Автономная некоммерческая организация
"Институт инженерной физики"
(АНО "Институт инженерной физики")
Большой Ударный пер., д. 1А, стр. 1, г. Серпухов,
г.о. Серпухов, Московская обл., 142210
тел. 8(4967)353193; 351371; 8-499-400-05-75
факс: 8(4967)354420
e-mail: info@iifmail.ru; http://www.iifrf.ru
ОКПО 58914325, ОГРН 1225000027108,
ИНН/КПП 5043075306/504301001

УТВЕРЖДАЮ
Генеральный директор –
Первый Вице-президент Института
почётный работник науки и техники РФ
кандидат технических наук, доцент

Е.М. Ананьев

«11» декабря 2025 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию Чернова Дениса Владимировича на тему: «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок», представленную на соискание учёной степени кандидата технических наук по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (технические науки).

Актуальность темы исследования

Современный этап развития государства характеризуется стремительной цифровизацией всех секторов промышленности и интеграцией критической информационной инфраструктуры (КИИ) в технологические процессы объектов стратегического значения. Объекты КИИ составляют основу таких ключевых отраслей, как топливно-энергетический комплекс, оборонно-промышленный комплекс, ракетно-космическая и нефтехимическая промышленность. Их устойчивое функционирование является залогом национальной безопасности и экономической стабильности. Вместе с тем, высокая степень интеграции делает эти системы привлекательной мишенью для киберугроз, реализация которых способна привести к непоправимым технологическим, экономическим и репутационным последствиям.

В этой связи обеспечение информационной безопасности на всех этапах жизненного цикла объектов КИИ приобретает характер первостепенной

государственной задачи, что подтверждается рядом нормативно-методических документов Российской Федерации.

С учетом вышеизложенного, тема диссертационной работы Чернова Д.В., посвященная разработке и исследованию новых методов и алгоритмов моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок, несомненно, является ***актуальной.***

Основные формальные положения работы

Объектом исследования является являются объекты критической информационной инфраструктуры, в отношении которых могут быть реализованы угрозы безопасности информации потенциальными нарушителями информационной безопасности.

Предметом исследования являются методы и алгоритмы моделирования угроз безопасности информации в объектах критической информационной инфраструктуры.

Целью диссертационной работы является повышение эффективности процесса моделирования угроз безопасности информации объектов критической информационной инфраструктуры на основе разработки методов и алгоритмов интеллектуального анализа данных, позволяющих повысить достоверность и объективность результатов анализа и оценки актуальных угроз безопасности информации с использованием аппарата экспертных оценок.

Для достижения указанной цели предполагается решение ***новой научной задачи***, заключающейся в повышения эффективности процесса моделирования угроз безопасности объектов критической информационной инфраструктуры на основе аппарата экспертных оценок.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Диссертационная работа изложена на 199 страницах, включает 36 рисунков, 32 таблицы и 9 приложений.

Во введении обоснована актуальность работы, степень разработанности темы исследования, приведены объект и предмет исследования, использованные методы, сформулированы цель и задачи диссертационной работы, положения, выносимые на защиту, представлены научная новизна и практическая значимость результатов научного исследования.

Первая глава посвящена анализу современного состояния исследований в области определения потенциала нарушителя информационной безопасности и моделирования угроз безопасности информации (БИ). Проанализирована существующая отечественная нормативно-правовая база, затрагивающая вопросы моделирования угроз. Рассмотрены различные методики оценки нарушителей и уровня опасности реализации угроз БИ. На основе результатов проведенного анализа сделан вывод об актуальности проблемы повышения эффективности процесса моделирования угроз БИ ОКИИ. Ее решение предложено осуществить за счет разработки методов и алгоритмов интеллектуального анализа данных, позволяющих повысить достоверность и объективность результатов анализа и оценки актуальных угроз БИ с использованием аппарата экспертных оценок.

Во второй главе предложены методы, позволяющие проводить мероприятия по моделированию угроз БИ ОКИИ, а именно: метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз; метод количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ; метод оценки защищенности уязвимых звеньев ОКИИ и метод экспертной оценки степени опасности реализации угроз БИ ОКИИ.

Третья глава посвящена алгоритмизации процедуры формирования модели угроз БИ ОКИИ, на основе оценок потенциалов возможных нарушителей, показателей опасности реализации ими угроз БИ и оценок защищенности фактических уязвимых звеньев. Предложены алгоритмы работы сканера безопасности, оценки опасности реализации угроз БИ, а также определения и оценки защищенности уязвимых звеньев ОКИИ. На основе указанных алгоритмов предложен алгоритм экспертной оценки опасности реализации угроз БИ ОКИИ

В четвертой главе представлена архитектура автоматизированной системы, реализующей предложенные методы и алгоритмы моделирования угроз БИ для объектов критической информационной инфраструктуры. Указано, что автоматизированная система позволяет экспериментально проверить эффективность разработанных методов и алгоритмов. Приводится общее описание, рассматривается графический интерфейс автоматизированной системы и основные функциональные возможности. Приводятся результаты экспериментальной проверки предложенных методов и алгоритмов с использованием разработанной автоматизированной системы.

В заключении сформулированы основные результаты и выводы, полученные в диссертационной работе, а также предложены возможные направления дальнейших исследований.

Новизна полученных результатов

1. Новизна предложенного метода определения потенциала нарушителя, заключается *в применении матриц идентификаторов угроз*. Метод позволяет *выявить и количественно оценить располагаемый потенциал возможных нарушителей ИБ*, что, в свою очередь, позволяет *повысить достоверность и объективность анализа и оценки актуальных угроз* БИ. Главным *отличием от существующих* является возможность применения предложенного метода к групповой оценке потенциалов нарушителей согласованным количеством экспертов.

2. Новизна разработанного метода количественной оценки степени опасности реализации угроз БИ ОКИИ заключается *в использовании интеллектуального анализа данных, имеющихся в подсистеме журналирования*. Метод позволяет *количественно оценить степень опасности реализации угроз БИ потенциальными нарушителями ИБ применительно к конкретному объекту КИИ*. Разработанный метод *дополняет* располагаемые оценки специалистов в области ИБ *путем формирования экспертных оценок со стороны дополнительно привлекаемых специалистов – профессионалов в области КИИ*.

3. Новизна разработанного алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ заключается *в использовании матрицы защищенности, составленной на основе оценок показателей защищенности уязвимых звеньев*, что позволило *повысить объективность выявления актуальных угроз БИ ОКИИ*.

4. Новизна предложенного алгоритма экспертной оценки степени опасности реализации угроз БИ ОКИИ заключается *в применении игр с несовершенной информацией вида «злоумышленник – система защиты информации», где в качестве возможных выигрышей сторон используются оценки потенциала нарушителя, опасности реализации им угроз БИ, а также оценки защищенности уязвимых звеньев, по отношению к которым потенциальный нарушитель реализует угрозы БИ*, что позволило *дополнять перечни актуальных угроз БИ, выявленные с использованием известных методик ФСТЭК России*.

Область исследования диссертации ***соответствует*** следующим пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность:

– п. 3 Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса;

– п. 8 Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации

в информационных системах любого вида и области применения;

– п. 10 Модели и методы оценки защищенности информации и информационной безопасности объекта.

Значимость полученных автором диссертации результатов для развития соответствующей отрасли науки

Теоретическая значимость полученных результатов работы заключается в том, что они вносят существенный вклад в решение задачи обнаружения актуальных угроз информационной безопасности. В диссертации разработаны: метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз; метод количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ с использованием оценок вероятностей реализации угроз БИ и ущерба от их реализации; алгоритм определения уязвимых звеньев ОКИИ и оценки их защищенности на основе предложенных матриц защищенности; алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ, а также структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ.

Практическая ценность полученных результатов заключается в разработке алгоритмов и программного обеспечения автоматизированной системы моделирования угроз БИ ОКИИ, позволяющей повысить эффективность построения моделей угроз БИ и выбора состава мер защиты по сравнению с известными методиками более чем в 2,6 раз. Применение разработанной системы позволяет поддерживать актуальность сведений о возможных угрозах БИ, потенциальных нарушителях ИБ и необходимых средствах защиты информации (СЗИ).

Разработанные соискателем методы и алгоритмы были использованы для моделирования угроз БИ ОКИИ в ООО «Комплексы системы и сети», ООО «БД Безопасность» и внедрены в учебный процесс кафедры информационной безопасности ФГБОУ ВО «Тульский государственный университет» Министерства науки и высшего образования РФ.

Разработанное ПО внедрено в процессы оценки угроз в АО ЦКБА.

Работа поддержана грантом РФФИ № 19-07-01107/19 «Разработка математических моделей и методов построения интеллектуальных распределенных адаптивных систем обеспечения ИБ» и грантом РТУ МИРЭА № 15/2020 «Разработка методов и алгоритмов моделирования угроз БИ».

Таким образом, можно сделать вывод о том, что диссертация имеет практическую направленность и соответствует критериям, изложенным в п. 10 «Положения о присуждении учёных степеней», утв. пост. Прав-ва РФ № 842 от 24.09.2013, о том, что в диссертации, имеющей прикладной

характер, должны приводиться сведения о практическом использовании полученных автором диссертации научных результатов.

Рекомендации по использованию результатов и выводов, приведенных в диссертации

АНО «Институт инженерной физики» рекомендует использовать представленные в диссертации результаты исследования в компаниях, специализирующихся на разработке средств защиты информации и средств ГосСОПКА, в частности: АО «НПО «Эшелон», ООО «Крипто-ПРО», ООО «Криптоком» ООО «Код Безопасности» и др., а также компаниях, представляющих услуги по проведению мероприятий по защите ОКИИ, в частности: АО «КОНСИСТ-ОС», ООО ЦБД «Айдеко», ООО «РТМ Технологии» и др.

Достоверность подтверждается корректной постановкой задач и выбором методов исследования; повторяемостью полученных результатов вычислительных экспериментов, проведенных с использованием известных и широко применяемых в аналогичных исследованиях банках данных угроз; практическим применением результатов работы, подтвержденным актами внедрения; обсуждением полученных результатов на научных конференциях; публикацией полученных результатов в рецензируемых научных изданиях.

Результаты диссертации в достаточной мере ***апробированы***, поскольку опубликованы в 30 научных работах, в том числе:

– в 4 научных статьях в научных журналах, включенных в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (Перечень ВАК) по научной специальности 2.3.6;

– в 10 научных публикациях в изданиях, индексируемых в библиографических и реферативных международных базах данных рецензируемой научной литературы: Web of Science и SCOPUS;

– в 16 научных статьях в иных научных изданиях.

Соискатель также является автором 2 программ для ЭВМ, зарегистрированных в Роспатенте.

К основным ***недостаткам*** данной работы, на наш взгляд, относятся следующие:

1) в автореферате указано наличие 7 приложений, в то время как в диссертации содержатся 9 приложений.

2) в первой главе диссертации на стр. 36 приводится описание термина

«уязвимое звено»; представляется возможным более подробное рассмотрение существующих способов их выявления;

3) в первой и второй главах диссертации рассмотрены различные методы и алгоритмы моделирования угроз БИ, – несомненно, результаты проведенных при этом экспериментов позволили соискателю выделить ряд наиболее эффективных методов оценки актуальности и опасности реализации угроз БИ, однако, хотелось бы видеть более четкие выводы, о том, каким конкретно методам и почему будет отдано предпочтение в дальнейшем;

4) в тексте диссертации не указано в каком формате используется база данных угроз БИ;

5) в табл. 3.2 диссертации на стр. 89 приводятся сокращение «КЗ» и «ОКЗ», однако, если для аббревиатуры «ОКЗ» приведена расшифровка, то для сокращения «КЗ» расшифровка отсутствует;

6) в табл. 4.12 диссертации приводится перечень защитных мер, необходимых к внедрению в ОКИИ в целях устранения выявленных актуальных угроз, однако далее в тексте не приводятся наименования конкретных средств защиты информации и их производителей необходимых к внедрению;

7) из текста диссертации не вполне ясно, должна ли предлагаемая система моделирования угроз использоваться в качестве основной системы оценки опасности реализации угроз безопасности информации для объекта КИИ или же в качестве дополнения к существующим системам;

8) в явном виде не указаны требуемые вычислительные ресурсы, необходимые для реализации, предложенной в работе автоматизированной системы.

Перечисленные замечания не являются принципиальными, не снижают научной и практической значимости представленной работы и не влияют на ее общую положительную оценку.

Анализ автореферата диссертации

Автореферат диссертации соответствует основным положениям диссертации и достаточно логично отражает ее содержание.

В целом, автореферат диссертации соответствует требованиям п. 25 «Положения о присуждении учёных степеней», утв. пост. Прав-ва РФ № 842 от 24.09.2013. В автореферате диссертации излагаются основные идеи и выводы диссертации, показываются вклад автора в проведенное исследование, степень новизны и практическая значимость приведенных результатов исследований, содержатся сведения об организации, в которой выполнялась диссертация, об оппонентах и ведущей организации, о научном консультанте соискателя учёной степени, приводится список публикаций

автора диссертации, в которых отражены основные научные результаты диссертации.

Оформление диссертации и автореферата диссертации соответствует ГОСТ Р 7.0.11-2011.

Заключение

Руководствуясь п. 24 «Положения о присуждении учёных степеней», утв. пост. Прав-ва РФ № 842 от 24.09.2013, после изучения и обсуждения диссертации сотрудниками АНО «Институт инженерной физики» по профилю представленной на отзыв диссертации, сделаны следующие выводы:

1) представленная на отзыв диссертация является самостоятельно выполненной научно-квалификационной работой, содержащей решение актуальной научной задачи, имеющей значение для развития технической отрасли знаний, в рамках теории, технологии и средств обеспечения информационной безопасности и защиты информации, а именно в повышения эффективности процесса моделирования угроз безопасности объектов критической информационной инфраструктуры на основе аппарата экспертных оценок;

2) диссертация соответствует критериям, изложенным в п. 10 «Положения о присуждении учёных степеней» в части практического использования полученных автором диссертации научных результатов; результаты работы реализованы и внедрены в 4-х организациях, ведущих исследования и разработки по профилю диссертационных исследований;

3) диссертационная работа соответствует требованиям пп. 9, 11, 13 и 14 «Положения о присуждении учёных степеней», утв. пост. Прав-ва РФ № 842 от 24.09.2013 и п. 6 «Положения о присуждении учёных степеней лицам, использующим в своих работах сведения, составляющие государственную тайну», утв. пост. Прав-ва РФ № 235 от 17.03.2015, а Чернов Денис Владимирович заслуживает присуждения ему учёной степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (технические науки).

Диссертация Чернова Дениса Владимировича на тему «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок», представленная на соискание учёной степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (технические науки) обсуждена и одобрена 11.12.2025 на заседании Научно-технического совета Института, отзыв

утвержден протоколом Научно-технического совета АНО «Институт инженерной физики» № 11/12/01 от 11.12.2025.

Отзыв составили:
Заместитель генерального директора по специальным проектам
Автономной некоммерческой организации
«Институт инженерной физики»
(АНО «Институт инженерной физики»)
почётный работник науки и высоких технологий РФ,
доктор технических наук
(науч. спец. 20.01.10 – «Военная разведка»), профессор
Олег Игоревич Атакищев

тел. 8 (4967) 35-31-93,
e-mail: oiatakishchev@iifmail.ru

Согласен на обработку персональных данных О.И. Атакищев
«11» декабря 2025 г.

Главный научный сотрудник
АНО «Институт инженерной физики»
почётный работник науки и техники РФ,
почётный специалист по защите информации,
доктор технических наук *(науч. спец. 20.02.14 – «Вооружение и военная техника. Комплексы и системы военного назначения»)*, доцент
Вадим Геннадьевич Грибунин

тел. 8 (4967) 35-31-93, доб. 693;
e-mail: vggribunin@iifmail.ru.

Согласен на обработку персональных данных В.Г. Грибунин
«11» декабря 2025 г.

Начальник научно-методического управления,
учёный секретарь специального диссертационного
совета Д 75.1.001.02 на базе АНО «Институт инженерной физики»
(науч. спец. 2.3.6. Методы и системы защиты информации, информационная безопасность)
почётный работник науки и высоких технологий РФ,
кандидат технических наук, доцент
Алексей Александрович Коробков

тел. 8 (4967) 35-31-93, доб. 148
e-mail: korobkow@iifmail.ru

Согласен на обработку персональных данных А.А. Коробков
«11» декабря 2025 г.

Старший научный сотрудник
управления комплексов средств информатизации
Центра специальных систем
АНО «Институт инженерной физики»
кандидат технических наук
(науч. спец. 2.3.6. Методы и системы защиты информации, информационная безопасность)
Ярослав Дмитриевич Смирнов

тел. 8 (4967) 35-31-93, доб. 7228
e-mail: iadsmirnov@iifmail.ru

Согласен на обработку персональных данных Я.Д. Смирнов
«11» декабря 2025 г.

Юридический и почтовый адреса организации:
142210, Россия, Московская обл., г.о. Серпухов, г. Серпухов,
Большой Ударный пер., д. 1А, стр. 1

Подписи Атакищева О.И., Грибунина В.Г., Коробкова А.А., Смирнова Я.Д. заверяю
Секретарь научно-технического совета
АНО «Институт инженерной физики»
кандидат технических наук М.М. Авдеева
«11» декабря 2025 г.

М.П.