ОТЗЫВ

официального оппонента на диссертацию Костина Владимира Николаевича «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов»,
представленную на соискание ученой степени доктора технических наук по специальности 05.13.01 – Системный анализ, управление и обработка информации (в науке и технике)

Актуальность темы диссертации. Проектирование сосредоточенных и распределенных критически важных объектов (КВО), классификация которых приведена в диссертации, является процессом создания сложной технической системы, важная особенность которого заключается в необходимости параллельного, а зачастую и с опережением во времени, построения системы физической защиты по отношению к процессу проектирования КВО. Это подтверждается тем, что в соответствии с нормативными требованиями при проектировании КВО система физической защиты (СФЗ) является обязательным элементом и разрабатывается на стадии проведения проектных работ. В процессе проектирования СФЗ необходимо учитывать результаты инженерных изысканий, а так же технические условия, модель нарушителя и др.

Исходные данные для проектирования СФЗ определены законодательными и нормативными актами ряда сфер деятельности. На основании подготовленных исходных данных разрабатываются функциональные, технологические, архитектурно-планировочные, инженерные и технологические решения, совокупность которых определяет, как технологический облик СФЗ в целом, так и каждой ее подсистемы в отдельности. В результате имеется совокупность множества технических решений, которые оцениваются, например, по таким параметрам как: сроки, стоимость, качество. Вариативность этих решений крайне высока, объективных критериев оценки нет. В результате создается противоречивая ситуация - можно создать СФЗ с одним и тем же качеством дешевле или дороже и все эти технические решения будут оправданы и пройдут экспертизу.

Таким образом, даже не смотря на четкую конкретику и высокую детализацию всех требований технических нормативов и исходных данных, остается высокой вариативность принимаемых решений о составе элементов СФЗ и ее структуре. Т.е. большое количество вариантов структуры СФЗ при разработке проектной документации затрудняет принятие наилучшего решения, что, в основном, приводит к увеличению времени проектирования и повышению стоимости проекта СФЗ. В настоящее время процесс определения соответствия выбранной структуры СФЗ требованиям заказчика и руководящих документов является субъективным и зависит от опыта эксперта и сложности КВО. Автоматизация этого процесса затруднена по ряду причин, основной из

которых является отсутствие системы методов, моделей и методик, критериев обоснования оценки эффективности той или иной СФЗ. В настоящее время критерии «разбросаны» по различным документам и зачастую противоречивы. Системное представление общего состояния КВО позволило автору работы выявить противоречия, возникающие при проектировании и функционировании СФЗ, разрешить которые возможно разрешив сформулированную в диссертации научную проблему. В связи с этим тема диссертации актуальна. Кроме того, действительно, важность исследования подтверждается содержанием Указа Президента РФ, в котором одним из приоритетных направлений развития науки является безопасность и противодействие терроризму. Актуальность также обусловлена все возрастающим уровнем информатизации общества. Во всех сферах деятельности общества осуществляется внедрение средств информатизации, в том числе на критически важных объектах, следовательно, защита критически важных объектов влияет на национальную безопасность в той же мере, как и физическая защита самих объектов информатизации.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

В первой главе Костин В.Н. обоснованно утверждает, что необходимая эффективность СФЗ закладывается на стадии концептуального проектирования, и от этого зависит оптимальность будущих проектно-технических решений. Автор убедительно показал наличие противоречий в задачах разработки СФЗ, а именно: противоречия между усложнением структуры объектов охраны, ростом возможностей инженерно-технических средств охраны (ИТСО) и неадекватной способностью СФЗ к реализации своих функций. Автором выявлено, что современные программные системы используются, как правило, только для оценки эффективности уже существующих СФЗ.

В результате проведенного системного анализа предметной области выявлены недостатки в технологии проектирования СФЗ. Методики проектирования СФЗ, как правило, имеют слабое математическое обоснование, многие этапы технологического процесса разработки основаны только на экспертных оценках, что обуславливает фактор субъективизма. Методики категорирования КВО и задания показателей защищенности объектов используют линейную шкалу оценки масштабов потерь, что не совсем согласуется с действительностью. Количество категорий КВО математически не обоснованно. Кроме того не используются информационные показатели и критерии, характеризующие степень информационного превосходства системы физической защиты над нарушителем. Модель типового нарушителя описывается только на вербальном уровне, нет сравнительной оценки опасности типовых нарушителей и структурного анализа их характеристик. На этой основе автором сделан вывод о необходимости разработки новых методик, моделей и методов для решения задач проектирования СФЗ, основанных на использовании

идеологии системного подхода и синтеза сложных организационно-технических систем, новых показателей и современных информационных технологиях.

Автором работы обоснованно введен термин «функционал обеспечения безопасности КВО», а также предложена схема управления процессом проектирования СФЗ, реализующая данный функционал.

Сказанное выше позволяет заключить, что первая частная научная задача решена.

Во второй главе, представлена разработанная, на основе информационно-вероятностного метода, методика категорирования КВО. Введена нелинейная энтропийная шкала оценки масштабов потерь КВО. Используя информационный критерий оптимальности развития систем автор предложил семь категорий опасности объектов, а также значения показателей безопасности для каждой категории. Изучение содержания второй главы позволяет заключить, что вторая частная научная задача решена.

В третьей главе автор работы, на основе проведенного системного анализа угроз безопасности предлагает методику оценки энтропийных потенциалов опасности типовых нарушителей. В результате сравнительного анализа опасности типовых нарушителей и их характеристик медом главных компонент определены и интерпретированы две компоненты. В отдельную компоненту выделены информированность и интеллектуальная подготовка нарушителя.

На основе формирования общего информационного поля масштабов потерь КВО от действий нарушителей в единых энтропийных шкалах разработана методика определения базовых нарушителей для категорий КВО.

Предложена методика оценки значимого изменения активности угроз (нарушителей) для прогнозирования периода модернизации СФЗ.

Сказанное выше позволяет заключить, что третья частная научная задача решена.

В четвертой главе Костиным В.Н. представлено описание имитационной модели функционирования СФЗ, с применением которой проводился эксперимент для оценки уровня риска с использованием введенного функционала управления безопасности КВО, и определения требуемых показателей эффективности подсистем СФЗ. На этой основе автор предложил методику размещения и выбора ИТСО объекта, обеспечивающую заданные критерии эффективности СФЗ, что является решением четвертой частной научной задачи.

Вообще говоря, практически вся глава посвящена доказательству достоверности и адекватности разработанных моделей и принятых решений.

В пятой главе представлена методика размещения и выбора ИТСО на объекте, обеспечивающая заданные требования эффективности СФЗ. Оригинальным и обоснованным является решение автора о введении в методику дополнительного показателя эффективности – контролируемая зона

для исключения утечки информации по техническим каналам и деструктивных воздействий на информационные ресурсы. Также представлена методика формирования организационных структур СФЗ с равномерной и оптимальной нагрузкой на элементы управления.

Таким образом, следует сделать вывод о том, что пятая частная научная задача решена.

В шестой главе представлен разработанный автором метод оценки и повышения эффективности на основе марковских цепей. Достоинством метода является то, что маршрут проникновения нарушителя разделен на множество разнородных участков и в качестве входных данных используются данные натурных испытаний на объекте, что повышает достоверность оценки эффективности СФЗ.

На этом основании следует заключить, что шестая частная научная задача решена.

Кроме того обоснованность результатов, полученных соискателем, основывается на согласованности данных экспериментов и научных выводов. Представлены результаты вычислительных экспериментов. Оценивалась работоспособность методики размещения инженерно-технических средств охраны на типовых объектах.

Достоверность научных результатов, полученных автором в работе, подтверждается глубоким изучением предметной области и обеспечивается использованием хорошо апробированных методов системного анализа, теории множеств, теории графов, имитационного моделирования, методов многомерного анализа и оптимизации, информационно-вероятностного метода, планирования эксперимента.

Для обеспечения достоверности и подтверждения результатов вся информация обрабатывалась разными методами с последующим проведением сравнительного анализа полученных результатов. Автор проверил согласованность результатов моделирования с данными, полученными при расчетах и при проведении исследований реальных систем, непротиворечивость полученных результатов известным работам ученых и специалистов в данной предметной области, сходимость теоретических расчетов с результатами экспериментальных исследований.

Дополнительно достоверность и обоснованность сформулированных научных положений и выводов подтверждена комплексностью подхода, системностью исследования и решения поставленных проблем и задач; использованием общенаучного и специального апробированного математического аппарата; выбором корректных, полных и объективных исходных данных;

Новизна научных результатов, полученных автором в работе, заключается в выявлении автором проблем, неизменно возникающих при проектировании СФЗ. На этом основании автором был сделан вывод о

необходимости разработки нового методического аппарата выработки обоснованных управленческих решений, основанного на новых информационных критериях оптимизации, совокупности применяемых математических методов и новых форм обработки информации. Результаты решения частных задач обладают признаками научной новизны.

Особенно следует отметить, что автор предложил информационно-вероятностный метод для решения вопросов категорирования КВО, оценки опасности типовых нарушителей, определения базовых нарушителей для КВО, прогнозирования интервала времени модернизации СФЗ и формирования организационной структуры СФЗ. Несомненно, оригинальное решение автора – введение нового показателя оценки эффективности СФЗ – «время утечки информации о функционировании СФЗ» и разработка метода оценки данного показателя, позволяющего уменьшить информационный потенциал нарушителя (повысить эффективность СФЗ).

Основным новым научным результатом, представленным Костиным В.Н. в диссертации, является схема управления технологическим процессом проектирования СФЗ. В ней реализовано множество функций управления на этапах задания критериев эффективности СФЗ, размещения и выбора инженерно-технических средств охраны и оценки соответствия показателей эффективности заданным требованиям.

Предложенные методики, модели и методы логически взаимосвязаны и сведены в систему в виде методологических основ и базируются на совокупности математических приемов для достижения цели исследования и разрешения научной проблемы.

В работе представлены важные научно-технические и технологические решения задачи построения СФЗ, направленные на повышение качества проектирования СФЗ за счет повышения достоверности и математического обоснования принимаемых решений для обеспечения необходимой безопасности КВО.

В результате следует заключить, что представленные Костиным В.Н. результаты исследования обладают достоверностью и новизной.

Основные научные результаты, которые представлены в данной работе, были **реализованы** в ряде организаций, например на объектах МО РФ; в профильных организациях, занимающихся аттестацией объектов информатизации критически важных объектов, а также в учебном процессе при подготовке студентов направления «Информационная безопасность» (Оренбургский государственный университет, Пензенский государственный университет). Это подтверждает то, что внедрение полученных Костиным В.Н. важных теоретических и практических результатов, а также предложенные методики, модели и методы внесло заметный вклад в развитие практики разработки СФЗ КВО.

Апробация результатов проведенных теоретических и экспериментальных исследований была проведена в научно-исследовательских работах, выполняемых организациях Минобороны России 3 ЦНИИ (ст. Донгуз) и предприятиях военно-промышленного комплекса «Радиозавод» г. Пенза, ООО концерн «Созвездие», в организациях занимающихся аттестацией объектов по информационной безопасности ЗАО «ЦИНТУР» г. Оренбург, ООО «УЦСБ» г. Екатеринбург, а также на конференциях, в том числе с международным участием (Самара, Челябинск, Уфа, Пенза и Оренбург), и в российских журналах ВАК «Труды ИСА РАН», «Вестник компьютерных и информационных технологий», «Информационные технологии», «Инфокоммуникационные технологии» и др.

Вместе с тем, при изучении диссертации сформулированы замечания и рекомендации:

1. В выражении 1.1 (с. 48) автор использует переменную «активности угроз λ_{ji}» и на с. 119 эта же переменная поясняется как «λ_{ji} – интенсивность проявления j-го нарушителя». Это одно и тоже? Кроме того неясно: как ее измерять, каков диапазон ее значений?

2. При ссылке на выражение 1.3 автор не указал источник.

3. В методике категорирования объектов (глава 2) объем выборки из генеральной совокупности составляет 31 объект. В тексте не приведено обоснование достаточности этой выборки для получения статистических оценок.

4. Выражение 2.4 (с. 72) требует более подробного пояснения.

5. В п. 3.3 (с.107) автор пишет о применении метода K-средних кластерного анализа, но обоснованность применения методов кластерного анализа и, как следствие, формулы для вычисления расстояния отсутствует.

6. В имитационной модели функционирования СФЗ глава 4 (с. 118-123) автор использовал нормальный закон распределения для моделирования временных интервалов, но обоснование об использовании в работе не приведено.

7. Не совсем понятно, как автор переходит от выражения 4.23 к выражению 4.24 (п.44, с. 132) и почему заданная эффективность определяется как произведение величины вероятности своевременного прибытия в точку перехвата на вероятность обнаружения угрозы.

8. В модели оценки эффективности на основе марковских цепей (глава 6) не проведена оценка адекватности модели реальному физическому процессу.

Указанные замечания не снижают научной и практической значимости полученных автором результатов и не влияют на общую положительную оценку диссертационной работы, а связаны с критическим ее изучением.

Общие выводы по диссертации.

Работа выполнена на высоком научном и методическом уровне с использованием современных инструментальных, программных средств и

методик, а основные выводы достаточно обоснованы и подтверждены результатами теоретических и экспериментальных исследований.

Результаты, полученные Костиным В.Н. и представленные в диссертации, соответствуют пп. 2, 3, 4, 7 паспорта специальности 05.13.01.

Содержание диссертации достаточно полно освещено в научных статьях, полученные результаты апробированы в дискуссиях на научно-технических конференциях различного уровня.

Структура диссертации логична, выполнена на должном уровне по оформлению.

Автореферат соответствует основному содержанию диссертации.

Вывод. Диссертация Костина В.Н. является законченной научно-квалификационной работой, содержит решение актуальной научной проблемы, заключающейся в необходимости повышения достоверности и обоснованности принимаемых решений на всех этапах проектирования систем физической защиты критически важных объектов, имеет важное экономическое значение и вносит значительный вклад в укрепление национальной безопасности РФ, соответствует требованиям пп. 9-14 «Положения о присуждения ученых степеней», предъявляемым к диссертациям на соискание ученой степени доктора наук, а автор – Костин Владимир Николаевич – заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.01 – Системный анализ, управление и обработка информации (в науке и технике).

Официальный оппонент:
заведующий кафедрой «Информационные системы и защита информации»
Федерального государственного бюджетного образовательного учреждения высшего образования «Тамбовский государственный технический университет»,
доктор технических наук, профессор В.В. Алексеев

«7» 07 2021 г.

Алексеев Владимир Витальевич
Адрес (рабочий): 392000, г. Тамбов, ул. Советская, д. 116, помещение 2В. Телефон: +74752630054, эл. почта: vvalex1961@yadex.ru

ПОДПИСЬ ЗАВЕРЯЮ
УЧЕНЫЙ СЕКРЕТАРЬ ТГТУ
Г.В. Мозгова
07 2021 г.