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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Иркутск – 2021

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук (ИСЭМ СО РАН)

Научный руководитель: кандидат технических наук
Массель Алексей Геннадьевич

Официальные оппоненты:
Ходашинский Илья Александрович
доктор технических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования Томский государственный университет систем управления и радиоэлектроники, кафедра комплексной информационной безопасности электронно-вычислительных систем, профессор

Булатов Юрий Николаевич
кандидат технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Братский государственный университет», кафедра электроэнергетики и электротехники, заведующий кафедрой

Ведущая организация:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет путей сообщения», г. Иркутск

Защита диссертации состоится «29» июня 2021 г. в 9.00 на заседании диссертационного совета Д003.017.01, созданного на базе Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук (ИСЭМ СО РАН) по адресу: 664033, г. Иркутск, ул. Лермонтова, д. 130, к. 355.

С диссертацией можно ознакомиться в библиотеке ИСЭМ СО РАН по адресу: 664033, г. Иркутск, ул. Лермонтова, к. 407 и на сайте ИСЭМ СО РАН https://isem.irk.ru/dissert/case/DIS-2021-5/.

Отзывы на автореферат в двух экземплярах с подписью составителя, заверенные печатью организации, просим направлять по адресу: 664033, г. Иркутск, ул. Лермонтова, д. 130, на имя ученого секретаря диссертационного совета.

Автореферат разослан «___» _____2021 г.

Ученый секретарь диссертационного совета Д003.017.01,
доктор технических наук, профессор

Клер
Александр Матвеевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность диссертационной работы определяется двумя основными факторами. Первый фактор обусловлен необходимостью рассмотрения энергетики как критической инфраструктуры, нарушение функционирования или разрушение которой приводит к экстремальным ситуациям (ЭкС), 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 г. «О безопасности критической информационной инфраструктуры Российской Федерации» и принятием в 2019 году Доктрины энергетической безопасности Российской Федерации. Несмотря на то, что Концепция стратегии кибербезопасности Российской Федерации до сих пор не принята, противодействие киберугрозам является одним из приоритетных направлений Государственной программы «Научно-технологическое развитие Российской Федерации» на 2019-2030 годы[2].

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[3].

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 (ЭО). 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 ИИ в области кибербезопасности, направленная на

[1] Проект «Цифровая энергетика» сформирован Минэнерго РФ в рамках национальной программы «Цифровая экономика Российской Федерации», утвержденной Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р

[2] Утвержденной Постановлением Правительства РФ от 29 марта 2019 г. № 377

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

повышение осведомленности о возможных ситуациях нарушений кибербезопасности и автоматическое обнаружение киберугроз[4]. В исследованиях КСО, в том числе, используют такие методы ИИ, как семантическое моделирование, байесовские сети доверия (БСД), технология экспертных систем, когнитивная графика.

Под термином «Киберситуационная осведомленность энергетических объектов» будем понимать осведомленность о состоянии киберсреды ЭО, включающую информацию: о критических уязвимостях ЭО с точки зрения кибербезопасности; о киберугрозах, использующих эти критические уязвимости; о техногенных угрозах ЭБ, 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» 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.

Степень изученности проблемы. Исследования критических инфраструктур[5] 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

[4] Frank U., Brynielsson J. Cyber Situational Awareness – A systematic review of literature // Computer Security. 2014. Vol. 46. P. 18–31. DOI: 10.1016/j.cose.2014.06.008

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

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., Папков Б.В. 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) энергетических объектов.

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, включающего:

• фрактальную стратифицированную модель (ФС-модель) [6] структурирования знаний в области кибербезопасности энергетической инфраструктуры;

[6] Массель Л.В. Фрактальный подход к структурированию знаний и примеры его применения // Онтология проектирования. Самара - Изд-во: Предприятие «Новая техника» Том 6, № 2 (20). 2016. – С. 149-161.

• 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 (2019-2021).

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 (2019-2021) 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 — СРТ2020», 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 статья, 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выполняемой работы, формулируется цель исследования, а также ставятся задачи, необходимые для ее достижения. Формулируются научная новизна и основные положения, выносимые на защиту, приводится общая характеристика работы.

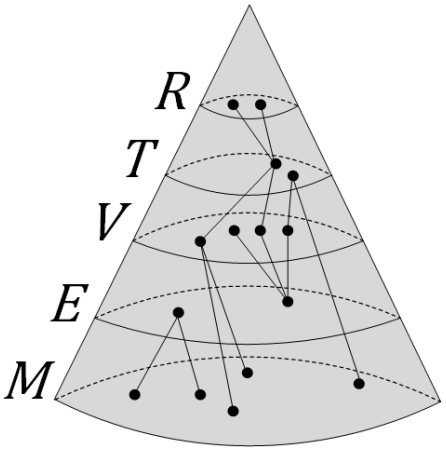
В первой главе работы выполнен анализ предметной области, которая охватывает проблемы обеспечения энергетической безопасности в условиях цифровой трансформации энергетики и появления нового типа угроз ЭБ – киберугроз. Рассматривается влияние киберугроз на возникновение ЭкС в энергетике и важность киберситуационной осведомленности в условиях появления нового типа рисков в киберсреде. Приводятся описания базовых методов и технологий, используемых в диссертационном исследовании.

В выводах по главе ставится проблема анализа киберситуационной осведомленности энергетических объектов в условиях внедрения новых информационно-коммуникационных технологий.

Во второй главе предложен подход к анализу киберситуационной осведомленности энергетических объектов, как синтез исследований кибербезопасности и ситуационной осведомленности. Представлен предлагаемый автором ***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.

Предложенная ФС-модель структурирования знаний в области кибербезопасности энергетической инфраструктуры представлена на рис. 1.



Типы отображений:
$F_M^E: E \to M$ – 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.

Рис. 1. ФС-модель структурирования знаний в области кибербезопасности энергетической инфраструктуры

Информационное пространство данных и знаний области кибербезопасности энергетической инфраструктуры представлено как:

$$D = \{M, E, V, T, R\}, \quad (1)$$

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

Структурирование знаний в области кибербезопасности энергетической инфраструктуры выполнено с применением фрактального подхода, позволяющего формально описать и представить любую информационную технологию как совокупность информационных слоев и их отображений. Слои представляют собой данные и знания предметной области, а типы отображений из слоя в слой описывают связи между слоями.

Для исследования энергетического сектора как критической инфраструктуры, включающей критическую информационную инфраструктуру, с позиции энергетической и кибернетической безопасности выполнен ***онтологический инжиниринг***[7] с использованием фрактального подхода. В результате разработана система онтологий (рис. 2) киберситуационной осведомленности энергетических объектов.

Разработаны подсистемы онтологий для решения следующих задач:

• анализ киберугроз энергетической инфраструктуры;

• моделирование сценариев ЭкС в энергетике, вызванных реализацией киберугроз;

• оценка рисков наступления ЭкС в энергетике, вызванных реализацией киберугроз на активы, и выработка рекомендаций.

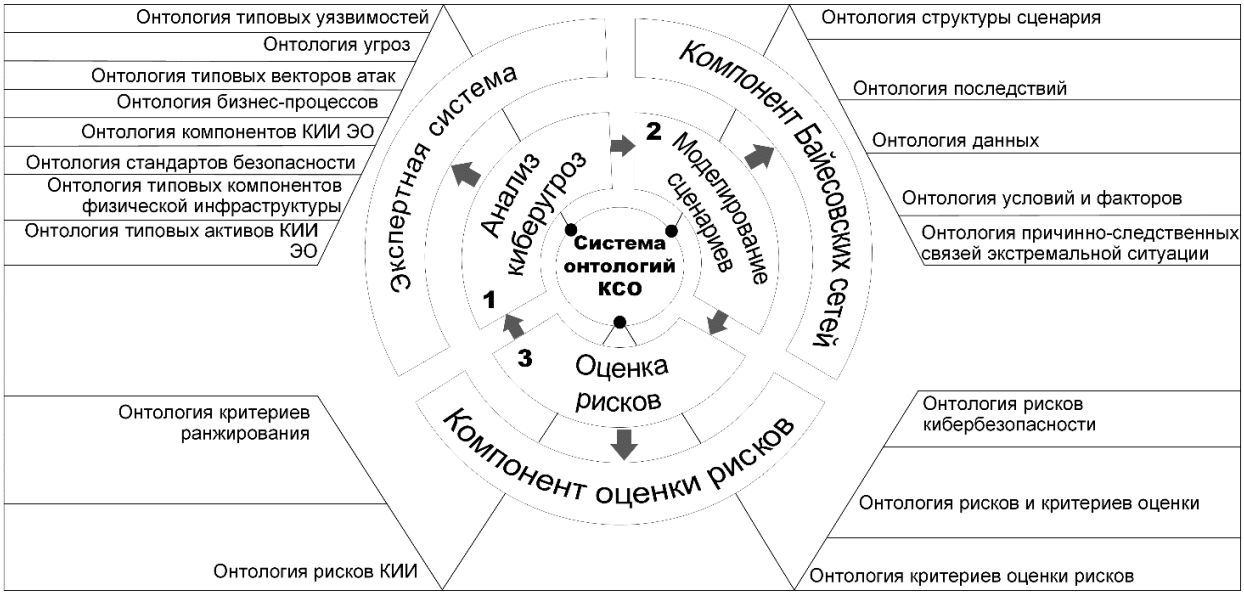


Рис. 2. Система онтологий КСО энергетических объектов

[7] Гаврилова Т.А. Кудрявцев Д.В., Муромцев Д.И. Инженерия знаний. Модели и методы. Учебник // — СПб.: Издательство «Лань», 2016. –324 с.

На основе структурирования знаний с использованием предложенной ФС-модели и системы онтологий разработана ***модель сценариев ЭкС в энергетике, вызванных киберугрозами***.

В общем виде модель M описывается как:

$$M = \{A, V, T, W, C, F\}, \quad (2)$$

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

$$A = \{A^{\mathrm{E}}, A^{\mathrm{I}}\}, \quad (3)$$

где A^{E} – множество активов 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, $i = \overline{1, |A^{\mathrm{E}}|}$:

$$V_i = \{v_{i1}, v_{i2} \ \dots, v_{ih}\}, V_i \subset V; \quad (4)$$

T – множество киберугроз активов ЛВС:

$$T = \{t_1, t_2 \ \dots, t_k\}, \quad (5)$$

W – множество техногенных угроз ЭБ, вызванных киберугрозами T:

$$W = \{w_1, w_2, \dots, w_m\}; \quad (6)$$

C – множество последствий реализации угроз:

$$C = \{c_1, c_2, \dots, c_z\}; \quad (7)$$

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

$$F = \{F_A^V, F_V^T, F_W^T, F_W^C\}, \quad (8)$$

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:

$$G = (N, U; q), \quad (9)$$

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:

$$X_i \in \{X^V \cup X^T \cup X^W \cup X^C\}, \quad (10)$$

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:

$$q: N \to B, \tag{11}$$

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 виде таблиц условных вероятностей (ТУВ)).

Для определения уровня КСО предлагается ***численный метод определения уровня КСО энергетического объекта***, основанный на использовании описанной выше модели. Алгоритм, представленный на рис 3 а, реализует этот численный метод. Блоки 4-7 представлены детализированным алгоритмом (рис. 3 б).

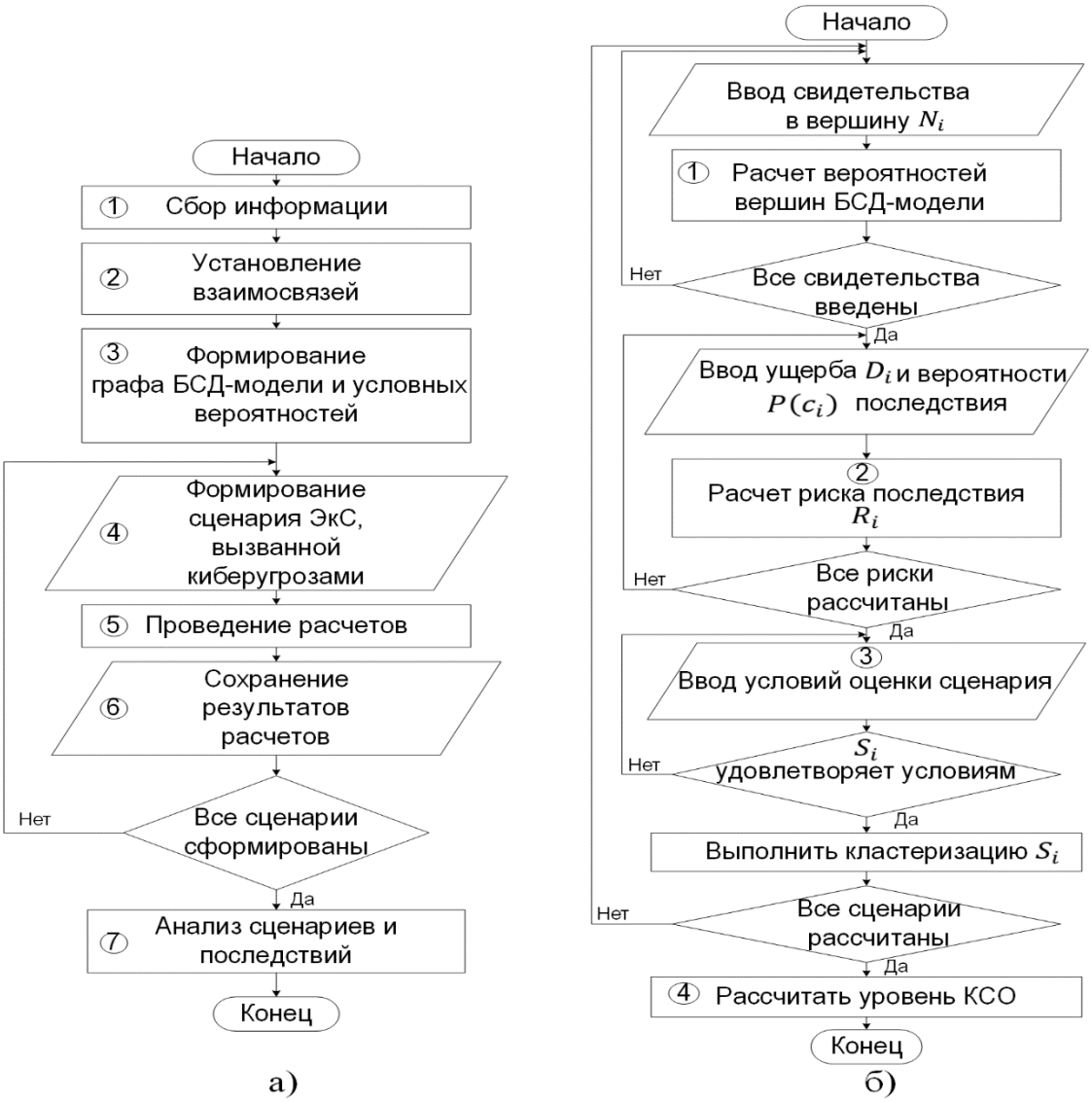


Рис. 3. а) алгоритм определения уровня КСО энергетического объекта, б) детализированный алгоритм блоков 4-7 алгоритма определения уровня КСО

Комментарий к рис. 3 а. Блоки 1-2 соответствуют сбору информации, который заключается в определении множеств активов A по формуле (3), критических уязвимостей V (4), киберугроз T (5), W – техногенных угроз ЭБ (6), C – последствий реализации угроз (7), установлении взаимосвязей F (8).

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:

$$P(X) = (P_1(X), P_2(X), \dots, P_n(X)),$$
$$P_i(X) = P(X_i|pa(X_i)) \quad (12)$$

где X_i введено в (10), $pa(X_i)$ – 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 дискретных случайных величин, являющихся свидетельствами E. Каждое свидетельство 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:

$$R = \{T, V, W, C, D\}, \quad (13)$$

где значения T, V, W, C введены ранее в (4-7), D – множество ущербов последствий сценариев.

Комментарий к рис. 3 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:

$$P(X_i|e) = \frac{\sum_{j=1}^{m} P_j(X,e)}{P(e)}, \quad (14)$$

где $P(X_i|e)$ – апостериорная вероятность X_i, e – значения случайных величин, соответствующих E, m – количество оставшихся случайных переменных, в которые не введены свидетельства.

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

$$R_i = P(c_i) \times D_i, \quad (15)$$

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 (14), 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 1.

Таблица 1. Условия оценки сценариев ЭкС, вызванных киберугрозами

Незначительный уровень опасности	Средний уровень опасности	Высокий уровень опасности
$\begin{cases} 0 \le P(\mathrm{c}_i) \times D_i < l_1 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (16)	$\begin{cases} l_1 \le P(\mathrm{c}_i) \times D_i < l_2 \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (17)	$\begin{cases} l_2 \le P(\mathrm{c}_i) \times D_i \\ 0 \le P(\mathrm{c}_i) \le 1 \\ 0 \le D_i \le D^{\mathrm{m}} \end{cases}$ (18)

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:

$$K_s = \{S_{s1}, S_{s2}, \dots, S_{sl}\}, \quad (19)$$

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:

$$L = \frac{\gamma}{2^n - 1}, \quad (20)$$

где L – уровень КСО энергетического объекта, γ – количество рассчитанных сценариев, $2^n - 1$ – общее количество сценариев, где в данном случае $n = |V| + |T| + |W|$. Значения V, T, W введены ранее в (4)-(6).

Для применения модели 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.

1. Методика анализа киберугроз энергетической инфраструктуры включает три этапа:

1.1 Описание энергетического объекта и определение критериев оценки (l_1, l_2, D^{m}).

1.2. Анализ уязвимостей (V) и угроз КИИ объекта (T, W), установление взаимосвязей (F).

1.3. Построение модели сценариев ЭкС в энергетике, вызванных киберугрозами (M), в виде правил «ЕСЛИ-ТО», которые описывают возможные способы нарушения кибербезопасности энергетического объекта.

2. Методика моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз, включает четыре этапа:

2.1. Формирование узлов (N) и их взаимосвязей в графе БСД-модели.

2.2. Определение вероятностных характеристик B_i сценария.

2.3. Проведение вероятностного эксперимента.

2.4. Анализ альтернативных сценариев (S_i).

3. Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры включает четыре основных этапа:

3.1. Описание рисков (R).

3.2. Оценивание рисков (R_i).

3.3. Ранжирование активов КИИ (A) и выработка рекомендаций.

3.4. Определение уровня киберситуационной осведомленности энергетического объекта (L).

Для поддержки предлагаемого методического подхода разработан интеллектуальный программный комплекс для анализа киберситуационной осведомленности ИПК «ОКО», описанный в следующей главе.

В выводах по главе обосновываются преимущества предложенного методического подхода.

В третьей главе описаны разработка интеллектуального программного комплекса для анализа киберситуационной осведомленности ИПК «ОКО», технология применения интеллектуальной системы и методического подхода, а также выполненная реализация основных компонентов ИПК «ОКО» на основе авторских алгоритмов.

Архитектура интеллектуального программного комплекса для анализа киберситуационной осведомленности ИПК «ОКО» представлена на рис. 4 (показана взаимосвязь пользователей и основных компонентов ИПК «ОКО», компоненты обведены пунктиром). Архитектура ИПК «ОКО» логически разделена на три основных компонента: 1) экспертная система «Cyber» для формирования векторов атак на КИИ; 2) компонент байесовских сетей доверия «ThreatNet» для моделирования сценариев нарушения кибербезопасности объекта КИИ и вычисления вероятностей возможных последствий от реализации киберугроз; 3) компонент «RiskMap» для оценки рисков реализации киберугроз, влияющих на наступление ЭкС, реализующий методы когнитивной графики. Интерфейс прототипа компонента «RiskMap» ИПК «ОКО» представлен на рис. 5.

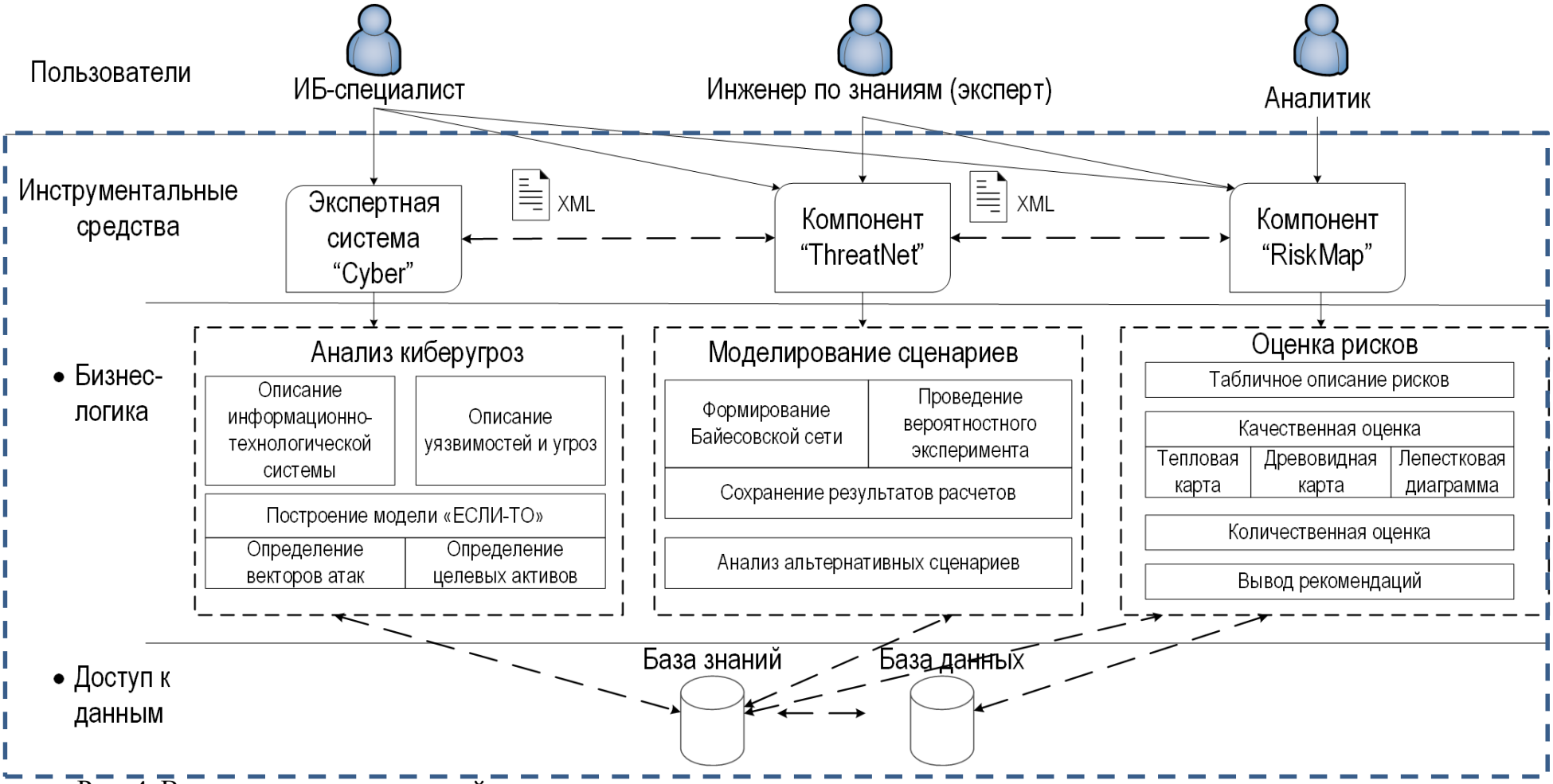


Рис. 4. Взаимосвязь пользователей и основных компонентов интеллектуального программного комплекса для анализа киберситуационной осведомленности ИПК «ОКО»

Рис. 5. Интерфейс прототипа компонента «RiskMap»

Для решения задачи анализа киберситуационной осведомленности энергетического объекта предложена технология, в которой используются предлагаемые методики и разработанный интеллектуальный программный комплекс для анализа киберситуационной осведомленности ИПК «ОКО».

Предлагаемая технология рассчитана на три группы пользователей (таблица 2), позволяет объединить экспертов различных предметных областей и выполнять гибридную оценку рисков киберугроз энергетической инфраструктуры.

Предложенная технология, в сравнении с традиционными подходами к обеспечению безопасности, направлена на определение уязвимостей и киберугроз, реализация которых может вызвать нарушение функционирования физической инфраструктуры энергетического объекта в такой мере, что можно расценивать сценарий нарушения кибербезопасности как экстремальную ситуацию в энергетике. Ниже представлен пример применения технологии.

Таблица 2. Этапы технологии, методики и инструментальные средства

Этапы технологии	**Группы пользователей**	**Методики**	**Инструмен-тальные средства**
Анализ киберугроз	Инженер по безопасности КИИ	Методика анализа киберугроз энергетической инфраструктуры	Экспертная система «Cyber»
Моделирование сценариев	Инженер по безопасности КИИ; Инженер по знаниям (эксперт в области ЭБ)	Методика моделирования сценариев ЭкС в энергетике, вызванных реализацией киберугроз	Компонент БСД «ThreatNet»
Оценка рисков	Инженер по знаниям (эксперт в области ЭБ); Аналитик	Методика оценки рисков нарушения кибербезопасности энергетической инфраструктуры	Компонент оценивания рисков «RiskMap»

Пример. Рассмотрим абстрактную теплоэлектростанцию (ТЭС), содержащую два генерирующих энергоблока. Топология ЛВС рассматриваемого объекта представлена на рис. 6.

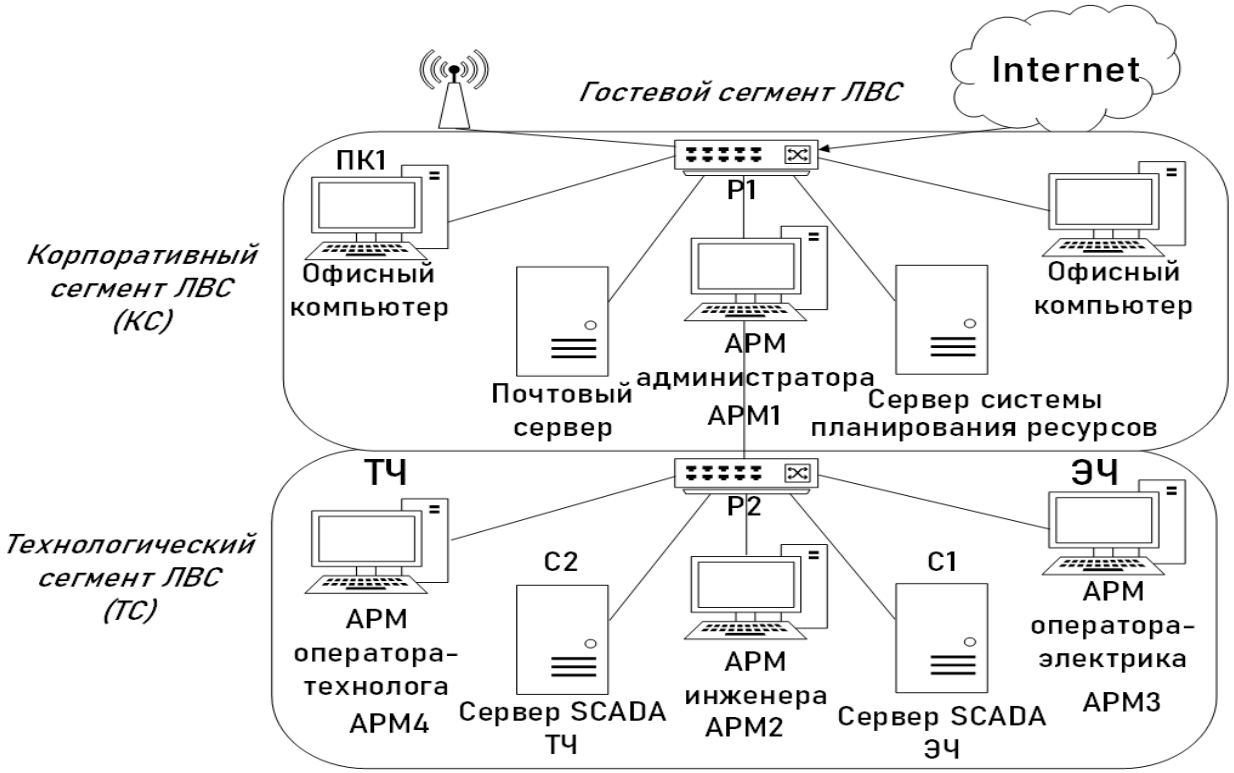


Рис. 6. Топология ЛВС рассматриваемого ТЭС (АРМ – автоматизированное рабочее место, ТЧ – теплотехническая часть, ЭЧ – электротехническая часть)

ЛВС включает ошибки разграничения на гостевой и корпоративный сегменты, а также на корпоративный и технологический сегменты сети, т.е. физически сеть одна, а разграничение осуществлено только на логическом уровне, причем некорректно настроен брандмауэр.

Модель нарушения кибербезопасности рассматриваемой ТЭС включает два вектора атак, описанных совокупностью продукционных правил «ЕСЛИ-ТО», пример такого правила представлен в таблице 3.

Таблица 3. Сценарий «ЕСЛИ-ТО»

ЕСЛИ	**Тип**	**Название**	**ТО**	**Тип**	**Название**
I. Вектор атаки через гостевой WI-FI					
Вектор проникновения 1. Через гостевой WI-FI					
Вектор развития атаки в ТС 1. Использование устаревших версий ПО					
ЕСЛИ	[актив]	SCADA сервер (управляющий сервер)	**ТО**	[актив]	SCADA сервер (управляющий сервер)
	[оператор]	**И**		[оператор]	**И**
	[уязвимость]	Нарушение политики обновлений		[кибер угроза]	Получение адм. доступа к критическому активу
	[оператор]	**И**			
	[уязвимость]	Устаревшая версия ПО, получение контроля			
	[оператор]	**И**			
	[уязвимость]	Ошибки разграничения сети			
II. Вектор атаки через фишинговую рассылку					
Вектор проникновения 2. Через фишинговую рассылку					
Вектор развития атаки в ТС 2. Доступность интерфейсов удаленного доступа					
Атака на целевой актив 1. Удаление данных с управляющего сервера					
Атака на целевой актив 2. Подмена управляющих команд					

На рис. 7 представлена вероятностная модель (на основе БСД), включающая значимые уязвимости и угрозы векторов атак на рассматриваемую ТЭС. Финансовый ущерб от выхода из строя целевых активов вычисляется по формуле (21). Подсчет рисков осуществляется в таблице 4.

$$D_i = O_i \times H_i \times U_i \quad (21)$$

где D_i – ущерб от i-го риска, O_i – потери от i-го риска, H_i – количество часов на устранение ЭкС от i-го риска, U_i – стоимость потерь i-го риска.

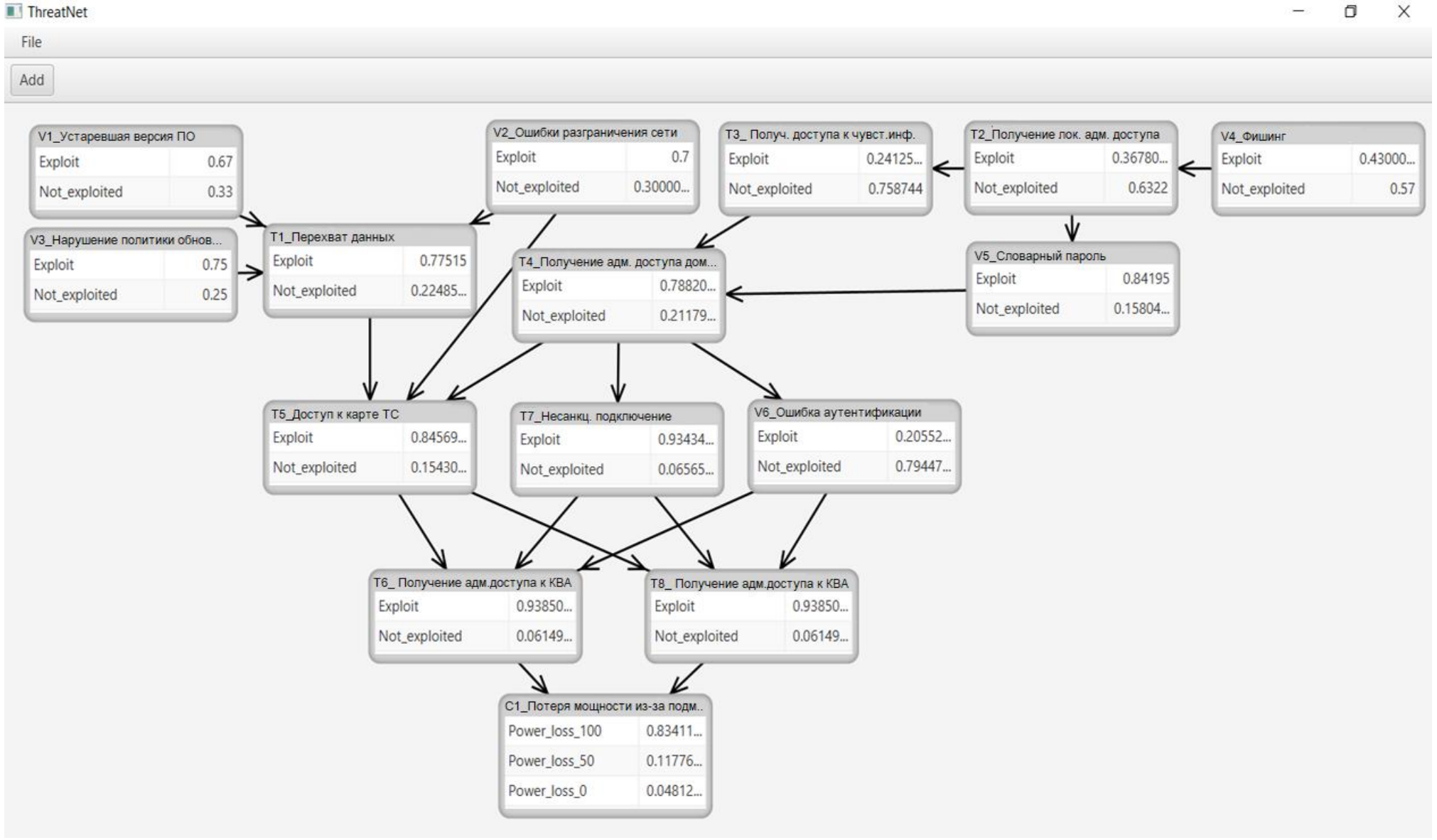


Рис. 7. Вероятностная модель сценариев ЭкС в энергетике, вызванных киберугрозами, рассматриваемого примера ТЭС

Таблица 4. Оценивание рисков последствий реализации киберугроз и уровня КСО

Наименование риска	***T***	***V***	$P(c_i)$,%	D_i,у.е.*	**Оценка**	
					R_i **(15)**	**Качественная**
Потеря 100% мощности	T1, T2, T3, T4, T5, T6, T7, T8	V1, V2, V3, V4, V6	87,0	21	18,3	Высокий
Потеря 50% мощности	T1, T5, T6, T8	V1, V6, V2, V5	11,5	17	1,9	Средний
Потеря 0% мощности	T2, T3, T4, T7, T6, T8	V3, V4, V2, V6	3,0	0	0	Низкий
Уровень КСО (L^{min}), формула (20)			50%			

*у.е. – условная единица оценки ущерба от реализации киберугроз

Рекомендуются организация: физического разграничения ЛВС на КС и ТС с запретом внешнего доступа к ТС в целом, а также создания ДМЗ с сервисами и службами, доступ к которым необходим из ТС; эмулятора среды функционирования программного обеспечения в ДМЗ; защищённых каналов передачи данных; а также использование защищённых протоколов передачи данных и усиления парольной политики.

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

Приведенный пример иллюстрирует применение разработанных технологии и методик.

В заключении приводятся основные результаты работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате выполнения диссертационной работы достигнута 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 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.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных ВАК (из них 1 – в журнале, входящем в перечень ВАК по научной специальности 05.13.18 (технические науки), 1 – в международном журнале, индексируемом в Scopus (Q2)):

1. 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. DOI: 10.18287/2223-9537-2019-9-2-225-238.

2. 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). – Pp. 61-73. DOI: 10.12700/APH.17.8.2020.8.5. Scopus: 2-s2.0-85091497119 (Q2).

Статьи в изданиях, рекомендованных ВАК по прочим специальностям:

3. 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. DOI: 10.21681/2311-3456-2019-2-42-49 (RSCI).

4. 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.

Статьи в зарубежных изданиях, индексируемых в Web of Science:

5. 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.

6. 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. DOI: 10.2991/iwci-18.2018.11.

7. 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.

Статьи в рецензируемых изданиях

8. Гаськова, Д.А. Метод определения уровня киберситуационной осведомлённости энергетических объектов // Информационные и математические технологии в науке и управлении. – 2020. –№ 4 (20). – С. 64-74. DOI: 10.38028/ESI.2020.20.4.006.

9. 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.

10. 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.

11. 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. – Vol. 1. 2017. – P. 159-163. ISBN 978-5-1030-8, ISBN 978-4-4221-1031-5 (v. 1).

12. 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.

13. 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.

Прочие публикации

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

15. Гаськова, Д.А. Реализация экспертной системы для анализа угроз кибербезопасности в энергетических системах // «Системные исследования в энергетике» / Труды молодых ученых ИСЭМ СО РАН. Вып. 46. – Иркутск: ИСЭМ СО РАН. – 2016. – С.155-161.

16. 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, М.: МВТУ им. Баумана, 2016. – С. 197-199.

17. Massel, A.G. Dynamic Fuzzy Cognitive Models as a Means of Visual Analytics and Cognitive Graphics / A.G. Massel, D.A Gaskova // Proceedings of the 21th international workshop on computer science and information technologies (CSIT'2019). Publisher: Atlantis Press. – 2019. – Austria, Vienna. – P. 258-262.

18. 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). Publisher: Atlantis Press. – 2019. – Austria, Vienna. P. 263-266.

19. Gaskova, D. Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security / D. Gaskova // 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. DOI: 10.2991/iwci-19.2019.31.

СВИДЕТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭВМ

1. Гаськова Д.А. Качественный анализ рисков (RiskMap). Свидетельство о государственной регистрации программы для ЭВМ № 2019662461 от 25.09.2019.

2. Массель А.Г., Гаськова Д.А. Анализ угроз энергетической безопасности (ThreatNet). Свидетельство о государственной регистрации программы для ЭВМ № 2019662462 от 25.09.2019.

3. Гаськова Д.А., Массель А.Г., Мамедов Т.Г. Редактор векторов кибератак (Cyber Attack Vector). Свидетельство о государственной регистрации программы для ЭВМ № 2019666927 от 17.12.2019.

Отпечатано в типографии "Дубль Принт"
664046, г. Иркутск, ул. Волжская, 14, оф. 112
Заказ № 2059, тираж 100 экз.