ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 003.017.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ ИНСТИТУТ СИСТЕМ ЭНЕРГЕТИКИ ИМ. Л.А. МЕЛЕНТЬЕВА СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК, МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело №_____

решение диссертационного совета от 29.06.2021 г. № 17

О присуждении Гаськовой Дарье Александровне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «**Методы, модели и комплекс программ анализа киберситуационной осведомленности энергетических объектов**» по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ принята к защите 26 апреля 2021 г. (протокол заседания № 11) диссертационным советом Д 003.017.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, Министерство науки и высшего образования Российской Федерации, 664033, г. Иркутск, ул. Лермонтова, д. 130, совет создан приказом Минобрнауки России № 105/нк от 11.04.2012 г.

Соискатель **Гаськова Дарья Александровна**, 1993 года рождения, в 2015 году с отличием окончила Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет» по специальности 230201 Информационные системы и технологии. В 2019 году окончила очную аспирантуру Федерального государственного бюджетного учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук по направлению подготовки 09.06.01 Информатика и вычислительная техника,

направленность: Математическое моделирование, численные методы и комплексы программ. С 2019 года работает младшим научным сотрудником в отделе Систем искусственного интеллекта в энергетике Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, Министерство науки и высшего образования Российской Федерации.

Диссертация выполнена в отделе Систем искусственного интеллекта в энергетике Федерального государственного бюджетного учреждения науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, Министерство науки и высшего образования Российской Федерации.

Научный руководитель – кандидат технических наук Массель Алексей Геннадьевич, Федеральное государственное бюджетное учреждение науки Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, отдел Систем искусственного интеллекта в энергетике, старший научный сотрудник.

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

дали **положительные** отзывы на диссертацию.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет путей сообщения», г. Иркутск, в своем положительном отзыве, подписанном Кирилловой Татьяной Климентьевной, кандидатом экономических наук, доцентом, заведующей

кафедрой «Информационные системы и защита информации» и утвержденном Хоменко Андреем Павловичем, доктором технических наук, профессором, исполняющим обязанности ректора Федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет путей сообщения», указала, что диссертация является завершенным научным исследованием, удовлетворяющим требованиям ВАК, изложенным в Положении о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 01.10.2018), а её автор Гаськова Дарья Александровна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ.

Соискатель имеет 21 опубликованную работу, в том числе по теме диссертации опубликовано 21 работа, из них 2 публикации в рецензируемых научных изданиях, рекомендованных ВАК (из них 1 – в журнале, входящем в Перечень ВАК по научной специальности 05.13.18, 1 – в международном журнале, индексируемом в Scopus (Q2)), 2 – в изданиях, рекомендованных ВАК по прочим специальностям, 4 – в зарубежных изданиях, индексируемых в WoS, 3 свидетельства о государственной регистрации программ для ЭВМ. В диссертации отсутствует недостоверные сведения об опубликованных соискателем ученой степени работах. Авторский вклад соискателя в опубликованных работах оценивается как основной. У диссертанта отсутствует конфликт интересов с соавторами по публикациям.

Наиболее значимые работы по теме диссертации:

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).

3. 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.

4. 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.

5. 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/itids19.2019.58.

6. 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).

На диссертацию и автореферат поступило 9 отзывов. Все отзывы положительные.

1. Отзыв **Москвичева Владимира Викторовича**, доктора технических наук, профессора, заслуженного деятеля науки Российской Федерации, директора Красноярского филиала Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр информационных и вычислительных технологий». Отзыв содержит *два замечания*: **1)** На стр. 6 указано, что методами и средствами исследования являются, в том числе, методы искусственного интеллекта. Однако, в работе эти методы на основе нейронных сетей не задействованы. Не приведена структура нейронной сети и анализ её выбора. **2)** Автором предложено использование байесовских сетей доверия на основе экспертных оценок вероятностей событий нарушения кибербезопасности. Предложенный метод вычисления КСО требует постоянного обучения системы экспертами разных служб организации. Стоит рассмотреть использование алгоритмов

машинного обучения без учителя, а также моделей глубокого обучения (deep learning) для выявления аномалий в информационных системах.

2. Отзыв **Грибовой Валерии Викторовны**, доктора технических наук, заместителя директора по научной работе Федерального государственного бюджетного учреждения науки Институт автоматики и процессов управления Дальневосточного отделения Российской академии наук. Отзыв содержит *два замечания*: **1)** На стр. 10 рис. 2 «Система онтологий КСО энергетических объектов» представлены онтологии «Онтология рисков и критериев оценки» и «Онтология критериев оценки рисков». Желательны пояснения в чем отличие. **2)** Из рис. 2 также следует, что компоненты интеллектуального программного комплекса реализованы на основе онтологического инжиниринга и представленной системы онтологий, однако в явном виде не указан язык представления разработанных онтологий.

3. Отзыв **Зориной Татьяны Геннадьевны**, доктора экономических наук, доцента, заведующей сектором «Экономика энергетики» Республиканского научно-производственного унитарного предприятия «Институт энергетики национальной академии наук Беларуси». Отзыв содержит *1 замечание* – выбранный пример оценивания рисков последствий реализации киберугроз и уровня КСО (таблица 4 автореферата) недостаточно информативен, т.к. рассматривает различные риски для разных векторов кибератак. Желательно было бы рассмотреть все комбинации рисков и угроз или обосновать выбранные для анализа варианты.

4. Отзыв **Маркова Алексея Сергеевича**, доктора технических наук, старшего научного сотрудника, президента Акционерного общества «Эшелон». Отзыв содержит *три замечания*: **1)** Автор защищает оригинальную математическую (вероятностную) модель, но в автореферате не в полной мере приводит характеристики её адекватности. 2) В автореферате при описании формулы (21) не совсем понятно ущерб D_i и потери O_i касаются угроз, кибератак или инцидентов? Без этого пояснения, на наш взгляд, возникает кажущийся эффект тавтологии (ущерб рассчитывается от риска, а риск оценивается от ущерба). **3)** На наш взгляд, в автореферате (например, на рис. 2.) автор весьма лаконично описал связь

уязвимостей и угроз кибербезопасности с известными таксономиями и каталогами, например, с БДУ ФСТЭК России.

5. Отзыв **Таратухина Виктора Владимировича**, кандидата технических наук, доктора философии (PhD in Computer Science and Engineering), профессора, профессора Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики». Отзыв содержит *1 замечание* – из автореферата не ясно как организуется взаимодействие специалиста по информационной безопасности, эксперта в области энергетической безопасности и аналитика. Так, на стр. 18 описаны этапы технологии, группы пользователей разработанных инструментальных средств, методики и компоненты предложенного интеллектуального программного комплекса, однако само взаимодействие не описано.

6. Отзыв **Мещерякова Романа Валерьевича**, доктора технических наук, профессора, главного научного сотрудника Лаборатории 80 киберфизических систем Федерального государственного бюджетного учреждения науки Институт проблем управления им. В. А. Трапезникова Российской академии наук, Исхакова Андрея Юнусовича, кандидата технических наук, старшего научного сотрудника Лаборатории 80 киберфизических систем Федерального государственного бюджетного учреждения науки Институт проблем управления им. В. А. Трапезникова Российской академии наук. Отзыв содержит *2 замечания:* **1)** Из приведенных методики анализа киберугроз энергетической инфраструктуры на стр. 15 и описания примера на стр. 19 неясно, как строятся вектора атак. Используется общепримененимая известная методика или модель, либо вектора атак строятся экспертами на основе их личного опыта? **2)** Несмотря на выделение множества активов киберсреды в модели сценариев ЭкС в энергетике, вызванных киберугрозами (стр. 11), в явном виде не освещена проблема безопасности Интернета вещей на энергетических объектах.

7. Отзыв **Нафисы Исламовны Юсуповой**, доктора технических наук, профессора, декана факультета информатики и робототехники, заведующий кафедрой вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего

образования «Уфимский государственный авиационный технический университет», **Натальи Михайловны Шерыхалиной**, доктора технических наук, профессора кафедры вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет». Отзыв содержит *2 замечания:* **1)** Из автореферата неясно, как обоснован выбор онтологического инжиниринга для исследования энергетического сектора. **2)** В автореферате не приведена количественная оценка эффективности разработанных моделей и методов.

8. Отзыв **Бухарова Дмитрия Сергеевича**, кандидата технических наук, заместителя начальника службы автоматизированных систем диспетчерского управления – начальника отдела внедрения и сопровождения Филиала акционерного общества «Системный оператор Единой энергетической системы» «Региональное диспетчерское управление энергосистемы Иркутской области». *Замечаний нет.*

9. Отзыв **Загорулько Юрия Алексеевича**, кандидата технических наук, заведующего лабораторией искусственного интеллекта Федерального государственного бюджетного учреждения науки Институт систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук. Отзыв содержит *1 замечание* – Во второй главе в первую очередь описаны модели структурирования знаний: фрактальная стратифицированная модель, система онтологий. Указано, что подсистемы онтологий направлены на решение трех задач анализа киберситуационной осведомленности энергетических объектов, однако не представлена онтология задач.

На все замечания диссертантом даны исчерпывающие ответы.

Выбор официальных оппонентов и ведущей организации обосновывается сферой их научных интересов и исследований и компетентностью в областях математического и компьютерного моделирования, информационной безопасности и электроэнергетических систем, что подтверждается научными публикациями официальных оппонентов и сотрудников ведущей организации. Они, безусловно, являются специалистами по теме защищаемой диссертации и способны определить её научную и практическую ценность.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **разработана** методика анализа киберситуационной осведомленности об энергетических объектах, базирующаяся на оригинальных моделях и численном методе определения уровня киберситуационной осведомленности об энергетическом объекте, основанном на использовании вероятностной модели сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз, и включающем расчет рисков каждого сценария в отдельности, кластеризацию рисков последствий и определение уровня киберситуационной осведомленности о рассматриваемом объекте;

- **предложен** методический подход к анализу киберситуационной осведомленности об энергетических объектах, включающий модели структурирования знаний (фрактальная стратифицированная модель, система онтологий), вероятностную модель сценариев экстремальных ситуаций в энергетике, вызванных киберугрозами, численный метод определения уровня киберситуационной осведомленности об энергетических объектах, методику анализа киберситуационной осведомленности об энергетических объектах;

-**доказана** применимость разработанных автором вероятностной модели, численного метода и интеллектуального программного комплекса для решения задачи анализа киберситуационной осведомленности об энергетических объектах;

- **введено** определение киберситуационной осведомленности об энергетических объектах, сформулированное на основе анализа особенностей данных объектов с позиции кибернетической и энергетической безопасности.

Теоретическая значимость исследования обоснована тем, что:

доказана применимость методики анализа киберситуационной осведомленности об энергетических объектах в исследованиях энергетической безопасности;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы методы искусственного интеллекта, математический аппарат байесовских сетей доверия, методы системного анализа, методы

теории графов, методы семантического моделирования и визуальной аналитики, методы когнитивной графики;

- **изложены** идеи комплексного подхода к анализу киберситуационной осведомленности об энергетических объектах, основанного на интеграции математического и семантического моделирования, в условиях цифровой трансформации энергетики, и включающего анализ киберугроз энергетической инфраструктуры, моделирование сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз и оценку рисков последствий такой реализации;

- **раскрыты** недостатки существующих методов анализа угроз кибернетической безопасности энергетических объектов и обоснована необходимость разработки нового подхода с использованием методов киберситуационной осведомленности;

- **изучено** и проанализировано современное состояние проблемы анализа киберугроз критической информационной инфраструктуры энергетических объектов;

- **проведены модернизация** и интеграция ранее предложенных методик моделирования угроз энергетической безопасности с помощью байесовских сетей доверия и анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов для решения новой задачи анализа киберситуационной осведомленности об энергетических объектах, возникшей в ходе продвижения концепции цифровой трансформации экономики в целом и энергетики в частности.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- **разработаны и внедрены** методический подход, технология и интеллектуальный программный комплекс анализа киберситуационной осведомленности об энергетическом объекте в Институте энергетики Национальной академии наук Беларуси; отдельные результаты исследований использовались при выполнении проектов по государственному заданию IV.35.1.3 программы фундаментальных исследований СО РАН, рег. № 01201361373 (2013-2016 гг.), III.17.2.1 программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310444-2, а также 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), в том числе под руководством соискателя проект РФФИ № 18-37-00271 мол_а (2018-2020).

- **определены** области практического применения разработанных моделей, методов и интеллектуального программного комплекса, которые могут быть полезны при совершенствовании используемого программно-технического комплекса эксплуатируемых автоматизированных систем управления, подготовке методических материалов, планов и программ проведения тренировок, деловых игр персонала.

- **созданы** численный метод и интеллектуальный программный комплекс для анализа киберситуационной осведомленности об энергетических объектах, направленные на дальнейшее формирование практических рекомендаций по повышению кибербезопасности;

- **представлены** научно-методические результаты, имеющие прикладное значение и позволяющие повысить осведомленность о состоянии информационно-коммуникационной инфраструктуры энергетических объектов.

Оценка достоверности результатов исследования выявила:

- **для экспериментальных работ** результаты получены с применением современных достижений в области искусственного интеллекта с учетом неполноты данных и отсутствия статистической информации;

- **теория** опирается на фундаментальные работы отечественных и зарубежных авторов в области математического и семантического моделирования, структурирования знаний и киберситуационной осведомленности;

- **идея базируется** на обобщении передового опыта и необходимости создания методов и программного инструментария для анализа киберситуационной осведомленности о критической информационной инфраструктуре, позволяющих прогнозировать последствия реализации нового типа угроз энергетической безопасности – киберугроз.

- **использованы** зарубежная и российская научная литература, ГОСТы, стандарты и методические рекомендации, информация Интернет-ресурсов, отчеты и аналитические статьи профильных организаций;

- **установлено**, что полученные диссертантом результаты практических исследований подтверждаются непротиворечивостью исходной теоретической базы, логикой исследования, соответствием машинной реализации формальной модели, экспертной оценкой специалистов на основе соблюдения принципа «здравого смысла»;

- **использованы** апробированная методика анализа киберситуационной осведомленности об энергетических объектах, включающая методику анализа киберугроз энергетической инфраструктуры, базирующуюся на технологии экспертных систем; методику моделирования сценариев экстремальных ситуаций в энергетике, вызванных реализацией киберугроз, поддерживаемой аппаратом байесовских сетей доверия; методику оценки рисков нарушения кибербезопасности энергетической инфраструктуры, использующую когнитивную графику.

Личный вклад соискателя состоит в разработке представленных в диссертации теоретических исследований; разработке численного метода, разработке моделей, разработке интеллектуального программного комплекса, разработке методики и технологии анализа киберситуационной осведомленности об энергетических объектах.

Диссертация посвящена решению важной научно-технической задачи анализа киберситуационной осведомленности об энергетических объектах, имеющей важное значение для энергетической безопасности Российской Федерации.

Диссертационным советом сделан вывод о том, что диссертация представляет собой законченную научно-квалификационную работу, соответствующую требованиям и критериям, которым должны отвечать диссертации на соискание ученых степеней, установленным пп. 9-14 «Положения присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года №842 (ред. от 01.10.2018, с изм. от 26.05.2020).

На заседании 29.06.2021 года диссертационный совет принял решение присудить Гаськовой Дарье Александровне ученую степени кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве – 17 человек, из них 7 докторов наук по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ, участвовавших в заседании, из 22 человек, входящих в состав совета, дополнительно введены на разовую защиту – 0 человек, проголосовали: за – 17, против – нет, недействительных бюллетеней – нет.

Председатель диссертационного совета — Николай Иванович Воропай

Ученый секретарь диссертационного совета — Александр Матвеевич Клер

«29» июня 2021 г.