ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА 99.2.038.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 02 ноября 2022 г. № 10

О присуждении Римше Андрею Сергеевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 22 декабря 2021 года, протокол № 11 объединенным диссертационным советом 99.2.038.03, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства науки и высшего образования Российской Федерации, Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства науки и высшего образования Российской Федерации, Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Римша Андрей Сергеевич, 20 октября 1992 года рождения, работает специлистом по защите информации в акционерном обществе "Ачимгаз". В 2019 году окончил освоение программы подготовки научных и научно-педагогических кадров в аспирантуре Федерального государственного автономного образовательного учреждения высшего образования "Тюменский государственный университет".

Диссертация выполнена в Высшей школе искусственного интеллекта Института компьютерных наук и технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Министерство науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, Большаков Александр Афанасьевич, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Высшая школа искусственного интеллекта, профессор.

Оппоненты: 1. Ажмухамедов Искандар Маратович, доктор технических наук, профессор, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный университет», факультет цифровых технологий и кибербезопасности, декан факультета; 2. Аникин Игорь Вячеславович, доктор технических наук, профессор, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», кафедра систем информационной безопасности, заведующий кафедрой, дали положительные отзывы о диссертации.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский государственный технический университет имени Гагарина Ю.А.», г. Саратов, в своем положительном заключении, подписанном Кондратовым Дмитрием Вячеславовичем, д-ром физ.-мат. наук, доц., заведующим кафедрой информационной безопасности автоматизированных систем, утвержденном Остроумовым Игорем Геннадьевичем, д-ром хим. наук, проф., проректором по науке и инновациям, указала, что диссертационная работа «Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур» содержит решение задач, связанных с повышением эффективности ИБ АСУ ТП в условиях деструктивных воздействий на основе использования риск-ориентированного подхода. Значимость результатов диссертационной работы заключается в разработке метода и алгоритмов, позволяющих управлять рисками ИБ АСУ ТП КИ. Предложенные соискателем способ оценки рисков ИБ и алгоритмы их обработки позволили выявить неприемлемые для организации информационные риски и сформировать необходимый перечень мер для их обработки, что позволяет повысить уровень ИБ АСУ ТП КИ. Результаты диссертационной работы также могут быть использованы как для исследовательских задач, так и для проведения анализа рисков на предприятии с последующей их обработкой. Практическая значимость полученных результатов диссертационной работы заключается в определении ущерба от воздействия потенциальных угроз на основе иерархии взаимодействия активов. Также разработанные алгоритмы обработки рисков ИБ позволяют составить экономически эффективный перечень мер в условиях финансовых ограничений для снижения значений оценки рисков до приемлемых величин. Основные результаты диссертационной работы подтверждены публикациями в научной печати и соответствием содержания автореферата основным положениям работы. Диссертационная работа является научно-квалификационной работой и соответствует п.п. 9-14 «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 № 842, а её

автор, Римша Андрей Сергеевич, заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6-Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 20 опубликованных работ, в том числе по теме диссертации 17, из них в рецензируемых научных изданиях, рекомендованных ВАК, – 3, в том числе 3 по искомой специальности, а также: 4 работы в изданиях, индексируемых в международных базах цитирования; 1 результат интеллектуальной деятельности; 9 статей в других научных журналах, сборниках научных статей, трудов и материалах конференций. Из них 4 работы опубликовано соискателем без соавторства. Общий объём авторского вклада в работы (без результатов интеллектуальной собственности) составляет 11,0 печ.л. из общего количества 14,0 печ.л. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах.

Наиболее значительные научные работы по теме диссертации.

Публикации в рецензируемых научных изданиях, рекомендованных ВАК:

1. Римша, А.С. Анализ средств обеспечения информационной безопасности АСУ ТП газодобывающих предприятий / А.С. Римша, К.С. Римша // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 3. – С. 102–121.

2. Римша, А.С. Об одном подходе к формированию перечня мер по защите информации в беспроводных сенсорных сетях газодобывающего предприятия / А.С. Римша, А.Н. Югансон, К.С. Римша // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 2(28). – С. 60–70.

3. Захаров, А.А. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия / А.А. Захаров, А.С. Римша, А.М. Харченко, И.Р. Зулькарнеев // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3(25). – С. 24–33.

Публикации в изданиях, индексируемых в МБЦ:

4. Rimsha, A.S. The Problem of Selecting APCS' Information Security Tools / A.S. Rimsha, K.S. Rimsha // Studies in Systems, Decision and Control. – 2020. – Vol. 260. – pp. 211–223.

5. Rimsha, A.S. Database Design for Threat Modeling and Risk Assessment Tool of Automated Control Systems / A.S. Rimsha, K.S. Rimsha // 2019 International Russian Automation Conference (RusAutoCon). – Sochi: South Ural State University, 8-14 September 2019. – 5 p.

6. Rimsha, A.S. Development of Threat Modeling and Risk Management Tool in Automated Process Control System for Gas Producing Enterprise / A.S. Rimsha, K.S. Rimsha // Complex Systems: Control and Modelling Problems XXI International Scientific Conference. – Samara: Samara State Technical University, 3-6 September 2019. – 5 p.

7. Rimsha, A.S. Method for Risk Assessment of Industrial Networks' Information Security of Gas Producing Enterprise / A.S. Rimsha, A.A. Zakharov // GloSIC 2018: Global Smart Industry Conference. – Chelyabinsk: South Ural State University, November 13-15, 2018. – 4 p.

Результаты интеллектуальной деятельности:

8. Римша, А.С. Risk Identification and Management Security Host-based Appliance / А.С. Римша, К.С. Римша // Свидетельство о регистрации программы для ЭВМ № 2019619989 от 29.07.2019, заявка № 2019618411 от 02.07.2019.

Публикации в других изданиях:

10. Большаков, А.А. Математическое обеспечение для анализа и управления информационными рисками в АСУ ТП газодобывающих предприятий / А.А. Большаков, А.С. Римша // Математические методы в технике и технологиях. – 2021. – № 10. – С. 73–78.

11. Римша, А.С. Методы, модель и программный комплекс для анализа информационных рисков АСУ ТП // Математические методы в технике и технологиях. – Санкт-Петербург, 2021. – № 6. – С. 129–136.

12. Римша, А.С. Анализ актуальных классов решений обеспечения информационной безопасности АСУ ТП газодобывающих предприятий /

А.С. Римша, К.С. Римша // Математические методы в технике и технологиях: сб. тр. междунар. науч. конф.: в 12 т. – Санкт-Петербург: СПбПУ, 3-7 июня, 2019. – № 4. – С. 58–63.

13. Римша, А.С. Метод, модель и программный комплекс для анализа информационных рисков в АСУ ТП газодобывающих предприятий // Математические методы в технике и технологиях: сб. тр. междунар. науч. конф.: в 12 т. – Санкт-Петербург: СПбПУ, 3-7 июня, 2019. – № 2. – С. 124–129.

14. Римша, А.С. Программно-алгоритмическое решение для оценки и учета рисков АСУ ТП газодобывающего предприятия / А.С. Римша, К.С. Римша // Безопасность информационного пространства: сборник трудов XVII Всероссийской научно–практической конференции студентов, аспирантов и молодых ученых. – Челябинск: Челябинский государственный университет (Челябинск), 29-30 ноября, 2018. – Том 2. – С. 165–175.

На диссертацию и автореферат поступили отзывы: официального оппонента Ажмухамедова И.М.; официального оппонента Аникина И.В.; ведущей организации ФГБОУ ВО СГТУ; Давидюка Н.В., к.т.н., доц., зав. кафедрой "Информационная безопасность" Астраханского государственного технического университета; Шестопалова М.Ю., д.т.н., доц., заведующего кафедрой автоматики и процессов управления Санкт-Петербургского государственного электротехнического университета "ЛЭТИ" им. В.И. Ульянова (Ленина); Алексеева В.В., д.т.н., проф., зав. кафедрой "Информационные системы и защита информации" Тамбовского государственного технического университета; Бойкова С.Ю., к.т.н., доц., зав. кафедрой "Информационные системы и технологии" Ярославского государственного технического университета; Гвоздика Я.М., к.т.н., начальника центра сертификации ООО "Газинформсервис"; Абросимова М.Б., д.ф.-м.н., доц., зав. кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н.Г. Чернышевского; Скобелева П.О., д.т.н., доц., зав. кафедрой "Электронные системы и информационная безопасность" Самарского государственного технического

университета; Богомолова В.А., к.т.н., доц., зав. кафедрой информационной безопасности Казанского национального исследовательского технологического университета; Давыдова Н.Н., д.т.н., доц., проф. кафедры "Физика и прикладная математика" Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых; Василькова Ю.В., д.т.н., проф., профессора кафедры кибернетики Ярославского государственного технического университета.

Все отзывы положительные, но имеются следующие замечания. В диссертационной работе для построения функции приемлемого риска сначала определяются актуальные угрозы, затем для каждой из них определяется предельно допустимый ущерб и приемлемая возможность его осуществления. Такой подход представляется не совсем целесообразным, поскольку для организации важен суммарный риск от реализации всей совокупности угроз и дать оценку указанных выше параметров для каждой из угроз весьма затруднительно. Данная оценка для каждой угрозы будет зависеть от оценок, полученных для других угроз информационной безопасности. В методике оценки рисков информационной безопасности (методика 1) упоминаются «угрозы, не эксплуатирующие уязвимости» и «угрозы, эксплуатирующие уязвимости». Смысл данных понятий ни в автореферате, ни в диссертации не раскрыт. В описании методики 2 и ее блок-схеме различаются формулировки последнего этапа: они имеют разную смысловую нагрузку, в описании этапов отсутствует упоминание массива O, приведенного в блок-схеме. В приложениях отсутствуют примеры бланков опросных листов для экспертов. Автору следовало более четко обосновать выбор предоставленного подхода к моделированию. Для формирования ряда оценок автор предлагает использовать групповую экспертизу с назначением экспертам весовых коэффициентов. Однако не указаны принципы формирования таких экспертных групп. Требует уточнения способ определения актуальных угроз на шаге 2 Алгоритма 1. Необходимо также обосновать использование принципа максимума при выборе результирующего влияния угроз с использованием уязвимостей на шаге 6 Алгоритма 6. Автору следовало

уточнить, что представляют собой защитные меры, включенные в множества S_ОРО, S_ОРПр. На стр. 95 диссертационной работы говорится о величине остаточного риска, равном нулю, при удовлетворении системе соотношений (3.15). В данном случае вместо нулевого уровня риска, следовало говорить о приемлемом уровне. Разработанный автором метод не учитывает категории, присваиваемые в соответствии с законодательством в сфере критических информационных инфраструктур. В предлагаемом эксперименте не учитывается ущерб для активов информационного обеспечения. Для применения предлагаемого соискателем подхода необходим анализ всей инфраструктуры АСУ ТП, включая все взаимосвязи на физическом и логическом уровнях между устройствами, что является достаточно трудоёмким процессом. В диссертационной работе не приводятся результаты сравнения с другими методами оценки рисков информационной безопасности, применяемыми для рассмотренного эксперимента, для определения эффективности, предлагаемого соискателем метода. При эксплуатации угрозой нескольких уязвимостей оценка CVSS в большинстве случаев будет близка к максимальному значению, таким образом оценки экспертов никак не будут влиять на результат при расчете ущерба. Алгоритм оценки возможности реализации угрозы (алгоритм 4) рассчитан только на меры обработки риска снижением, таким образом в алгоритме оценки возможности реализации угроз (алгоритм 7) не будут учтены другие применяемые меры. Не уточняется, о том, что угрозы группируются по определенному принципу для разных активов, таким образом 14 актуальных угроз выглядят недостаточно убедительным по количеству для действующего предприятия. Не ясно, насколько согласуются предложенные автором методики и алгоритмы с требованиями нормативно-правовых документов о безопасности критической информационной инфраструктуры (Федеральный закон 187-ФЗ, приказы ФСТЭК № 239, ФСБ № 366-368). Не описано: зависят предложенные автором методики и алгоритмы, а также меры обработки рисков от категории значимости объектов критической информационной инфраструктуры. Автором не уточняется: предполагают предложенные алгоритмы управления рисками

возможность подключения к технической инфраструктуре национального координационного центра по компьютерным инцидентам. Не в полной мере раскрыт принцип выбора актуальных угроз для действующего предприятия. При сравнении блок-схем процесса управления рисками информационной безопасности из стандарта ГОСТ Р ИСО/МЭК 27005-2010 и предлагаемой автором блок-схемы процесса управления рисками информационной безопасности АСУ ТП можно заметить, что в варианте, предлагаемом автором, отсутствует процесс «коммуникация риска». При определении группой экспертов достаточно высокого показателя времени нарушения или прекращения работы подверженной группы активов после нормализации потенциального ущерба относительно максимально принятого ущерба полученное значение показателя может превысить единицу. Автору следовало бы для более полной оценки и обработки рисков предусмотреть возможность учета модели нарушителя. В пятом разделе рассматривается пример использования разработанного программного комплекса управления информационными рисками, где в качестве результата приводится оценка эффективности до и после внедрения выбранных мер обработки рисков. Полученная оценка никак не сравнивается с другими методами по оценке и обработке рисков.

Выбор оппонентов и ведущей организации обосновывается компетентностью и значимой позицией в научных кругах крупнейших специалистов в области информационной безопасности, в том числе в областях, связанных с профилем диссертационной работы, а также значительным числом публикаций в рецензируемых научных изданиях по тематике диссертационного исследования.

Официальные оппоненты также известны своими публикациями в области диссертационной работы, д.т.н., профессор, Ажмухамедов И.М. автор ряда работ по анализу защищённости информационных систем и моделирования угроз информационной безопасности, д.т.н., профессор, Аникин И.В. активно занимается исследованиями по тематике определения нарушителей информационной безопасности и оценке рисков информационной безопасности

чему посвящены публикации в ведущих научных журналах. Кафедра информационной безопасности автоматизированных систем внесла значительный вклад в исследования процессов моделирования угроз информационной безопасности, в частности, силами таких ученых, как Байбурин В.Б., Губенков А.А., Данилова Т.В. Проведено большое количество исследований по выявлению и оценке уязвимостей программного обеспечения в автоматизированных системах применительно к решению прикладных задач.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур, позволяющие идентифицировать активы системы и установить связь с актуальными угрозами безопасности информации; **предложен** подход учета особенностей многоуровневой структуры АСУ ТП, отражающий реальную взаимосвязь критических процессов системы с остальными активами и способный учитывать уязвимости компьютерной безопасности активов при реализации угрозы, что позволяет проводить комплексную оценку риска для каждой угрозы; **доказана** возможность использования разработанных метода и алгоритмов в рамках оценки актуальных угроз безопасности информации АСУ ТП критических инфраструктур, а также в процессе выбора мер для обработки рисков; **введена** новая модель АСУ ТП критических инфраструктур на основе теоретико-множественного подхода описания активов, описывающая логическую и физическую структуры взаимодействия между активами, а также воздействие на критические процессы АСУ ТП, которые подвергаются угрозам информационной безопасности.

Теоретическая значимость исследования обоснована тем, что: доказана эффективность применения метода управления рисками информационной безопасности АСУ ТП, вносящих вклад в расширение представлений о процессе оценки и обработки актуальных угроз безопасности информации; **применительно к проблематике диссертации результативно использованы** методы анализа иерархии, экспертных оценок, анализ дерева событий и

динамическое программирование; **изложены** идеи сочетания принципа защиты в глубину и анализа дерева событий для оценки возможности реализации угроз информационной безопасности АСУ ТП, а также установление взаимосвязи между используемыми мерами обработки рисков и возможностью реализации угрозы; **раскрыты** несоответствия в существующих методических документах, регламентирующих определение актуальныз угроз безопасности информации, выявление проблемы построения взаимосвязи физических, логических активов и их воздействия на критические процессы АСУ ТП; **изучены** противоречия в процессах определения угроз информационной безопасности, предлагаемых различными методическими документами; **проведена модернизация** существующего подхода по управлению рисками информационной безопасности, адаптированного к условиям многоуровневой иерархической структуры с учетом финансовых ограничений на основе анализа взаимосвязей активов АСУ ТП критических инфраструктур.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены модель угроз информационной безопасности АСУ ТП на предприятиях топливно-энергетического комплекса: АО "Ачимгаз" в г. Новый Уренгой и ООО "РН-Уватнефтегаз" в г. Тюмень; **определены** перспективы использования предложенных метода, методик и алгоритмов в составе программного комплекса для управения рисками информационной безопасности; **создана** система практических рекомендаций по поиску оптимальных мер обработки рисков в условиях финансовых ограничений, позволяющих сократить потенциальные затраты; **представлены** предложения по дальнейшему совершенствованию метода управления рисками информационной безопасности АСУ ТП критических инфраструктур, что позволит проводить более подробный анализ системы.

Оценка достоверности результатов исследования выявила: для экспериментальных работ произведено сравнение количества и величины критичности неприемлемых угроз до применения методики обработки рисков и после ее применения в АСУ ТП критической инфраструктуры; **теория** построена

на известных системах оценки уязвимостей и методических рекомендациях оценки ущерба угроз информационной безопасности, а также способах определения активов АСУ ТП; **идея базируется** на анализе методик оценки угроз информационной безопасности и методах управления рисками информационной безопасности; **использованы** результаты сравнения экономических затрат при подготовке перечня мер обработки рисков информационной безопасности по разработанной методике; **установлено** совпадение качественных параметров алгоритмов авторского метода с методами управления рисками информационной безопасности, представленными в независимых источниках по данной тематике; **использованы** современные методики сбора и анализа данных с применением метода анализа иерархий и метода экспертных оценок.

Личный вклад соискателя состоит в том, что все результаты диссертационной работы получены автором самостоятельно. В разработке модели АСУ ТП критических инфраструктур для описания различных видов активов, подверженных угрозам информационной безопасности, и особенностей их взаимодействия, которая позволяет анализировать и обрабатывать риски безопасности информации в системе. В работах по теме диссертации, опубликованных в соавторстве, а также при постановке и решении задач соискателю принадлежит существенная роль.

В ходе защиты диссертации были высказаны следующие критические замечания о предложенной методики экспертной оценки.

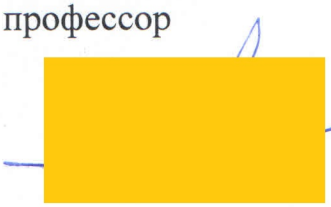
Соискатель Римша А.С. в ходе заседания ответил на задаваемые ему вопросы и привел собственную аргументацию о выборе экспертных групп.

Диссертационный совет установил, что диссертация «Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 7, 14 и 15 паспорта научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

На заседании 02 ноября 2022 года объединенный диссертационный совет принял решение присудить Римше А.С. ученую степень кандидата технических наук за решение научной задачи имеющей значение для отрасли информационной безопасности, а именно повышение эффективности информационной безопасности АСУ ТП в условиях деструктивных воздействий за счет использования риск-ориентированного подхода, а также разработке метода управления информационными рисками на основе анализа активов АСУ ТП критических инфраструктур и их взаимосвязей с применением методик оценки и обработки рисков информационной безопасности.

При проведении тайного голосования объединенный диссертационный совет в количестве 17 человек, из них 4 докторов наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 17, против – нет, недействительных бюллетеней – нет.

И.о. председателя диссертационного совета,
доктор технических наук, профессор



Бабук Валерий Александрович

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент

Владыко Андрей Геннадьевич

03 ноября 2022 года