

## ОТЗЫВ

официального оппонента на диссертационную работу «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» Костина Владимира Николаевича, 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 исследования.** В целях противодействия противоправным действиям, в том числе террористическим актам или покушениям на его совершение, угрожающие безопасному функционированию критически важных объектов (КВО) принят ряд Федеральных законов, например, Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

Главная цель принятых законов заключается в том, чтобы с помощью системы правовых, экономических, организационных и иных мер, устанавливаемых государством, обеспечить антитеррористическую защищенность КВО.

В соответствии с этими законами одним из требований является обязанность субъектов КВО уже на стадиях проектирования и строительства объектов предусматривать осуществление комплекса специальных мер по безопасному функционированию таких объектов, локализации и уменьшению последствий чрезвычайных ситуаций.

Эффективным способом анализа уязвимости защищаемых объектов, выявления узких мест, потенциально опасных участков и критических элементов, а также оценки проектируемой системы физической защиты (СФЗ) служит системный подход к проектированию СФЗ.

В результате системного анализа должна быть предложена эффективная структура системы физической защиты, включающая в себя подсистему обнаружения несанкционированных действий с помощью инженерно-технических средств обнаружения и подсистему защиты объекта, состоящую из различного рода физических барьеров, препятствующих нарушителю, а также штата сотрудников охраны и сил реагирования, которые выполняют задачу по защите объекта.

Проектирование эффективной СФЗ на базе системного подхода требует методологического подхода, при котором разработчик находит баланс между целями СФЗ и имеющимися ресурсами, и на основании этого оценивает предложенный проект, чтобы определить насколько он соответствует поставленным целям.

Однако на сегодняшний день теоретические и методологические вопросы оценки эффективности вновь проектируемых систем физической безопасности остаются малоисследованными. Математический аппарат, который используется для решения вопросов проектирования СФЗ, также далек от совершенства в части обоснованности и достоверности принимаемых решений, и, как показывает практика, в основном

используются только на этапе оценки эффективности уже разработанных СФЗ. Кроме того, проводимые исследования, как правило, опираются на теорию экспертных оценок, что вносит элемент субъективизма при обосновании решений из-за малого количества специалистов в данной предметной области и трудности обеспечить согласованность их мнений.

Поэтому тема данного исследования несомненно актуальна. Поставленные в диссертационном исследовании цель и задачи, направленные на создание методик, моделей и методов повышения обоснованности принимаемых решений при разработке СФЗ КВО с использованием математического моделирования, оптимизации и современных методов обработки данных позволяют повысить качество (обоснованность и достоверность) процесса проектирования и оценки СФЗ.

**Новизна исследований и полученных в работе результатов.**

Новизна проведенного исследования и полученных результатов имеется. Оригинальными (впервые полученными в данной работе) являются следующие результаты:

- разработана трехконтурная схема управления проектированием СФЗ, реализующая введенный критерий обеспечения безопасности КВО, и методологические основы проектирования СФЗ в виде совокупности последовательных методик, моделей и методов реализации целевой установки исследований;

- предложена нелинейная энтропийная шкала оценки масштабов потерь на основе которой разработана методика категорирования КВО с использованием адаптированного информационно-вероятностного метода (ИВМ). Предложен численный критерий оптимальности развития систем, позволяющий обоснованно производить декомпозицию спектра опасности на значимо различные по опасности категории;

- для каждой категории объектов, в соответствии с характером изменения энтропийного показателя опасности, определены требования безопасности;

- проведен системный анализ структурных связей характеристик нарушителей с использованием метода главных компонент, в результате чего выделено две главные компоненты нарушителя, первая из которых интерпретируется как «техническая и физическая подготовка нарушителя»; вторая – «информационная подготовка нарушителя». На основе ИВМ определены энтропийные показатели опасности нарушителей и проведен их сравнительный анализ;

- на основе приведения характеристик КВО и нарушителя к общей энтропийной шкале сформирована общая информационная матрица и разработана методика определения базовых угроз для каждой категории КВО;

- представлен метод оценки интервала времени значимого изменения внешней ситуации (активности нарушителей) для прогнозирования момента модернизации СФЗ по причине изменения условий ее функционирования;

- разработана методика размещения и выбора инженерно-технических средств охраны (ИТСО) на КВО, обеспечивающая заданные показатели эффективности подсистем СФЗ. В методике реализован дополнительный показатель эффективности – радиус контролируемой зоны для обеспечения безопасности объектов информатизации от утечки и деструктивных воздействий на информацию по техническим каналам;

- разработана методика объединения инженерно-технических средств обнаружения в группы для формирования организационных структур управления СФЗ. Методика обеспечивает равномерную и оптимальную нагрузку на элементы организационного управления;

- разработан метод оценки эффективности СФЗ на основе теории марковских цепей. Метод позволяет получить более достоверные оценки из-за детализации маршрутов проникновения и точности входных данных модели, а также вырабатывать эффективные решения по повышению эффективности СФЗ;

- впервые введен показатель оценки эффективности СФЗ – «время утечки информации о функционировании СФЗ» и разработан метод оценки данного показателя, который позволяет повысить эффективность СФЗ за счет уменьшения потенциала опасности нарушителя.

**Значение полученных результатов для науки и практики.** Значимость результатов исследования для науки и практики продемонстрирована.

Отмеченный выше комплекс методик, моделей и методов принятия решений применим на всех этапах проектирования и оценки СФЗ.

Главным итогом работы является разработка новых научно-технических и технологических решений в задачах создания СФЗ для обеспечения антитеррористической и информационной безопасности КВО, направленных на построение методик, моделей и методов выработки обоснованных управлений решений при проектировании СФЗ.

**Достоверность полученных результатов.** Степень обоснованности и достоверности обеспечивается использованием современных средств, методик, включающих: методы системного анализа; теории множеств; теории графов; методов многомерного анализа; информационно-вероятностного метода, методов оптимизации, марковских моделей; теории электрических цепей. В данной работе грамотно используется разный математический аппарат на каждом этапе исследования.

Научные результаты, представленные в диссертации, неоднократно обсуждались на научных семинарах и конференциях, в том числе и международных, получили положительную оценку.

Достоверность и обоснованность сформулированных научных положений и выводов подтверждена комплексностью подхода, системностью исследования и решения поставленных проблем и задач; согласованностью результатов моделирования с данными, полученными при расчетах и при проведении исследований реальных систем; сходимостью теоретических расчетов с результатами экспериментальных исследований.

**Реализация результатов работы.** Разработанные в диссертационной работе основные научные результаты реализованы в ряде проектов в организациях занимающихся аттестацией объектов информатизации критически важных объектов (например, ЗАО «ЦБИ «ЦИНТУР», ООО «УЦСБ»), на предприятии государственной корпорации «Ростех»: «Радиозавод», на объектах министерства обороны РФ (например, ИП ЗЦИИ МО РФ), в учебных процессах (Оренбургский ГУ, Пензенский ГУ)

Таким образом, вышесказанное подтверждает, что Костиным В.Н. получены не только важные теоретические и практические результаты, но и предложены методики, модели и методы, внедрение которых внесло заметный вклад в развитие практики разработки СФЗ КВО.

**Апробация результатов и публикации по работе.** Основные результаты диссертационного исследования опубликованы в печати. Научные положения диссертации полностью отражены в ведущих рецензируемых журналах и изданиях, утвержденных ВАК. Результаты диссертационной работы непосредственно отражены в 41 публикациях, в том числе в 1 монографии, 35 статьях (включая 13 в изданиях из перечня ВАК, 1 в изданиях, индексируемых в изданиях Scopus), 5 свидетельствах об официальной регистрации программ для ЭВМ, 5 отчетах по НИР.

**Соответствие диссертации критериям**, установленным Положением о порядке присуждения учёных степеней (Постановление Правительства РФ от 24 сентября 2013 г. №842) имеется. Диссертация соответствует этим критериям в полной мере. Соблюдены все принципы соответствия, изложенные в пунктах 9 – 14 положения о порядке присуждения учёных степеней.

**Строгость авторской аргументации.** Диссертационная работа Костина В.Н. изложена технически грамотным языком и в научном стиле, содержит незначительное количество стилистических погрешностей и опечаток, хорошо структурирована и характеризуется внутренним единством и согласованностью теории с практикой проектирования и применения систем физической защиты КВО.

#### **Замечания по работе:**

1. Исследован узкий спектр потенциальных нарушителей. Автор обосновал шесть типов нарушителя нормативными документами 2007-2014 годов (приказ Министра промышленности и энергетики РФ от 04.05.2007 г. № 150 «Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики», Постановлением Правительства № 875 от 29.08.2014 г. «Об антитеррористической защищенности объектов ФСТЭК»). Существуют иные модели нарушителя, включая специальные службы иностранных государств, конкурирующие организации, лица, привлекаемые к монтажу и пусконаладочным работам систем безопасности и т.д. Более широкий спектр типов нарушителя мог бы позволить выявить иные латентные характеристики нарушителя, а не только «степень подготовки и мотивации к совершению террористического акта» и «информированность об объекте», описываемых двумя первыми главными

компонентами факторного анализа типов нарушителя, проведенного в работе.

2. При исследовании угроз (типовых нарушителей) рассматривались как внешние, так и внутренние нарушители, хотя в дальнейшем проектируемая СФЗ была ограничена лишь для защиты объектов от внешних нарушителей.

3. При оценке показателя эффективности – «время утечки информации о функционировании СФЗ» не приведены расчеты, каким образом получили снижение потенциала опасности нарушителя на 13 %.

4. Эффективность СФЗ оценивается недостаточным количеством показателей. Так, например, для объектов первой категории (ядерно и радиационно опасные объекты и т.д.) построение экономически оптимальных СФЗ на базе предлагаемой методологии может быть обосновано лишь при проверке статистической гипотезы о безопасности объектов с заданным уровнем значимости ошибок 1-го или 2-го рода, которые можно положить в ограничения задачи оптимизации.

5. При проведении исследований данной предметной области стоит острыя проблема получения исходных экспертных данных, которые всегда можно оспорить, и их низкая достоверность может снизить и даже свести на нет практическую ценность самого хорошего метода. В диссертации при проведении исследования типовых нарушителей не отражено, знания каких экспертов использованы в работе при формировании исходных данных в методике определения базовых нарушителей.

6. Имеют место терминологические неточности. Так, например, автор неоднократно применяет вместо термина «доля объяснимой дисперсии» в методе главных компонент термин «информационная нагрузка».

Отмеченные замечания, тем не менее, не снижают научной и практической значимости диссертационной работы и не влияют на общую положительную оценку проведенного исследования.

### **Выводы**

В рассматриваемой работе решена важная научно-практическая проблема разработки методик, моделей и методов принятия обоснованных решений в задачах разработки и оценки СФЗ КВО.

Рассматриваемая диссертационная работа является законченным исследованием, в котором решены комплекс общетеоретических вопросов разработки методик, моделей и методов, которые применены к проектированию и оценке СФЗ КВО.

Полученные соискателем научные результаты хорошо обоснованы, обладают новизной и имеют высокую практическую значимость для обеспечения физической безопасности КВО и внесли заметный вклад в развитие теории и практики проектирования систем обеспечения физической безопасности КВО.

Таким образом, диссертация Костины В.Н. является законченным научным исследованием, характеризующимся внутренним единством,

содержащим важные теоретические и прикладные результаты, имеющие важное хозяйственное значение.

Работа отвечает критериям «Положения о порядке присуждения ученых степеней», которым должны соответствовать диссертации, представленные на соискание ученой степени доктора наук, а соискатель 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:

декан факультета управления и бизнеса  
федерального государственного бюджетного образовательного учреждения  
высшего образования «Ангарский государственный технический  
университет»,  
доктор технических наук, доцент  
28 июля 2021 г.



А. Л. Истомин

Адрес (рабочий): 665835, Иркутская область, г. Ангарск, ул. Чайковского, д. 60. Телефон: +7(3955)673417, E-mail: [a.l.istomin@mail.ru](mailto:a.l.istomin@mail.ru)

Наименование организации (место работы): Федеральное государственное  
бюджетное образовательное учреждение высшего образования «Ангарский  
государственный технический университет»

Подпись Истомина Андрея Леонидовича заверяю:

Проректор по научной работе  
доктор технических наук, профессор



А.В. Бальчугов

28 июля 2021 г.