необходимо пересчитать вероятности дискретных случайных величин X, соответствующих вершинам N графа G.

Анализ сценариев и последствий (блок 7) осуществляется путем анализа распределения рисков отдельных сценариев по кластерам, сопровождается описанием рисков R:

$$R = \{T, V, W, C, D\}, \quad (2.21)$$

где значения T, V, W, C введены ранее в (2.9-2.14), D – множество ущербов последствий сценариев.

Комментарий к рисунку 2.8 б. Вершины, в которые введены свидетельства, имеют множество вершин-потомков. Для того, чтобы в каждой из таких вершин-потомков пересчитать апостериорную вероятность (после наблюдения) в их матрицах весов B требуется не учитывать все несовместимые со свидетельством в вершине-предке случаи. Если случай становится невозможным, то его вероятность принимается равной нулю (невозможное событие). Вероятности прочих случаев пересчитываются (блок 2) по формуле Байеса:

$$P(X_i | e) = \frac{\sum_{j=1}^{m} P_i(X, e)}{P(e)}, \quad (2.22)$$

где $P(X_i|e)$ – апостериорная вероятность X_i, E – множество дискретных случайных величин, являющихся свидетельствами, e – значения этих случайных величин, m –

количество оставшихся случайных переменных, в которые не введены свидетельства.

Количественная оценка рисков последствий сценария S_i (блок 2) выполняется по формуле:

$$R_i = P(c_i) \times D_i, \quad (2.23)$$

где вероятность P является функцией Y от сценария S_i: $P(c_i) = Y(S_i)$, $P(c_i)$ – вероятность последствия сценария S_i, рассчитываемая по формуле (2.22), D_i – ущерб от реализации киберугроз этого сценария, $i = \overline{1, 2^n - 1}$.

Условия оценки сценариев ЭкС, вызванных киберугрозами (блок 3), имеют вид, представленный в таблице 2.1.

Таблица 2.1 – Условия оценки сценариев ЭкС, вызванных киберугрозами

Незначительный уровень опасности	Средний уровень опасности	Высокий уровень опасности
$\begin{cases} 0 \le P(\mathrm{c}_i) \times D_i < l_1 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (2.24)	$\begin{cases} l_1 \le P(\mathrm{c}_i) \times D_i < l_2 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (2.25)	$\begin{cases} l_2 \le P(\mathrm{c}_i) \times D_i \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (2.26)

где l_1, l_2 – критерии кластеризации сценариев ЭкС, вызванных киберугрозами, D^{m} – максимальный ущерб, $i = \overline{1, 2^n - 1}$.

Кластеризация сценариев описывается как:

$$K_s = \{S_{s1}, S_{s2}, \dots, S_{sl}\}, \quad (2.27)$$

где K_s – множество кластеризованных сценариев ЭкС в энергетике, вызванных киберугрозами (все сценарии разбиваются на три кластера: норма, предкризис, кризис), $s = \overline{1,3}$. Принимается, что существует взаимно-однозначное соответствие между сценарием S_i и вероятностью его последствия $P(c_i)$, $i = \overline{1, 2^n - 1}$,$n = |V| + |T| + |W|$.

Определение уровня КСО энергетического объекта осуществляется по формуле (2.19) [128].

2.5 Методика анализа киберситуационной осведомленности энергетических объектов

Для применения вероятностной модели сценариев ЭкС в энергетике, вызванных киберугрозами, и численного метода предлагается методика определения уровня киберситуационной осведомленности энергетического объекта, включающая: 1) методику анализа киберугроз, 2) методику моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз и 3) методику оценки рисков последствий реализации угроз. Анализ киберситуационной осведомленности энергетических объектов в нотации IDEF0 [129], отображающей структуру и функции системы, а также потоки информации и материальных объектов, преобразуемые этими функциями, представлен на рисунке 2.9.

Рисунок 2.9 – Контекстная диаграмма анализа киберситуационной осведомленности энергетических объектов в нотации IDEF0

На рисунке 2.9 представлен блок, описывающего функцию верхнего уровня, которая заключается в анализе киберситуационной осведомленности энергетических объектов. Входными стрелками (слева) обозначены данные и

знания, которые преобразуются в ходе анализа; выходными стрелками (справа) обозначены данные и знания, полученные в результате анализа; стрелки управления (сверху) соответствуют условиям, при выполнении которых выход блока будет правильным (нормативные документы); стрелки механизмов (снизу) отображают средства, используемые для выполнения анализа и включают программные продукты и человеческие ресурсы [129].

Предлагаемые методики разработаны в соответствии со стандартом ГОСТ ИСО/МЭК 27005-2010 [53] на основе методик анализа угроз и оценки рисков информационно-технологической безопасности энергетических комплексов [106] и моделирования угроз энергетической безопасности с помощью байесовских сетей [105].

Основные этапы анализа киберугроз и оценки рисков нарушения кибербезопасности энергетической инфраструктуры представлены на рисунке 2.10.

Рисунок 2.10 – Декомпозиция первого уровня анализа киберситуационной осведомленности энергетических объектов в нотации IDEF0

На первом уровне декомпозиции анализа киберситуационной осведомленности энергетических объектов выделены три основных процесса, представленные блоками на диаграмме. Анализ киберугроз энергетической инфраструктуры предлагается выполнять по соответствующей предложенной методике и с использованием предложенной экспертной системы и дополнительных инструментальных средств, обычно используемых при проведении аудита безопасности КИИ. Моделирование сценариев ЭкС в энергетике, вызванных реализацией киберугроз, предлагается выполнять по соответствующей методике с использованием компонента БСД и инструментальных средств, реализующих математическое моделирование энергетических объектов. Оценку рисков предлагается осуществлять с учетом предыдущих процессов, используя компонент оценки рисков. Предлагаемые методики подробно рассмотрены далее.

2.5.1 Методика анализа киберугроз энергетической инфраструктуры

Методика анализа киберугроз энергетической инфраструктуры включает три этапа.

Этап 1. Описание энергетического объекта и установление критериев оценки. Включает описание основных характеристик ЭО, бизнес-процессов и КИИ ЭО. Шкалы критериев оценки устанавливаются в отношении активов КИИ, угроз и уязвимостей.

Описание объекта включает выделение критичных бизнес-процессов организации, в рамках которых определяются критичные системы, их основные компоненты и функциональное назначение. Функциональное назначение систем потребуется при формировании предположений о возможных киберфизических последствиях угроз [130].

Для каждого компонента системы определяется состав основных активов. Активами являются информация, программное обеспечение, аппаратное

обеспечение, информационная система (сложный актив, включающий предыдущие) [131] и другое.

Структуру состава основных активов рассматриваемого объекта предлагается формировать по подсистемам КИИ. Для описания информационно-технологической системы энергетического объекта выделены следующие подсистемы [132]:

- корпоративная информационная система;
- локальная вычислительная сеть (ЛВС);
- автоматизированная система управления технологическим объектом;
- средства защиты.

Для оценки угроз нарушения кибербезопасности энергетической инфраструктуры в диссертационном исследовании предлагается использовать следующие критерии.

Критерий значимости (критичности) актива. Категоризация компонентов рассматриваемого объекта по уровню их критичности позволяет более точно определить степень тяжести возможных последствий от воздействия угрозы на конкретный компонент [130]. В качестве возможных критериев, используемых для определения ценности актива, могут использоваться его исходная стоимость, стоимость его замены или воссоздания, или ценность, которая может быть абстрактной, например, ценность репутации организации [53]. Для качественного определения ценности актива обычно используется шкала: пренебрежительно мала, очень низкая, низкая, средняя, высокая, очень высокая, критичная. С одной стороны, присвоенная качественная оценка значимости компонентам рассматриваемого объекта определяет степень тяжести последствий, а с другой, количественная (финансовая) оценка его значимости может быть использована на этапе определения ущерба от его сбоя, повреждения или уничтожения.

Критерий значимости (критичности) физического актива определяется в соответствии со шкалой значимости (критичности) актива. Пример шкалы значимости физического актива для объекта энергетики, целью которого является генерация и передача энергии, представлен в таблице 2.2.

Значимым активом считаем активы с оценкой «Очень высокая», «Высокая» и «Средняя».

Таблица 2.2 – Шкала значимости физического актива КИИ при нарушении кибербезопасности объекта

Качественные значения	Расположение	Характеристика
Очень высокая	Технологическая сеть	Сбой, повреждение или уничтожение актива напрямую влияет на выполнение основных бизнес-процессов ЭО, таких, как генерация и передача энергии.
Высокая	Технологическая сеть	Сбой, повреждение или уничтожение и/или перехват административного доступа к активу напрямую и в значительной степени влияет на выполнение основных функций КИИ, таких, как управление генерацией и диспетчеризация.
Средняя	Технологическая сеть, корпоративная сеть	Сбой, повреждение или уничтожение не влияет на выполнение основных функций КИИ, однако перехват административного доступа к активу может повлечь развитие атаки, т.е. косвенно влияет на выполнение основных функций КИИ.
Низкая	Гостевая сеть, корпоративная сеть	Сбой, повреждение или уничтожение актива напрямую не влияет на выполнение основных функций КИИ.
Очень низкая	Гостевая сеть, корпоративная сеть	Сбой, повреждение или уничтожение актива не влияет на выполнение основных функций КИИ.

Критерии оценивания уязвимостей и угроз. Как правило, базируются на «The Common Vulnerability Scoring System» (CVSS) [45], включающей три группы метрик: базовые, временные и контекстные. Метрики учитывают способ и сложность получения доступа, влияние на конфиденциальность, целостность, доступность и др. При рассмотрении угроз на энергетические объекты большее внимание уделяются угрозам, влияющим на доступность. При оценивании уязвимостей и угроз также применяют классификации угроз и источников

уязвимостей. Шкалы оценки угроз и рисков рассматривались, например, в работах [52, 133].

Критерии оценивания уязвимостей и угроз определяются в соответствии со шкалой, представленной в таблицах 2.3-2.4.

Таблица 2.3 – Шкала степени уязвимости актива КИИ

Качественные значения	Расположение	Характеристика
Очень высокая	Значимый актив	Обнаруженную уязвимость нет возможности устранить, её просто использовать и содержится она в значимом активе.
Высокая	Значимый актив	Устранение обнаруженной уязвимости влияет на технологический процесс, возможно использовать.
Средняя	Значимый актив	Устранение обнаруженной уязвимости возможно в обозримом будущем, для нее существует известный эксплойт*.
Низкая	Значимый актив	Обнаруженную уязвимость возможно устранить в обозримом будущем, практически невозможно использовать, но содержится она в значимом активе.
Очень низкая	Актив	Обнаруженную уязвимость возможно устранить в обозримом будущем и практически невозможно использовать, но содержится она в незначимом активе.

* термин 2.49

Таблица 2.4 – Шкала степени киберугрозы актива КИИ ЭО

Качествен-ные значения	Актив	Уязви-мость	Характеристика
Очень высокая	Значимый актив	Очень высокая, Высокая	Критическая угроза, существует несколько способов её реализовать, которые невозможно устранить в полной мере, не требуется высокий уровень навыков её реализации
Высокая	Значимый актив	Очень высокая, Высокая, Средняя	Серьезная угроза, может существовать несколько способов её реализации, которые возможно устранить в обозримом будущем, требуются специализированные навыки для её реализации.

Качественные значения	Актив	Уязвимость	Характеристика
Средняя	Значимый актив	Очень высокая, Высокая, Средняя	Умеренная угроза, не существует множества способов её реализации и требуется высокий уровень навыков для её реализации.
Низкая	Актив	Очень низкая	Незначительная угроза, которую можно устранить.
Очень низкая	Актив	Очень низкая	Угроза, которой можно пренебречь.

В дальнейшем рекомендуется рассматривать уязвимости и угрозы с оценкой «Очень высокая», «Высокая» и «Средняя», а также угрозу с уровнем «Низкая».

Оценивание векторов атак предлагается осуществлять в соответствии со шкалой, представленной в таблице 2.5.

Таблица 2.5 – Шкала оценки векторов кибератак ЭО

Качественные значения	Актив	Уязвимости и угрозы	Характеристика
Очень высокая	Значимый актив	Очень высокая, Высокая	Целевым активом вектора является значимый актив, для реализации вектора не требуется высокий уровень навыков, используются известные эксплойты (термин 2.16) или уязвимости zero day, вектор включает небольшое количество шагов для получения административного доступа к целевому активу. В эту категорию входят и APT-атаки (термин 2.17).
Высокая	Значимый актив	Очень высокая, Высокая, Средняя	Получение административного доступа к целевому активу или нарушение его функционирования напрямую влияет на основные бизнес-процессы ЭО.
Средняя	Значимый актив, Актив	Очень высокая, Высокая, Средняя, Низкая	Получение административного доступа к целевому активу или нарушение его функционирования косвенно влияет на основные бизнес-процессы ЭО.

Качественные значения	Актив	Уязвимости и угрозы	Характеристика
Низкая	Актив	Очень низкая	Получение административного доступа к активу невозможно. Реализация вектора возможна при больших затратах и высоком уровне навыков.
Очень низкая	Актив	Очень низкая	Административный доступ к целевому активу невозможен.

Результатом этапа является список активов рассматриваемого объекта, включающий оценку актива, а также шкалу оценивания уязвимостей, угроз и векторов атак по установленным критериям оценивания.

Этап 2. Анализ уязвимостей и угроз КИИ объекта. Включает анализ КИИ с последующим оцениванием активов КИИ, выявлением критически важных активов (КВА), выявлением киберуязвимостей в активах КИИ и киберугроз, выделение возможных целевых активов кибератаки. Результат этапа записываются в таблицу 2.6 следующего вида:

Таблица 2.6 – Перечень активов, уязвимостей и киберугроз

№	Технические средства	Программное обеспечение	Факторы	Тип уязвимости	Угрозы

Анализ КИИ, как правило, осуществляется путем проведения внутреннего или внешнего аудита безопасности. Данное мероприятие регламентируется в соответствии с руководящими документами и законодательством.

Анализ уязвимостей и угроз включает сбор и анализ информации о системе и выявление уязвимостей и киберугроз. Сбор данных и их анализ осуществляются путем анализа соответствия нормативным документам существующих политик безопасности и реализации их на местах. Далее для списка значимых активов формируются перечни угрожающих факторов и событий, слабых мест (уязвимостей) анализируемой системы. Такая информация может быть получена как путем анализа внутренних произошедших инцидентов безопасности, так и внешней статистической информации. На основе собранной информации

осуществляется выявление уязвимостей. Для каждого актива рассматриваемого объекта необходимо выявить список уязвимостей. Формирование такого списка, как правило, основывается на информации из общедоступных баз данных уязвимостей в соответствии с используемыми версиями оборудования и программного обеспечения [130]. Уязвимости и угрозы содержатся в базах данных, например, «Банк данных угроз безопасности информации» ФАУ «ГНИИИ ПТЗИ ФСТЭК России» [134], международная база данных уязвимостей «Common Vulnerabilities and Exposures» (CVE) [135].

Известные уязвимости выявляются методами сканирования и экспертными методами проверки безопасности программного кода в процессе сертификационных испытаний и тематических исследований по требованиям безопасности [136].

Для выявления технических уязвимостей также применяют автоматизированные инструментальные средства поиска уязвимостей. Кроме того, при формировании списка уязвимостей могут быть использованы имеющиеся результаты анализа защищенности и тестирования на проникновение. Анализ мер защиты для каждой уязвимости позволит оперативно устранить уязвимости, которые можно минимизировать или полностью исключить безболезненно для бизнес-процессов организации [130]. Кроме того, для определения дополнительных системных уязвимостей следует использовать непрерывный анализ рекомендаций по вопросам безопасности от разработчика, системных журналов и развернутых систем обнаружения вторжений [118].

После установления потенциально угрожающих факторов для каждого значимого актива рассматриваемого объекта, на основе информации об источниках и выявленных уязвимостях, анализируется список угрожающих факторов и выбираются те, которые могут оказать воздействие на активы, классифицированные как КВА, и для каждого актива рассматриваемого объекта определяются потенциальные события, при которых угрожающие факторы могут создать угрозу его компрометации.

Анализ должен включать как случайные (киберхалатность), так и умышленные события (кибератаки), связанные с реализацией угроз. Для каждого потенциального события необходимо проанализировать угрожающие факторы по степени вероятности и предполагаемым последствиям.

Далее проводится оценивание активов КИИ и агрегация информации о них, включая проранжированный по значимости список активов, с учетом количества и критичности выявленных в них уязвимостей, вероятности реализации на них угроз и уровня предполагаемых последствий для КИИ. Ранжирование предлагается осуществлять с учетом критериев оценки активов, оценки эффективности существующих средств защиты, уровня последствий для КИИ, вероятности использования уязвимости и реализации угрозы. Активы, имеющие наиболее низкие показатели по уровню защиты, и наиболее высокие по уровню последствий и критериям значимости, далее будем называть критически важный актив.

Результатом этапа является список уязвимостей для каждого значимого актива КИИ рассматриваемого объекта. Описание каждой уязвимости строится на критериях оценки уязвимостей.

Этап 3. Построение модели сценариев ЭкС в энергетике, вызванных киберугрозами. Включает описание реализации киберугрозы, выделение векторов проникновения и векторов атак на целевые активы, а также их анализ. При этом векторы атак направлены на целевые активы, являющиеся составляющей технологической инфраструктуры энергетического объекта. Используя результаты анализа уязвимостей системы, необходимо описать возможные сценарии киберхалатности (сотрудников и временных пользователей) и векторов атак (сценарий состоит из одного или нескольких событий, вызванных угрожающим фактором, способных привести к компрометации актива). Уязвимости активов, угрозы их использования и последствия для КИИ проанализировать с использованием логического сценария: «ЕСЛИ-ТО». Моделирование сценариев начинается с определения киберуязвимостей на энергетическом объекте. Далее формируются цепочки «уязвимость-угроза» и «угроза-угроза», отражающие тривиальные (предсказуемые) атаки и поведение нарушителя кибербезопасности.

Затем следует определить логический смысл сценариев угроз и обосновать исключение сценариев [106], после чего можно приступать к построению модели нарушения кибербезопасности энергетической инфраструктуры (таблица 2.7).

Таблица 2.7 – Сценарий «ЕСЛИ-ТО»

Опе-ратор	**Тип концепта /оператор**	**Наимено-вание**	**Опе-ратор**	**Тип концепта /оператор**	**Наименование**
Вектор проникновения					
ЕСЛИ	[актив]	Актив [источник уязвимости]	**ТО**	[актив]	Актив [источник уязвимости]
	[оператор]	**И/ИЛИ**		[оператор]	**И/ИЛИ**
	[уязвимость]	Уязвимость актива		[кибер-угроза]	Киберугроза, направленная на актив
ЕСЛИ	…	…	**ТО**	…	…
Вектор развития атаки					
ЕСЛИ	…	…	**ТО**	…	…
Атака на целевой актив					
ЕСЛИ	…	…	**ТО**	…	…

Модель нарушения кибербезопасности представляет собой сценарий, содержащий правила «ЕСЛИ-ТО», которые описывают способы реализации киберугрозы.

Формирование концептов сценария базируется на выделении векторов проникновения, векторов атак, векторов киберхалатности, включающих используемые уязвимости и возможные угрозы, с указанием степени их значимости: «очень низкая», «низкая», «средняя», «высокая», «очень высокая». Используя таблицы 2.2-2.8, определяются наиболее значимые вектора на основе определения значимых угроз и уязвимостей, участвующих в них.

Таблица 2.8 – Уровень значимости вектора атаки

Возможность реализации и критичность уязвимостей и угроз	Степень влияния вектора на целевой актив				
	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Очень высокая	Низкая	Средняя	Высокая	Очень высокая	Очень высокая
Высокая	Низкая	Средняя	Средняя	Высокая	Очень высокая
Средняя	Низкая	Низкая	Средняя	Средняя	Высокая
Низкая	Очень низкая	Низкая	Низкая	Средняя	Средняя
Очень низкая	Очень низкая	Очень низкая	Низкая	Низкая	Низкая

Анализ киберугроз предлагается проводить с привлечением внутренних или внешних специалистов, обладающих компетенциями в области информационной безопасности и/или администрирования локально-вычислительной сети. В результате выполнения этапа будут получены сценарии использования всех уязвимостей, включающие реализацию цепочек угроз, приводящих к нарушению нормального функционирования технологической инфраструктуры ЭО и некоторым негативным последствиям [137].

2.5.2 Методика моделирования сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз

Выбор условий моделирования. В рамках исследований энергетической безопасности выделяют экстремальные ситуации, включающие чрезвычайные и критические ситуации, определение которых базируется на оценке состояния систем или объектов по шкале: “норма”, “предкризис” – критическая ситуация, “кризис” – чрезвычайная ситуация. Под критическими ситуациями понимаются ситуации, когда возникают угрозы бесперебойному функционированию технических объектов и объектов обеспечения жизнедеятельности и/или угрозы

жизни или здоровью как отдельных людей, так и социальных (профессиональных) групп. Эти угрозы могут быть устранены принятием соответствующих превентивных и оперативных мер, которые не позволят критической ситуации перерасти в чрезвычайную, при которой необходимы оперативные и ликвидационные мероприятия [138]. Причинно-следственные связи влияния киберугроз на возникновение экстремальной ситуации в энергетике представлены на рисунке 2.11 [121].

Рисунок 2.11 – Экстремальная ситуация в энергетике, вызванная реализацией киберугрозы на объекте энергетики (в нотации диаграмм Исикавы)

Рисунок 2.11 в нотации Исикавы, или «рыбьего скелета» отражает рассматриваемые причины (причины первого порядка – стрелки под углом к горизонтальной прямой, второго (факторы) – линии под углом к стрелкам) влияния на возникновение экстремальной ситуации в энергетике как следствия (горизонтальная прямая). Факторы могут как усиливать влияние причин (линии со стороны тупого угла, образованного горизонтальной прямой и стрелкой причины первого порядка), так и ослаблять (линии со стороны острого угла, образованного горизонтальной прямой и стрелкой причины первого порядка).

Этап 1. Формирование узлов и их взаимосвязей вероятностного сценария. Сценарий представляет собой байесовскую сеть доверия (термин 3.2), построенную в соответствии со структурой сценария нарушения

кибербезопасности энергетического объекта (рисунок 2.12), где каждый блок отражает тип концепта для построения сети.

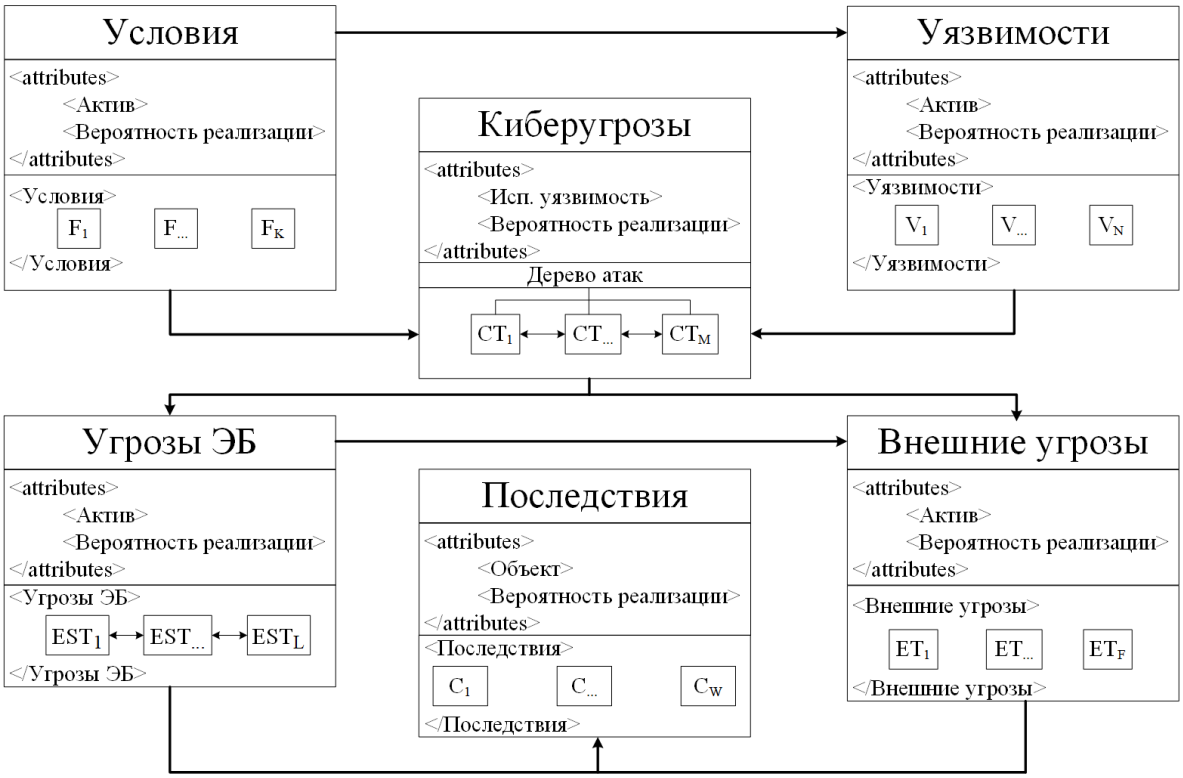

Рисунок 2.12 – Структура сценария экстремальной ситуации в энергетике

Предлагаются следующие типы концептов:

- факторы возникновения негативных последствий, либо, наоборот, условий, смягчающих их;
- уязвимости информационно-технологической системы энергетического объекта;
- киберугрозы, возникающие вследствие успешного использования кибер-уязвимостей нарушителем;
- угрозы энергетической безопасности, вызванные реализацией киберугрозы;
- угрозы для внешней среды, вызванные реализацией киберугроз исследуемого (ых) объектов;
- последствия, на основе которых определяются ущербы и оцениваются риски наступления экстремальной ситуации, вызванной реализацией киберугроз.

Основными узлами сети являются значимые уязвимости и угрозы, выявленные на предыдущих этапах. Дополнительные узлы отражают характеристики моделируемой экстремальной ситуации. Взаимосвязь узлов и их отношения «предок-потомок» устанавливаются на основе определенных ранее векторов проникновения, векторов атак и киберхалатности.

В первую очередь формируются цепочки узлов типа «уязвимость-киберугроза» и «киберугроза-киберугроза» в соответствии с моделью нарушения кибербезопасности. Такими узлами могут быть выявленные уязвимости, угрозы их использования, угрозы для КИИ и факторы реализации уязвимостей или угроз.

Далее, цепочки дополняются концептами типа «угроза ЭБ» и «последствия», исходя из того, что киберугрозы рассматриваются как инициирующие угрозы ЭБ. В зависимости от уровня детализации исследования взаимосвязи между концептами устанавливаются на уровне рассматриваемых объектов, домена объекта, активов или его конкретной составляющей. При необходимости сценарий дополняется концептами типа «фактор» и «внешняя угроза».

В результате получаем набор концептов сценария, сформированный путем отсечения, разбиения, группировки, уточнения, агрегации некоторых узлов.

Этап 2. Определение вероятностных характеристик сценария. Каждому узлу сети сопоставляется тип концепта. Каждый узел представляет собой переменную, которая описывается состояниями. Для каждого узла-потомка (термин 3.3) указываются оценки вероятностей различных значений переменной этого узла в зависимости от значений, принимаемых его узлом-предком (термин 3.4). Состояния должны описывать все возможные поведения узла. Например, для узлов типа «уязвимость» или «угроза» предлагаются два состояния: «используется», «не используется». Априорная вероятность состояния «используется» для узла-потомка отражает вероятность использования уязвимости или угрозы при реализации уязвимости или угрозы, являющихся узлами-предками. Априорная вероятность состояния «не используется» отражает статистические данные о реализации угрозы или уязвимости. Информация о вероятностных

характеристиках задается на основе опыта эксперта или имеющейся статистической информации.

Данный этап завершает построение сценария. После заполнения сети информацией она полностью готова для проведения на ней экспериментов.

Этап 3. Проведение вероятностного эксперимента. Используется прямой вывод на сети, позволяющий вычислить распределение вероятностей узлов, соответствующих концептам последствия, основываясь на предполагаемых априорных распределениях узлов – предков. Предлагается осуществлять обход графа по векторам атак.

Этап 4. Анализ альтернативных сценариев. Каждый сценарий представлен в виде графовой модели, содержащей причинно-следственную цепочку угроз кибернетической и энергетической безопасности, причин их возникновения, последствий, а также вероятность их наступления. Полученные на предыдущем этапе результаты анализируются, выявляются наиболее подверженные уязвимостям КВА, наиболее вероятные киберугрозы и последствия для функционирования как самой КИИ, так и энергетического объекта в целом. Для каждого вектора строится таблица, отражающая вероятность состояний узлов типа «последствие».

Введение тех или иных свидетельств в сеть позволяет определить наиболее неблагополучные ситуации на рассматриваемой сети. Описание состояний узлов типа «последствие» можно представить в таблице 2.9.

Состояния такого узла отражают шкалу оценивания экстремальной ситуации в энергетике: «норма», «предкризис», «кризис». Результатом этапа является сценарий(ии) экстремальной ситуации в энергетике, вызванной киберугрозами, включающий список уязвимостей, угроз кибернетической и энергетической безопасности, последствий и их вероятности, а также общая вероятность наступления такой ЭкС.

Таблица 2.9 – Описание последствий

сценариев ЭкС в энергетике, вызванных киберугрозами

№ сце-нария	Последствия	Состояния концепта «последствия»	Вероят-ность	Физические характери-стики ущерба	Список влияющих концептов предков
1	Концепт № 1 типа «последствия»	Наименование состояния № 1	X%	мВТ/ ч / мВТ/ч и др.	Узлы
	…	…	…	мВТ/ ч / мВТ/ч и др.	
	…	Наименование состояния № M	100-X-…%	мВТ/ ч / мВТ/ч и др.	
	…	…	…	…	…
	Концепт № N типа «последствия»				
…	…	…	…	…	…

2.5.3 Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры

Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры направлена на формирование риска, его качественное и количественное оценивание, а также включает ранжирование рассмотренных энергетических объектов по установленным критериям, в качестве которых могут выступать как величина интегрального показателя рисков по объекту, так и по отдельным типам рисков, связанных с каскадными авариями, экологическими последствиями, безальтернативностью энергоресурсов для потребителей и другое [139].

Этап 1. Описание рисков. Риск рассматривается как произведение вероятности на ущерб. Для каждого рассматриваемого сценария описываются состояния узла типа «последствие» и их вероятности, а также описывается набор узлов - предков и их состояний, приводящих к данному последствию. Экспертно определяется возможный ущерб для каждого состояния узла типа «последствие»,

т.е. риски описываются в соответствии с (2.21) [140] и могут быть записаны в таблицу 2.10.

Таблица 2.10 – Описание рисков

Наименование риска [состояние узла типа последствие]	**Угрозы, уязвимости, условия**	**Вероятность**	**Ущерб**

В зависимости от детализации исследования, риски могут быть описаны как для каждого последствия сценария, так и для сценария в целом. Следует выполнить описание рисков всех значимых сценариев в соответствии с классификацией рисков (Приложение А, рисунок 4.3).

Этап 2. Оценивание рисков. Включает два этапа: качественный и количественный. При формировании шкалы последствий следует отталкиваться от уровня их влияния на энергетическую безопасность [53]. При формировании шкалы вероятности следует учесть статистические данные по самой организации и аналогичным внешним инцидентам. Выполнение качественного оценивания рисков осуществляется с использованием матрицы рисков, представленной в таблице 2.11, где в качестве критериев оценки рисков выступают вероятность наступления риска и уровень ущерба.

Таблица 2.11 – Матрица рисков

Вероятность наступления риска	Уровень ущерба				
	Незначитель-ный	Небольшой	Средний	Серьезный	Катастрофичес-кий
Крайне высокая	Низкий	Средний	Высокий	Высокий	Высокий
Высокая	Низкий	Средний	Средний	Высокий	Высокий
Средняя	Низкий	Низкий	Средний	Средний	Высокий
Низкая	Низкий	Низкий	Низкий	Средний	Средний
Крайне низкая	Низкий	Низкий	Низкий	Низкий	Низкий

Количественное измерение уровня риска основывается на байесовской вероятности наступления последствий и оценке возможного ущерба в денежном

эквиваленте. Количественная оценка выражается в вычислении вероятностного ущерба по формуле (2.23).

В качестве критериев количественной оценки рисков сценариев ЭкС в энергетике, вызванных реализацией киберугроз, предлагается использовать критерии кластеризации, описанные в формулах 2.24-2.26. Риски с наибольшим отклонением от нормы и наибольшей вероятностью требуют дальнейшей обработки рисков в первую очередь.

Этап 3. Ранжирование активов КИИ энергетических объектов. Наличие уязвимости при оценке риска позволяет определить список критических активов на предприятии с целью дальнейшего обоснования финансовых затрат на обеспечение безопасности. При наличии информации о кибернетической безопасности группы энергетических объектов, располагающихся на некоторой территории и находящихся во взаимозависимости, можно проранжировать их в соответствии с рисками нарушения кибербезопасности (2.29):

$$K = \{C, R, F\}, \tag{2.29}$$

где K – критерий значимости, C – критерий оценки рисков, R – интегральный показатель рисков объекта, F – объект, представленный совокупностью основных характеристик.

Предлагаемые методики поэтапно описывают обследование энергетического объекта на предмет выявления уязвимостей и киберугроз, формирования сценария гипотетической экстремальной ситуации на объекте и выявление рисков для их дальнейшей обработки. В качестве рекомендаций приводится перечень критических активов и наиболее вероятных для реализации угроз и уязвимостей, способных привести к значительному ущербу.

Итогом этого этапа в зависимости от уровня детализации исследования является проранжированый список объектов защиты, активов либо энергетических объектов.

Для поддержки методического подхода предлагается разработка интеллектуальной системы на основе принципов построения интеллектуальных систем [141], представленная в следующей главе.

Этап 4. Определение уровня киберситуационной осведомленности энергетического объекта. Выполнить подсчет отношения количества рассмотренных сценариев к количеству возможных сценариев в модели по формуле (2.19).

2.6 Выводы по главе

В главе представлены предлагаемый автором методический подход к анализу и оценке КСО, включающий модели структурирования знаний в области кибербезопасности и киберситуационной осведомленности энергетического объекта, вероятностную модель сценариев ЭкС в энергетике, вызванных киберугрозами, численный метод определения уровня КСО энергетического объекта и методики анализа киберситуационной осведомленности энергетического объекта. Отличием подхода от существующих является синтез исследований кибербезопасности и ситуационной осведомленности для анализа киберситуационной осведомленности энергетического объекта, отличающийся использованием семантического моделирования, технологии экспертных систем и методов визуализации. Приведены задачи, которые необходимо решить для анализа КСО ЭО (объединенные в три группы).

Подробно рассмотрена модель структурирования знаний кибербезопасности энергетической инфраструктуры, представленная с помощью фрактальной стратифицированной модели (ФС-модели) информационного пространства. Выделены слои методов (M), энергетической инфраструктуры (E), уязвимостей (V), угроз (T) и рисков (R), описаны отображения между слоями.

Рассмотрена система онтологий КСО ЭО, выполненная на основе онтологического инжиниринга предметной области с применением ФС-модели. Предложены компоненты интеллектуального программного комплекса для решения выделенных групп задач анализа КСО ЭО.

На основе теоретико-множественного подхода и теории графов описывается вероятностная модель сценариев ЭкС в энергетике, вызванных киберугрозами,

разработанная на основе моделей структурирования знаний и с использованием БСД. Модель основывается на декомпозиции компонентов киберсреды ЭО по сегментам ЛВС: гостевой, корпоративный, технологический. Предложен численный метод определения уровня КСО энергетического объекта с использованием вероятностной модели. Описывается методика определения уровня киберситуационной осведомленности энергетического объекта, включающая: 1) методику анализа киберугроз, 2) методику моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз и 3) методику оценки рисков последствий реализации угроз.

Глава 3. Разработка интеллектуального программного комплекса для анализа киберситуационной осведомленности (ИПК «ОКО»)

Аннотация главы

В главе описываются проектирование и реализация интеллектуального программного комплекса (ИПК) для анализа киберситуационной осведомленности энергетического объекта с применением экспертных систем, байесовских сетей доверия и методов визуализации рисков. Описаны проектирование архитектуры ИПК «ОКО», внутренней бизнес-логики его компонентов и алгоритмов работы компонентов. Приводятся интерфейсы пользователя. Представлена технология анализа киберситуационной осведомленности энергетического объекта и приведен пример применения предложенных технологии, методики и интеллектуального программного комплекса.

3.1 Проектирование ИПК «ОКО»

Проектирование интеллектуального программного комплекса основано на методике анализа угроз и оценки рисков (АУОР) нарушения информационно-технологической безопасности энергетических комплексов [106], переработанной для ЭО и дополненной аспектами киберситуационной осведомленности. ИПК разрабатывается для решения следующих групп задач:

- анализ киберугроз;
- моделирование сценариев;
- оценивание рисков и вывод рекомендаций.

Для реализации первой задачи предлагается спроектировать экспертную систему, в которой векторы атак (киберугроз) описываются в виде продукционных правил, в соответствии с которыми строится граф для определения вероятности наступления экстремальных ситуаций в энергетике.

Моделирование сценариев предлагается осуществлять с использованием компонента байесовских сетей, поддерживающего построение графа, установление вероятностных взаимосвязей между идентифицированными уязвимостями активов, угрозами, средствами контроля и последствиями, а также вывод на сети.

Для оценивания рисков предлагается компонент оценки рисков, который включает качественное и количественное оценивание рисков инцидентов кибербезопасности, приводящих к экстремальным ситуациям в энергетике. Группа задач ранжирования активов связана с определением критических активов на основе величины риска внутри объекта, а также определением объектов энергетики, наиболее подверженных рискам наступления экстремальных ситуаций за счёт реализации киберугроз.

Целью разработки является реализация методического подхода к анализу угроз и оценке рисков нарушения кибербезопасности энергетической инфраструктуры с учетом использования экспертных суждений в области возникновения экстремальных ситуаций в энергетике, вызванных реализацией киберугроз.

Для достижения этой цели ставятся следующие задачи:

1. Разработка экспертной системы построения векторов атак на энергетический объект ЭС «Cyber».
2. Разработка компонента «ThreatNet», поддерживающего моделирование киберугроз, способных вызвать экстремальные ситуации в энергетике, с помощью байесовских сетей доверия.
3. Разработка компонента «RiskMap» оценки рисков с применением методов семантического моделирования и методов визуализации данных.
4. Интеграция разработанных компонентов в единый интеллектуальный программный комплекс «ОКО» для поддержки исследований киберситуационной осведомленности энергетических объектов.

Определены основные задачи исследования и программные средства для их решения, представленные в онтологии задач и инструментальных средств на рисунке 3.1.

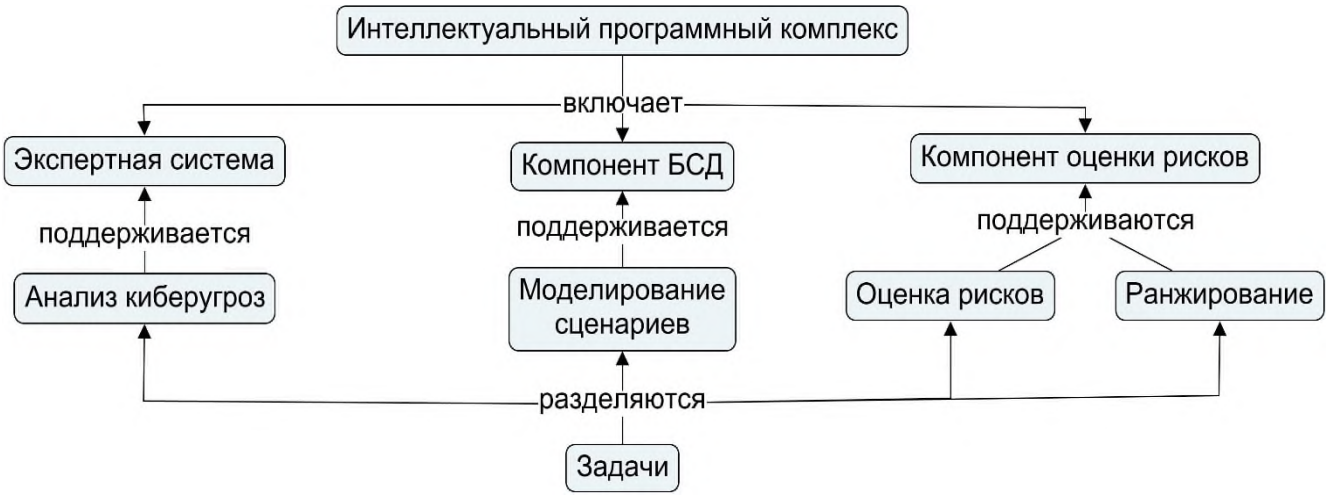

Рисунок 3.1 – Онтология задач и инструментальных средств анализа киберситуационной осведомленности энергетических объектов

При проектировании ИПК «ОКО» построена диаграмма классов (рисунок 3.2), отражающая основные понятия, отношения между ними и взаимодействия на основе объектно-ориентированного подхода.

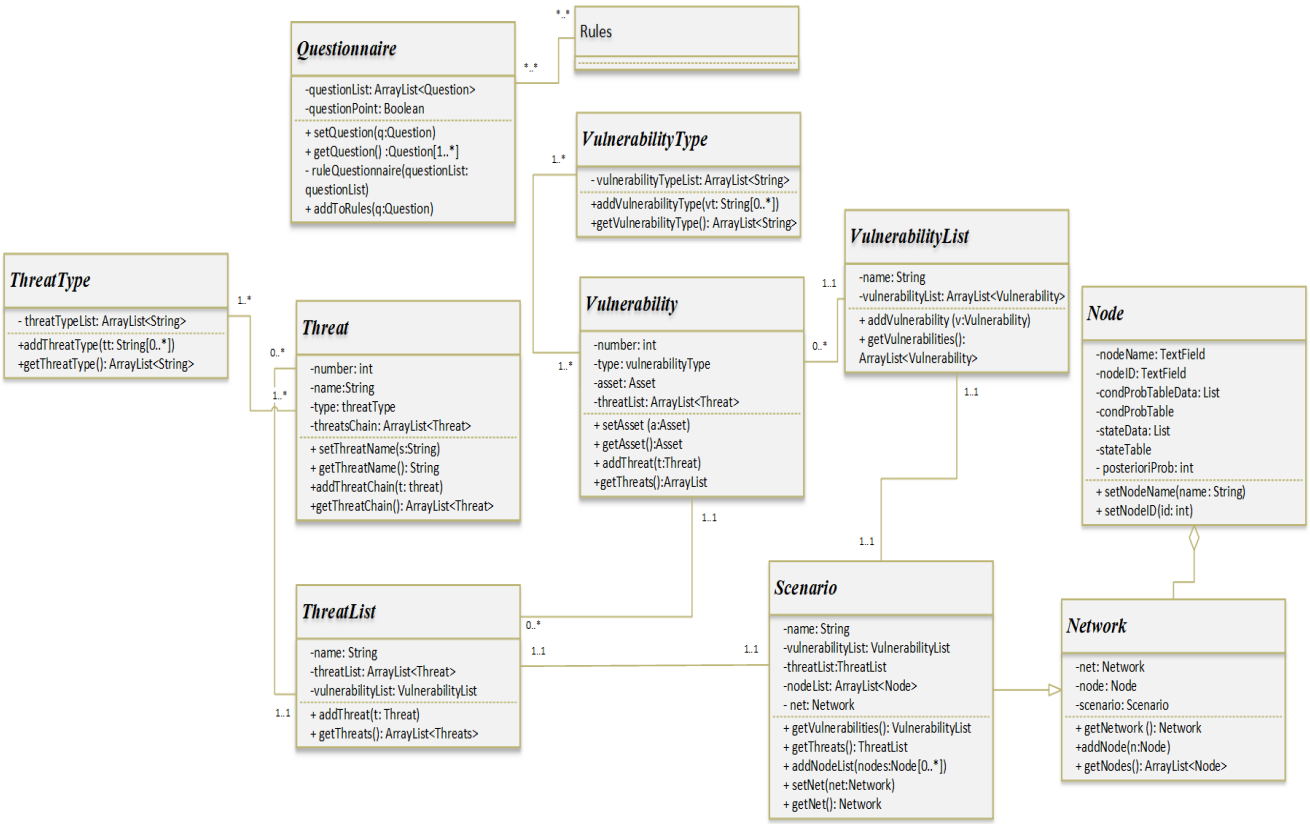

Рисунок 3.2 – Фрагмент диаграммы классов в нотации UML

Диаграмма является общей схемой для интеграции классов каждого блока разрабатываемой интеллектуальной системы.

3.1.1 Архитектура и функции интеллектуальной системы

С целью исследования возможных обстоятельств нарушения энергетической безопасности, вызванных реализацией киберугроз, разработан интеллектуальный программный комплекс для анализа киберситуационной осведомленности энергетических объектов [58]. Общая архитектура ИПК представлена на рисунке 3.3 (блоки, обведенные пунктиром), показана взаимосвязь пользователей и основных блоков ИПК «ОКО».

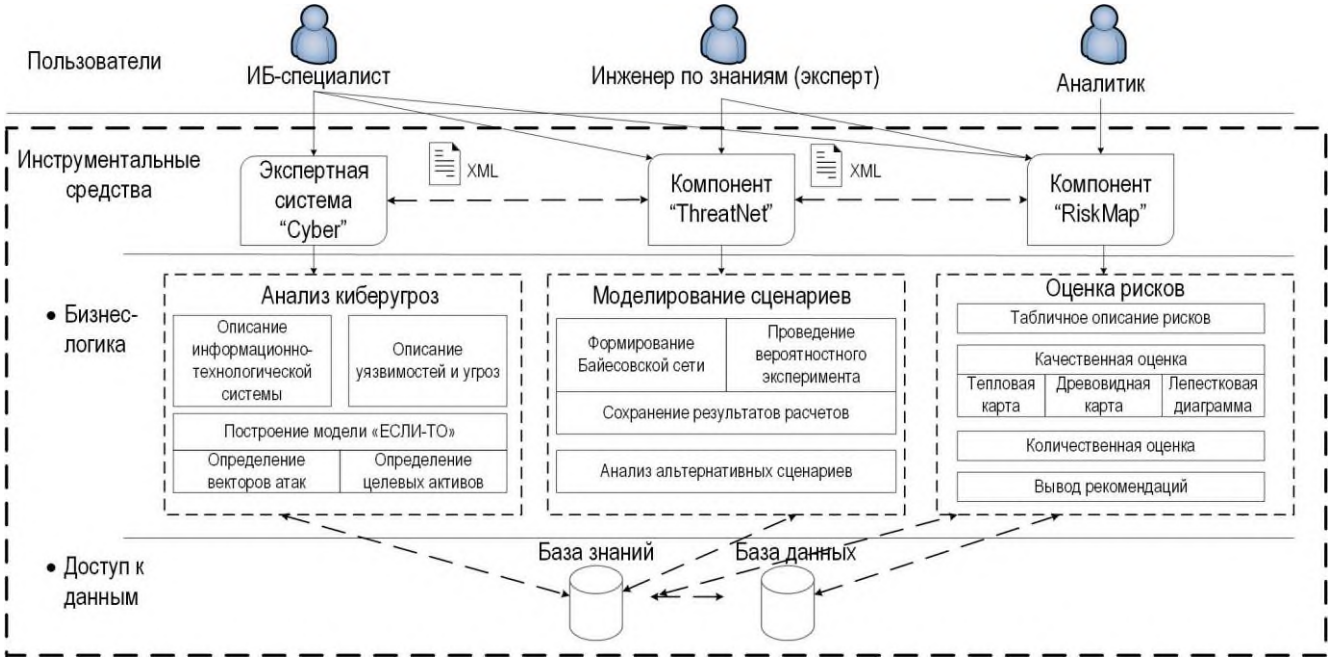

Рисунок 3.3 – Взаимосвязь пользователей и основных компонентов ИПК «ОКО» ЭО

ИПК включает:

- экспертную систему «Cyber» – продукционную ЭС, предназначенную для сопровождения аудита безопасности на энергетическом предприятии и выявления типовых уязвимостей, угроз и векторов атак КИИ объекта [142];
- компонент байесовских сетей доверия, предназначенный для моделирования экстремальной ситуации, вызванной нарушением кибербезопасности, и определения вероятности наступления последствий;

- компонент оценки рисков последствий от реализации киберугроз, включающий ранжирование активов и ЭО в соответствии с величиной риска и критериев ранжирования.

3.1.2 Экспертная система «Cyber» для анализа киберугроз

Основные компоненты экспертной системы и задачи, которые они решают, представлены на рисунке 3.4.

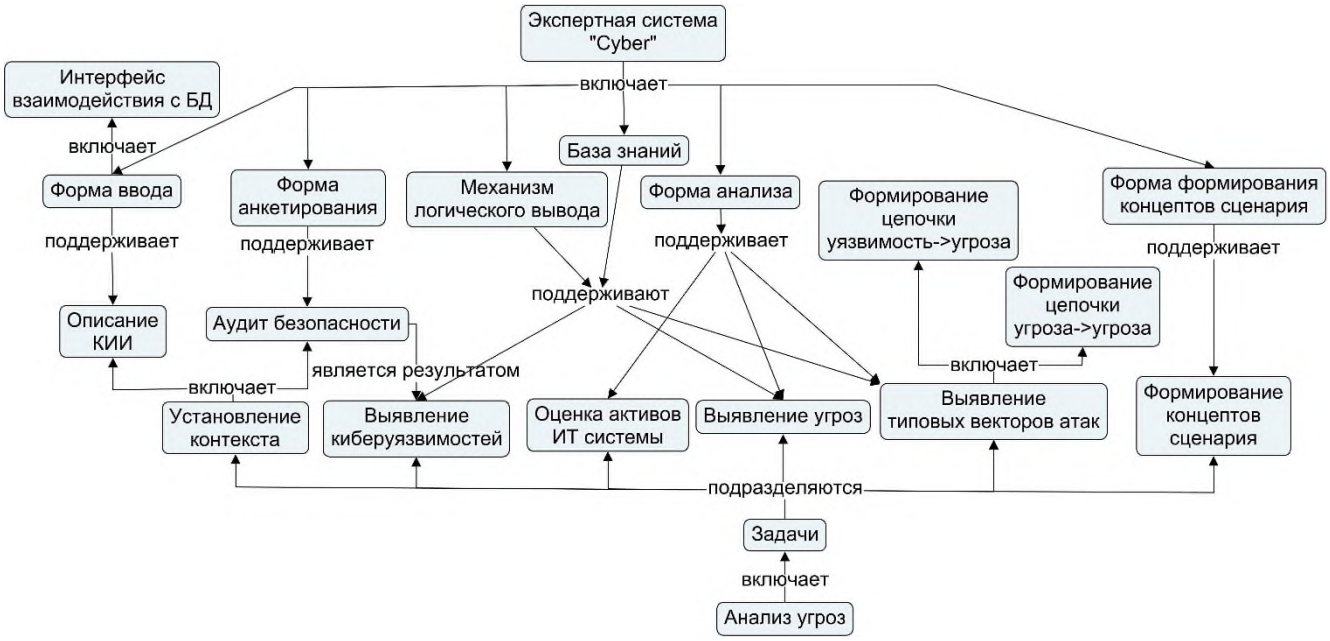

Рисунок 3.4 – Онтология основных компонентов ЭС «Cyber» и задачи, которые решаются с их использованием

Прототип экспертной системы «Cyber» реализован средствами объектно-ориентированного языка Java, а также процессора правил Drools. Основными классами прототипа ЭС «Cyber» являются:

Main – точка входа в приложение.

InputForm – класс описывает интерфейсы ввода данных (формы установления контекста) об энергетическом объекте, включая информационно-технологическую систему.

FactForm – класс описывает интерфейсы ввода фактов пользователя.

OutputListsForm – класс описывает интерфейс вывода списков угроз и уязвимостей, позволяет их редактировать и формировать в виде XML графовой модели для дальнейшей работы в компоненте «ThreatNet».

Asset – класс используется для описания активов информационно-технологической системы объекта, экземпляры которого представляют собой pojo и используются при продукционном выводе в качестве фактов.

Vulnerability – класс используется для описания уязвимостей активов.

VulnerabilityList – класс используется для формирования списка уязвимостей в рамках одной открытой сессии при продукционном выводе. Экземпляром класса является класс «Vulnerability».

Threat – класс используется для описания угроз безопасности.

ThreatList – класс используется для формирования списка угроз в рамках одной открытой сессии при продукционном выводе. Экземпляром класса является класс «Threat».

Rules.drl – класс используется в качестве базы знаний для выявления уязвимостей и угроз.

В рамках работы разработаны следующие ***компоненты*** ЭС «Cyber»:

База знаний прототипа ЭС «Cyber» включает три группы правил:

- правила сопоставления активов и уязвимостей, в соответствии с типом объекта ТЭК, составом активов КИИ и правил обеспечения безопасности, в результате выполнения которых создаются экземпляры класса «Уязвимость»;
- правила сопоставления уязвимостей и угроз, в результате выполнения которых создаются экземпляры классов «Угрозы» в соответствии с критерием значимости активов КИИ и выявленных уязвимостей;
- правила построения векторов атак, при выполнении которых осуществляется присваивание порядков в цепочке угроз на целевой актив в зависимости от его критичности и выявленных уязвимостей.

Для каждой группы разработан обобщенный шаблон в соответствии с синтаксисом процессора правил Drools [143].

Шаблон правил для сопоставления активов и уязвимостей:

rule CheckAsset

salience 100

when

asset : Asset(getParameter() = "Parameter")

questionnaire : Questionnaire(getAnswer() <Condition>)

vulnerabilityList : VulnerabilityList()

then

Vulnerability vulnerability = new Vulnerability (<ID>, <Parameters of Vulnerability>);

vulnerabilityList.addVulnerability(vulnerability);

insert(vulnerability);

end

В таблице 3.1 содержится описание концептов шаблона правила для сопоставления активов и уязвимостей.

Таблица 3.1 – Описание концептов шаблона правил для сопоставления активов и уязвимостей

Наименование	Описание
CheckAsset	Наименование правила
salience	Приоритет правила
asset, questionnaire, vulnerabilityList, vulnerability	Внутренние переменные правила типа классов Asset, Questionnaire, VulnerabilityList, Vulnerability
getParameter()	Метод получения переменной класса Asset
getAnswer()	Метод получения переменной класса Questionnaire
addVulnerability	Метод добавления переменной класса VulnerabilityList
Parameter	Параметр актива, удовлетворяющий условиям правила
<Condition>	Условие возникновения уязвимости в рассматриваемом активе
<ID><Parameters of Vulnerability>	Переменные экземпляра класса «Уязвимость»
insert(vulnerability)	Добавление факта в текущую сессию вывода правил в виде экземпляра класса «Уязвимость»

Шаблон правил сопоставления уязвимостей и угроз:

rule CheckThreat

salience 50

when

vulnerability : Vulnerability (getParameter() = "Parameter")

questionnaire : Questionnaire(getAnswer() <Condition>)

threatList : ThreatList()

then

Threat threat = new Threat (<ID>, <category>, <vulnerability><Parameters of threat>);

threatList.addThreat(threat);

insert(threat);

end

В таблице 3.2 содержится описание концептов шаблона правила для сопоставления уязвимостей и угроз.

Таблица 3.2 – Описание концептов шаблона правил для сопоставления уязвимостей и угроз

Наименование	Описание
CheckThreat	Наименование правила
salience	Приоритет правила
vulnerability, questionnaire, vulnerabilityList	Внутренние переменные правила типа классов Vulnerability, Questionnaire, VulnerabilityList
getParameter()	Метод получения переменной класса Vulnerability
getAnswer()	Метод получения переменной класса Questionnaire
addThreat	Метод добавления переменной класса Threat
Parameter	Параметр уязвимости, удовлетворяющий условиям правила
<Condition>	Условие использование рассматриваемой уязвимости угрозой
<ID><category><Parameters of Vulnerability>	Переменные экземпляра класса «Угроза». Переменная «category» имеет значение «primary»

Наименование	Описание
insert(threat)	Добавление факта в текущую сессию вывода правил в виде экземпляра класса «Угроза»

Шаблон правил построения векторов атак:

rule CheckVector

salience 30

when

vulnerability : Vulnerability (getParameter() = "Parameter")

threat : Threat(getParameter() = "Parameter")

questionnaire : Questionnaire(getAnswer() <Condition>)

threatList : ThreatList()

then

Threat threat = new Threat (<ID>, <category>, <threat><Parameters of threat>);

threatList.addThreat(threat);

insert(threat);

end

В таблице 3.3 содержится описание концептов шаблона правила для формирования вектора атаки.

Таблица 3.3 – Описание концептов шаблона правил для сопоставления уязвимостей и угроз

Наименование	Описание
CheckVector	Наименование правила
salience	Приоритет правила
vulnerability, threat questionnaire, threatList	Внутренние переменные правила типа классов Vulnerability, Threat, Questionnaire, VulnerabilityList
getParameter()	Метод получения переменной классов Vulnerability, Threat
getAnswer()	Метод получения переменной класса Questionnaire
addThreat	Метод добавления переменной класса Threat
Parameter	Параметр уязвимости/ угрозы удовлетворяющий условиям правила
<Condition>	Условие использование рассматриваемой уязвимости угрозой

Наименование	Описание
<ID>, <category>, <threat><Parameters of threat>	Переменные экземпляра класса «Угроза». Переменная «category» имеет значение «secondary»
insert(threat)	Добавление факта в текущую сессию вывода правил в виде экземпляра класса «Угроза»

Алгоритм построения дерева уязвимостей и угроз представлен на рисунке 3.5. Подготовительным этапом является внесение в базу данных параметров и характеристик, описывающих энергетический объект. К таким параметрам относятся тип объекта, класс защищенности, а также параметры подсистем технологической системы.

1. Факты о параметрах энергетического объекта вносятся в базу знаний.
2. Запускается форма ввода фактов касающихся существующего обеспечения безопасности активов корпоративной информационной системы, локальной вычислительной сети, автоматизированной системы управления технологическим процессом и используемых средств защиты на активах.
3. При удовлетворении фактов об активах для продукционных правил с приоритетом «pr 1», создается экземпляр класса «Уязвимость» с привязкой к активу, о котором сформирован факт.
4. Далее осуществляется продукционный вывод на правилах с приоритетом «pr 2». Если в базе существуют правила относительно наличия типа уязвимости в рассматриваемом типе актива, то создается экземпляр класса «Угроза». При этом указывается, что данная угроза является инициализирующей (первичной).
5. Пункты 3-4 повторяются, пока для факта о типе уязвимости находятся необработанные правила с приоритетом «pr 2».
6. Пункт 5 повторяется, пока для факта об активе находятся необработанные правила с приоритетом «pr 1».

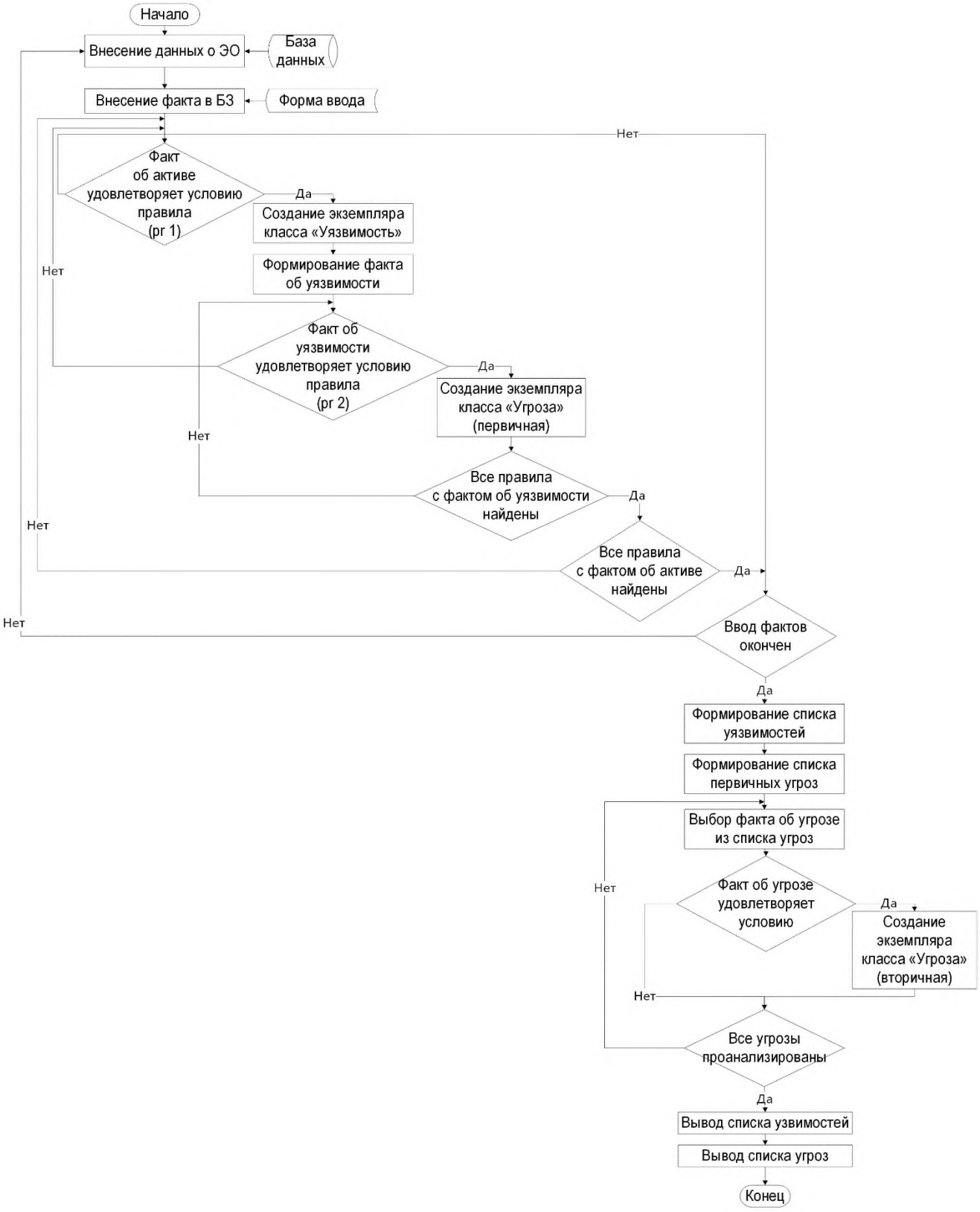

Рисунок 3.5 – Алгоритм построения дерева уязвимостей и угроз

7. Пункты 2-6 повторяются, пока в базу знаний не попадут все факты об информационно-технологической системе.
8. Далее формируется список уязвимостей и список угроз (первичных).

9. Информация о инициализирующей (первичной) угрозе формируется в виде факта и передается в базу знаний.
10. При удовлетворении факта о угрозе (первичной) для правил с приоритетом «pr 3» создаются экземпляры класса «Угроза». При этом указывается, что данная угроза является вторичной.
11. Пункт 10 повторяется, пока находятся правила, условия которых удовлетворяют факту о угрозе (первичной).
12. Пункты 10-11 повторяются, пока все угрозы из списка угроз (первичных) не будут обработаны.
13. Выводится список уязвимостей и список угроз.

Для работы со списком уязвимостей и угроз для формирования XML узлов байесовской сети доверия разработан алгоритм формирования узлов, представленный на рисунке 3.6.

1. Формируется список уязвимостей, выявленных при выводе фактов, проанализированного и исправленного пользователем с ролью «Инженер по безопасности».
2. Создается XML-файл и открывается для редактирования.
3. Пока в списке есть необработанные уязвимости, для каждой уязвимости из списка создается и заполняется блок тэгов, описывающих узел байесовской сети доверия, в соответствии со структурой XML-файла, представленного ниже.
4. Список угроз сортируется по полю «category»: в начале списка первичные угрозы, значение поля которых равно «primary»; в конце – «secondary».
5. Для угрозы из списка создается и заполняется блок тэгов, описывающих узел байесовской сети доверия, в соответствии со структурой XML-файла.
6. Если поле «category» рассматриваемой угрозы соответствует «primary», то в тэг «Parents» записывается ID уязвимости из соответствующего поля.
7. Если поле «category» рассматриваемой угрозы соответствует «secondary», то в тэг «Parents» записывается ID угрозы из соответствующего поля.
8. Пункты 5-7 повторяются, пока в списке угроз есть необработанные угрозы.
9. XML-файл сохраняется и закрывается.

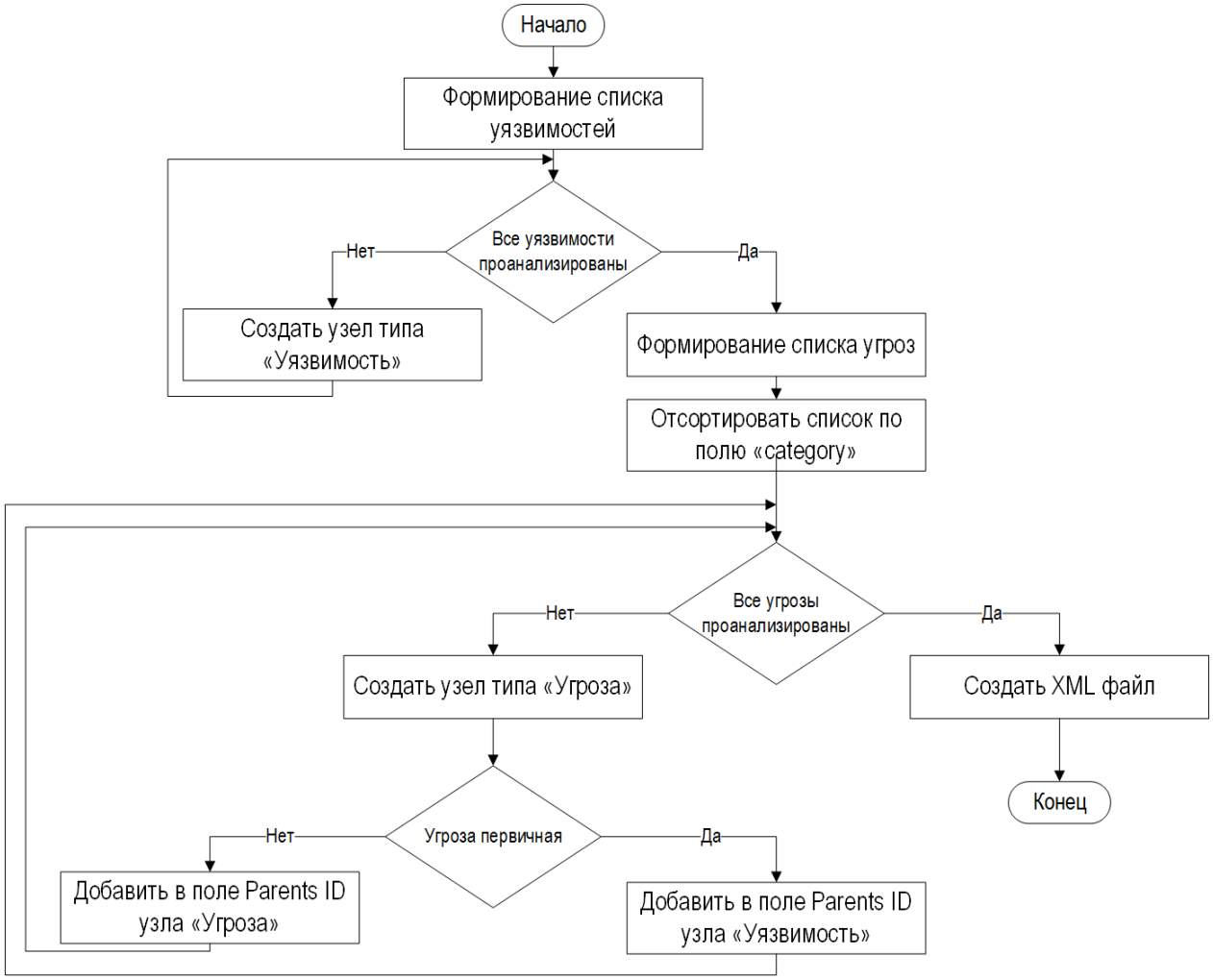

Рисунок 3.6 – Алгоритм формирования узлов в XML файл

Интерфейс прототипа ЭС «Cyber» представлен на рисунке 3.7.

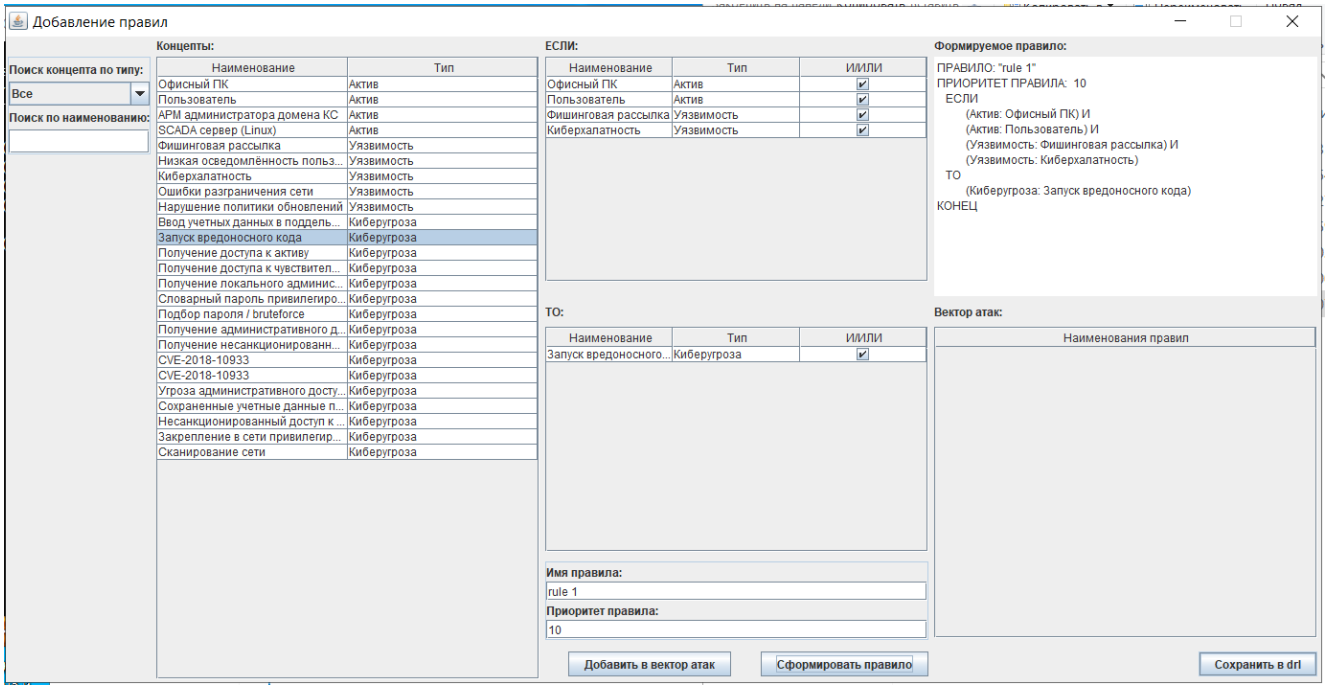

Рисунок 3.7 – Интерфейс прототипа ЭС «Cyber»

3.1.3 Компонент Байесовских сетей доверия «ThreatNet» для вероятностного моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз

Основные компоненты и решаемые задачи представлены на рисунке 3.8.

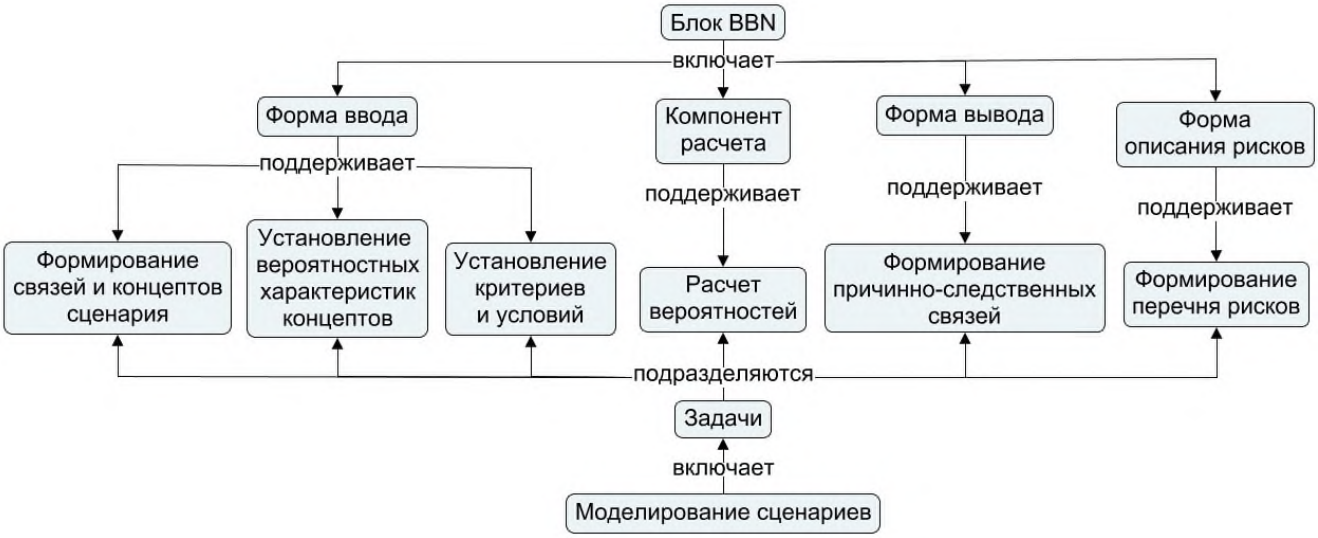

Рисунок 3.8 – Онтология основных компонентов блока «ThreatNet» и задачи, которые решаются с их применением

Прототип компонента «ThreatNet» реализован средствами объектно-ориентированного языка Java. В настоящее время основными классами прототипа являются:

Main – точка входа в приложение.

BayNet – класс интерфейсной формы для работы с БСД с применением библиотеки «Smile».

Node – класс, основных характеристик узла БСД.

Интерфейс прототипа компонента БСД «TreatNet» представлен на рисунке 3.9. На панели каждого узла доступны кнопки для создания и удаления этого узла и создания узла потомка, а также установления связи. Таблица условных вероятностей отображается внизу экрана в табличной форме.

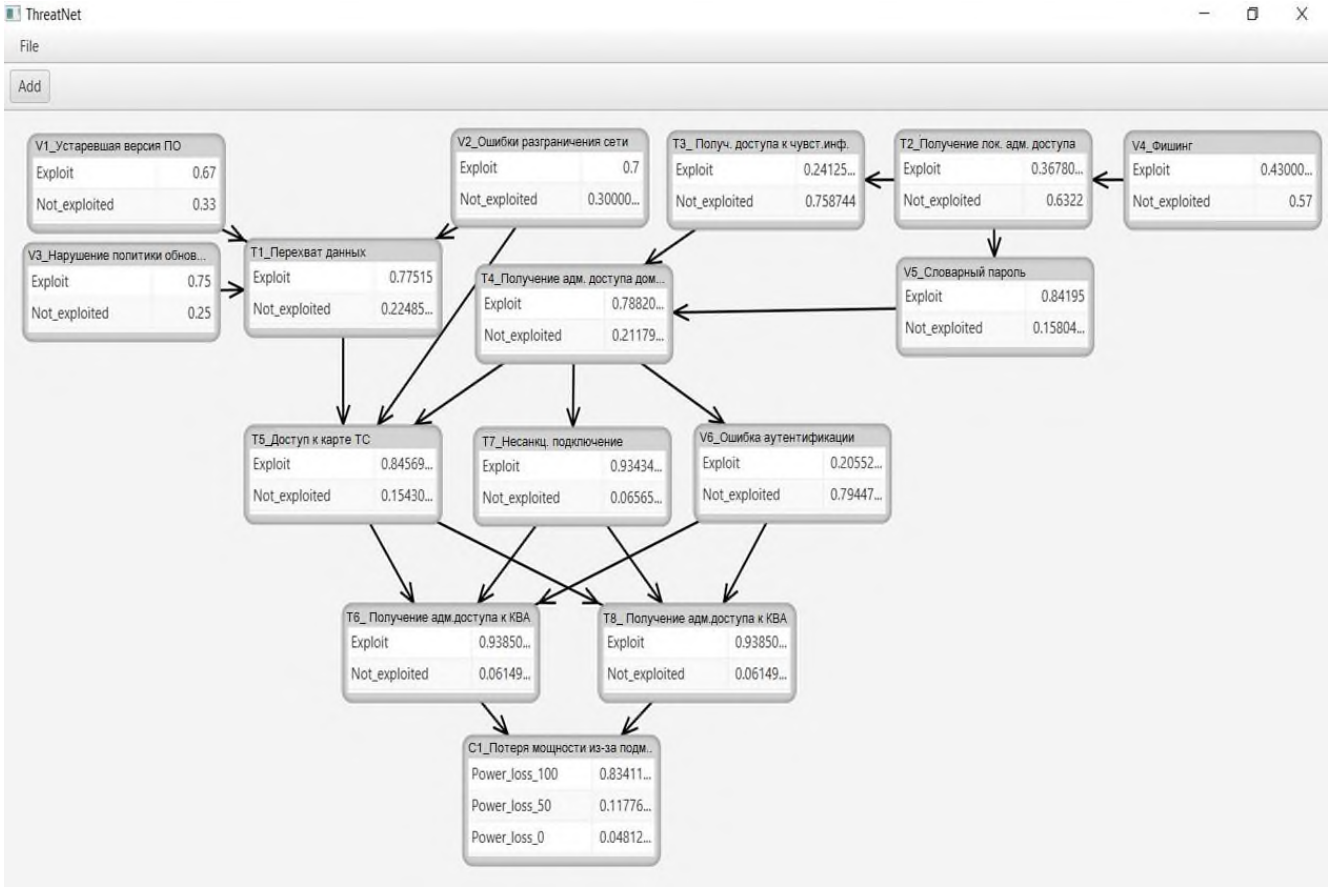

Рисунок 3.9 – Интерфейс прототипа «ThreatNet»

3.1.4 Компонент «RiskMap» для оценки рисков нарушения кибербезопасности энергетических объектов

Основные компоненты и решаемые задачи представлены на рисунке 3.10.

Прототип компонента «RiskMap» реализован средствами объектно-ориентированного языка Java. Основными классами прототипа «RiskMap» являются:

Main – точка входа в приложение.

TabelStage – класс используется для табличного представления рисков.

HeatMap – класс используется для отображения количества рисков в зависимости от их качественного оценивания на тепловой карте.

RadarChart – класс используется для отображения количества рисков по типам на лепестковой диаграмме.

Asset – класс используется для описания активов информационно-технологической системы объекта, экземпляры которого представляются пользователю в табличном виде.

VulnerabilityList – класс используется для формирования списка уязвимостей в рамках одной открытой сессии при продукционном выводе.

ThreatList – класс используется для формирования списка угроз в рамках одной открытой сессии при продукционном выводе.

Risk – класс используется для описания рисков.

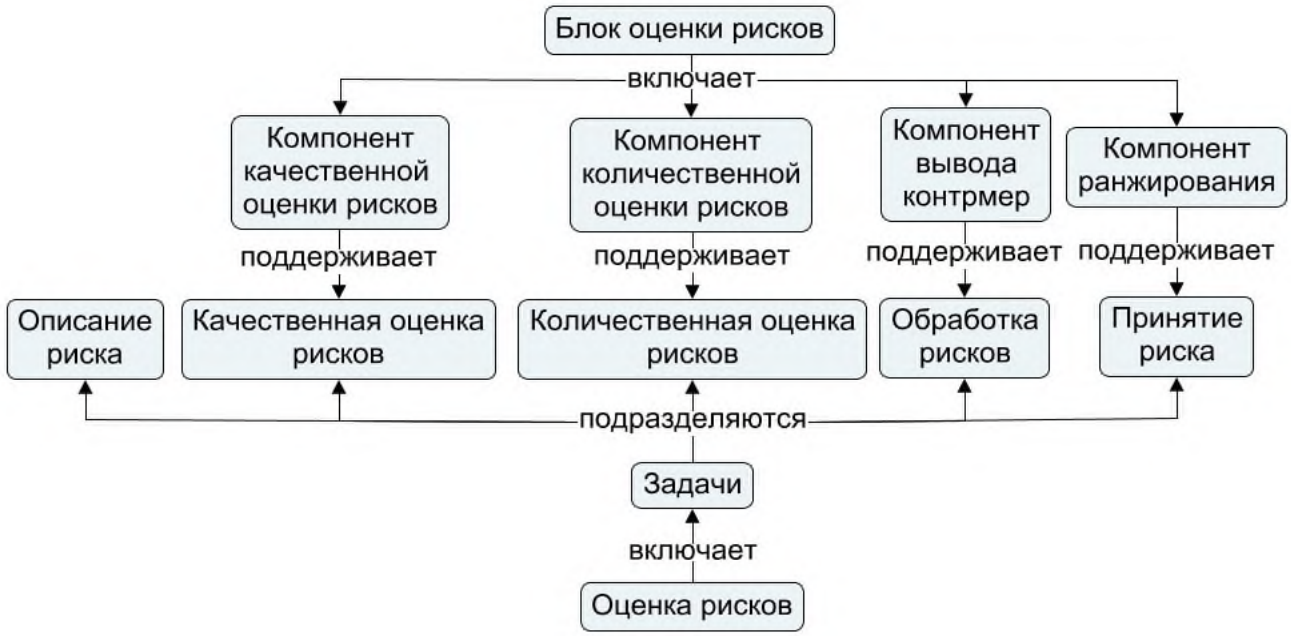

Рисунок 3.10 – Онтология основных компонентов блока «RiskMap» и задачи, которые решаются с их применением

Интерфейс прототипа компонента оценки рисков «RiskMap» представлен на рисунке 3.11. Прототип «RiskMap» предназначен для визуализации рисков на тепловой карте и лепестковой диаграмме. Данный прототип используется для оценивания удобства представления данных при качественной оценке рисков нарушения кибербезопасности в энергетике на примере одного вида структуры сценария. Прототип поддерживает функции отображения на тепловой карте количества и наименований рисков по трем категориям: слабый (обозначен зеленым цветом), средний (желтый цвет), критический (красный цвет) – по каждому из заданных типов рисков. Продемонстрирована возможность

отображения рисков по типам рисков с помощью лепестковой диаграммы. Описание риска предлагается выполнять в табличном виде.

Рисунок 3.11 – Интерфейс прототипа компонента «RiskMap»

3.2 Технология применения ИПК «ОКО» для анализа киберситуационной осведомленности энергетического объекта

Для решения задачи анализа киберситуационной осведомленности энергетического объекта разработана технология, которая реализует алгоритм применения предлагаемых методик с использованием разработанного интеллектуального программного комплекса.

Интеграция этапов технологии, методик и компонентов интеллектуального программного комплекса представлена в таблице 3.4.

Таблица 3.4 – Этапы технологии, методики и инструментальные средства

Этапы	**Группы пользователей**	**Методики**	**Инструментальные средства**
Анализ киберугроз	Инженер по безопасности	Методика анализа киберугроз энергетической инфраструктуры	Экспертная система ЭС «Cyber»
Моделирование сценариев	Инженер по безопасности КИИ; Инженер по знаниям (эксперт в области энергетической безопасности)	Методика моделирования сценариев экстремальных ситуаций в энергетике	Компонент байесовских сетей доверия «ThreatNet»
Оценивание рисков	Инженер по знаниям (эксперт в области ЭБ); Аналитик	Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры	Компонент оценки рисков «RiskMap»

Предлагаемая технология рассчитана на следующие группы пользователей:

- инженер по безопасности, т.е. специалист в области информационной безопасности предприятия, либо, при отсутствии такового, администратор локальной вычислительной сети;
- инженер по знаниям в энергетике (эксперт): в зависимости от уровня детализации исследования в его роли может быть как эксперт в области энергетической безопасности, так и оператор / инженер энергетик на объекте; в области безопасности: инженер по безопасности;
- аналитик, в качестве которого может выступать инженер по знаниям [144].

На определенных в таблице 3.4 этапах подразумевается коллективная работа специалистов в областях кибербезопасности КИИ и экспертов-энергетиков.

Дальнейшие действия лиц, принимающих решения по обработке риска, в работе не рассматриваются. В основе технологии лежит цикл Шухарта-Деминга

(PDCA), который подходит для периодической проверки безопасности, необходимой для проведения в соответствии с приказом ФСТЭК от 14 марта 2014 года № 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 природной среды» [39]. Технология в общем виде в нотации BPNM 2.0 для каждой роли пользователей представлена на рисунке 3.12 [145].

Результатом 1 этапа технологии является описание активов КИИ, критических уязвимостей, а также перечень киберугроз энергетического объекта, а также описание векторов атак для конкретного объекта энергетики.

В результате выполнения 2-го этапа технологии сформирован сценарий экстремальной ситуации на объекте энергетики, вызванной реализацией киберугроз, проведено рассуждение на сети, определены вероятности наступления последствий.

Результат взаимодействия пользователя с компонентом оценки рисков возникновения экстремальных ситуаций в энергетике, вызванных реализацией киберугроз, может быть использован при планировании технологических режимов работы энергетических объектов в условиях экстремальных ситуаций, при совершенствовании используемого программно-технического комплекса эксплуатируемых автоматизированных систем управления, разработке и внедрении новых моделей и алгоритмов задач автоматизированного управления, при подготовке методических материалов, планов и программ проведения тренировок, деловых игр персонала.

Поскольку результат работы с блоком представляет собой перечень рисков наступления экстремальных ситуаций на объектах, такая информация, например, в области электроэнергетики, может быть полезна энергосбытовым компаниям, обеспечивающим контроль соблюдения условий минимизации хозяйственного риска, в том числе, и в случае экстремальных ситуаций.

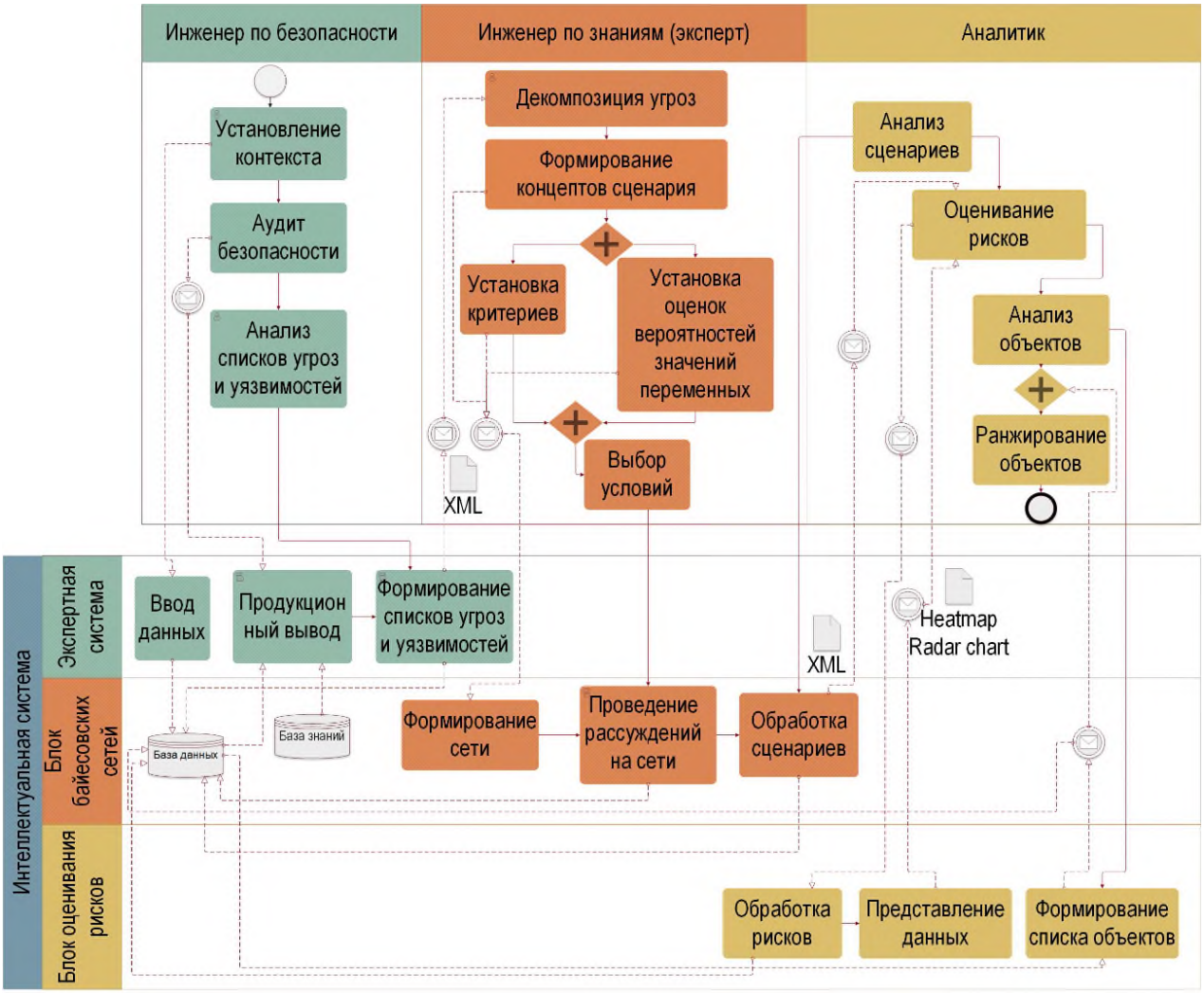

Рисунок 3.12 – Технология анализа киберситуационной осведомленности энергетического объекта в нотации BPMN 2.0

Технология применения ИПК «ОКО» объединяет экспертов различных предметных областей и позволяет выполнить гибридную оценку рисков киберугроз энергетических объектов.

Предложенная технология в сравнении с традиционными подходами к обеспечению безопасности направлена на определение уязвимостей и киберугроз, реализация которых может вызвать нарушение функционирования энергетического объекта в такой мере, что можно расценивать инцидент как экстремальную ситуацию в энергетике, позволяя проводить вероятностную оценку экстремальных ситуаций в энергетике, вызванных киберугрозами. Такая оценка

традиционно рассматривается при проектировании, внедрении и эксплуатации сложных технологических объектов.

3.3 Применение предложенных методики, модели и технологии анализа киберситуационной осведомленности энергетического объекта

В процессе цифровой трансформации энергетики предприятия можно условно разделить на три группы: 1) ещё не вышедшие на уровень применения передовых информационных технологий; 2) уже начавшие использовать цифровые технологии, но не осознающие их опасность; 3) применяющие цифровые технологии и предпринявшие меры безопасности, согласно стандартам и основополагающим документам, а также существующим практикам. Наиболее уязвимыми являются предприятия второй группы, одно из которых далее представлен в примере.

Технология. Этап 1. Анализ киберугроз.

1.1. Описание энергетического объекта.

Рассмотрим абстрактную теплоэлектростанцию (ТЭС), содержащую два генерирующих энергоблока. Описание типовых компонентов теплоэлектростанции представлено в [130]. Перечень функциональных подсистем АСУ ТП рассматриваемого объекта представлен в таблице 3.5.

Таблица 3.5 – Обобщенный перечень функциональных подсистем АСУ ТП типового объекта теплоэлектрогенерации*

№	Теплотехническая часть (ТЧ)	Электротехническая часть (ЭЧ)	Информационно-измерительная часть (ИИЧ)
1	Химическая водоочистка (ХВО)	Диспетчеризация и управление (СДУ)	Коммерческий /технический учет электроэнергии (АИИС КУЭ и АСТУЭ)
2	Топливоподготовка и топливоподача	Релейная защита и автоматика (РЗА)	Регистрация аварийных событий (РАС)

№	Теплотехническая часть (ТЧ)	Электротехническая часть (ЭЧ)	Информационно-измерительная часть (ИИЧ)
3	Управление котлоагрегатами	Управление электротехническим оборудованием	Обмен технологической информацией с Автоматизированной системой Системного оператора (СОТИ АССО)
4	Управление турбоагрегатами		
5	Вибродиагностика и измерение механических величин		

* Материал основан на источнике [130].

Топология сети рассматриваемого объекта представлена на рисунке 3.13.

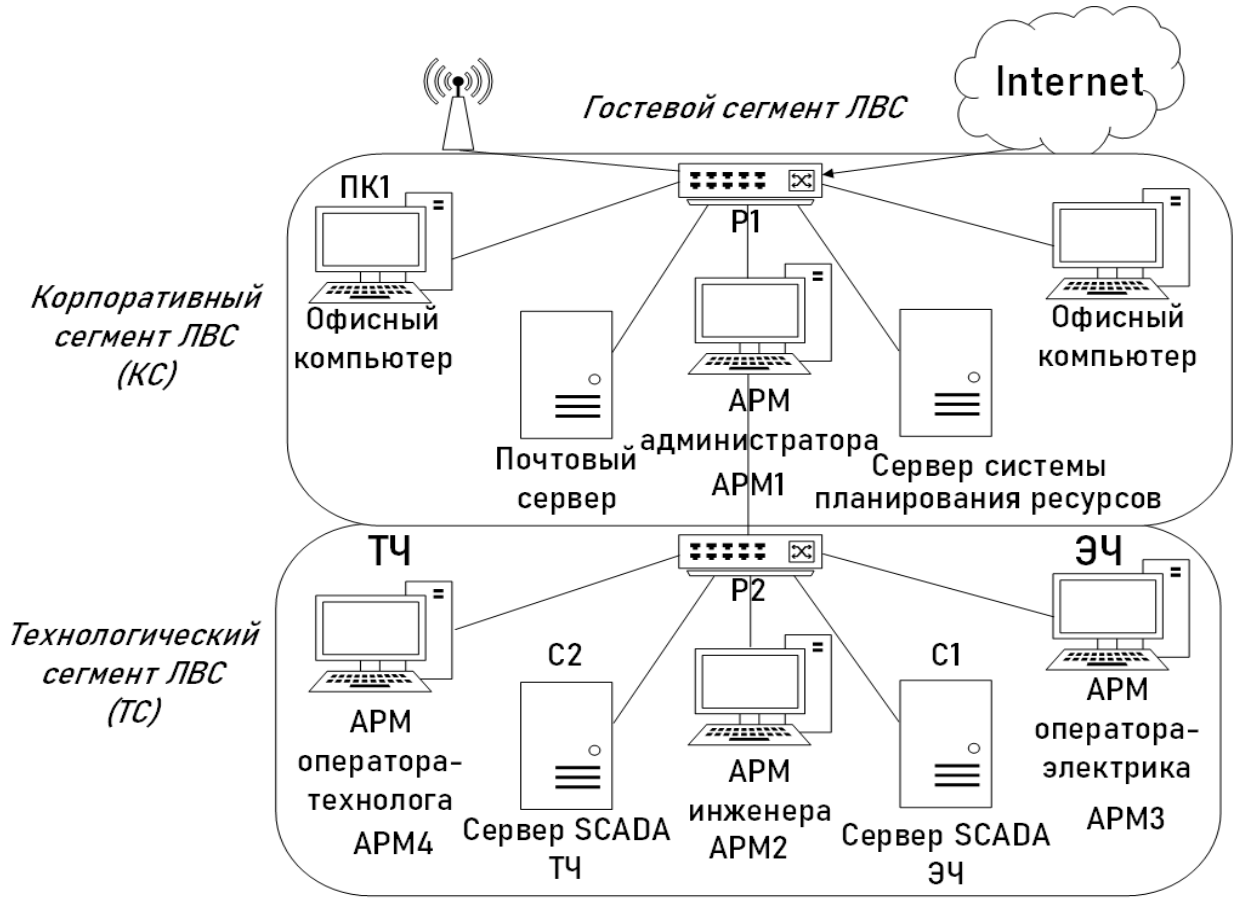

Рисунок 3.13 – Топология ЛВС рассматриваемого примера ТЭС

ЛВС имеет разделение на корпоративный и технологический сегменты, но отсутствует демилитаризованная зона, а автоматизированное рабочее место (АРМ) администратора подключено к двум вышеперечисленным сегментам. Роутеры Р1 и Р2 содержат уязвимость операционной системы (ОС) «устаревшее ПО». ЛВС рассматриваемого объекта разделена на логическом уровне на три сегмента: гостевой сегмент, корпоративный сегмент (КС) и технологический сегмент. Роутер Р1 осуществляет сегментацию ЛВС на гостевую и корпоративную подсети. Роутер Р2 осуществляет сегментацию на корпоративную и технологическую подсети. КС включает офисные компьютеры и АРМ администратора (АРМ1). ТС включает два сервера SCADA (С1, С2), АРМ инженера, а также АРМ оператора-технолога и АРМ оператора-электрика.

1.2. Анализ уязвимостей и угроз критической информационной инфраструктуры. По результатам анализа в таблице 3.6 представлено описание активов, уязвимостей и угроз рассматриваемого объекта.

Таблица 3.6 – Перечень активов, уязвимостей и киберугроз

Обозначение	Технические средства	ПО	Тип уязвимости	Угрозы
Р1	Wi-Fi роутер	ОС роутера	Устаревшая версия ПО, позволяющая получить контроль доступа	Получение административного доступа
				Запуск вредоносного ПО
				Перехват данных (анализ сетевого трафика)
ПК1	Офисный компьютер	Почтовый клиент	Некорректно настроенный СПАМ фильтр	Фишинговая рассылка
				Киберхалатность
		ОС	Некорректно настроенный антивирус	Запуск вредоносного ПО
				Получение локального административного доступа

Обозначение	Технические средства	ПО	Тип уязвимости	Угрозы
Р2	Роутер КС и ТС	ОС роутера	Устаревшая версия ПО, позволяющая получить контроль доступа	Получение административного доступа
				Запуск вредоносного ПО
				Перехват данных (анализ сетевого трафика)
АРМ 1	АРМ администратора КС	ОС	Избыточные права и привилегии, недостаточный контроль доступа	Получение административного доступа к КС
			Некорректный контроль доступа	
АРМ 2	АРМ инженера	ОС		Получение локального административного доступа
		SCADA/HMI (клиент)	Стандартный/словарный пароль привилегированных пользователей	Получение административного доступа к КВА
		Удаленный рабочий стол	Сохраненная сессия	
АРМ 3	АРМ оператора (ЭЧ)	SCADA/HMI (клиент)	Стандартный/словарный пароль привилегированных пользователей	Получение административного доступа к КВА
АРМ 4	АРМ технолога (ТЧ)	SCADA/HMI (клиент)	Стандартный/словарный пароль привилегированных пользователей	Получение административного доступа к КВА
С1	Сервер SCADA (ЭЧ)	ОС сервера	Устаревшее ПО	Нарушение политики обновлений
				Нарушение основных бизнес-процессов ЭО

Обозначение	Технические средства	ПО	Тип уязвимости	Угрозы
С2	Сервер SCADA (ТЧ)	ОС сервера	Устаревшее ПО	Нарушение политики обновлений
				Нарушение основных бизнес-процессов ЭО

1.3. Построение модели нарушения кибербезопасности. Составим описание модели нарушения кибербезопасности рассматриваемой ТЭС в соответствии с типовой схемой атаки на технологический сегмент ЛВС [32]. Типовая схема такой атаки содержит три основных этапа:

1. Проникновение в КИС.

2. Проникновение из КИС в ТС.

3. Атака на целевой актив.

Рассмотрим два вектора атаки. Целевыми активами рассматриваемых векторов являются сервера SCADA ТЧ и ЭЧ.

Вектор атаки через гостевой Wi-Fi. ЛВС включает ошибку разграничения на гостевой и корпоративный сегменты, а также на корпоративный и технологический сегменты ЛВС, т.е. физически сеть одна, а разграничение осуществлено только на логическом уровне, причем некорректно настроен файервол. Роутер Р1 осуществляет сегментацию сети на гостевую и корпоративную и использует устаревшее ПО, позволяющее получить административный доступ к активу. Используя вредоносное ПО, злоумышленник может осуществить перехват данных с анализом сетевого трафика и получить доступ к карте сети корпоративного сегмента. Поскольку роутер Р2 осуществляет сегментацию сети на корпоративный и технологический сегменты и также использует устаревшую версию ПО, становится возможным осуществить подобные действия для него и осуществить анализ сетевого трафика в технологическом сегменте сети. Получив доступ к карте технологического сегмента сети, становится возможным получить чувствительную информацию о

целевом активе (IP, DNS). Поскольку целевой актив использует устаревшее ПО, становится возможным получение административного доступа к нему как к критическому активу, используя известную уязвимость. Далее в примере рассмотрены две атаки на целевой актив, которые можно провести в рамках двух рассматриваемых векторов.

Вектор атаки через фишинговую рассылку. Применение социальной инженерии и получение доступа к ПК1, находящемуся в КИС, путем фишинговой рассылки на почтовый клиент и применения вредоносного ПО. Далее закрепление в КИС, получение доступа локального администратора на ПК1 и повышение привилегий путем получения доступа администратора домена КИС. Поскольку в рассматриваемом примере отсутствует демилитаризованная зона (ДМЗ), то такой доступ позволяет осуществить поиск узлов сегмента ТС. Используя уязвимую версию ОС АРМ инженера, осуществляется закрепление в ТС, а использование сохраненных сессий удаленного подключения позволяет получить доступ к целевому активу.

В качестве атак на целевой актив рассмотрены два варианта: 1) удаление или шифрование данных серверов SCADA; 2) отправка деструктивных управляющих команд на энергоблок. Далее в таблице 3.7 представлены примеры правил в соответствии с предложенной структурой сценария «ЕСЛИ-ТО».

Таблица 3.7 – Сценарий ЕСЛИ-ТО**

Опера-тор	**Тип концепта /оператор**	**Наименование**	**Опера-тор**	**Тип концепта /оператор**	**Наименование**
I. Вектор атаки через гостевой WI-FI					
Вектор проникновения 1. Через гостевой WI-FI					
ЕСЛИ	А	Wi-Fi роутер	**ТО**	А	Wi-Fi роутер
	О	**И**		О	**И**
	У	Устаревшая версия ПО, позволяющая получить контроль доступа		К	Получение административного доступа
				О	**И**
				К	Установка вредоносного ПО

Опера-тор	Тип концепта /оператор	Наименование	Опера-тор	Тип концепта /оператор	Наименование
ЕСЛИ			**ТО**	О	**И**
				К	Перехват данных (анализ сетевого трафика)
				О	**И**
				К	Несанкционированный доступ к карте сети сегмента КС
ЕСЛИ	А	Wi-Fi роутер	**ТО**	А	Роутер КС и ТС
	О	**И**		О	**И**
	К	Получение административного доступа		К	Получение административного доступа
	О	**И**		О	**И**
	К	Несанкционированный доступ к карте сети КС		К	Установка вредоносного ПО
	О	**И**		О	**И**
	А	Роутер КС и ТС		К	Перехват данных (анализ сетевого трафика)
	О	**И**			
	У	Устаревшая версия ПО, позволяющая получить контроль доступа			
ЕСЛИ	А	Роутер КС и ТС	**ТО**	А	Роутер КС И ТС
	О	**И**		О	**И**
	К	Получение административного доступа		К	Получение административного доступа
	О	**И**		О	**И**
	А	Роутер КС и ТС		К	Установка вредоносного ПО
	О	**И**		О	**И**
	У	Устаревшая версия ПО, позволяющая получить контроль доступа		К	Перехват данных (анализ сетевого трафика)
				О	**И**
				К	Несанкционированный доступ к карте сети сегмента ТС

Оператор	Тип концепта /оператор	Наименование	Оператор	Тип концепта /оператор	Наименование
ЕСЛИ	А	Роутер КС и ТС	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	К	Получение административного доступа		К	Получение доступа к чувствительной информации
	О	**И**			
	К	Перехват данных (анализ сетевого трафика)			
	О	**И**			
	К	Несанкционированный доступ к карте сети сегмента ТС			
Вектор развития атаки в ТС 1. Использование устаревших версий ПО					
ЕСЛИ	А	SCADA сервер	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	У	Нарушение политики обновлений		К	Получение административного доступа к КВА
	О	**И**			
	У	Устаревшая версия ПО, позволяющая получить контроль			
	О	**И**			
	У	Ошибки разграничения сети			
Атака на целевой актив 1. Шифрование данных с управляющего сервера					
Атака на целевой актив 2. Подмена управляющих команд					
II. Вектор атаки через фишинговую рассылку					
Вектор проникновения 2. Через фишинговую рассылку					
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	А	Почтовый клиент		К	Фишинговая рассылка
	О	**И**			
	У	Некорректно настроенный СПАМ фильтр			
ЕСЛИ	А	Пользователь офисного ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	У	Низкая осведомлённость пользователя в вопросах ИБ		К	Киберхалатность

Оператор	Тип концепта /оператор	Наименование	Оператор	Тип концепта /оператор	Наименование
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	К	Киберхалатность		К	Ввод учетных данных в поддельную форму аутентификации
	О	**И**		О	**ИЛИ**
	К	Фишинговая рассылка		К	Запуск вредоносного ПО
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	К	Ввод учетных данных в поддельную форму аутентификации		К	Получение доступа к активу
	О	**ИЛИ**			
	К	Запуск вредоносного ПО			
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	К	Получение доступа к активу		К	Получение доступа к чувствительной информации
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	К	Получение доступа к активу		К	Получение локального административного доступа к активу
	О	**И**			
	К	Получение доступа к чувствительной информации			
ЕСЛИ	А	Офисный ПК	**ТО**	А	Офисный ПК
	О	**И**		О	**И**
	К	Получение локального административного доступа к активу		К	Запуск вредоносного кода
				О	**И**
				К	Несанкционированный доступ к карте сети сегмента КС
				О	**И**
				К	Закрепление в сегменте КС

Оператор	Тип концепта /оператор	Наименование	Оператор	Тип концепта /оператор	Наименование
ЕСЛИ	А	Офисный ПК	**ТО**	А	АРМ администратора домен
	О	**И**		О	**И**
	К	Несанкционированный доступ к карте сети сегмента КС		К	Запуск вредоносного ПО
	О	**И**		О	**И**
	К	Закрепление в сегменте КС		К	Получение доступа к чувствительной информации
ЕСЛИ	А	АРМ администратора домена	**ТО**	А	АРМ администратора домена
	О	**И**		О	**И**
	К	Получение доступа к чувствительной информации		К	Подбор пароля (bruteforce)
	О	**И**		О	**И**
	К	Словарный пароль привилегированного пользователя		К	Получение административного доступа администратора домена
ЕСЛИ	А	АРМ администратора домена	**ТО**	А	АРМ администратора домена
	О	**И**		О	**И**
	К	Получение административного доступа администратора домена		К	Запуск вредоносного кода
				О	**И**
				К	Несанкционированный доступ к карте сети сегмента ТС
				О	**И**
				К	Закрепление в сегменте ТС
ЕСЛИ	К	Несанкционированный доступ к карте сети сегмента ТС	**ТО**	А	SCADA сервер
	О	**ИЛИ**		О	**И**
	К	Закрепление в сегменте ТС		К	Получение доступа к чувствительной информации

Опе-ратор	Тип концепта /оператор	Наименование	Опе-ратор	Тип концепта /оператор	Наименование
Вектор развития атаки в ТС 2. Доступность интерфейсов удаленного доступа					
ЕСЛИ	А	АРМ администратора домена	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	К	Сохраненные учетные данные подключения к удаленному рабочему столу		К	Несанкционированное подключение к удаленному рабочему столу
	О	**И**			
	У	Ошибки разграничения сети			
	О	**И**			
	А	АРМ администратора домена			
	К	Получение административного доступа администратора домена			
ЕСЛИ	А	АРМ администратора домена	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	К	Несанкционированное подключение к удаленному рабочему столу		К	Получение административного доступа к КВА
Атака на целевой актив 1. Шифрование данных с управляющего сервера					
ЕСЛИ	А	SCADA сервер	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	К	Получение административного доступа к КВА		К	Полная потеря данных
	О	**И**			
	К	Запуск вредоносного ПО			
ЕСЛИ	А	SCADA сервер	**ТО**	А	Технологическая инфраструктура
	О	**И**		О	**И**
	К	Полная потеря данных		К	Потеря контроля над ресурсом
ЕСЛИ	А	Технологическая инфраструктура	**ТО**	А	Технологическая инфраструктура
	О	**И**		О	**И**
	К	Потеря контроля над ресурсом		Э	Нарушение функционирования

Оператор	Тип концепта /оператор	Наименование	Оператор	Тип концепта /оператор	Наименование
Атака на целевой актив 2. Подмена управляющих команд					
ЕСЛИ	А	SCADA сервер	**ТО**	А	SCADA сервер
	О	**И**		О	**И**
	К	Получение административного доступа к КВА		К	Подмена управляющих команд
ЕСЛИ	А	SCADA сервер	**ТО**	А	Технологическая инфраструктура
	О	**И**		О	**И**
	К	Подмена управляющих команд		Э	Потеря мощности

**В таблице А – актив, О – оператор, У – уязвимость, К – киберугроза, Э – угроза ЭБ

В таблице 3.8 представлены значимые уязвимости, угрозы и степень их критичности.

Таблица 3.8 – Значимые угрозы и уязвимости рассматриваемых векторов атак

I. Вектор атаки через гостевой WI-FI					
Уязвимости					
№	**Уязвимость**		**Актив**		**Критичность уязвимости**
	Наименование	**Обозначение**	**Наименование**	**Обозначение**	
1	Устаревшая версия ПО, позволяющая получить контроль	V1	Wi-Fi роутер	P1	К
			Роутер КС и ТС	P2	
2	Ошибки разграничения сети	V2	Роутер КС и ТС	P2	К
3	Нарушение политики обновлений	V3	SCADA сервер ЭЧ	C1	К
			SCADA сервер ТЧ	C2	К
Киберугрозы					
№	**Кибергроза**		**Актив**		**Критичность киберугрозы**
	Наименование	**Обозначение**	**Наименование**	**Обозначение**	
4	Перехват данных (анализ сетевого трафика)	T1	Wi-Fi роутер	P1	С
			Роутер КС и ТС	P2	К
5	Несанкционированный доступ к карте сети сегмента ТС	T5	SCADA сервер ЭЧ	C1	К
			SCADA сервер ТЧ	C2	

№	Кибергроза	Обозначение	Актив	Обозначение	Критичность киберугрозы
6	Получение административного доступа к КВА	T6	SCADA сервер ЭЧ	C1	К
7	Получение административного доступа к КВА	T8	SCADA сервер ТЧ	C2	К

Угрозы ЭБ

№	Угроза ЭБ		Детализация угрозы		Критичность угрозы ЭБ
	Наименование	Обозначение	Описание		
8	Потеря мощностей вследствие подмены управляющих команд	T9	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300		К
			Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300		К
			Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300		Н

II. Вектор атаки через фишинговую рассылку

Уязвимости

№	Уязвимость		Актив		Критичность уязвимости
	Наименование	Обозначение	Наименование	Обозначение	
1	Ошибки разграничения сети	V2	Роутер КС и ТС	P2	К
2	Фишинговая рассылка на почтовый клиент ПК КС	V4	Офисный компьютер сегмента КС	ПК1	Н
3	Словарный пароль привилегированного пользователя	V5	АРМ администратора домена	АРМ 1	В
4	Ошибка аутентификации	V6	SCADA сервер ЭЧ	C1	К
			SCADA сервер ТЧ	C2	К

Киберугрозы

№	Кибергроза		Актив		Критичность киберугрозы
	Наименование	Обозначение	Наименование	Обозначение	
1	Получение локального административного доступа к активу	T2	Офисный компьютер сегмента КС	ПК1	С
2	Получение доступа к чувствительной информации	T3	АРМ администратора домена	АРМ 1	К

№	Наименование	Обозначение	Наименование	Обозначение	Критичность киберугрозы
3	Получение административного доступа администратора домена	T4	АРМ администратора домена	АРМ 1	К
			Wi-Fi роутер	Р1	Н
4	Несанкционированное подключение к удаленному рабочему столу	T7	SCADA сервер ЭЧ	С1	К
			SCADA сервер ТЧ	С2	К
5	Получение административного доступа к КВА	T6	SCADA сервер ЭЧ	С1	К
6	Получение административного доступа к КВА	T8	SCADA сервер ТЧ	С2	К

Угрозы ЭБ

№	Угроза ЭБ		Детализация угрозы	Критичность угрозы ЭБ
	Наименование	Обозначение	Описание	
7	Потеря мощностей вследствие подмены управляющих команд	T9	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	К
			Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	К
			Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	Н

Далее построим вероятностную модель реализации киберугроз в рамках рассматриваемых векторов атак. Рекомендуется включать в вероятностный сценарий уязвимости и угрозы с оценкой значимости: «низкая» (Н), «средняя» (С), «высокая» (В), «крайне высокая» (К).

Этап 2. Моделирование сценариев нарушения кибербезопасности энергетической инфраструктуры

2.1. Формирование узлов и их взаимосвязей вероятностного сценария. Узлами вероятностного сценария нарушения кибербезопасности рассматриваемого примера ТЭС являются выявленные в рамках векторов атак уязвимости и угрозы. На рисунке 3.14 отражены узлы сценария, их взаимосвязи, состояния узлов и их априорные вероятности.

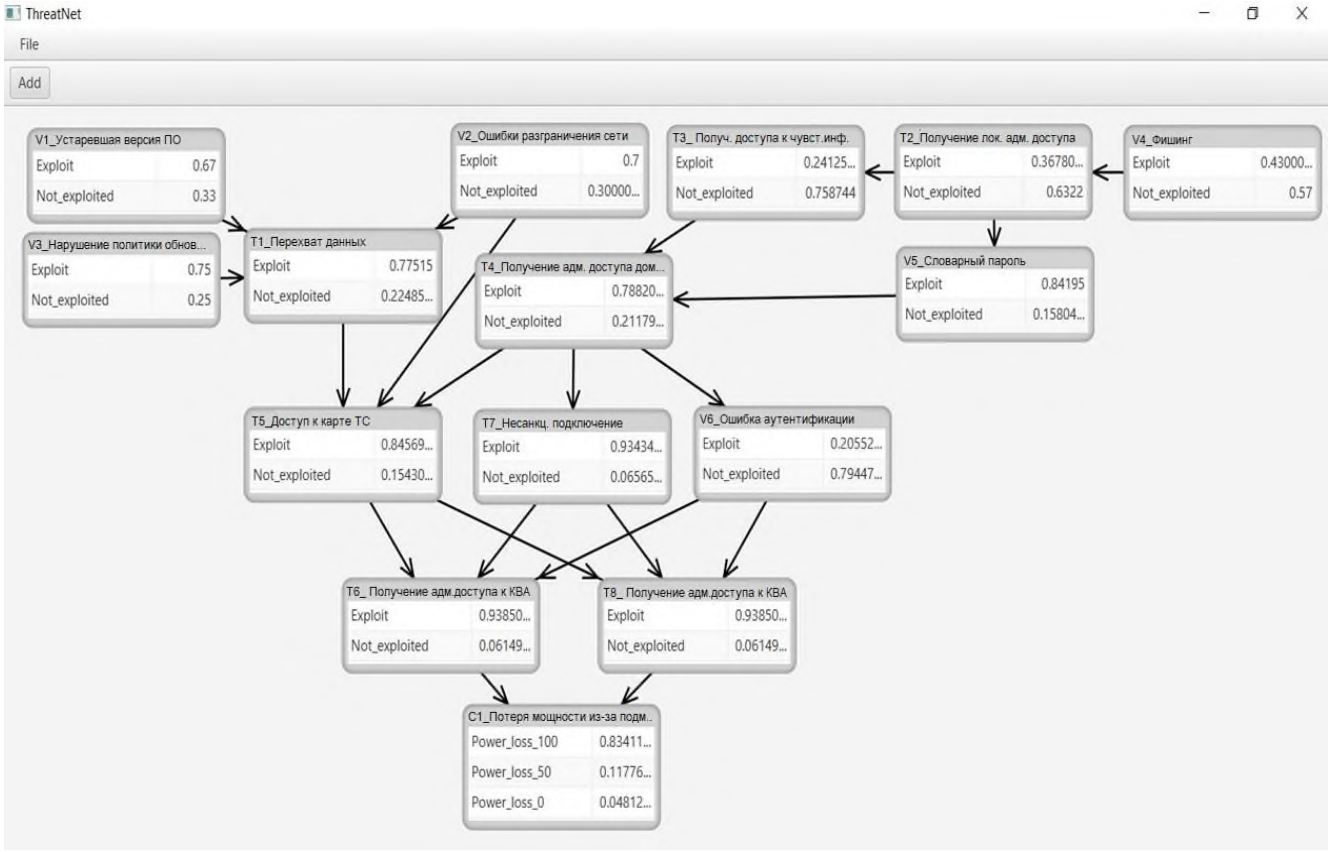

Рисунок 3.14 – Вероятностная модель нарушения кибербезопасности рассматриваемого примера ТЭС

2.2. Определение вероятностных характеристик сценария. В таблицах 3.9 представлены таблицы условных вероятностей (ТУВ) каждого из узлов. Введенные в ТУВ значения основаны на экспертных оценках и обобщенных обезличенных статистических данных о реализации уязвимостей и угроз на объектах ТЭК за 2018-2019 гг., полученных из отчетов ведущих российских частных компаний в области информационной безопасности, которые проводят собственные расследования инцидентов в области ИБ, а также предоставляют услуги по проведению аудита ИБ и тестов на проникновение.

Таблица 3.9 – Таблицы условных вероятностей вероятностного сценария рассматриваемого примера ТЭС

Устаревшая версия ПО, позволяющая получить контроль (V1)	
V1_Outdated_software_version	
T	**F**
67	33

Нарушение политики обновлений (V3)	
V3_Update_policy_violation	
T	**F**
75	25

Ошибки разграничения сети (V2)	
V2_Network_division_error	
T	**F**
70	30

Фишинговая рассылка на почтовый клиент ПК КС (V4)	
V4_Phishing	
T	**F**
43	57

Перехват данных (анализ сетевого трафика) (T1)				
T1_Data_interception				
V1	**V2**	**V3**	**T**	**F**
T	T	T	88	12
T	T	F	88	12
T	F	T	80	20
T	F	F	80	20
F	T	T	83	17
F	T	F	83	17
F	F	T	10	90
F	F	F	10	90

Получение локального административного доступа к активу (T2)		
T2_PC_Local_admin_access		
V4_	**T**	**F**
T	63	37
F	17	83

Получение доступа к чувствительной информации (T3)		
T3_Sensitive_inf_access		
T2	**T**	**F**
T	57	43
F	5	95

Получение административного доступа администратора домена (T4)			
T4_PCdomain_admin_access			
T3	**V5**	**T**	**F**
T	T	100	0
T	F	90	10
F	T	90	10
F	F	0	100

Словарный пароль привилегированного пользователя (V5)		
V5_Vocabulary_pas		
V4_	**T**	**F**
T	100	0
F	75	25

Ошибка аутентификации (V6)		
V6_Authentication_error		
T4	**T**	**F**
T	25	75
F	4	96

Несанкционированное подключение к удаленному рабочему столу (T7)		
T7_Stored_remote_desktop_con		
T4	**T**	**F**
T	100	0
F	69	31

Несанкционированный доступ к карте сети сегмента ТС (T5)				
T5_Tec_network_access				
V2	**T4**	**T1**	**T**	**F**
T	T	T	95	5
T	T	F	95	5
T	F	T	85	15
T	F	F	85	15
F	T	T	80	20
F	T	F	80	20
F	F	T	10	90
F	F	F	10	90

Получение административного доступа к КВА (T8)				
T8_Server_admin_access				
T5	**V6**	**T7**	**T**	**F**
T	T	T	99	1
T	T	F	98	2
T	F	T	99	1
T	F	F	80	20
F	T	T	70	30
F	T	F	27	73
F	F	T	65	35
F	F	F	98	2

Получение административного доступа к КВА (T6)				
T6_Server_admin_access				
T5	**V6**	**T7**	**T**	**F**
T	T	T	99	1
T	T	F	98	2
T	F	T	99	1
T	F	F	80	20
F	T	T	70	30
F	T	F	27	73
F	F	T	65	35
F	F	F	98	2

Потеря мощностей вследствие подмены управляющих команд (T9)				
T9_Command_Loss_of_Power				
T6_	**T8**	**100%**	**50%**	**0%**
T	T	87	11	2
T	F	65	28	7
F	T	58	12	30
F	F	10	10	80

Узлы, соответствующие угрозам и уязвимостям, описываются двумя состояниями: используется (T), не используется (F). Безусловное локальное распределение вероятностей, соответствующее узлам, не имеющим предков, введено на основе имеющихся оценок (экспертных и статистических). Вероятностная оценка состояния T узлов-потомков основана на гипотезе «Какова вероятность того, что событие произойдет, если произойдет событие, соответствующее состояниям узла-предка», т.е.:

- «На сколько вероятна реализация киберугрозы, если известно, что некоторая уязвимость, которая ею может быть использована, обнаружена в КИИ»,
- либо «На сколько вероятно, что зависимая угроза в цепочке угроз будет реализована, если инициирующая её угроза будет реализована».

Вероятностная оценка состояния *F* узлов-потомков основана на имеющихся оценках (экспертных и статистических), что такое событие вообще может произойти, т.е. как часто может быть в принципе использована уязвимость или реализована угроза в данном векторе атак в поставленных условиях.

2.3. Проведение вероятностного эксперимента. Вероятностный эксперимент включал введение свидетельств об использовании уязвимостей и реализации угроз для каждого вектора атаки отдельно и одновременной их реализации. Результаты вероятностного эксперимента для киберугроз по векторам представлены в таблице 3.10; для конечного узла, соответствующего угрозе ЭБ, представлены в таблице 3.11.

Таблица 3.10 – Результаты вероятностного моделирования киберугроз сценария рассматриваемого примера ТЭС

I. Вектор атаки через гостевой WI-FI			
Кибер-угрозы	**Априорные вероятности (вероятность реализации)**	**Свиде-тельства**	**Апостериорная вероятность состояния Т (вероятность инцидента)**
T1	77,5	V1, V2, V3	88
T5	84,6		92,9
T6	93,9		95,9
T8	89,1		93,3
II. Вектор атаки через фишинговую рассылку			
T2	36,8	V2, V4, V5, V6	70,4
T3	24,1		43,2
T4	78,8		99
T7	93,4		99,7
T6	93,9		97,5
T8	89,1		97,5

Таблица 3.11 – Результаты вероятностного моделирования узла Т9 рассматриваемого примера ТЭС

Вектор атаки	**Состояния**	**Апостериорная вероятность (вероятность инцидента)**
I. Вектор атаки через гостевой WI-FI	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	85,7
	Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	11,5
	Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	2,84

Вектор атаки	Состояния	Апостериорная вероятность (вероятность инцидента)
II. Вектор атаки через фишинговую рассылку	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	85,6
	Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	11,4
	Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	3,02
Реализация всех уязвимостей и угроз сценария	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	87,0
	Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	11,0
	Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	2,0

После проведения вероятностного эксперимента возможно описать частную модель угроз, включающую несколько альтернатив развития событий, соответствующих состояниям концепта «угроза ЭБ» и являющегося последствием.

2.3. Построение частной модели угроз. Частная модель угроз для рассматриваемого примера ТЭС на основе сценария, рассмотренного выше, имеет вид, представленный в таблице 3.12.

Таблица 3.12 – Частная модель угроз рассматриваемого примера ТЭК

	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	**Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300**	**Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300**
I. Вектор атаки через гостевой WI-FI			
Киберугроза	**Вероятность реализации**	**Вероятность реализации**	**Вероятность реализации**
Т1 - Перехват данных (анализ сетевого трафика) ГС, КС и ТС сегментов ЛВС	78	76,8	72,2
Т5 – Несанкционированный доступ к карте сети сегмента ТС (получение чувствительной	88,5	78,5	40,9

	Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	**Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300**	**Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300**
информации о SCADA серверах ЭЧ и ТЧ)	88,5	78,5	40,9
Т6 - Получение административного доступа к SCADA серверу ЭЧ	97,5	94,5	39,8
Т8 Получение административного доступа к SCADA серверу ТЧ	93,5	79,9	46,0
II. Вектор атаки через фишинговую рассылку			
Т2 - Получение локального административного доступа к офисному ПК	37,4	35,9	30,4
Т3 - Получение доступа к чувствительной информации о АРМ администратора домена	24,6	23,4	18,9
Т4 - Получение административного доступа администратора домена через Wi-Fi роутер	80,4	76,4	61,6
Т7 - Несанкционированное подключение к удаленному рабочему столу серева SCADA	93,6	93,1	91,0
Т6 - Получение административного доступа к SCADA серверу ЭЧ	97,5	94,5	39,8
Т8 Получение административного доступа к SCADA серверу ТЧ	93,5	79,9	46,0

Реализация угроз, входящих в первый вектор атак, имеет более высокую вероятность, кроме того, такие угрозы имеют высокую качественную оценку (табл. 3.14) влияния на КИИ ЭО.

Этап 3. Оценка рисков нарушения кибербезопасности энергетической инфраструктуры

3.1. Описание рисков нарушения киберезопасности для двух векторов атак рассматриваемого примера ТЭС представлен в таблице 3.13. В данном примере вычислялся ущерб от простоя по формуле (3.1):

$$D_i = \tau \times t \times \phi, \quad (3.1)$$

где D_i – ущерб от i-го риска,τ – потери, t – количество часов на устранение ЭкС, ϕ – стоимость потерь.

Таблица 3.13 – Описание рисков
нарушения кибербезопасности рассматриваемого примера ТЭС

Риск	**Киберугрозы**	**Вероятность**	**Ущерб**
Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	T1, T2, T3, T4, T5, T6, T7, T8	87,0	21 у.е.
Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	T1, T5, T6, T8	11,5	17 у.е.
Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	T2, T3, T4, T7, T6, T8	3,02	0 у.е.

3.2. Оценивание рисков представлено в таблице 3.14.

Таблица 3.14 – Оценивание рисков

Наименование	**Киберугрозы**	**Вероятность**	**Ущерб**	**Оценка**	
				Количественная	**Качественная**
Потеря 100% мощности и нарушение функционирования 2х генерирующих энергоблоков К-300	T1, T2, T3, T4, T5, T6, T7, T8	87,0 %	21 у.е.	18,27 у.е.	Высокий
Потеря 50% мощности и нарушение функционирования 1го генерирующего энергоблока К-300	T1, T5, T6, T8	11,5 %	17 у.е.	1,955 у.е.	Средний

Наименование	Киберугрозы	Вероятность	Ущерб	Оценка	
				Количественная	Качественная
Потеря 0% мощности и нормальной функционирование 2х генерирующих энергоблоков К-300	T2, T3, T4, T7, T6, T8	3,02 %	0 у.е.	0 у.е.	Незначительный

3.3. Выработка рекомендаций. Приведенный пример иллюстрирует применение разработанных технологии и методик. В данном примере рекомендуется устранить уязвимость V2 – ошибка разграничения сети используется угрозой T5 – получение несанкционированного доступа к сегменту ТС. Устранение предлагается путем организации физического разграничения ЛВС на корпоративную и технологическую с запретом внешнего доступа к ТС в целом, а также создания ДМЗ с переносом в неё сервисов и служб, доступ к которым необходим из ТС, например, таких, как почтовые сервера (SMTP), ERP-система (рисунок 3.15). Необходимо предусмотреть организацию защищённых каналов передачи данных при помощи VPN как для работы внутри организации, так и для возможных подключений извне к узлам корпоративного сегмента. Угроза T4 – получения административного доступа администратора домена, вызывает критические угрозы административного доступа к целевому активу. Усилить защиту аутентфикационной информации при её передаче путём использования защищённых протоколов передачи данных (например, TLS) и усиления парольной политики (избежание словарных паролей, установка срока действия пароля, ограничение неуспешных попыток доступа, логирования действий пользователей).

Для предотвращения реализации угроз T6 и T8 «административный доступ к целевому активу» рекомендуется устранить аутентификационные ошибки на сервере за счёт соблюдения политики обновлений и ограничения внешних процессов. Кроме того, представляется необходимой организация эмулятора среды функционирования программного обеспечения (Honeypot) в ДМЗ. Данный

эмулятор позволит отслеживать попытки вторжения в ЛВС организации, изучать поведение злоумышленников, а также применяемое ими вредоносное ПО.

Общая рекомендация касается корректной настройки антивирусной защиты, соблюдения политики обновления программного обеспечения, установки и настройки брэндмауэров на критически значимых активах, повышение общей грамотности сотрудников организации в области компьютерных технологий и информирование их о возможных типах информационных и кибернетических угроз.

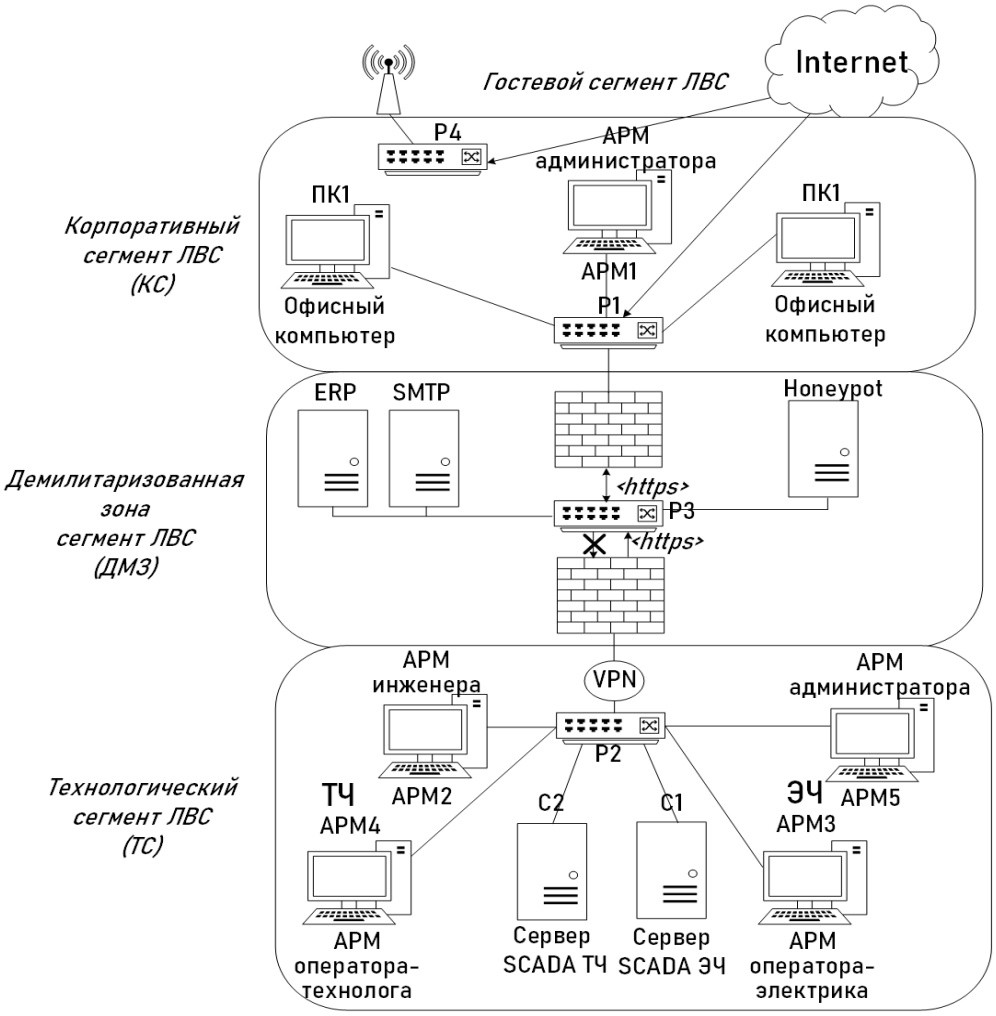

Рисунок 3.15 – Топология сети рассматриваемого примера ТЭС в соответствии с предложенными рекомендациями

3.4 Выводы по главе

В главе рассмотрены проектирование и реализация компонентов интеллектуального программного комплекса «ОКО»:

- продукционной экспертной системы «Cyber», предназначенной для формирования векторов атак на КИИ;
- компонента байесовских сетей доверия «ThreatNet» для вероятностного моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз;
- компонента «RiskMap» для оценки рисков реализации киберугроз, влияющих на наступление ЭкС в энергетике.

Описывается технология применения интеллектуального программного комплекса анализа киберситуационной осведомленности энергетических объектов, предложенных методики, модели и численного метода определения уровня КСО.

В конце главы представлен пример применения разработанной технологии на примере небольшой ЛВС ТЭС, состоящей из 12 физических активов, представлены результаты анализа киберситуационной осведомленности энергетического объекта на каждом этапе технологии.

Заключение

В результате выполнения диссертационной работы достигнута поставленная цель: разработаны методы, модели и интеллектуальный программный комплекс для анализа киберситуационной осведомленности энергетических объектов.

Автором получены следующие основные результаты:

1. Выполнен анализ существующих методов исследования критических инфраструктур, проблем кибербезопасности и киберситуационной осведомленности.

2. Разработан методический подход к анализу киберситуационной осведомленности энергетических объектов, включающий:

- ФС-модель структурирования знаний в области кибербезопасности энергетической инфраструктуры;
- систему онтологий киберситуационной осведомленности энергетических объектов;
- вероятностную модель сценариев ЭкС в энергетике, вызванных реализацией киберугроз, с использованием БСД-модели;
- численный метод определения уровня киберситуационной осведомленности энергетического объекта;
- методику анализа киберситуационной осведомленности энергетических объектов.

3. Разработана архитектура интеллектуального программного комплекса «ОКО» для анализа киберситуационной осведомленности, реализующего предложенные методы и модели, отличающегося интеграцией экспертной системы, компонента байесовских сетей доверия и компонента визуальной оценки рисков, разработанных на основе авторских алгоритмов.

4. Предложена технология анализа киберситуационной осведомленности энергетического объекта на основе методик и разработанного интеллектуального программного комплекса.

5. Выполнена реализация и апробация разработанных методов, моделей и интеллектуального программного комплекса для анализа киберситуационной осведомленности энергетических объектов. Результаты применены в проектах по госзаданию ИСЭМ СО РАН, проектах, поддержанных РФФИ и переданы в Институт энергетики НАН Беларуси.

Список сокращений

АРМ – автоматизированное рабочее место

АСУ ТП – автоматизированная система управления технологическим процессом

БСД – Байесовские сети доверия

БСССМ – большая сложная система стратегического масштаба

ИБ – информационная безопасность

ИС – интеллектуальная система

ИТ – информационная технология

ИТС – информационно-технологические системы

КВА – критические важный актив

КВО – критически важные объекты

КИ – критическая инфраструктура

КИИ – критическая информационная инфраструктура

КИС – корпоративная информационная система

КС – корпоративная сеть

КФС – киберфизические системы

ЛВС – локально-вычислительная сеть

ЛПР – лицо, принимающее решения

НБ – национальная безопасность

ОС – операционная система

ПК – персональный компьютер

ПО – программное обеспечение

ТС – технологический сегмент ЛВС

ТЭК – топливно-энергетический комплекс

ФС-модель – фрактальная стратифицированная модель

ЭБ – энергетическая безопасность

ЭкС – экстремальная ситуация

ЭО – энергетический объект

ЭС – экспертная система

UML – (Unified Modeling Language) унифицированный язык моделирования

XML – (eXtensible Markup Language) расширяемый язык разметки

Словарь терминов

Критические инфраструктуры

1.1. **инфраструктуры**: Крупномасштабные антропогенные системы, которые взаимозависимо функционируют с целью производства и распределения основных продуктов и услуг [10].

1.2. **энергетический сектор**: Совокупность энергетических объектов и систем энергетики, включая энергетические транспортные магистрали [146].

1.3. **большая сложная система стратегического масштаба** (БССCM): Совокупность значительного количества элементов разного типа, объединенных связями различной природы, и обладает общим свойством (назначением, функцией), отличным от свойств отдельных элементов всей совокупности [8].

1.4. **киберфизические системы** (cyber-physical system, CPS, КФС): Результат высокоуровневой интеграции вычислительных, сетевых и физических процессов [147, 148]. Их ключевой характеристикой является интенсивное взаимодействие аппаратных и программных ресурсов для решения вычислительных и коммуникационных задач наряду с управлением физическими компонентами [149]. Принцип функционирования КФС состоит в постоянном получении данных из окружающей среды, их обработки и применения для дальнейшей оптимизации процессов управления [20].

1.5. **интернет вещей** (internet of things, IoT): Совокупность любых физических объектов (не только привычных компьютеров), которым могут быть назначены IP-адреса и которые могут передавать данные: к ним относятся бытовые приборы, различные датчики, автомобили, камеры видеонаблюдения и медицинские (в том числе и вживленные) устройства. Этот термин используется для описания объектов, подключенных к Интернету и способных автоматически собирать и передавать данные без взаимодействия с людьми [136].

1.6. **беспроводная сенсорная сеть** (WSN, wireless sensor network): Распределённая, самоорганизующаяся, устойчивая к отказу отдельных элементов сеть, состоящая из множества необслуживаемых и не требующих специальной

установки датчиков (сенсоров) и исполнительных устройств, объединенных посредством радиоканала [150].

1.7. **энергетическая безопасность**: Состояние защищенности страны, ее граждан, общества, государства, экономики от обусловленных внутренними и внешними факторами угроз дефицита в обеспечении их обоснованных потребностей в энергии экономически доступными топливно-энергетическими ресурсами приемлемого качества в нормальных условиях и при чрезвычайных обстоятельствах, а также от нарушений стабильности, бесперебойности топливо- и энергообеспечения. [57].

Кибернетическая безопасность

2.1. **кибернетическая безопасность**: Набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты кибернетической среды, ресурсов организации и пользователя [26].

2.2. **кибернетическая среда**: Совокупность пользователей, сетей, устройств, всего программного обеспечения, процессов, сохраненной или транзитной информации, приложений, услуг и систем, которые могут быть прямо или косвенно соединены с сетями [26].

2.3. **ресурсы организации и пользователя**: Подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в кибернетической среде [26].

2.4. **безопасность приложений**: Управление рисками, применяемое не только к самим приложениям (их процессам, компонентам, программному обеспечению и результатам), но и к данным (данным конфигурации, пользовательским данным, организационным данным), а также ко всем технологиям, активностям и факторам, вовлеченным в жизненный цикл приложения [28].

2.5. **информационная безопасность** (ИБ): Обеспечение конфиденциальности, целостности, и доступности информации, необходимой для удовлетворения потребностей пользователей [28].

2.6. **безопасность сетей**: Техническое состояние сети, достигаемое в процессе ее разработки, создания, функционирования и модернизации, гарантирующее конфиденциальность, целостность и доступность информации пользователей этой сети [28].

2.7. **безопасность в сети Интернет**: Расширенное понятие сетевой безопасности за счет включения в него защищенных Интернет-зависимых сервисов, систем и сетей [28].

2.8. **защита ключевых информационных систем объектов критической инфраструктуры**: Обеспечение гарантии того, что системы и сети устойчивы в отношении рисков информационной безопасности, сетевой безопасности, безопасности приложений и безопасности Интернет. Рассматривается в контексте критически важных секторов, таких как энергетика, телекоммуникации или, например, водоснабжение [28].

2.9. **критическая информационная инфраструктура**: Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

объекты критической информационной инфраструктуры: Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры [2].

2.10. **вредоносное программное обеспечение, вредоносная программа** (ВПО): Программа, преднамеренно созданная для выполнения несанкционированных, зачастую вредоносных действий [151].

2.11. **трояны**: Вредоносные программы, осуществляющие несанкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей [151].

2.12. **бот-сети** (ботнет, зомби-сеть): Ряд взломанных компьютеров, на которых выполняются вредоносные программы, удаленно контролируемые киберпреступниками с помощью ботов [151].

2.13. **фишинг** (phishing): Форма киберпреступности, основанная на методах социальной инженерии. Предполагает кражу конфиденциальных данных с компьютера пользователя и их дальнейшее использование [151].

2.14. **DDoS атака** (distributed denial of service): Распределенная атака типа «отказ в обслуживании», отличается от обычной тем, что проводится с нескольких компьютеров. Для атаки обычно используется ботнет, состоящий из зараженных компьютеров или устройств IoT [151].

2.15. **атака «человек посередине»** (MITM-атака, «man-in-the-middle»): Атака, при которой злоумышленник осуществляет анализ веб-трафика жертвы, которая об этом не догадывается. Трафик проходит через промежуточный узел злоумышленника, который таким образом получает все отправляемые пользователем данные (логин, пароль, ПИН-код и т. п.) [151].

2.16. **анализ трафика** (traffic analysis): Анализ совокупности шифрованных сообщений, передаваемых по системе связи, не приводящий к дешифрованию, но позволяющий противнику и/или нарушителю получить косвенную информацию о передаваемых открытых сообщениях, а также о функционировании наблюдаемой системы связи. При этом используются особенности шифрования сообщений, их длина, время передачи, данные об отправителе и получателе и т.п. [152].

2.17. **SSL** (secure sockets layer): Технология обеспечения защищенной передачи данных между веб-сервером и браузером. Чаще всего используется с протоколом HTTP (при наличии защищенного соединения к названию добавляется суффикс «s» – протокол HTTPS) [151].

2.18. **TLS** (transport layer security): Технология безопасной передачи данных в интернете. Является развитием стандарта SSL и выступает в качестве надстройки протокола HTTP. Для создания защищенного соединения TLS использует симметричное и асимметричное шифрование данных, несколько

криптографических алгоритмов и сертификаты открытого ключа. Разработкой и поддержкой TLS занимается Инженерный совет интернета (IETF) [151].

2.19. **IPSec** (IP security): Комплект протоколов, предложенный IETF для передачи информации в виртуальных частных сетях. Обеспечивает аутентификацию, проверку целостности и шифрование IP-пакетов [153].

2.20. **SSH** (secure shell): Сетевой протокол для передачи данных в зашифрованном виде. SSH применяют в качестве туннеля для других протоколов (например, TCP), что позволяет отправлять через него практически любое содержимое. SSH создает защищенные каналы для передачи паролей, видеопотока, удаленного управления компьютером. Важной особенностью протокола является возможность сжатия данных. Недостатком SSH является слабая защита от действий злоумышленников, обладающих root-привилегиями [151].

2.21. **MACsec** (media access control (MAC) security): Стандарт безопасности IEEE, определяющий набор протоколов в соответствии с требованиями безопасности для защиты данных в локальных сетях. Обеспечивает выявление несанкционированных действий в локальной сети и предотвращение взаимодействия с ними, позволяет выявить несанкционированные соединения и исключить их [154].

MAC-адрес (media access control): Уникальный идентификатор сетевого устройства, использующего подключение на базе одного из стандартов семейства IEEE 802, например, Ethernet, Wi-Fi, Bluetooth. Устанавливается при производстве и предназначен для однозначного распознавания каждого хоста, а также точной маршрутизации пакетов в широковещательных сетях. Уникальность MAC-адресов контролируется специальным комитетом консорциума IEEE, который по просьбе производителей выдает им блок из нескольких миллионов идентификаторов [151].

2.22. **бэкдор** (backdoor): киберугроза, при реализации которой предоставляется возможность удаленного управления компьютером жертвы. В отличие от обычных утилит удаленного администрирования, трояны этого типа устанавливаются, запускаются и работают незаметно. После установки бэкдоры могут получать команду на отправку, прием, исполнение и удаление файлов, сбор

конфиденциальных данных, информации о действиях пользователя и многое другое [151].

2.23. **атака на цепь поставок** (supply chain attack): Кибератака, при которой злоумышленник внедряет вредоносный код или использует другие уязвимости перед установкой скомпрометированного программного обеспечения в организации с целью фильтрации данных, манипулирования аппаратными средствами или программным обеспечением, операционными системами, периферийными устройствами (продуктами информационных технологий) или службами в любой точке жизненного цикла [151].

2.24. **защита конечной точки** (endpoint protection platform, EPP): Защитные меры, реализованные с помощью программного обеспечения для защиты компьютеров конечных пользователей, таких, как рабочие станции и ноутбуки от атак. Такими мерами, как правило, являются антивирус, антишпионское ПО, антирекламное ПО, персональные брандмауэры, системы обнаружения и предотвращения вторжений и т.д [155].

2.25. **перехват TCP/IP** (TCP/IP hijacking): Кибератака, при которой авторизованный пользователь получает доступ к легитимному соединению другого клиента сети. Перехватив TCP/IP сеанс, нападающий получает возможность читать и изменять передаваемые пакеты данных, а также отправлять адресату свои собственные запросы. Перехват TCP/IP является одним из вариантов атаки «человек посередине». Злоумышленник может определить IP-адреса двух участников сеанса, при помощи DoS-атаки сделать одного из них недоступным и подключиться ко второму, подделав сетевой идентификатор первого [151].

2.26. **подмена DNS** (DNS spoofing): Атака, заключающаяся в искажении данных кэша DNS-сервера, в результате чего трафик жертвы будет перенаправлен на адрес, указанный злоумышленником (вместо легитимного IP-адреса) [151].

DNS (служба доменных имен): Иерархическая система имен сайтов в Интернете. При помощи DNS устанавливается соответствие IP-адреса конкретного хоста и его названия. Система имеет распределенную структуру – обслуживанием и администрированием доменов разного уровня занимаются разные организации.

Единая база данных для осуществления маршрутизации запросов поддерживается системой связанных между собой DNS-серверов [151].

2.27. **DNSSEC** (domain name system security extensions): Расширение протокола DNS, использующее цифровую подпись данных DNS для обеспечения безопасности процесса преобразования доменных имен [156].

2.28. **BGP** (border gateway protocol): Прикладной протокол, применяемый для маршрутизации пакетов между автономными сегментами сети Интернет. Используется для передачи информации об узлах сети, доступных для группы хостов, между которыми установлено соединение. На основании этой информации определяется кратчайший путь прохождения каждого конкретного пакета. Задача BGP состоит исключительно в маршрутизации. Непосредственная доставка пакетов осуществляется при помощи протокола TCP [151].

2.29. **шпионская программа**: Программа, которая скрытным образом устанавливается на компьютер пользователя с целью сбора данных о нем и его системе. В отличие от вредоносного ПО, не наносит вреда операционной системе, программам или файлам [151].

2.30. **клавиатурные шпионы**: Троянские программы, которые ждут подключения пользователя к подлинной банковской веб-странице и затем перехватывают введённые с клавиатуры символы (то есть, логин и пароль). Для этого они следят за запуском и активностью приложений и, если пользователь работает в интернет-браузере, сравнивают название веб-сайта с «зашитым» в код троянца списком банков. Если веб-сайт обнаружен в списке, то включается клавиатурный шпион, а затем перехваченная информация (последовательность нажатых клавиш) отсылается злоумышленнику. Данные троянские программы никак не проявляют своего присутствия в системе [151].

2.31. **брандмауэр** (firewall): Барьер между компьютерной системой (корпоративной или отдельным потребителем) и внешним миром, препятствующий несанкционированному доступу к защищенной сети. Брандмауэр отслеживает входящий и исходящий сетевой трафик и решает, передавать его

дальше или блокировать, в зависимости от установленных политик безопасности [151].

корпоративный брандмауэр: Брандмауэр, предназначенный для защиты периметра локальной сети от несанкционированного доступа для обеспечения доступа локальных пользователей в Интернет.

брандмауэр веб-приложений (web application firewall, WAF): Средства фильтрации трафика прикладного уровня, специально ориентированные на веб-приложения [157].

2.32. **системы обнаружения вторжений** (СОВ, intrusion detection system, IDS): Служба безопасности, которая отслеживает и анализирует сетевые или системные события с целью обнаружения и предоставления предупреждений в реальном времени (или почти в реальном времени) попыток получить доступ к системным ресурсам несанкционированным образом [155].

2.33. **средство доверенной загрузки**: Программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешного контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы [158].

2.34. **тестирование на проникновение** (penetration testing): Методология тестирования, предназначенная для обхода функции безопасности системы. Примечание. Тестирование на проникновение может использовать системную документацию (например, проектирование системы, исходный код, руководства) и проводится в рамках определенных ограничений. Некоторые методы испытаний на проникновение используют методы грубой силы [155].

2.35. **межсайтовый скриптинг** (cross site scripting, XSS): Атака, при которой в страницу сайта внедряется вредоносный код. При открытии страницы пользователем, код выполняется на его компьютере и устанавливает соединение с

веб-сервером злоумышленника, который таким образом получает контроль над системой.

XSS-уязвимости бывают двух видов: активная и пассивная. При активной уязвимости код внедряется на уровне базы (или в виде файла на сервере). Тогда жертвами становятся все посетители сайта. При пассивной уязвимости код встраивается в определенную страницу, на которую пользователь привлекается, к примеру, с помощью фишинга [151].

2.36. **спам**: Нежелательная электронная почта. Она фактически является нежелательной рекламой, эквивалентом физической нежелательной рекламы в форме писем или телефонных звонков [151].

2.37. **спуфинг электронной почты** (email spoofing, forged email): Подмена адреса отправителя в письмах электронной почты с целью обмана пользователя [151].

2.38. **антиспам, спам-фильтр**: Программа для определения и фильтрации нежелательных электронных сообщений, которые могут поступать через корпоративные почтовые серверы и публичные сервисы электронной почты [157].

2.39. **политика защиты контента** (content security policy, CSP): Дополнительный уровень безопасности, позволяющий распознавать и устранять определенные типы атак, таких как Cross Site Scripting (XSS) и атаки внедрения данных. Спектр применения этих атак включает, но не ограничивается кражей данных, подменой страниц и распространением зловредного ПО [159].

2.40. **инфраструктура политики отправителя** (sender policy framework, SPF): Технология, при которой сервер-получатель должен иметь возможность проверить, совпадает ли адрес сервера, с которого фактически было отправлено сообщение, с адресом подлинного почтового сервера, ассоциированного с доменом отправителя [160].

2.41. **domainkeys identified mail** (DKIM): Технология, создающая криптографическую подпись заголовка и части тела сообщения при помощи закрытого ключа. Впоследствии подпись может быть проверена с помощью открытого ключа, опубликованного в системе доменных имен (DNS) [160].

2.42. **domain-based message authentication, reporting and conformance** (DMARC): Технология, позволяющая администратору домена выбрать, какой механизм защиты будет использоваться на сервере – SPF, DKIM или оба [160].

2.43. **словарная атака**: Метод подбора пароля (или ключа шифрования), заключающийся в переборе слов из словаря до тех пор, пока пароль не будет найден. Такой метод сработает, в случае если в качестве пароля используется обычное слово, а не комбинация букв, чисел и специальных символов. В случае, когда используется сложный пароль, взломщикам приходится применять брутфорс-атаку. Один из способов снизить шансы успеха словарной атаки – ограничить количество попыток ввода пароля [151].

2.44. **атака по сторонним каналам** (side-channel attack): Способ взлома криптографического алгоритма, основанный на анализе работы вспомогательных систем, участвующих в шифровании. В отличие от классического способа декодирования, который фокусируется на математической модели ключа, атака по сторонним каналам использует для этой цели косвенные данные. Одним из примеров реализации такого подхода является атака по времени. Суть метода заключается в анализе продолжительности обработки каждого этапа шифрования и сопоставлении этих данных с другими для выявления взаимосвязей [160].

2.45. **троянец-стилер** (trojan-PSW, password Stealing ware): Вредоносное ПО, предназначенное для кражи паролей и другой учетной информации. Стилеры могут извлекать сохраненные секретные ключи из браузеров и других утилит, анализировать кэш и файлы cookie и получать доступ к данным криптокошельков. Собранные сведения троянец обычно отправляет на командный сервер [160].

2.46. **управление идентификацией и доступом** (identity and access management, IAM): Технология обеспечение доступа легитимных пользователей к запрашиваемым ресурсам в нужное время в точном соответствии с их правами. Наиболее критичное значение проблема обеспечения гарантий соответствующего доступа приобретает в связи с широким применением технологически неоднородного оборудования и необходимостью точного соответствия требованиям усиленных политик безопасности. Данная проблема имеет ключевое

значение для любой организации. Правильная организация у. и. д. предоставляет возможность оптимизации затрат и, что более важно, создает условия для подключения новых приложений [152].

2.47. **двухфакторная аутентификация**: Метод использования информации из двух источников для идентификации личности. При этом обычный пароль «объединяется» с внешним устройством проверки подлинности, например с аппаратным токеном, который генерирует случайный одноразовый пароль, со смарт-картой, SMS-сообщением (где мобильный телефон является токеном) или уникальным физическим атрибутом, например, отпечатком пальца [151].

2.48. **шифрование**: Термин, описывающий процесс «перемешивания» данных таким образом, что неавторизованным лицам, не обладающим ключом для дешифровки, невозможно их понять. Шифрование используется для того, чтобы защитить передаваемые данные. Например, при передаче их через Интернет во время банковской транзакции [151].

2.49. **эксплойт**: Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему).

2.50. **атака типа advanced persistent threat** (APT-атака): Хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или целую отрасль. За APT-атакой, как правило, стоят преступные группировки, имеющие значительные финансовые ресурсы и технические возможности [64].

Методы

3.1. **инженерия знаний**: Ветвь информатики, изучающая модели и методы извлечения, структурирования и формализации (представления) знаний для их обработки в интеллектуальных и информационных системах [76].

3.2. **байесовская сеть доверия** (БСД, BBN): Графическая модель вероятностных и причинно-следственных отношений между наборами переменных, представляющая собой направленный ациклический граф, вершины

которого представляют переменные, а ребра показывают условные зависимости между переменными [98].

3.3. **родитель вершины графа**: Такая вершина A, которая удовлетворяет условию, что если из вершины A выходит дуга в вершину B, то A называют родителем B B, а B называют потомком A.

3.4. **предок и потомок вершины графа**: Такая вершина A и B, которые удовлетворяют условию, что если из вершины A существует ориентированный путь в вершину B, то A называется предком B, а B называется потомком A.

3.5. **экспертные системы** (ЭС, expert systems): Интеллектуальные информационные системы, в которые включены знания специалистов о некоторой конкретной области и которые в пределах этой области способны принимать экспертные решения [84].

3.6. **бизнес-процесс**: Особый процесс, который служит осуществлению основных целей предприятия (бизнес-целей) и описывает центральную сферу его деятельности. Основными признаками бизнес-процессов являются точки соприкосновения этого процесса с бизнес-партнерами предприятия (например, клиенты, поставщики).

процесс производства: Сумма всех бизнес-процессов предприятия, определяется как пошаговое выполнение целей предприятия [161].

технологический процесс: Часть производственного процесса, содержащая действия по изменению и последующему определению состояния предмета производства. т. п. представляет собой совокупность механич., физ., хим. процессов - операций, изменяющих форму и размеры деталей, их свойства, внешний вид и т. п.[162].

Список литературы

1. Распоряжение Правительства Российской Федерации «Цифровая экономика Российской Федерации» от 28.07.2017 №1632-р // «Собрание законодательства РФ», 07.08.2017, № 32, ст. 5138.

2. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 года № 187-ФЗ // «Собрание законодательства РФ», 31.07.2-17, № 31, ст. 4736.

3. Об утверждении Доктрины энергетической безопасности Российской Федерации: Указ Президента Российской Федерации от 13 мая 2019 года № 216 // «Собрание законодательства РФ», 20.05.2019, № 20, ст. 2421.

4. Концепция стратегии кибербезопасности Российской Федерации (проект) [Электронный ресурс]. – URL: http://www.council.gov.ru/media/files/41d4b3dfbd b25cea8a 73.pdf (дата обращения 26.07.2018).

5. Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации»: Постановление Правительства Российской Федерации от 29 марта 2019 года № 377 // «Собрание законодательства РФ», 15.04.2019, № 15, ст. 1750.

6. Массель, Л.В. Киберопасность как одна из стратегических угроз энергетической безопасности России / Л.В. Массель, Н.И. Воропай, С.М. Сендеров, А.Г. Массель //Вопросы кибербезопасности. – 2016. – № 4 (17). – С. 2-10.

7. Pappaterra, M. J., Flammini, F. A Review of Intelligent Cybersecurity with Bayesian Networks / Published in: 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). Publisher: IEEE, 2019. DOI:10.1109/smc.2019.8913864.

8. Кондратьев, А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / А. Кондратьев // Зарубежное военное обозрение. – 2012. – № 1. – С. 19-30.

9. Массель, Л.В. Конвергенция исследований критических инфраструктур, качества жизни и безопасности / Л.В. Массель // Информационные технологии и системы: Труды Шестой Международной научной конференции, 2017. – Челябинск: ЧелГУ. – С. 170-175.

10. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Электронный ресурс]. – URL: https://eur-lex.europa.eu/legal-ontent/EN/ALL/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG (дата обращения 26.04.2019).

11. Zio, E. Challenges in the vulnerability and risk analysis of critical infrastructures / E. Zio // Reliability Engineering and System Safety. – 2016. – 152. – Pp. 137-150.

12. Махутов, Н.А. Обеспечения безопасной эксплуатации объектов техносферы и населения с использованием критериев риска / Н.А. Махутов, М.М. Гаденин // Тезисы докладов XXI Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций, 2016. – Москва: ФГБУ ВНИИ ГОЧС (ФЦ). – С. 137-146.

13. Клаузевиц, Карл фон. О войне. Избранное / Карл фон Клаузевиц ; пер. с нем. А.К. Рачинского ; предисл. – коммент. Л.В. Ланника. – Москва : Издательство АСТ, 2017. – 320 с.: ил. – (Иллюстрированная военная история).

14. Strange, J. Centers of gravity and critical vulnerabilities: Building on the Clausewitzian Foundation So That We Can All Speak the Same Language // Perspectives on Warfighting. – 1996. – Second Edition. – Number Four. – 90 p.

15. Warden, John A. III. Enemy as a System // Airpower Journal. – Spring 1995. – Vol. 9 (1). – P. 40-55.

16. Lehto M. Theoretical examination of the cyber warfare environment // Proceedings of the 11th International Conference on Cyber Warfare and Security. – ICCWS. – 2016. – P. 223-230.

17. Albert R., Barabasi A.-L. Statistical mechanics of complex networks // Rev. Mod. Phys. – 2002. – Vol. 74. – P. 47–97.

18. Buldyrev S., Parshani R., Paul G., Stanley H., Havlin S. Catastrophic cascade of failures in interdependent networks // Nature. – 2010. – 464(7291). – P. 1025–1028. doi:10.1038/nature08932.

19. Массель, Л.В. Семиотический подход к созданию интеллектуальных систем ситуационного управления в энергетике / Л.В. Массель, А.Г. Массель // XLIII Международная конференция «Информационные технологии в науке, образовании и управлении»: труды под ред. проф. Е.Л. Глориозова. – 2015. – С. 182-193.

20. Usmonov, B. The cybersecurity in development of IoT embedded technologies / B. Usmonov, O. Evsutin, A. Iskhakov, A. Shelupanov, A. Iskhakova, R. Meshcheryakov // Proceedings of the International Conference on Information Science and Communications Technologies (ICISCT, 2017). Publisher: IEEE, 2017. doi:10.1109/ICISCT.2017.8188589 (Scopus).

21. Haimes Y. Systems-based risk analysis // Global Catastrophic Risks / Nick B., Milan C. (ed), – Oxford, 2008, – P. 146-163.

22. Цифровая трансформация электроэнергетики. Материалы конференции «Совещание главных инженеров-энергетиков 2017 (СГИЭ)» от 4 октября 2017 года [Электронный ресурс]. – URL: http://digitenergy.ru/archive/energetics/transformation/materials-transform/ (дата обращения 13.01.2020).

23. Концепция «Цифровая трансформация 2030» компании «РОССЕТИ», 2018 год [Электронный ресурс]. – URL: https://www.rosseti.ru/investment/Kontseptsiya_Tsifrovaya_transformatsiya_2030.pdf (дата обращения 13.01.2020).

24. Газпром нефть. Цифровая трансформация компании до 2030 года. [Электронный ресурс]. – URL: https://digital.gazprom-neft.ru/home (дата обращения 11.01.2021).

25. Цифровизация энергетики. [Электронный ресурс] // Институт энергетики Высшей школы экономики. – 2020. – URL: https://energy.hse.ru/digitalization (дата обращения 13.01.2020).

26. T-REC-X.1205: Overview of cybersecurity [Электронный ресурс] // ITU-T. – 2008. – URL: https://www.itu.int/rec/T-REC-X.1205-200804-I (дата обращения 16.05.2019).

27. ISO/IEC 27032:2012 ISO standard of Information technology. Security techniques. Guidelines for cybersecurity [Электронный ресурс] // 2012. – URL: https://www.iso.org/ru/standard/44375.html (дата обращения 16.05.2019).

28. Наставления по кибербезопасности (ISO/IES 27032:2012) [Текст]: излож. стандарта ISO/IES 27032:2012 «Информационные технологии. – Методы обеспечения безопасности. – Наставления по кибербезопасности.» / Мохор В. В., Богданов А. М., Килевой А. С. – Киев: Три-К, 2013. - 129 с.

29. Гаськова, Д.А. Анализ нарушений кибербезопасности в энергетическом секторе // «Системные исследования в энергетике» / Труды конференции молодых ученых ИСЭМ СО РАН, Вып. 47. – Иркутск: ИСЭМ СО РАН, 2017. – С. 101-107.

30. Society for Risk Analysis Glossary [Электронный ресурс]. – URL: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (дата обращения 10.01.2021).

31. Массель, А.Г. Кибератаки как угроза энергетической безопасности России / А.Г. Массель // Труды Международной конференции «Кибербезопасность-2013». – Украина, Киев, Институт специальной связи и защиты информации НТУ Украины «КПИ». – 2013. – №1 (3). – С. 49–56.

32. Промышленные компании: векторы атак. [Электронный ресурс] // Positive Technologies. – 2018 – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/ (дата обращения 11.11.2018).

33. Аналитические статьи компании Positive Technologies. [Электронный ресурс] // Positive Research. – 2019. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf (дата обращения: 20.08.2019).

34. Массель, А.Г. Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики / А.Г. Массель, Д.А. Гаськова // Энергетическая политика. – 2018. – №5. – С. 62-72.

35. Zhang, C. From Numerical Model to Computational Intelligence: The Digital Transition of Urban Energy System / C. Zhang, A. Romagnoli, L. Zhou, M. Kraft // Energy Procedia: 2017. – Vol. 143. – P. 884–890. – DOI: 10.1016/j.egypro.2017.12.778.

36. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства: руководство. [Электронный ресурс] // Организация по безопасности и сотрудничеству в Европе (ОБСЕ). – 2013. – URL: https://www.osce.org/files/f/documents/5/2/110472.pdf (дата обращения: 20.08.2019)

37. Безкоровайный, М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – № 1(2). – 2014. – С. 22-27.

38. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [Электронный ресурс] // Постановление Правительства Российской Федерации от 8 февраля 2018 года. – № 127. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1614-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127 (дата обращения 26.04.2019).

39. Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации [Электронный ресурс] // Приказ ФСТЭК России от 6 декабря 2017 года. – № 227. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (дата обращения 26.07.2018).

40. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования [Электронный ресурс] // Приказ ФСТЭК России от 21 декабря 2017 года. – № 235. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236 (дата обращения 26.07.2018).

41. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации

одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий [Электронный ресурс] // Приказ ФСТЭК России от 22 декабря 2017 года. – № 236. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (дата обращения 26.07.2018).

42. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации [Электронный ресурс] // Приказ ФСТЭК России от 25 декабря 2017 года. – № 239. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 26.07.2018).

43. О безопасности объектов топливно-энергетического комплекса [Электронный ресурс] // Федеральный закон от 21 июля 1997 года. – № 116-ФЗ. – URL: http://base.garant.ru/11900785/ (дата обращения 26.04.2019).

44. 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 окружающей среды [Электронный ресурс] // Приказ ФСТЭК России от 14 марта 2014 года. – № 31. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.07.2018).

45. Common Vulnerability Scoring System v3.0: Specification Document [Электронный ресурс]. – URL: https://www.first.org/cvss/specification-document (дата обращения 29.03.2018).

46. Chee-Wooi, T. Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees / T. Chee-Wooi, L. Chen-Ching, M. Govindarasu. // Power Engineering Society General Meeting. – 2007. – IEEE. DOI: 10.1109/PES.2007.385876.

47. Chee-Wooi T., M. Govindarasu, and L. Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling / T. Chee-Wooi, M. Govindarasu, L. Chen-

Ching // Transactions on Systems, Man, and Cybernetics. Part A: Systems And Humans. – IEEE. – Vol. 40. – No. 4. – July 2010. DOI: 10.1109/TSMCA.2010.2048028.

48. Калашников, А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности. – 2014. – № 3(4). – С. 35-41.

49. Аникин, И.В. Управление рисками информационной безопасности: учебное пособие – Казань: Редакционно-издательский центр «Школа». – 2018. – 160 с.

50. Чукляев, И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем / И.И. Чукляев // Вопросы кибербезопасности. – № 4(17). – 2016. – С. 61-71.

51. Миков, Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности / Д.А. Миков // Вопросы кибербезопасности. – № 4(7). – 2014. – С. 49-54.

52. Булдакова, Т.И. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности / Т.И. Булдакова, Д.А. Миков // Вопросы кибербезопасности. – 2017. – № 3(21). – С. 8-15.

53. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс] // ГОСТ ИСО/МЭК 27005-2010. – URL: http://docs.cntd.ru/document/1200084141 (дата обращения 19.06.2019).

54. Fung, C.C. A proposed study on economic impacts due to cyber attacks in Smart Grid: A risk based assessment / C.C. Fung, A.R. Mehrnaz, K.P. Wong // IEEE Power & Energy Society General Meeting. – 2013. – P. 1-5. DOI:10.1109/pesmg.2013.6672302.

55. Дорофеев, А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции / А.В. Дорофеев, А.С. Марков // Вопросы кибербезопасности. – № 1(2). – 2014. – С. 67-73.

56. О стратегии научно-технологического развития Российской Федерации [Электронный ресурс] // Указ Президента Российской Федерации от 1 декабря 2016 года – № 642. – URL: http://static.kremlin.ru/media/acts/files/0001201612010007.pdf (дата обращения 26.04.2019).

57. Пяткова Н.И., Рабчук В.И., Сендеров С.М., Чельцов М.Б. Энергетическая безопасность России: проблемы и пути решения. Отв. ред. Воропай Н.И. – Новосибирск: Изд-во СО РАН, 2011. – 211 с.

58. Gaskova, D. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility / D. Gaskova D., A. Massel // Proceedings of the 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC). Vladivostok. Publisher: IEEE. – 2018. DOI: 10.1109/RPC.2018.8482229.

59. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018 [Электронный ресурс] // Kaspersky Lab ICS CERT, 27 марта 2019. – URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018 (дата обращения: 07.04.2019).

60. Уязвимости в АСУ ТП: итоги 2018 года [Электронный ресурс] // Аналитические статьи Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019/ (дата обращения: 07.04.2019).

61. Безопасность АСУ ТП: итоги 2017 года [Электронный ресурс] // Аналитические статьи Positive Technologies. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf (дата обращения: 07.04.2019).

62. Ландшафт угроз для систем промышленной автоматизации, второе полугодие 2017 [Электронный ресурс] // Kaspersky Lab ICS CERT, 26 марта 2018. – URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/ (дата обращения: 07.04.2019).

63. Згоба, А.И. Кибербезопасность: угрозы, вызовы, решения / А.И. Згоба, Д.В. Маркелов, П.И. Смирнов // Вопросы кибербезопасности – № 5(8). – 2014. – С. 30-38.

64. APT-атаки на топливно-энергетический комплекс России: обзор тактик и техник [Электронный ресурс] // Аналитические статьи Positive Technologies.c URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019/ (дата обращения: 15.11.2019).

65. MITRE ATT&CK [Электронный ресурс] // Globally-accessible knowledge base. – URL: https://attack.mitre.org/ (дата обращения: 15.11.2019).

66. Экспертно-аналитический доклад «Цифровой переход в электроэнергетике России» – 2018 [Электронный ресурс]. – URL: https://www.csr.ru/issledovaniya/tsifrovoj-perehod-v-elektroenergetike-rossii/ (дата доступа 10.08.2018).

67. Материалы 2-й отраслевой конференции «Цифровая трансформация электроэнергетики России» – Москва, октябрь 2017–2018 [Электронный ресурс]. – URL: http://digitenergy.ru/ (дата доступа 13.11.2017).

68. Массель, Л.В. Использование современных информационных технологий в Smart Grid как угроза кибербезопасности энергетических систем России / Л.В. Массель // Information technology and security: Труды. Киев. Институт специальной связи и защиты информации НТУ Украины «КПИ». – 2013. – №1 (3). – С. 56–65.

69. Массель, Л.В. Онтологический инжиниринг ситуационного управления в энергетике / Л.В. Массель, А.Г. Массель, Т.Н. Ворожцова, Н.Н. Макагонова // Всероссийская конференция с международным участием «Знания, онтологии, теории» (ЗОНТ-2015)». – Новосибирск. ИМ СО РАН. – 2015. – Т.2. – С. 36–43.

70. Endsley, M.R. Situation awareness global assessment technique (SAGAT) / M.R. Endsley // Proceedings of the IEEE 1988 National Aerospace and Electronics Conference – Dayton, OH, USA, 1988 – vol.3, – P. 789-795 DOI: 10.1109/NAECON.1988.195097.

71. Массель, Л.В. Моделирование этапов принятия решений на основе сетецентрического подхода / Л.В. Массель, Р.А. Иванов, А.Г. Массель // Вестник ИрГТУ. – 2013. – №10(81). – С. 16–22.

72. Endsley, M.R. Theoretical underpinnings of situation awareness: A critical review. In: Endsley M.R, Garland D.J. Situation awareness analysis and measurement. – 2000. – P. 3-32.

73. MITRE Capabilities overviews [Электронный ресурс]. – URL: https://www.mitre.org/capabilities/cybersecurity/situation-awareness (дата обращения 15.11.2020).

74. Frank, U. Cyber Situational Awareness / U. Frank, J. Brynielsson. // A systematic review of literature. – Computer Security 46 – Stockholm, Sweden, 2014. – P 18-31.

75. National Institute of Standards and Technology (NIST) Glossary [Электронный ресурс]. – URL: https://csrc.nist.gov/glossary (дата обращения 15.11.2020).

76. Cheng, Y. Metrics of Security / Y. Cheng, J. Deng, J. Li, S.A. DeLoach, A. Singhal, X. Ou. In: Kott A., Wang C., Erbacher R. (eds) Cyber Defense and Situational Awareness. // Advances in Information Security. – Springer, Cham, 2014. – Vol 62.

77. Eckhart, M. Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins / M. Eckhart, A. Ekelhart, E. Weippl // Proceedings of the 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). – 2019. – P. 1222-1225. DOI:10.1109/etfa.2019.8869197.

78. Okolica, J.S. Developing Systems for Cyber Situational Awareness / J.S. Okolica, J.T. McDonald, G.L. Peterson, R.F. Mills, M.W. Haas // Proceedings of the 2nd Cyberspace Research Work-shop. – Shreveport, Louisiana. – 2009.

79. Irmak, E. An overview of cyber-attack vectors on SCADA systems / E. Irmak, I. Erkek // Proceedings of 6th International Symposium on Digital Forensic and Security (ISDFS). – 2018. – DOI: 10.1109/isdfs.2018.8355379.

80. Aven, T. Quantitative Risk Assessment: The Scientific Platform. // Cambridge: Cambridge University Press. – 2011 DOI: 10.1017/CBO9780511974120.

81. Rot, A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, 22 – 24 October 2008, San Francisco, USA. DOI: 10.21742/apjcri.2015.03.04

82. Гаврилова, Т.А. Инженерия знаний. Модели и методы: учебник / Т.А. Гаврилова, Д.В. Кудрявцев, Д.И. Муромцев. – Санкт-Петербург: Лань, 2016. – 324 с.

83. Силич, В.А. Теория систем и системный анализ: учебное пособие / В.А. Силич, М.П. Силич // Томский политехнический университет. – Томск: Издательство Томского политехнического университета, 2011. – 276 с.

84. Гаврилова Т.А. От инженерии знаний к онтологическому инжинирингу [Электронный ресурс] // URL: http://masters.donntu.org/2013/fknt/niftaliev/library/article3.htm (дата доступа 13.05.2019).

85. Mizogushi, R. Using Ontological Engineering to Overcome Common AI-ED Problems / R. Mizogushi, J. Bourdeau // International Journal of Artificial Intelligence in Education. – 2000. – Vol. 11. – P1-12.

86. Массель, Л.В. Онтологический инжиниринг для поддержки принятия стратегических решений в энергетике / Л.В. Массель, Т.Н. Ворожцова, Н.И. Пяткова // Онтология проектирования. – 2017. – Т. 7, № 1(23). – С. 66-76. DOI: 10.18287/2223-9537-2017-7-1-66-76.

87. Пяткова, Н.И. Моделирование критических инфраструктур энергетики с учетом требований энергетической безопасности / Н.И. Пяткова, Н.М. Береснева // Информационные и математические технологии в науке и управлении. . – 2017. – № 3(7). – С. 54-65.

88. Ворожцова, Т.Н. Онтологическая модель пространства знаний для ситуационного управления в энергетике / Т.Н. Ворожцова // XX Байкальская Всероссийская конференция «Информационные и математические технологии в науке и управлении»: труды. Т. 3. – Иркутск. ИСЭМ СО РАН, 2015. – С. 85-88.

89. Копайгородский, А.Н. Применение онтологий в семантических информационных системах / А.Н Копайгородский // Онтология проектирования. – 2014. – № 4 (14). – С. 78-89.

90. Загорулько, Ю.А. Онтологический подход к разработке системы поддержки принятия решений на нефтегазодобывающем предприятии / Ю.А. Загорулько, Г.Б. Загорулько // Вестник НГУ. Серия: Информационных технологии. – 2012. – Том 10. Выпуск 1. – С. 121-128.

91. Ворожцова, Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности / Т.Н. Ворожцова // Онтология проектирования. – № 4 (14). – 2014. – С. 69-77.

92. Массель, Л.В. Фрактальная модель структурирования знаний / Л.В. Массель // Сб. науч. трудов Национальной конференции с международным участием «Искусственный интеллект-94». – Рыбинск, 1994. – т.1. – С. 46-49.

93. Массель, Л.В. Фрактальный подход к структурированию знаний и примеры его применения / Л.В. Массель // Онтология проектирования. – 2016. – Том 6, № 2 (20). – С. 149-161.

94. Массель, А.Г. Фрактальный подход к семантическому моделированию / А.Г. Массель // Труды V Всероссийской конференции «Информационные технологии интеллектуальной поддержки принятия решений». – Уфа: УГАТУ, 2017. – Т.I. – С. 15-19. ISBN 978-5-4221-0985-2 ISBN 978-5-4221-0986-9.

95. Массель, Л.В. Фрактальный подход к построению информационных технологий / Л.В. Массель // Информационная технология исследований развития энергетики / Л.Д. Криворуцкий, Л.В. Массель. – Новосибирск: «Наука», 1995. – С. 40-67.

96. Самарский, А.А. Математическое моделирование и вычислительный эксперимент / А.А. Самарский // Вестник АН СССР. 1979. Избранные труды. Раздел 3. Математическое моделирование. – №5. – С. 38-49.

97. Копайгородский, А.Н., Массель Л.В. Фрактальный подход к проектированию архитектуры информационных систем / А.Н. Копайгородский, Л.В. Массель // Вестник ИрГТУ, 2010. – № 6 (46). – С. 8-12.

98. Heckerman, D. A Tutorial on Learning with Bayesian Networks // Technical Report MSR-TR-95-06, Microsoft Research, March, 1995. – 57 p.

99. Zhang, Q. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems / Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, S. Huang // Proceedings of IEEE Transactions on Systems, Man, and Cybernetics: Systems. – 2016. – Vol. 46. – № 10. – P. 1429-1444. DOI: 10.1109/TSMC.2015.2503399.

100. Феофанов, К.А. Сценарные возможности современного прогнозирования и управления / К.А. Феофанов // Вестник МГТУ Станкин, 2009. – № 4. – С. 126-132.

101. Кульба, В.В. Информационное управление. Часть 2: Сценарный подход / В.В. Кульба, В.Л. Шульц, А.Б. Шелков // Национальная Безопасность / NOTA BENE, 2015. – С. 111-124.

102. Гаськова, Д.А. Сценарный подход к определению критически важных объектов / Д.А. Гаськова, А.Г. Массель // «Молодёжь и современные информационные технологии» / Сборник трудов XV Международной научно-практической конференции студентов, аспирантов и молодых учёных. – Национальный исследовательский Томский политехнический университет. – Томск. 2018. – С. 243-244.

103. Массель, Л.В. Применение байесовских сетей доверия для интеллектуальной поддержки исследований проблем энергетической безопасности / Л.В. Массель, Е.В. Пяткова // Вестник ИрГТУ. – 2012. – № 2(61). – С. 8-13.

104. Массель, Л.В. Интеграция информационных технологий в системных исследованиях энергетики / Л. В. Массель, Е. А. Болдырев, А. Ю. Горнов и др.; под ред. Н.И. Воропая. – Новосибирск: Наука. Сиб. изд. фирма РАН, 2003. – 320 с.

105. Пяткова, Е.В. Методика моделирования угроз энергетической безопасности с помощью байесовских сетей доверия / Е.В. Пяткова // Современные технологии. Системный анализ. Моделирование. – № 3(39). – 2013. – С. 133-139.

106. Массель, А.Г. Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов / А.Г.

Массель // Труды XX Байкальской Всероссийской конференции. – Иркутск: ИСЭМ СО РАН, 2015. – Т.III. – С. 186-195.

107. Massel, A. Identification of critical objects in reliance on cyber threats in the energy sector / A. Massel, D. Gaskova // Acta Polytechnica Hungarica, 2020. – 17(8). – P. 61-73. DOI: 10.12700/APH.17.8.2020.8.5 (Scopus: 2-s2.0-85091497119).

108. Гаськова, Д.А. Фрактальная стратифицированная модель объектов энергетической инфраструктуры с позиции кибербезопасности / Д.А. Гаськова, А.Г. Массель // «IT&IS'2018» / Труды Конгресса по интеллектуальным системам и информационным технологиям. Том II. ЮФУ. – Таганрог, 2018. – С. 390-394.

109. Gaskova, D. Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security // Proceedings of the VIth International Workshop «Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security (IWCI 2019)». Publisher: Atlantis Press. – 2019. - Irkutsk: MESI SB RAS. – P. 179-183.

110. Гаськова, Д.А. Онтологический инжиниринг анализа угроз кибербезопасности критических инфраструктур / Д.А. Гаськова, А.Г. Массель // Онтология проектирования. – 2019. – Т. 9, № 2 (32). –С. 225-238.

111. Гаськова, Д.А. Выявление критически важных объектов с позиции нарушения кибербезопансоти на примере энергетики // «Информационные технологии в науке, управлении, социальной сфере и медицине» / Сборник научных трудов IV Международной конференции: в 2 частях. Томский политехнический университет. – Томск, 2018. – С. 18-21.

112. Юдин, А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности Smart Grid систем / А. Юдин, Г. Пирогов // Научно-технический сборник «КПИ им. Игоря Сикорского» «Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине». Выпуск 25. – 2013. – С. 88-95.

113. Литвинов, П. Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищённости и оптимизации затрат [Электронный ресурс] // Портал «Мир компьютерной автоматизации». – URL:

http://www.rtsoft.ru/press/23432/imitatsionnoe-modelirovanie-voprosov-informatsionnoy-bezopasnosti-kak-instrument-otsenki-zashchishch/ (дата обращения 15.12.2018).

114. Гаськова, Д.А. Разработка экспертной системы для анализа угроз кибербезопасности в энергетических системах / Д.А. Гаськова, А.Г. Массель // Информационные и математические технологии в науке и управлении. – 2016. – № 1. – С. 113-122.

115. Gaskova, D. Development of expert system for the analysis of cyber security threats in energy systems // Workshop Proceedings «Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security», 2017. – Irkutsk: MESI SB RAS. – P. 75-76.

116. WannaCry в промышленных сетях: работа над ошибками [Электронный ресурс]. – URL: https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/ (дата обращения 11.11.2018).

117. Аналитические статьи компании Positive Technologies. [Электронный ресурс] // Positive Research 2018. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (дата обращения 11.11.2018).

118. Sridhar, S. Cyber-physical system security for the electric power grid / S. Sridhar, A. Hanh, M. Govindarasu // Proc. IEEE, 2012. – Vol. 100. – No. 1. – P. 210-224.

119. Мусина, В.Ф. Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков / В.Ф. Мусина // Труды СПИИРАН, 2013. Выпуск 25. – С. 35-254.

120. Dantu, R. Risk management using behavior based Bayesian networks / R. Dantu, P. Kolan // Intelligence and Security Informatics, 2005. – P. 165-184.

121. Massel, A.G. Scenario approach for analyzing extreme situations in energy from a cybersecu-rity perspective / A.G. Massel, D.A. Gaskova // Industry 4.0, 2018. – Issue 5. Publisher: Scientific Technical Union of Mechanical Engineering “Industry 4.0”. – P. 266-269.

122. Kolosok, I. Cyber Resilience of SCADA at the Level of Energy Facilities / I. Kolosok, E. Korkina // Proceedings of the Vth International workshop «Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security» (IWCI 2018), 2018. – P. 100-105.

123. Массель, Л.В. Экспертная система Advice для выбора управляющих воздействий в ситуационном управлении в энергетике / Л.В. Массель, А.Г. Массель, А.Ю. Мякотина // Информационные и математические технологии в науке и управлении : Труды XX Байкальской Всероссийской конференции, т. III. – Иркутск: ИСЭМ СО РАН, 2015. – С. 132–138.

124. Багрова, Л.А. Опасные техногенные катастрофы в энергетике как факторы экологического риска / Л.А. Багрова, В.А. Боков, А.С. Мазинов // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «География». – 2012. – Т. 25 (64). – № 2. – С. 9-19.

125. Барабанов, А.В. Семь безопасных информационных технологий / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов / под ред. А.С. Маркова. – М.: ДМК Пресс, 2017. – 224 с.

126. Gaskova, D. Analysis of cybersecurity violations in energy sector // Workshop Proceedings «Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security», 2017. – Irkutsk: MESI SB RAS. – P. 22-23.

127. Массель, А.Г. Онтологический инжиниринг энергетических рисков в топливно-энергетическом комплексе / А.Г. Массель, С.А. Александрович, Д.А. Гаськова // Информационные и математические технологии в науке и управлении. – 2020. – № 3 (19). – С. 25-33. DOI: 10.38028/ESI.2020.19.3.003.

128. Гаськова Д.А. Метод определения уровня киберситуационной осведомленности энергетических объектов // Информационные и математические технологии в науке и управлении. 2020. № 4 (20). С. 64-74. DOI: 10.38028/ESI.2020.20.4.006

129. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования [Электронный ресурс] / Р 50.1.028-

2001: Постановление Госстандарта России от 2 июля 2001 года № 256-ст. – URL: http://docs.cntd.ru/document/1200028629 (дата обращения 26.03.2020).

130. Дащенко, Ю. Моделирование угроз в условиях методической неопределенности [Электронный ресурс] / Kaspersky Lab ICS CERT. – URL: https://ics-cert.kaspersky.ru/media/KL-ICS-CERT-Model-ugroz.pdf (дата обращения: 13.02.2019).

131. Дорофеев, А.В. Менеджмент информационной безопасности: основные концепции / А.В. Дорофеев, А.С. Марков // Вопросы кибербезопасности. – 2014. – № 1(2). – С.67-73.

132. Gaskova, D. Methods to Analyze Critical Facilities in Energy with Regard to Cyber Threats / D. Gaskova, A. Massel // Proceedings of the Vth International workshop «Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security» (IWCI 2018). Publisher: Atlantis Press. – 2018. – P. – 62-67.

133. Колосок, Н.И. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы / Н.И. Колосок, Л.А. Гурина // Информационные и математические технологии в науке и управлении, 2019. – № 2 (14). – С. 40-51.

134. Банк данных угроз безопасности информации [Электронный ресурс] // ФАУ «ГНИИИ ПТЗИ ФСТЭК России. – URL: https://bdu.fstec.ru/ дата обращения: 13.02.2019).

135. Международная база данных уязвимостей Common Vulnerabilities and Exposures (CVE) [Электронный ресурс]. – URL: https://cve.mitre.org (дата обращения: 15.03.2019).

136. Марков, А.С. Опыт выявления уязвимостей в зарубежных программных продуктах / А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. – 2013. – № 1 (1). – С. 42-48.

137. Gaskova, D. Semantic modeling of cyber threats in the energy sector using Dynamic Cognitive Maps and Bayesian Belief Network / D. Gaskova, A. Massel // Proceedings of the 7th Scientific Conference on Information Technologies for Intelligent

Decision Making Support (ITIDS 2019). Publisher: Atlantis Press. – 2019. – P. 326-329. DOI: 10.2991/itids-19.2019.58.

138. Массель, Л.В. Технологии и инструментальные средства интеллектуальной поддержки принятия решений в экстремальных ситуациях в энергетике / Л.В. Массель, А.Г. Массель // Вычислительные технологии. – 2013. – Т.18, специальный выпуск. – С. 37-44.

139. Massel, A.G. Application of risk-based approach to identify critical facilities in the energy sector with regard to cyber threats / A.G. Massel, D.A. Gaskova // Proceedings of the 19th International Workshop on Computer Science and Information Technologies. Germany, Baden-Baden. Publisher Ufa: USATU. – 2017. – Vol. 1 – P. 159-163.

140. Массель, А.Г. Кибербезопасность в критических инфраструктурах (на примере энергетики) / А.Г. Массель, Л.В. Массель, Д.А. Гаськова // Безопасные информационные технологии (БИТ-2016) / Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева, 2016. – С. 197-199.

141. Массель, Л.В. Интеллектуальные вычисления в исследованиях

направлений развития энергетики / Л.В. Массель, А.Г. Массель // Известия Томского политехнического университета. Управление, вычислительная техника и информатика. – 2012. – Т.321. – №5. С. 135–140.

142. Гаськова, Д.А. Реализация экспертной системы для анализа угроз кибербезопасности в энергетических системах / Д.А. Гаськова // «Системные исследования в энергетике» / Труды молодых ученых ИСЭМ СО РАН, Вып. 46. – Иркутск: ИСЭМ СО РАН, 2016. – С.155-161.

143. Overview. Drools [Электронный ресурс]. – URL: https://www.drools.org/ (дата обращения: 19.01.2019).

144. Gaskova, D.A. Technology of the Intelligent System Application for Cyber Threat Analysis at Energy Facilities / , D.A. Gaskova, A.G. Massel // Proceedings of the 21th international workshop on computer science and information technologies (CSIT’2019), Austria, Vienna, Publisher: Atlantis Press. – 2019. P. 263-266.

145. 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.

146. Воропай, Н.И. Надежность систем электроснабжения. / Новосибирск: «Наука», 2015. 208 с. ISBN 978-5-02-019201-0.

147. Lee, E.A. Introduction to Embedded Systems - A Cyber-Physical Systems Approach. 2 edition. // E.A. Lee, S.A. Seshia. Berkeley, CA, 2015.

148. Cardenas, A.A. Research challenges for the security of control systems / A.A. Cardenas, S. Amin, S.S. Sastry // Proceedings of the 3rd Conference on Hot Topics in Security. – 2008. P. 6:1–6:6.

149. Poovendran, R. Cyber-physical systems: Close encounters between two parallel worlds [Point of View] / R. Poovendran // Proceedings of the IEEE. – 2010. – Vol. 98(8). – P. 1363-1366.

150. Алиев, Т.И. Сети ЭВМ и телекоммуникации / Т.И. Алиев. Санкт-Петербург: СПбГУ ИТМО, 2011. – 400 с.

151. Глоссарий Лаборатория Касперского [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/glossary/ (дата обращения: 19.01.2019).

152. Словарь терминов по информационной безопасности [Электронный ресурс] // Отраслевой портал IB-BANK.RU. – URL: https://glossary.ib-bank.ru/ (дата обращения: 10.03.2020).

153. Краткий словарь сетевых терминов компании НПО РАПИРА [Электронный ресурс]. – URL: https://www.nporapira.ru/sections/4/articles/32 (дата обращения: 10.03.2020).

154. The IEEE 802.1 Working Group [Электронный ресурс]. – URL: https://1.ieee802.org/security/802-1ae/ (дата обращения: 10.03.2020).

155. Information Technology Laboratory Computer Security Resource Center [Электронный ресурс] // NIST Glossary. – URL: https://csrc.nist.gov/glossary (дата обращения: 10.03.2020).

156. Internet Corporation for Assigned Names and Numbers (ICANN). оф. сайт [Электронный ресурс]. – URL: https://www.icann.org/resources/pages/dnssec-2012-02-25-en (дата обращения: 10.03.2020).

157. Песочница Positive Technologies [Электронный ресурс]. – URL: https://www.anti-malware.ru/ (дата обращения: 10.03.2020).

158. Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты /Методический документ: ИТ.СДЗ.ПР4.ПЗ ФСТЭК от 30 декабря 2013 г.

159. MDN web docs Mozila [Электронный ресурс]. – URL: https://developer.mozilla.org/ru/docs/Web/HTTP/CSP (дата обращения: 10.03.2020).

160. Дрозжин, А. Почему электронные письма легко подделать // Kaspersky daily [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/36c3-fake-emails/26277/ (дата обращения: 10.03.2020).

161. Менеджмент процессов: [пер. с нем.] / Под ред. Й. Беккера, Л. Вилкова, В. Таратухина, М. Кугелера, М. Роземанна. – М.: Эксмо, 2010. – 384 с. – (Качественный менеджмент).

162. Технологический процесс [Электронный ресурс] // Большой энциклопедический политехнический словарь. – URL: 9420-ТЕХНОЛОГИЧЕСКИЙ%20ПРОЦЕСС (дата обращения: 10.07.2020).

Приложение А. Примеры онтологий

Рисунок 4.1 – Онтология угроз

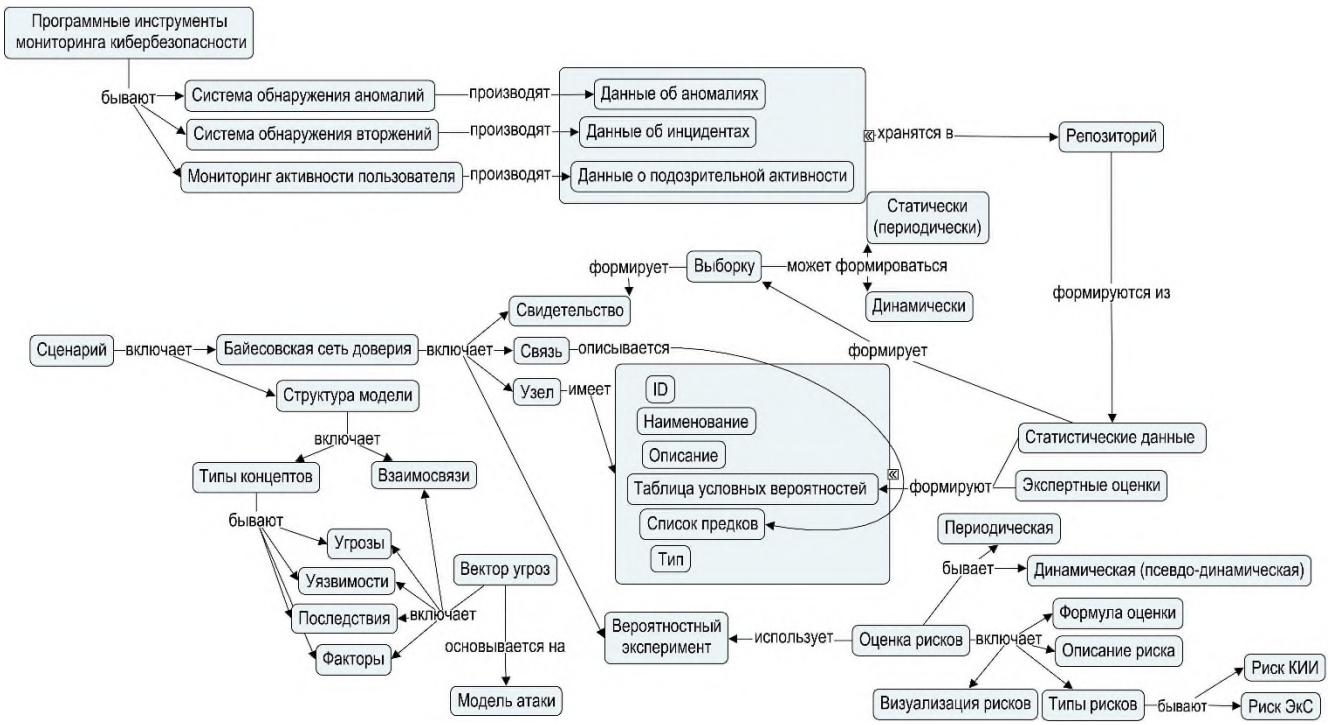

Рисунок 4.2 – Онтология сценария экстремальной ситуации в энергетике, вызванной киберугрозами

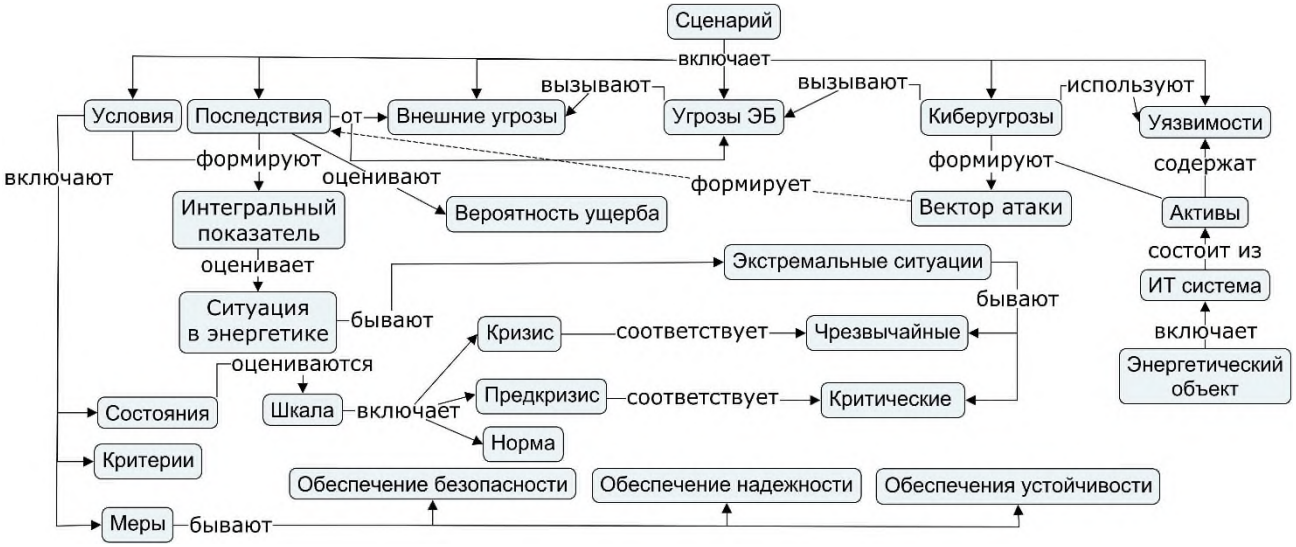

Рисунок 4.3 – Онтология причинно-следственных связей экстремальной ситуации, вызванной киберугрозами

Рисунок 4.4 – Онтология рисков кибербезопасности в энергетике

Приложение Б. Свидетельства о регистрации программ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019666927

Редактор векторов кибератак (Cyber Attack Vector)

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук (RU)***

Авторы: ***Гаськова Дарья Александровна (RU), Массель Алексей Геннадьевич (RU), Мамедов Тимур Габилович (RU)***

Заявка № **2019665661**
Дата поступления **02 декабря 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***17 декабря 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019662462

Анализ угроз энергетической безопасности (ThreatNet)

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук (RU)***

Авторы: ***Массель Алексей Геннадьевич (RU),***
Гаськова Дарья Александровна (RU)

Заявка № **2019661408**
Дата поступления **17 сентября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***25 сентября 2019 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019662461

Качественный анализ рисков (RiskMap)

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук (RU)***

Автор: ***Гаськова Дарья Александровна (RU)***

Заявка № **2019661409**
Дата поступления **17 сентября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***25 сентября 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Приложение В. Акт о внедрении

Рэспубліканскае навукова-вытворчае
унітарнае прадпрыемства
«ІНСТЫТУТ ЭНЕРГЕТЫКІ
НАЦЫЯНАЛЬНАЙ АКАДЭМІІ
НАВУК БЕЛАРУСІ»
вул. Акадэмічная, 15, корп.2, 220072, г. Мінск
тэл. (017) 257 64 72, факс (017) 378 15 54
e-mail: ipe@bas-net.by
Р р BY22 AKBB 3012 0818 1001 8550 0000 у
ААТ "АСБ Беларусбанк", г. Мінск
БІК AKBBBY2X
УНП 101292548 АКПА 37465805

Республиканское научно-производственное
унитарное предприятие
«ИНСТИТУТ ЭНЕРГЕТИКИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК БЕЛАРУСИ»
ул. Академическая, 15, корп. 2, 220072, г.Минск
тел. (017) 257 64 72, факс (017) 378 15 54
e-mail: ipe@bas-net.by
Р/с BY22 AKBB 3012 0818 1001 8550 0000 в
ОАО "АСБ Беларусбанк", г. Минск
БИК AKBBBY2X
УНП 101292548 ОКПО 37465805

16.03.2021 № 122-205

СПРАВКА О ВНЕДРЕНИИ

Настоящим подтверждается, что результаты кандидатской диссертации Гаськовой Дарьи Александровны «Методы, модели и комплекс программ анализа киберситуационной осведомленности энергетических объектов» использовались при выполнении Международного проекта (Беларусь, Россия), по гранту Белорусского республиканского фонда фундаментальных исследований – проект Бел_мол_а-РФФИ №19-57-04003 «Методы оценки энергетических рисков и их влияния на энергетическую безопасность на основе интеллектуальных информационных технологий» (2019-2021), а именно:

1) методический подход к анализу киберситуационной осведомленности энергетических объектов с использованием семантического моделирования (онтологического и вероятностного);

2) технология анализа киберситуационной осведомленности энергетического объекта с использованием разработанного методического подхода, отличающаяся применением интеллектуального программного комплекса и реализованных прототипов экспертной системы, компонента байесовских сетей доверия и компонента визуальной оценки рисков.

Вышеперечисленные результаты диссертационного исследования Гаськовой Дарьи Александровны (в т.ч. инструментальные средства анализа киберситуационной осведомленности энергетических объектов)

приняты к использованию в деятельности Института энергетики Национальной академии наук Беларуси (ИЭ НАНБ).

Директор Института энергетики
Национальной академии наук Беларуси,
к. ф.-м. н. А.А. Бринь

Научный руководитель Института энергетики
Национальной академии наук Беларуси,
д. т. н., академик А.А. Михалевич