УТВЕРЖДАЮ
Начальник Воронежского института МВД России
кандидат философских наук

_____ А.П. Нахимов
«15» 06 2021 г.

**О Т З Ы В**

ведущей организации 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)

**1. Актуальность работы.**

Задача обеспечения безопасности критически важных объектов (КВО) является крайне актуальной. Президентом Российской Федерации, Правительством Российской Федерации и ФСТЭК России принимается множество нормативных документов, направленных на обеспечение безопасности КВО. Кроме того, в настоящее время информационные технологии присутствуют во всех сферах жизнедеятельности. Не исключением являются КВО, а именно автоматизированные системы управления технологическими процессами (АСУ ТП), которые обеспечивают управление производственными и технологическими процессами КВО. Это накладывает дополнительные повышенные требования к обеспечению безопасности АСУ ТП критически важных объектов, так как деструктивные действия нарушителей в отношении критических элементов и систем управления могут привести к возникновению чрезвычайных ситуаций (ЧС). В связи с изложенным развитие систем физической защиты (СФЗ) для обеспечения необходимой антитеррористической и информационной безопасности КВО является актуальной задачей.

Решение проблемы обеспечения безопасности КВО требует комплексного научного подхода к разработке в том числе и СФЗ. В связи с тем, что процесс разработки СФЗ требует системного похода к данной предметной области исследования, необходимо развивать методический аппарат выработки обоснованных решений в задачах проектирования СФЗ. Однако до сих пор не создавался методический аппарат, который бы применялся для принятия решений на всех этапах разработки СФЗ.

Данная проблема неразрывно связана с разработкой методик, моделей и методов обоснования и разработки СФЗ КВО, рассматриваемых в диссертационной работе Костина В.Н.

В связи с этим тема диссертации Костина В.Н. и сформулированная в работе научная проблема, направленная на повышение достоверности и

обоснованности принимаемых решений в задачах разработки СФЗ для обеспечения необходимой безопасности КВО, является актуальной и имеет важное практическое значение.

**2. Связь работы с планами соответствующих отраслей науки и народного хозяйства**.

Диссертационная работа Костина В.Н. тесно связана с одним из приоритетных направлений развития науки – безопасностью и противодействием терроризму, а сама технология обеспечения защиты и жизнедеятельности населения и опасных объектов, к которым относятся и критически важные объекты при угрозах террористических проявлений, включена в перечень критических технологий. Это положение отражено в Указе Президента Российской Федерации от 07.07.2011 № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации».

**3. Краткое содержание диссертационной работы.**

***Во введении*** рассмотрена актуальность работы, определены цель и решаемые задачи для ее достижения.

***В первой главе*** проведен анализ проблем проектирования СФЗ объектов. С системных позиций представлена предметная область исследований: объект защиты, внешняя среда, СФЗ. Рассмотрены диалектика развития угроз и СФЗ объектов как постоянно развивающиеся и совершенствующиеся противоборствующие системы. Обоснована актуальность заявленных исследований.

Отмечено, что современные КВО в своем составе, как правило, имеют АСУ ТП, которые осуществляют управление производственными и технологическими процессами КВО. Деструктивные действия нарушителей (внешние, внутренние угрозы) могут привести к возникновению ЧС.

Введен функционал обеспечения безопасности КВО и разработана схема управления безопасностью объекта при проектировании СФЗ, реализующая данный функционал.

Указано, что существующие программные комплексы используются только на этапе анализа эффективности уже спроектированных СФЗ, и перспективным направлением будет создание методологического аппарата выработки управленческих решений на всех этапах проектирования СФЗ, ориентированного на использование методов системного анализа.

***Во второй главе*** определена нелинейная функциональная зависимость энтропийного потенциала опасности масштабов чрезвычайных ситуаций, которая введена для оценки величины потенциалов опасности для КВО.

На основе адаптированного информационно-вероятностного метода (ИВМ) разработана методика категорирования КВО. Предложен информационный (энтропийный) критерий формирования категорий, позволяющий производить декомпозицию всего спектра опасностей на

категории, при этом величина опасности смежных категорий значимо отличается друг от друга.

На основе метода главных компонент (МГК) проведена оценка связи характеристик потерь объекта защиты, определены понятия привлекательности и опасности объекта. Предложены обоснованные значения величины показателя безопасного состояния для каждой категории КВО.

***В третьей главе*** предложена методика определения энтропийных потенциалов опасности нарушителей и исследования структуры характеристик нарушителей на основе обработки их МГК и ИВМ. Определены потенциалы опасности (подготовленности) шести типовых нарушителей различными методами. Степень опасности нарушителя представлена двумя компонентами: физической (технической) подготовкой и информационной (интеллектуальной) подготовкой.

На основе формирования общего информационного поля проведена оценка связи характеристик категорируемых объектов и нарушителей для определения базовых нарушителей. В результате для каждой категории объектов были получены соответствующие базовые нарушители.

Разработана методика прогнозирования временного интервала значимого изменения активности внешней среды для определения периода модернизации СФЗ.

***В четвертой главе*** разработана модель определения требований к подсистемам СФЗ на основе реализации функционала управления безопасностью КВО. Сформирована концептуальная имитационная модель противоборства нарушителя и СФЗ. Проведена оценка адекватности модели реальному физическому процессу в контрольных точках моделирования результатов. На основе проведения эксперимента на модели сформировано уравнение отклика функции потерь. Путем градиентного спуска получена минимальная величина уровня потерь для задания требований эффективности к подсистемам СФЗ.

***В пятой главе*** разработана методика оптимального размещения и выбора инженерно-технических средств охраны (ИТСО) СФЗ. В основу разработки методики положены требования руководящих документов ФСТЭК России. Введен показатель обеспечения информационной безопасности КВО – граница контролируемой зоны.

Методика формирования оптимального размещения и выбора ИТСО охраняемого объекта обеспечивает антитеррористическую и информационную безопасность КВО (безопасность контролируемой зоны).

Разработана методика формирования элементов структуры организационного управления. На основе МГК и ИВМ предложен вариант формирования элементов структуры организационного управления СФЗ.

***В шестой главе*** разработаны методы оценки эффективности СФЗ и утечки информации о функционировании СФЗ.

Каждый маршрут проникновения и реакция на проникновение СФЗ моделировались с помощью двух взаимосвязанных марковских цепей. На основе вероятностей конечных событий оценивалась вероятность пресечения

нарушителя на каждом маршруте проникновения. При неудовлетворительных оценках повышение эффективности СФЗ рассматривалось за счет структурных изменений СФЗ по критерию «эффективность/стоимость». Для формирования уравнения регрессии «эффективность/стоимость» проводился эксперимент, и по функции отклика было установлено направление изменения определяющего параметра для повышения эффективности СФЗ.

Впервые введен показатель эффективности СФЗ – время утечки информации о функционировании СФЗ – и разработан метод его оценки. На основе МГК и ИВМ сформирована семантическая структура информации и соответствующая ей структура носителей этой информации в виде графа Кенига. Произведен переход к эквивалентной электрической схеме с переходными процессами, и на ее основе проведена оценка времени выработки решений по изменению информационной среды СФЗ.

**4. Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации.**

Новизна проведенных в работе исследований и полученных результатов состоит в теоретическом обобщении и решении важной научной проблемы. Автором самостоятельно получены следующие новые научные результаты.

1. Разработаны методологические основы исследования процесса проектирования СФЗ, отличающиеся введением формализованного критерия обеспечения безопасности КВО при управлении проектированием СФЗ, новым информационным наполнением этапов проектирования, введением в процесс разработки методики объединения технических средств обнаружения в группы, а также методов оценки эффективности и времени утечки информации о функционировании СФЗ для выработки обоснованных решений по повышению эффективности СФЗ.

2. Разработаны методики, использующие впервые введенный информационный критерий оптимальности развития СФЗ на основе информационно-вероятностного метода (ИВМ), а именно:

- методика категорирования КВО, отличающаяся введением энтропийной шкалы оценки масштаба потерь при ЧС и использованием информационного критерия в интерпретации значимого различия опасности категорий, позволяющего обоснованно производить декомпозицию спектра опасностей на категории;
- методика оценки опасности типовых нарушителей на основе анализа их характеристик методом главных компонент, позволяющая производить сравнительный анализ их опасности для КВО;
- методика определения базовых нарушителей для категорируемых объектов, отличающаяся оценкой однородности потенциалов опасности КВО и типовых нарушителей, повышающая уровень достоверности назначения нарушителей для КВО;
- методика оценки активности нарушителей во времени с использованием информационного критерия, позволяющая определить

параметры активности нарушителей на момент времени предполагаемой модернизации СФЗ по причине значимого изменения внешней среды.

3. Разработана модель обоснования комплексного критерия эффективности СФЗ, позволяющая обоснованно задавать требуемые критерии эффективности подсистем СФЗ.

4. Разработана методика размещения и выбора ИТСО объекта, отличающаяся использованием совокупности методов (модернизированной задачи о покрытии и синтезе вариантов назначения ИТСО на покрытия), позволяющая формировать структурную схему размещения ИТСО СФЗ.

5. Разработана методика объединения технических средств обнаружения в группы для формирования структуры организационного управления, позволяющая формировать организационные структуры управления с равномерной и оптимальной информационной нагрузкой на ее элементы.

6. Разработаны методы оценки эффективности СФЗ и выработки на этой основе управленческих решений:

- метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей, позволяющий вырабатывать рациональные решения о структурных изменениях СФЗ для повышения ее эффективности;

- метод оценки времени утечки информации о функционировании СФЗ, отличающийся впервые введенным информационным показателем СФЗ, – временем утечки информации о СФЗ, позволяющий вырабатывать управленческие решения по изменению информационной среды СФЗ для снижения информационного потенциала опасности нарушителя.

**5. Значимость для науки и производства (практики) полученных автором диссертации результатов.**

Оценивая диссертационную работу Костина В.Н. с точки зрения значимости для науки и производства, можно выделить высокий уровень реализации полученных научных результатов, а также возможность дальнейшего использования этих результатов на практике при проектировании СФЗ КВО.

Научная значимость результатов диссертационного исследования Костина В.Н. состоит в создании нового информационного подхода к принятию обоснованных решений при разработке СФЗ и разработке комплекса методик, моделей и методов для построения оптимальной структуры СФЗ при ее разработке.

В качестве важной особенности диссертационной работы Костина В.Н. следует отметить, что большинство научных результатов внедрены в практику проектирования СФЗ.

Другим важным и полезным практическим применением результатов диссертации Костина В.Н. является использование их в учебном процессе (Оренбургский государственный университет, Пензенский государственный университет).

По результатам анализа представленной работы можно говорить о том, что автор внес значительный вклад в развитие методического аппарата проектирования СФЗ.

**6. Соответствие автореферата основным положениям диссертации.**

Автореферат полностью отражает содержание диссертации. Название диссертации соответствует её содержанию и характеру выполненных исследований.

**7. Подтверждения опубликованных основных результатов диссертации в научной печати.**

Основные положения и результаты диссертационных исследований Костина В.Н. отражены в 41 публикации, в том числе в 1 монографии, 13 статьях в изданиях из перечня ВАК, в 1 издании, индексируемом в Scopus, 5 свидетельствах об официальной регистрации программ для ЭВМ, 5 отчетах по НИР.

**8. Заключение о соответствии диссертации критериям, установленным Положением о порядке присуждения ученых степеней.**

Диссертационная работа Костина В.Н. соответствует критериям, которым должна отвечать диссертация на соискание ученой степени, а именно пунктам 9 – 14, согласно постановлению правительства Российской Федерации «О порядке присуждения ученых степеней» от 24 сентября 2013 г. № 842.

**9. Недостатки и критические замечания.**

Диссертационная работы не лишена некоторых недостатков. К их числу следует отнести следующие.

1. В работе при назначении средств обнаружений на выбранные покрытия графа задача динамического программирования решена тривиально путем прямого перебора вариантов композиции технических средств обнаружения. Отсутствует обратный выбор оптимального решения.
2. В работе при формировании организационных структур СФЗ рассмотрен только фрагмент формирования структур при использовании однородных элементов, находящихся в одной компоненте. Неясно, каким образом формировать организационную структуру, когда элементы управления будут находиться в разных компонентах.
3. В работе при оценке эффективности СФЗ не определено, в течение какого промежутка времени необходимо моделировать перемещение нарушителя, сил реагирования и нейтрализации.
4. В методе оценки времени утечки информации о функционировании СФЗ параметры утечки информации между исполнителями имеют одинаковые значения, что не в полной мере согласуется с действительной реальностью.

**10. Заключение.**

Перечисленные выше недостатки не снижают общей положительной оценки диссертации Костина В.Н.

Диссертантом решена важная проблема, направленная на разработку методик, моделей и методов разработки СФЗ КВО на всех этапах ее проектирования.

Работа выполнена на современном методическом и научном уровне и содержит новые важные результаты в области проектирования СФЗ.

В целом диссертационная работа представляет законченную научно-квалификационную работу, в которой изложены научно обоснованные технические и технологические решения, необходимые для проектирования систем физической защиты критически важных объектов, внедрение которых вносит значительный вклад в обеспечение безопасности критически важных объектов. Диссертационная работа соответствует критериям «Положения о порядке присуждении ученых степеней» (утверждено Постановлением Правительства РФ № 842 от 24.09.2013 в ред. 02.08.2016) и паспорту специальности 05.13.01 – Системный анализ, управление и обработка информации (в науке и технике), а диссертант достоин присвоения ему ученой степени доктора технических наук по указанной специальности.

Отзыв ведущей организации на диссертацию Костина В.Н. на тему «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» обсужден и одобрен на заседании кафедры информационной безопасности Воронежского института МВД России (протокол № 10 от 08.06.2021).

Начальник кафедры
информационной безопасности
Воронежского института МВД России
кандидат технических наук О.И. Нестеровский

Почтовый адрес (рабочий):
394065, Россия, г. Воронеж, проспект Патриотов, д. 53,
Федеральное государственное казенное образовательное учреждение
высшего образования «Воронежский институт
Министерства внутренних дел Российской Федерации»,
кафедра информационной безопасности.
Телефон рабочий: +7 (732) 200-52-40.
E-mail: onesterovskii@mvd.ru.

Подпись Нестеровского О.И.
удостоверяю
начальник отделения
делопроизводства и режима
Воронежского института
МВД России Е.М. Долгих