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 настоящее время современные критически важные объекты (КВО), являются основными центрами обработки информации, в которых информационные и автоматизированные системы осуществляют управление технологическими процессами. Поэтому резко увеличивается значимость защищенности КВО от воздействия террористических угроз. В этом случае последствия от несанкционированного доступа и деструктивных действий в отношении объектов информатизации КВО и их критических элементов могут привести к техногенным катастрофам и человеческим жертвам. Это накладывает дополнительные требования по обеспечению безопасности КВО. К сожалению, меры физической безопасности не всегда адекватно соответствуют направленным на объект угрозам, так как часто проектирование систем физической защиты (СФЗ) КВО происходит без привлечения соответствующих теоретических научных результатов. Если для небольших объектов это не является критичным, то для крупных КВО ошибки разработчиков непосредственно сказываются на эффективности эксплуатации СФЗ и могут привести к более серьезным последствиям.

Процесс разработки и оценки СФЗ представляет последовательность взаимосвязанных этапов и крайне сложен. Без внедрения современного методического аппарата в процесс принятия решений разработки СФЗ нельзя качественно решить задачу ее проектирования. В связи с этим диссертационная работа Костин В.Н. направленная на разработку методологических основ обоснования и разработки СФЗ для обеспечения антитеррористической и информационной безопасности КВО является актуальной.

Новизна исследований и полученных в работе результатов. Процесс разработки и оценки СФЗ сопровождается почти отсутствием входных исходных данных, большой неопределенностью, многовариантностью построения систем защиты, трудно формализуем и невозможностью описать аналитическим выражением функционирование СФЗ. В этих условиях автор использовал целый спектр математического и методического аппарата, позволяющего производить анализ: угроз, объекта защиты, формировать размещение инженерно-технических средств охраны (ИТСО) на основе синтеза сложных систем и моделировать процесс функционирования и оценки СФЗ для принятия обоснованных решений по повышению эффективности защиты.

Заслугой автора является то, что разнородные этапы разработки и оценки СФЗ приведены в связанную систему методик, моделей и методов, направленных на построение методологических основ проектирования СФЗ. Кроме того, математический аппарат информационно-вероятностного метода внедрен во все этапы разработки и оценки СФЗ в виде методик, моделей и методов, позволяющих повысить качество (обоснованность) разработки и оценки СФЗ.

Кратко остановлюсь на основных результатах, полученных соискателем впервые. В этих результатах и состоит научная новизна исследования.

В первой главе автор подробно на основе системного подхода рассмотрел элементы предметной области как системы взаимно связанных и развивающихся элементов. Выявил, что в настоящее время программные системы используются в основном только для оценки эффективности на этапе уже созданной СФЗ. Поэтому основным звеном процесса разработки является принятие решений на всех этапах технологии проектирования СФЗ.

Автор ввел функционал управления безопасностью КВО и предложил схему управления безопасностью, реализующую данный функционал.

Определил недостатки существующего методического аппарата на каждом этапе проектирования СФЗ и обосновал содержание методологических основ, построенных на новых информационных подходах.

Во второй главе автор разработал методику категорирования объектов защиты. Ввел нелинейную энтропийную шкалу оценки масштабов потерь КВО при возникновении чрезвычайных ситуаций и предложил методику категорирования КВО на основе информационно-вероятностного метода. На основе полученных потенциалов опасности категорий КВО предложил необходимые показатели защищенности категорий объектов.

В третьей главе проведена сравнительная оценка энтропийных потенциалов опасности типовых угроз и структурный анализ их характеристик. Определены и интерпретированы две компоненты нарушителей. Первая компонента - техническая и физическая подготовка (мотивация), вторая - информационная подготовка нарушителя. То есть современный нарушитель безопасности КВО - это хорошо информационно подготовленный человек.

На основе формирования общего информационного поля потерь КВО от воздействий угроз в энтропийных шкалах определены базовые типовые нарушители для каждой категории КВО.

Так как СФЗ создается на определенный период жизненного цикла, на основе оценки значимого изменения внешней ситуации спрогнозирован временной интервал модернизации СФЗ.

В четвертой главе разработана имитационная модель функционирования СФЗ. Используя теорию планирования эксперимента на имитационной модели, реализован функционал управления безопасностью КВО и позволяющий задавать требуемые показатели эффективности к подсистемам СФЗ.

В пятой главе разработана методика размещения и выбора ИТСО, реализующая показатели эффективности подсистем СФЗ, заданные в четвертой главе. Введен дополнительный показатель обеспечения информационной безопасности – контролируемая зона безопасности информационных систем для исключения утечки информации и деструктивных воздействий на информацию по техническим каналам. Предложена методика формирования организационных структур СФЗ, обеспечивающая равномерную информационную нагрузку на элементы управления СФЗ.

В шестой главе представлен метод оценки эффективности СФЗ на основе марковских цепей. Отличие метода состоит в возможности вырабатывать эффективные решения структурных изменений СФЗ для повышения ее эффективности.

Впервые введен показатель эффективности СФЗ – «время утечки информации о функционировании СФЗ» для принятия управленческих решений по генерации новых параметров (шифров, паролей и т.д.) СФЗ. Введение данного показателя снижает потенциал информационной подготовки нарушителя.

Достоверность полученных результатов

Достоверность полученных научных результатов подтверждается корректностью и обоснованностью автором предложенных методов, математических выкладок и доказательств, результатами экспериментов.

Научные результаты, представленные в диссертации, неоднократно обсуждались на научных семинарах и конференциях, в том числе и международных, получили положительную оценку, в достаточно полной степени отражены в многочисленных публикациях автора по теме диссертационной работы.

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; согласованностью результатов моделирования с данными, полученными при расчетах; непротиворечивостью полученных результатов с известными методами и моделями в данной предметной области; сходимостью теоретических расчетов с результатами экспериментальных исследований.

Значение полученных результатов для науки и практики

Работа имеет научный и практический характер. Научное значение диссертации заключается в том, что решена актуальная научная проблема, имеющая важное хозяйственное значение и представляющая собой методологическое обоснование и решение ключевых задач проблемы обоснованности принимаемых решений при разработке и оценке СФЗ КВО.

Практическая значимость заключается в разработке комплекса методик, моделей и методов принятия обоснованных решений на всех этапах проектирования СФЗ: методики категорирования КВО, оценки опасности нарушителей, определения базовых типовых нарушителей для каждой категории КВО, определения периода модернизации СФЗ, модели задания показателей эффективности подсистем СФЗ (что очень важно для проектировщика), методики размещения ИТСО, обеспечивающая заданные показатели эффективности СФЗ, методики формирования организационных структур СФЗ, методов оценки эффективности СФЗ, позволяющий принимать эффективные решения по структурной модернизации СФЗ и времени утечки информации о функционировании СФЗ, позволяющей уменьшать потенциал подготовки нарушителя на 13%.

Реализация результатов работы

Предлагаемые методики, модели и методы принятия обоснованых решений на всех этапах разработки и оценки СФЗ были успешно применены в ряде организаций, в частности, на предприятиях министерства обороны РФ, в частных компаниях, занимающихся аттестацией КВО по информационной безопасности, а также в учебных процессах ряда высших образовательных заведениях России.

Практическое использование результатов диссертационной работы подтверждено соответствующими документами о внедрении.

Апробация результатов и публикации по работе

Согласно автореферату, апробация основных теоретических положений докладывались, обсуждались и получили положительную оценку на научно-технических конференциях различного уровня, проводившихся в нашей стране и за рубежом по проблемам системного анализа, управления, информационным технологиям, комплексной защиты КВО.

Результаты теоретических и экспериментальных исследований легли в основу курсов лекций, читаемых автором: «Основы информационной безопасности» – Оренбургский государственный университет. Результаты изданной монографии широко используются студентами Оренбургского государственного университета при проведении научно-исследовательских работ, написании выпускных квалификационных работ и магистерских диссертаций.

Результаты диссертационной работы непосредственно отражены более чем в 40 публикациях, в том числе в 1 монографии, 41 статьях (включая 13 в изданиях из перечня ВАК), 5 свидетельствах об официальной регистрации программ для ЭВМ, 5 отчетах по НИР.

Работа Костина В.Н. ориентирована на решение сложной научно-технической проблемы, комплексное решение которой актуально и направлено на повышение достоверности и обоснованности принимаемых решений на всех этапах проектирования СФЗ КВО, заключающейся в разработке методик, моделей и методов на базе информационных критериев оптимальности, совокупности математических методов и современных форм обработки информации.

Научные положения, выводы и рекомендации удовлетворяют критериям новизны, достоверности и обоснованности.

Замечания.

1. Чем объяснить возникновение перегиба на функции энтропийных потенциалов опасности критически важных объектов (рисунок 2.3) и как это влияет на формирование категорий.

2. Не обосновано, почему в методике размещения и выбора элементов инженерно-технических средств охраны решение задачи задержки времени проникновения нарушителя были рассмотрены только за счет более раннего обнаружения нарушителя, т.е. инженерные средства задержки нарушителей (барьеры и т. д.) не рассматривались.

3. В работе рассмотрены частные оценки показателей эффективности методов разработки СФЗ. Однако общая оценка прироста критерия эффективности от внедрения множества разработанных методик, моделей и методов не приводится.

4. В диссертации базовые типовые нарушители определены для критически важных объектов, а не для критических элементов объекта. Это может привести к завышению показателей защищенности для менее значимых критических элементов КВО.

Указанные замечания не влияют на основные результаты диссертационного исследования.

Выводы.

Содержание автореферата диссертации, а также многочисленные публикации автора полностью отражают содержание диссертационной работы.

Диссертационная работа Костина В.Н. изложена технически грамотным языком и в хорошем стиле, содержит незначительное количество стилистических погрешностей и опечаток, хорошо структурирована и характеризуется внутренним единством и согласованностью теории с практикой проектирования и оценкой СФЗ КВО.

Диссертационная работа Костина В. Н. представляет собой самостоятельную научно-квалификационную работу, в которой **изложены научно-обоснованные технические и технологические решения** по повышению эффективности функционирования систем физической защиты критически важных объектов, **внедре-**

ние которых вносит значительный вклад в обеспечение безопасности критически важных объектов и развитие экономики страны. Диссертационная работа соответствует требованиям п.п. 9÷14 Постановления Правительства РФ «О порядке присуждения ученых степеней» от 24.09.2013 г. № 842, предъявляемых к докторским диссертациям, а ее 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 «Информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»,
доктор технических наук, профессор В.Т. Еременко
« 11 » июня 2021 г.

Подпись профессора Еременко Владимира Тарасовича заверяю:
Проректора по научно-технологической деятельности и аттестации научных кадров,
доктор технических наук, профессор С.Ю. Радченко
« 11 » июня 2021 г.
Телефон (рабочий): +7 (4862) 75-13-18, E-mail: info@oreluniver.ru

Адрес (рабочий): 302026, Российская Федерация, Орловская область, г. Орел, ул. Комсомольская, д. 95. Телефон: +7(920) 8126564, E-mail: wladimir@orel.ru
Наименование организации (место работы): Федеральное государственное бюджетное образовательное учреждение высшего образования «Орловский государственный университет имени И.С. Тургенева»