Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

На правах рукописи

ШНЯКИНА Елена Александровна

МЕТОДИКА ПРИНЯТИЯ РЕШЕНИЙ ПО ОБЕСПЕЧЕНИЮ ТРЕБУЕМОЙ ЭФФЕКТИВНОСТИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ НА ОСНОВЕ МНОГОМЕРНЫХ СТАТИСТИЧЕСКИХ МЕТОДОВ

2.3.1. Системный анализ, управление и обработка информации, статистика

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:
доктор технических наук, доцент
Костин Владимир Николаевич

Оренбург, 2025

Оглавление

Введение

Актуальность темы. Противодействие всем видам опасности для общества, экономики, государства предписано законодательством Российской Федерации, и внесено в перечень приоритетных направлений развития науки, технологий и техники. Физическую безопасность объектов обеспечивают системы физической защиты (СФЗ). При проектировании и эксплуатации СФЗ, особенно при изменении характеристик объектов, степени угрозы свершения террористического акта и т.д., проводится контроль соответствия существующего и требуемого уровней безопасности. В связи с этим, разработка методов для решения задачи оценки эффективности СФЗ и выработки решений для её повышения, является актуальной проблемой, имеющей научную и практическую значимость.

Степень разработанности темы исследования. Решение различных задач в области систем физической защиты представлены в работах Т.З. Аралбаева, А.В. Бояринцева, А.С. Боровского, А.Н. Бражника, Джеймс Ф. Бродера (James F. Broder), М. Гарсия (Mary Lynn Garcia), С.С. Звежинского, А.Г. Зуева, А.В. Измайлова, С.И. Корчагина, Р.Г. Магауенова, А.С. Олейника, О.А. Панина, Е.Г. Царьковой, И.М. Янникова и др.

Вопросами, связанными с эффективностью СФЗ, занимались М. Гарсия, О.А. Панин, А. В. Бояринцев, С. И. Корчагин, А. В. Леус. Учеными разработаны методы проектирования и оценки эффективности СФЗ, предложены методики категорирования и анализа уязвимости объектов, рассмотрены способы повышения вероятности обнаружения нарушителей техническими средствами обнаружения (ТСО). Однако, вопросы анализа СФЗ на основе декомпозиции её структуры, технологии выработки решений по обеспечению заданной эффективности СФЗ разработаны не достаточно и слабо отвечают современным тенденциям изменения внешних условий, а также, внутренней среды охраняемых объектов (ОО).

Существующие специализированные программные комплексы (EASI, ASSESS, SAFE, СПРУТ, Вега-2, PROSA, Итерация, Полигон) в основном используются только на этапе оценки эффективности СФЗ и не определяют оптимальные пути достижения требуемой эффективности.

Объект исследования: системы физической защиты охраняемых объектов.

Предмет исследования: модели, алгоритмы, методики, методы оценки и повышения эффективности СФЗ.

Целью диссертационной работы является повышение эффективности принятия решений для систем физической защиты на основе многомерных статистических методов.

Для достижения поставленной цели необходимо решить **задачи:**

1. На основе системного анализа предметной области разработать концептуальную модель, позволяющую исследовать пути повышения эффективности СФЗ.

2. Разработать методику идентификации потенциальных нарушителей для каждой категории ОО.

3. Построить имитационную модель оценки эффективности функционирования СФЗ.

4. Разработать методику принятия решений по изменению структуры СФЗ для повышения ее эффективности с целью обеспечения требуемой безопасности ОО.

Научная новизна работы.

1. Разработана концептуальная модель исследования путей повышения эффективности СФЗ, отличающаяся математическим обоснованием принимаемых решений на всех этапах исследования, позволяющая проводить рациональные изменения структуры СФЗ для обеспечения требуемой эффективности (4 пункт паспорта (ПП) специальности 2.3.1).

2. Разработана методика идентификации потенциальных нарушителей для каждой категории ОО, *отличающаяся* использованием соотношений

оценок потенциалов опасности нарушителей и ОО, вычисленных с использованием уточненной шкалы масштабов ЧС, *позволяющая* повысить обоснованность принимаемых решений (4 ПП специальности 2.3.1).

3. Разработана имитационная модель оценки эффективности функционирования СФЗ, *отличающаяся* возможностью моделирования всех маршрутов проникновения нарушителей с их детализацией на разнородные по величине защищенности участки (зоны) и использованием натурных статистических данных преодоления разнородных зон ОО, *позволяющая* повысить достоверность оценки эффективности СФЗ (4, 5 ПП специальности 2.3.1).

4. Разработана методика принятия решений по повышению эффективности СФЗ, отличающаяся декомпозицией модели уязвимости на компоненты и проведением множественного эксперимента для получения уравнения эффективности СФЗ, позволяющая принимать решения, направленные на структурные изменения СФЗ для повышения её эффективности до требуемого уровня (4 п. ПП специальности 2.3.1).

Теоретическая значимость работы заключается в разработке методики идентификации потенциальных нарушителей на основе перекрытия диапазонов требуемых вероятностей защиты от нарушителей и вероятностей безопасного состояния объектов; разработка имитационной модели физического процесса функционирования СФЗ; разработка методики принятия управленческих решений по повышению эффективности СФЗ, учитывающая неоднородность структуры СФЗ.

Практическая значимость работы заключается в развитии технологии и практической возможности оценки показателей эффективности СФЗ, а также, возможности вырабатывать оптимальные решения по изменению структуры СФЗ для повышения ее эффективности.

Методологической основой работы являются: методы системного анализа, принцип потенциального распределения вероятностей Хоменюка, многомерные статистические методы (кластерного и дискриминантного

анализа, главных компонент, факторный анализ, полный факторный эксперимент типа 2^k, корреляционно-регрессионный анализ), теория имитационного моделирования.

Достоверность и обоснованность результатов подтверждается использованием апробированного известного математического аппарата, а также согласованностью полученных результатов при обработке идентичной информации разными методами, детализацией маршрутов проникновения в имитационной модели оценки эффективности СФЗ и использованием входных данных по результатам натурных оценок на физическом объекте.

Основные положения, выносимые на защиту:

1. Концептуальная модель методического аппарата исследования эффективности СФЗ, позволяющая изменять структуру СФЗ для обеспечения требуемой эффективности на основе математически обоснованных решений;

2. Методика идентификации потенциальных нарушителей для категорий ОО, основанная на соотношении интервальных оценок вероятности безопасного состояния ОО и требуемой вероятности защиты от нарушителя, полученных с использованием уточненной шкалы потенциалов опасности масштабов ЧС для повышения обоснованности принимаемых решений;

3. Имитационная модель оценки эффективности функционирования СФЗ, позволяющая моделировать маршруты проникновения нарушителей, учитывая детализацию их на разнородные по величине защищенности участки (рубежи охраны), для повышения достоверности оценки эффективности СФЗ;

4. Методика принятия решений по повышению эффективности СФЗ до требуемого уровня, основанная на интерпретации уравнений эффективности СФЗ, полученных в ходе проведения множественного эксперимента.

Область исследования. Работа соответствует следующим пунктам паспорта специальности 2.3.1. «Системный анализ, управление и обработка информации, статистика»: п.4. – разработка методов и алгоритмов решения задач системного анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта; п.5. – разработка

специального математического и алгоритмического обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта.

Внедрение результатов работы. Материалы диссертации внедрены в практику оценки рисков критически важных объектов Оренбургского регионального отделения общероссийской общественной организации «Российское научное общество анализа риска», в процесс оценки эффективности СФЗ критически важных объектов 3 «ЦНИИ Минобороны России», в учебный процесс ФГБОУ ВО «Оренбургского государственного университета»

Основные положения и результаты диссертации докладывались и обсуждались на конференциях: XXXII международной научно-практической конференции «Приоритетные направления развития науки и технологий» (Тула, 2023 г.), Всероссийской научно-технической конференции «Современные научно-исследовательские и технологические аспекты программной инженерии» (Оренбург, 2023 г.), XXX Международной научно-практической конференции «Актуальные проблемы науки и образования в условиях современных вызовов» (Москва, 2024 г.), на XXVI Международной научно-технической конференции «Проблемы техники и телекоммуникаций» (Самара, 2024 г.).

Публикации. Теоретические и прикладные результаты отражены в 11 печатных работах, в том числе, 5 статей, опубликованы в изданиях рекомендованных ВАК РФ. Получены 2 свидетельства о государственной регистрации программ для ЭВМ.

Личный вклад. Все результаты, представленные в диссертации, получены автором лично. Выбор общего направления исследований и постановка задач осуществлялись совместно с научным руководителем. В работах, опубликованных автором в соавторстве, лично автором получены следующие результаты: [105, 119, 120, 121] – разработка методики идентификации потенциальных нарушителей; [87, 132] - разработка методики

принятия управленческих решений для повышения эффективности СФЗ до требуемого уровня; [48, 134] – разработка концептуальной модели методического аппарата исследования эффективности СФЗ; [110, 131] – разработка алгоритмов программ.

Структура и объем работы. Работа состоит из введения, 5 глав, заключения, библиографического списка, состоящего из 138 источников, приложений. Работа изложена на 160 страницах машинописного текста, содержит 18 рисунков, 51 таблица и 3 приложения.

Глава 1 Исследования в области повышения эффективности систем физической защиты

1.1 Современное состояние проблемы оценки и повышения эффективности систем физической защиты охраняемых объектов

Согласно 2 статьи Конституция Российской Федерации (РФ): «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства». Права и свободы личности, материальные и духовные ценности общества, а также конституционный строй, суверенитет и территориальная целостность государства относятся к основным объектам безопасности [1]. Главным субъектом обеспечения безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей [1]. Указом Президента РФ от 01.12.2016 г. № 642 «О Стратегии научно-технологического развития РФ» задачи, «связанные с безопасностью и противодействием техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики, государства, являются приоритетами научно-технологического развития РФ» [2].

Достижение целей обеспечения государственной и общественной безопасности, согласно Указа Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности РФ» (Ст. 4 П. 7), осуществляется «путем реализации государственной политики, направленной на решение следующих задач: повышение уровня антитеррористической защищенности мест массового пребывания людей, объектов жизнеобеспечения населения, организаций оборонно-промышленного, атомного, энергопромышленного, ядерного, оружейного, химического, топливно-энергетического комплексов страны, объектов транспортной инфраструктуры, других критически важных и потенциально опасных объектов; предупреждение и пресечение

террористической и экстремистской деятельности организаций и физических лиц, попыток совершения актов ядерного, химического и биологического терроризма» [3].

Федеральным законом от 31.07.2023 № 398-ФЗ «О внесении изменений в Уголовный кодекс РФ и статью 151 Уголовно-процессуального кодекса РФ» устанавливается уголовная ответственность за нарушение требований к антитеррористической защищённости объектов (территорий) [4]. Согласно перечисленным правовым документам обеспечение безопасности является обязательной задачей и регулируется законодательством РФ.

Анализ словарей [5-8] показал, что «отсутствие опасности» есть общий смысловой аспект дефиниции понятия «безопасность». В нормативно-правовых актах [3, 9-12] под безопасностью понимается «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз или опасностей». В работе [13] безопасность рассматривается с двух позиций:

как «состояние защищенности, предотвращающее возможность реализации угроз, минимизирующее воздействие угроз на объект, в случае их возникновения, и обеспечивающее защиту материальных и иных ценностей»;

как «свойство систем, входящих в состав физической безопасности объекта, заключающееся в способности предотвращать угрозы и противостоять им с целью защиты жизненно важных интересов объекта». [13, с.25]

Обеспечение безопасности можно определить как, «создание условий, при которых действие внешних и внутренних факторов (угроз) не приводит к выходу значений параметров состояния объекта за допустимые пределы» [14, с.9].

Базовый термин «безопасность» лежит в основе производных терминов: национальная безопасность, информационная безопасность, безопасность жизнедеятельности, и др.

Объектом настоящего исследования являются системы физической защиты (СФЗ), обеспечивающие «физическую безопасность» (ФБ) объектов,

представляющую собой «систему мероприятий, обеспечивающих защиту объекта от опасных воздействий» [15]. Основными (общими) задачами, которые решает СФЗ являются [16]:

- «предотвращение угроз, поддержание безопасного состояния объекта;
- своевременное обнаружение источника угроз;
- противодействие возникшим угрозам для замедления их развития и уменьшения последствий;
- пресечение угроз до момента нанесения объекту существенного ущерба;
- нейтрализация последствий, минимизация ущерба от реализации угрозы; (?)
- анализ произошедшего с целью совершенствования используемых средств СФЗ и методов их использования».

Перечисленные задачи формируют основные функции СФЗ:

- обнаружение: выявление скрытых или явных намерений нарушителей и передача сигнала тревоги в центр управления для определения его истинности или ложности. В случае, если сигнал тревоги является истинным устанавливаются его причины: место нарушения, количество нарушителей и т.д...» [17];
- задержка: замедление продвижения нарушителей к цели. Задержка является следующим этапом после обнаружения, до обнаружения задержка представляет собой сдерживание;
- реагирование: последовательность действий сил реагирования (сотрудников службы безопасности объекта и подразделений внешних охранных организаций), направленная на предотвращение достижения целей нарушителями: получение информации об обнаружении нарушителей; развертывание (действия в период между получением информации до занятия требуемых позиций); прерывание попытки нападения (определяется как прибытие в соответствующее место для остановки последовательности действий нарушителя) [17].

Решение задач и реализация функций обеспечиваются основными составляющими СФЗ: персоналом, организационными и техническими мероприятиями, комплексом инженерных и технических средств. Структура СФЗ представлена на рисунке 1.1.

Рисунок 1.1 - Структура СФЗ

Состав и структура СФЗ регулируются нормативно-правовыми актами [18-32]. При этом, для каждого конкретного объекта на основе общей разрабатывается своя, адаптированная СФЗ, учитывающая характер его деятельности, расположение, особенности обстановки и окружающей среды, условия функционирования.

Разработка СФЗ ведётся на основе комплексного научного подхода, важным (первым) этапом которого является создание концептуального проекта (модели). Концептуальный проект включает в себя принципы физической защиты ОО, структуру и состав инженерно-технических средств физической защиты, технико-экономическое обоснование СФЗ, сформированные на основе анализа уязвимости объекта. [15 с.46, 33, 34]. Технические решения, полученные в процессе концептуального проектирования, документируются на

завершающем этапе – рабочем проектировании. Анализ уязвимости объекта начинается с определения (понимания) того, что нужно защищать и в каких условиях [13, 15, 17]. Изучение ОО проводится с учетом рабочих процессов, условий деятельности и существующих ограничениях. На принятие решения о необходимом уровне защиты влияют следующие характеристики ОО:

- деятельность объекта, государственная, общественно-социальная, коммерческая или личностная значимость;
- военно-политическая, криминальная обстановки и тенденции их развития в районе расположения объекта и в соседних регионах;
- физико-географические условия функционирования объекта (местоположение, план объекта и поэтажные планы находящихся на нем зданий; инфраструктура; описание окружающей местности, климатические условия, наличие вблизи: шумового фона, электромагнитных помех, других объектов),
- рабочие процессы на объекте (количественный и качественный состав персонала, режим работы, процедуры, регламентирующие доступ различных категорий персонала в охраняемые зоны и их полномочия и т.д.);
- согласованность аварийной безопасности и СФЗ,
- юридические вопросы (ответственность при защите объекта (избыточность или недостаточность безопасности на объекте), трудовые отношения, критерии приема на работу) [17].

Физическая безопасность объектов, независимо от вида их деятельности, должна удовлетворять определенным стандартам, установленным органами государственного регулирования. Их требования к безопасности необходимо учитывать при разработке СФЗ.

Потенциальные возможности совершения действий, направленных на нарушение безопасности, формируют конкретные цели СФЗ ОО. Угроза безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [35]. Анализ угроз безопасности - это часть анализа риска, представляющего собой

комбинацию вероятности их успешной реализации и, возникающего при этом, величины потенциального ущерба [36 с.18]. Среди источников угроз выделяют:

- антропогенные (нарушители);

- техногенные (сбои в работе технических систем, неправильная конфигурация средств защиты и т.д.);

- стихийные (стихийные бедствия, события социально-политического характера) [37].

ФБ – это «отсутствие недопустимого риска от угроз, источником которых являются злоумышленные, противоправные действия физических лиц» [37], поэтому основные цели СФЗ ОО определяют угрозы, создаваемые антропогенным источником, представляющим собой субъектов – «нарушителей внутри или вне ОО, ошибочные или целенаправленные действия которых являются причинами нарушения безопасности» [37]. Совокупность характеристик нарушителя: уровень технической и физической подготовленности, осведомленности, спектр угроз формирует модель потенциального нарушителя ОО.

Основными угрозами безопасности являются:

- чрезвычайные ситуации;

- хищение, порча, уничтожение имущества;

- несанкционированный съем конфиденциальной информации;

- ухудшение эффективности функционирования [36, с.19].

Из всех угроз самыми критическими являются чрезвычайные ситуации. Источники угрозы (виды воздействия), цели защиты, последствия воздействий формируют пространство угроз (рисунок 1.2).

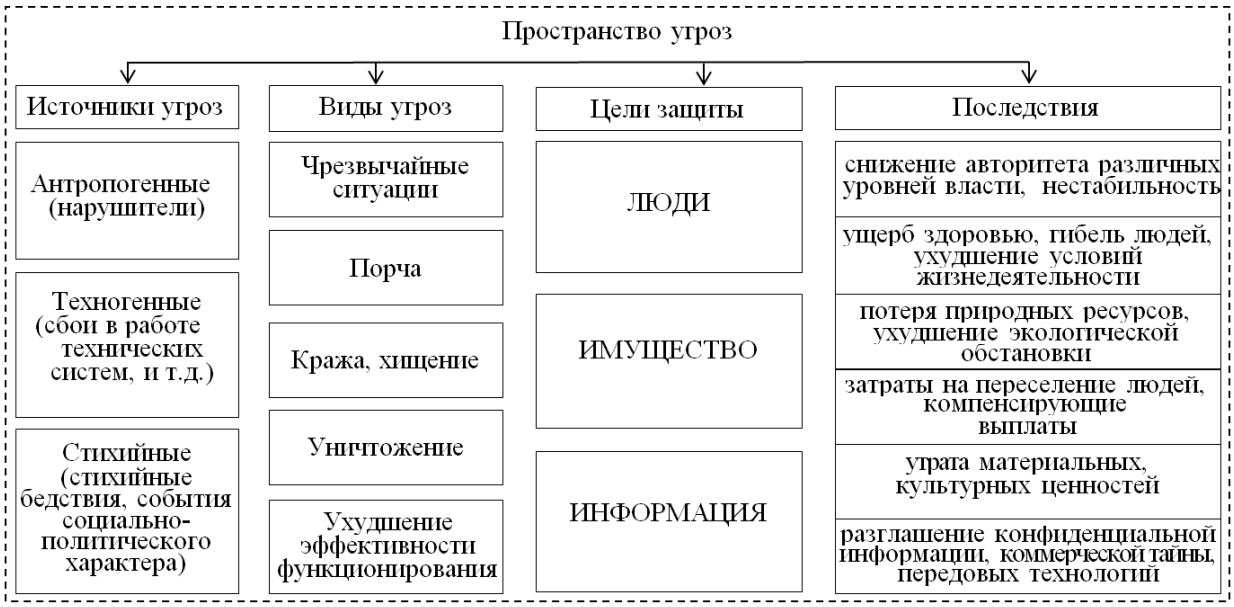


Рисунок 1.2 - Пространство угроз безопасности ОО

Выявленные угрозы и разработанные на их основе принципы физической защиты формируют концепцию физической безопасности объекта.

На основе сформированных целей и задач определяются характеристики существующей СФЗ (определяется способность существующей СФЗ обеспечивать необходимый уровень защиты) или создается проект новой системы. При проектировании СФЗ придерживаются концептуальных принципов обеспечения физической безопасности (ФБ):

- приоритет превентивного подхода к обеспечению безопасности;
- адекватность мер защиты пространству угроз;
- адаптивность;
- зональная (эшелонированная) защита;
- раннее обнаружение;
- постоянство уровня эффективности защиты во времени;
- баланс средств [36, с. 28].

Заключительным этапом создания СФЗ является оценка эффективности. В рамках концептуального проектирования, согласно существующим канонам, должно быть сформировано как минимум два варианта СФЗ [38]. Проектирование новой или анализ существующей СФЗ включает этап оценки эффективности, позволяющей определить уровень решения поставленных

перед ней задач. Эффективная СФЗ должна быть лишена недостаточности и избыточности.

Таким образом, в концептуальном проектировании можно выделить три основных этапа: определение требований к СФЗ; создание проекта СФЗ; анализ и оценка эффективности спроектированной СФЗ (рисунок 1.3).

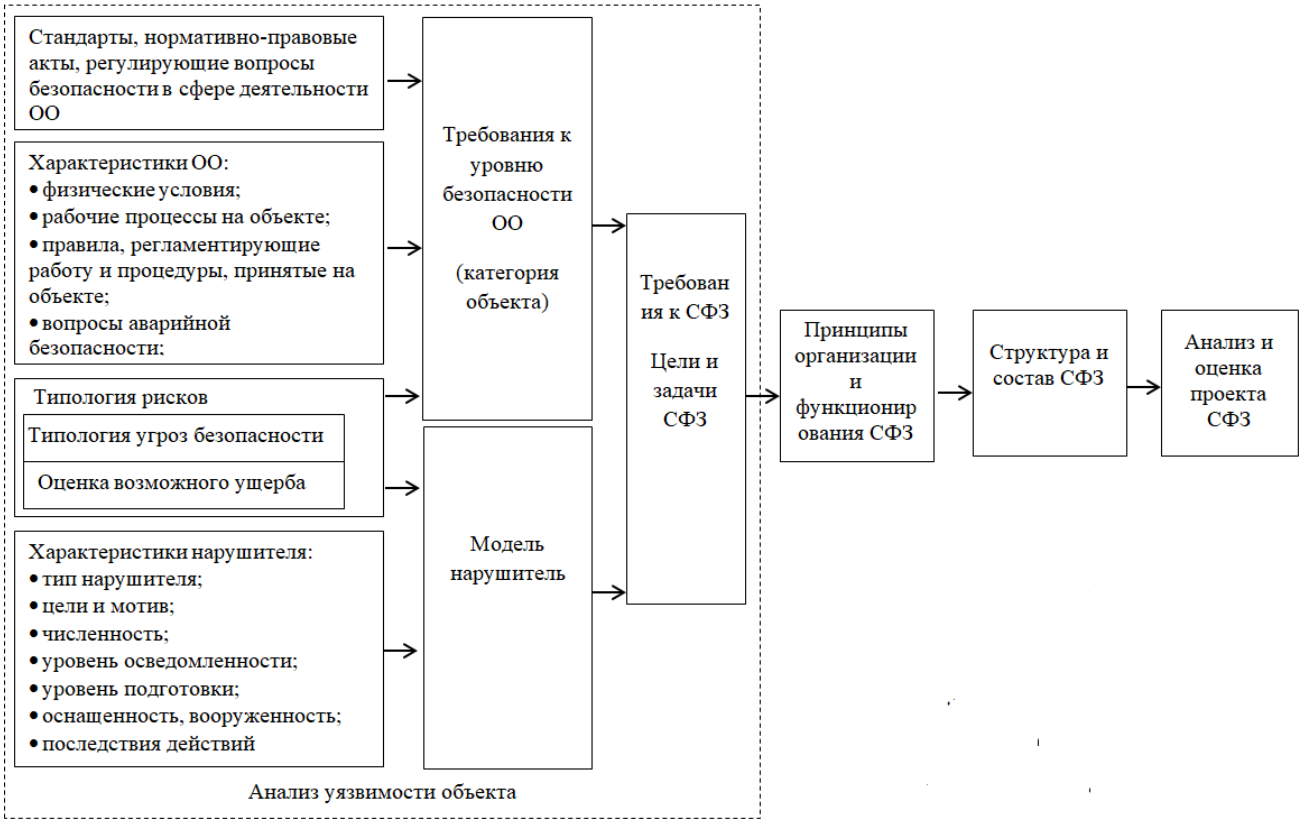


Рисунок 1.3 - Концептуальная модель проектирования СФЗ

Системный подход к проектированию СФЗ позволяет разработать интегрированную систему, объединяющую процедуры, инженерно-технические средства и людей, для решения задач защиты [17, с 36].

Жизненный цикл СФЗ представлен на рисунке 1.4.

Рисунок 1.4 – Жизненный цикл СФЗ

Жизнедеятельность ОО сопровождается изменением его внешней и внутренней сред. Внутренняя среда объекта определяется такими его характеристиками, как экономическая, экологическая, политическая и др. значимости, технологические процессы, физико-географические условия и т.д. К внешней среде ОО относятся: террористическая и криминогенная обстановки в регионе; руководящие документы в области обеспечения защищенности объектов; угрозы и т.д. Динамика перечисленных характеристик (факторов) влечет изменение требований к обеспечению безопасности объектов. В соответствии с этим, оценка эффективности СФЗ проводится при изменении какой-либо из характеристик, влияющих на безопасность ОО в течение срока, установленного нормативно-правовыми актами регулирующими вопросы безопасности в области народного хозяйства, к которому относится ОО. Кроме того, плановая оценка эффективности СФЗ проводится независимо от изменения ключевых характеристик, влияющих на безопасность, с периодичностью установленной нормативными документами (от трех до пяти лет, в зависимости от категории объекта) [39].

Следовательно, оценка эффективности СФЗ осуществляется:

- при вводе ОО в эксплуатацию (на этапе проектирования СФЗ);
- в отношении функционирующих (эксплуатируемых) ОО с частотой, установленной нормативно-правовыми документами;
- в случае изменения характеристик ОО, которые могут повлиять на требования к его безопасности.

По результатам оценки, в случае необходимости, проводится модернизация – изменение СФЗ с целью повышения эффективности до требуемого уровня.

1.2 Оценка эффективности систем физической защиты

Анализ государственных стандартов, словарей и научных работ в области организации безопасности объектов [16, 34, 40-46] позволил выявить следующие толкования термина «эффективность»:

- эффективность как результативность (effectiveness), под которой понимается «степень реализации запланированной деятельности и достижения запланированных результатов» [40]. Так, под эффективностью системы, в общем случае, принято понимать «совокупность свойств, характеризующих качество функционирования системы, оцениваемое как соответствие требуемого и достигаемого результата» [41]. Эффективность автоматизированной системы государственный стандарт [42] определяет как «свойство, характеризуемое степенью достижения целей, поставленных при ее создании».

- экономическая (ресурсоемкая) эффективность (efficiency) - «связь между достигнутым результатом и использованными ресурсами» [40], «соотнесение полученных выгод с ресурсами, затраченными для получения этих выгод» [43].

В рамках данного исследования, опираясь на иерархию понятий: «эффективность» → «эффективность системы» → «эффективность автоматизированной системы» → «эффективность СФЗ», под результативной эффективностью СФЗ понимается способность системы физической защиты обеспечить безопасное состояние ОО. Ресурсоемкая эффективность СФЗ – это соотношение стоимости СФЗ и прогнозируемого ущерба в случае реализации угрозы ОО.

Перечисленные определения эффективности формируют две стратегии оптимизации эффективности СФЗ. Постановка задачи первой стратегии заключается в обеспечении требуемого уровня безопасности СФЗ при минимальных затратах (оптимизация затрат при наложении ограничений на показатель характеризующий степень выполнения СФЗ своих функций). Второй – обеспечение максимально возможного уровня безопасности СФЗ при фиксированных затратах (оптимизация показателя, характеризующего степень выполнения СФЗ своих функций при фиксированных затратах). В отечественной и международной практике принято придерживаться первой стратегии повышения эффективности СФЗ (СФЗ должна обеспечивать уровень

безопасности не ниже допустимого (требуемого) при минимальных затратах на ресурсы, не превышающих величину потенциального ущерба ОО) [14, 45, 46]. Первая стратегия является приоритетной и в нашем исследовании.

Оценка эффективности выполняется на основе критерия – показателя эффективности, удовлетворяющего следующим требованиям:

- наличие определенного физического смысла;
- соответствие целям системы;
- возможность количественной оценки;
- чувствительность к изменениям параметров системы [34].

Вопросам способности СФЗ выполнять свои функции, посвящены работы отечественных и зарубежных авторов [16, 17, 47-55]. Их анализ позволил выделить основные методы оценки эффективности СФЗ: натурный эксперимент; логико-вероятностного моделирования; детерминистический; анализа иерархий; вероятностно-временного анализа.

1.2.1 Метод натурного эксперимента

Поэтапный метод оценки эффективности СФЗ. Чаще всего реализуется в форме тактических учений. [50]. Состоит из трех основных этапов:

1. Подготовительный этап. На данном этапе ставятся цели и задачи эксперимента. Разрабатываются сценарии проведения эксперимента, методики документирования действий группы, имитирующей действия «нарушителя» и реакции на них СФЗ.

2. Основная фаза эксперимента. Заключается в реализации разработанных сценариев проникновения нарушителей и документировании процесса защиты объекта в соответствии с разработанной методикой.

3. Подведение итогов. На основе анализа полученных результатов делается вывод об эффективности СФЗ, на основе которых принимается решение о необходимости её совершенствования.

Исходные данные: разработанный сценарий эксперимента.

Выходные данные: результаты эксперимента определяют эффективность СФЗ.

Метод в формате учений регулярно применяется на объектах ядерно-энергетического комплекса и других объектах с войсковой охраной.

Достоинства метода:

- наглядность результатов.

Недостатки метода:

- серьёзные организационные, материальные, временные затраты;

- рассматриваются «упрощенные» сценарии, с ограниченными разрушающими последствиями для ОО и СФЗ, исключающие травмы и потери среди участников эксперимента, с минимальными ограничениями функционирования ОО;

- отсутствие возможности многократного повторения эксперимента, и как следствие, невозможность ведения статистической оценки результатов эксперимента;

- «участники» эксперимента не имеют возможности инициативы, они действуют строго по сценарию учений;

- существует возможность разработки сценария эксперимента, предполагающего положительный результат в ущерб объективности [50].

1.2.2 Детерминистический метод

Экспертный метод оценки эффективности СФЗ, который заключается в проверке на соответствие требованиям, изложенным в проектной документации, ведомственных руководящих документах и т.д. трех составляющих [51]:

1. организационных мероприятий (группа a);

2. инженерно-технических средств охраны (группа b);

3. действий подразделений охраны (группа c).

Каждому физическому средству (ФС) каждый из экспертов (в зависимости от характера внешних и внутренних угроз, типа охраняемой зоны ОО (защищенной, внутренней или особо важной) в которой находится анализируемый элемент ФЗ ОО) назначает вес из диапазонов $a_{ij}=1, \ldots, 5$; $b_{ij}=1,$

…, 7; c_{ij}=1, ..., 10 (i - номер физического средства из групп a, b, c, j - номер эксперта).

Каждому i-му ФС, выбранному в ФЗ ОО, эксперты дают оценку степени реального состояния в диапазоне от 0 до 3. Более высокие значения весов ФС и показателей реального состояния ФС дают больший вклад соответствующих им элементов ФЗ ОО в несоответствие ФЗ требованиям к ФЗ ОО.

Эксперты определяют среднее значение показателя реального состояния каждого ФС

$$d_i = \frac{\sum_{j=1}^{n} d_{ij}}{n}, \qquad (1.1)$$

где d_{ij}- показатель реального состояния i-го ФС, назначенного j-м экспертом; n- число экспертов [51].

Определяются значения средних весов ФС для каждого класса:

$$a_i = \frac{\sum_{j=1}^{n} a_{ij}}{n}, \quad b_i = \frac{\sum_{j=1}^{n} b_{ij}}{n}, \quad c_i = \frac{\sum_{j=1}^{n} c_{ij}}{n} \qquad (1.2)$$

где a_{ij}, $b_{ij?}$ c_{ij} - показатель веса i-го ФС, назначенного j-м экспертом в соответствующей группе [51].

Оценка состояния ФЗ ОО вычисляется через показатели состояния составных частей:

а) организационных частей

$$N_1 = \frac{\sum_{i=1}^{k} a_i d_i}{d_m k a_m}; \qquad (1.3)$$

б) инженерно-технических средств

$$N_2 = \frac{\sum_{i=1}^{l} b_i d_i}{d_m k b_m}; \qquad (1.4)$$

в) действий подразделений охраны

$$N_3 = \frac{\sum_{i=1}^{m} c_i d_i}{d_m k c_m}, \qquad (1.5)$$

где k- число ФС в организационных мероприятиях;

l - в инженерно-технических средствах ФЗ;

m - в действиях подразделений охраны;

d_m- максимально возможное значение показателя реального состояния ФС (d_m =3);

a_m=5, b_m=7, c_m=10- максимально возможные значения весов ФС.

Среднее арифметическое значений N_1, N_2, N_3 есть показатель состояния ФЗ ОО:

$$N = \frac{N_1 + N_2 + N_3}{3} \qquad (1.6)$$

Оценка СФЗ объекта определяется на основе значения, полученного по формуле (1.6) (таблица 1.1).

Таблица 1.1 Оценка ФЗ ОО

Значение N	Интерпретация
0	базовое значение
≤ 0,05	соответствие требованиям норм и правил
(0,05; 0,07]	имеются отдельные отступления от требований норм и правил
(0,07; 0,1]	имеются значительные отступления от требований норм и правил, требующие использования компенсирующих мероприятий
>0,1	ФЗ ОО не обеспечивается

Исходные данные*:* матрица экспертных оценок, составленная на основе документации, соответствующей категории ОО.

Выходные данные: эффективность СФЗ определяемая через показатель состояния СФЗ, вычисленный по формуле (1.6).

Данный подход был разработан и применяется для оценки состояния ФЗ ядерно-опасных и радиационно-опасных объектов с учетом их специфики и руководящих документов в этой области. Для остальных видов ОО данный

метод может использоваться в качестве предварительного этапа оценки эффективности СФЗ или в качестве профилактических мероприятий.

Достоинства метода:

- простота применения;
- отсутствие сложных математических расчетов;
- отсутствие необходимости использования специализированного программного обеспечения;
- возможность применения как ко всей СФЗ в целом, так и её отдельным частям.

Недостатки метода:

- зависимость достоверности оценки от компетентности экспертов, их осведомленности об объекте, угрозах, структуре СФЗ;
- отсутствие учета реальных характеристик СФЗ;
- отсутствие возможности оценки правильности размещения и настройки инженерно-технических средств защиты охраны и т.д.;
- оценка объектов разного типа требует пересмотра перечня факторов и их критериев;
- зависимость исходных данных (факторов защиты) от действующих нормативных документов;
- узкая специфика метода [16].

1.2.3 Метод логико-вероятностного моделирования

Метод логико-вероятностного моделирования (ЛВМ) или логико-вероятностного анализа (ЛВА) представляет собой построение модели развития угрозы объекту, представленной в формализованном виде с применением операций булевой алгебры, и дальнейшем расчете степени риска с помощью теории вероятности [52,53]. В общем виде процедура анализа состоит из 4 этапов.

1. Построение модели функционирования системы с целью исследования проблемы. Для СФЗ ОО логико-вероятностной моделью функционирования системы является сценарий развития опасности, представленный в виде

ациклического графа. Множеством вершин графа являются инициирующие, промежуточные и конечные события сценария. Несанкционированные действия нарушителя (внешние воздействия) это инициирующие события. Например, такие как, преодоление ограждения периметра ОО с помощью нарушения его целостности или подкопа, перелезание через ограждение, проникновение на территорию через КПП путем подбора ПИН-кода, подделки проксимити карты, проникновение через служебный вход по сговору с сотрудником и т.д. Каждое инициирующее событие характеризуется вероятностью наступления. В качестве инициирующих событий выбираются конкретные, а не абстрактные события, вероятности которых можно достоверно оценить. Конъюнкции или дизъюнкции двух и более инициирующих событий представляют собой промежуточные события. Конечное событие описывает опасное состояние системы – реализацию угрозы.

2. Структурно-логическое моделирование на основе алгебры логики. Представленный в виде графа сценарий развития опасности описывается логической функцией опасности системы $f(z_1, z_2, \ldots, z_n)$, где $z_1, z_2, \ldots, z_n$ инициирующие события. n – их количество. Значение функции это конечное событие (опасное состояние системы). Дизъюнктивная нормальная форма $f(z_1, z_2, \ldots, z_n)$ интерпретируется как совокупность всех путей опасного функционирования объекта – конъюнктов инициирующих событий:

$$f(z_1, z_2, \ldots, z_n) = \bigvee[\bigwedge z_i], \qquad (1.7)$$

где $\bigvee$ - дизъюнкция, $\bigwedge$ - конъюнкция.

Кратчайший путь представляет собой минимальный набор инициирующих событий.

Инвертированная по правилу де Моргана функция опасности системы, есть функция безопасности системы:

$$\overline{f(z_{1,}, \ldots, z_{n,})} = \bigwedge[\bigvee \bar{z}_i], \qquad (1.8)$$

где $[\bigvee \bar{z}_i]$ – минимальные сечения предотвращения опасности, есть конъюнкция отрицаний инициирующих событий.

3. Преобразование функции опасности к стандартному виду, замена её вероятностной функцией. Совершенная дизъюнктивная нормальная форма или ортогональная дизъюнктивная нормальная форма функции опасности являются основой для построения вероятностной функции $P\{f(z_1, \ldots, z_m)\}$. Суть её построения заключается в замене элементов функции опасности:

z_i на вероятность наступления соответствующего ему i-го инициирующего события R_i,

$\overline{z_i}$ на вероятность того, что i-ое инициирующее событие не произойдет

$$Q_i = 1 - R_i. \qquad (1.9)$$

4. Количественная оценка степени риска. Вероятностная функция $Y(f) = P\{f(z_1, \ldots, z_m)\}$ интерпретируется как степень риска системы безопасности. Обратная величина

$$\Omega(f) = 1 - Y(f) \qquad (1.10)$$

характеризует эффективность СФЗ ОО.

Исходные данные: инициирующие события, интерпретируемые как нежелательные внешние воздействия на ОО, сценарий развития опасности.

Выходные данные: эффективность СФЗ ОО, определяемая через вероятность нахождения системы в безопасном состоянии в рамках построенного сценария развития опасности и вычисленная по формуле (1.10).

Областью применения метода являются оценки показателей надежности, живучести и безопасности, а также анализ причин отказов технических систем и прогнозирования аварий.

Достоинства метода:

- построение наглядной структуры функционирования СФЗ с указанием всех её подсистем;
- выявление слабых мест СФЗ и оценка степени риска каждого из них;
- получение обоснованного показателя эффективности СФЗ.

Недостатки метода:

- оценивается вероятность проникновения нарушителя на ОО без учета вероятности его задержания;

- отсутствие учета временных характеристик процесса преодоления физических барьеров;

- трудности с отображением последовательных действий на схеме для сложных объектов;

- проблема исходных данных (вероятностных характеристик СФЗ и нарушителя);

- для сложных объектов и при работе со сложными сценариями развития угроз, возникает большое количество трудоемких логических операций (устраняется применением программного обеспечения, использующих алгоритм метода ЛВА).

1.2.4 Метод анализа иерархий

Математический аппарат метода анализа иерархий (МАИ) применяется для решения различных задач, в том числе, и для оценки эффективности СФЗ. Результатом сравнения оценок экспертов является категорирование объектов рассматриваемой совокупности по степени уязвимости. Сравнение происходит последовательно, по этапам (иерархиям), представленным в таблице 1.2. На каждом уровне иерархии эксперты проводят парные сравнения элементов по степени важности относительно общей для них характеристики [16, 54, 55, 56, 57], которые сводятся в матрицы парных сравнений.

Таблица 1.2 Этапы методики анализа иерархий категорирования объектов

Этап	Задача	Альтернативы (факторы)
Модель нарушителя	Определить тип нарушителя	внешний
		смешанный
		внутренний
	Определить уровень подготовки нарушителя	хорошо подготовлен и оснащен
		средне подготовлен и оснащен
		плохо подготовлен и оснащен
Модель угроз	Определить вид возможного противоправного воздействия	Саботаж
		Кража
		Диверсия
		Теракт

Модель защиты	Определить эффективность элементов СФЗ с учетом модели нарушителя и модели угроз	инженерно-технические средства охраны
		охрана объектов специальными подразделениями
		организационное и нормативно-правовое обеспечение
Сравнение объектов	Провести сравнение объектов между собой на полноту выполненных на них мероприятий по созданию СФЗ	Объект № 1
		…
		Объект № N
Категорирование	Назначить категории сравниваемым объектам (в соответствии со степенью уязвимости объекта)	Категория I. Абсолютно уязвимый объект
		Категория II. Сильно уязвимый объект
		Категория III. Уязвимый объект
		Категория IV. Слабо уязвимый объект
		Категория V. Абсолютно неуязвимый объект

Шкала оценок, используемая экспертами, приведена в таблице 1.3.

Таблица 1.3 Шкала экспертных оценок

Шкала интенсивности	Интерпретация	Шкала интенсивности	Интерпретация
1	равная важность	7	значительное (очень сильное) превосходство
3	слабая значимость	9	абсолютное превосходство
5	существенная или сильная значимость	2, 4, 6, 8	промежуточные значения между соседними значениями шкалы

Для первого этапа (таблицы 1.2) матрица парных сравнений A представлена в таблице 1.4. Элементы матрицы a_{ij} (*i, j=1, 2, 3*) заполняются на основе шкалы экспертных оценок (таблица 1.3), причем $a_{ji}=1/a_{ij}$, $a_{ii}=1$.

Таблица 1.4 Матрица парных сравнений для определения типа нарушителей

Тип нарушителей	внешний	смешанный	внутренний	Приоритеты
внешний	$a_{11}=1$	a_{12}	a_{13}	k_1^1
смешанный	$a_{21}=1/a_{12}$	$a_{22}=1$	a_{23}	k_2^1
внутренний	$a_{31}=1/a_{13}$	$a_{32}=1/ a_{23}$	$a_{33}=1$	k_3^1

$k^1 = (k_1^1, k_2^1, k_3^1)^T$ – вектор локальных приоритетов, представляет собой относительные веса элементов сравнения. Существуют различные подходы к вычислению его элементов. Например, это могут быть нормализация среднегеометрических значений строк матрицы парных сравнений; или нормализация построчных сумм возведенных в достаточно высокие степени элементов матрицы парных сравнений a_{ij} [16, 54, 55, 56, 57].

Для оценки степени согласованности приоритетов вычисляется приближенное значение максимального собственного числа матрицы парных сравнений:

$$\lambda_{max}= Sk^i, \qquad (1.11)$$

где k^i – вектор локальных приоритетов, S – вектор–строка, составленная из сумм элементов столбцов матрицы сравнений A:

$$S = (\sum_{i=1}^{n} a_{i1}; \sum_{i=1}^{n} a_{i2}; ...; \sum_{i=1}^{n} a_{in}) , \qquad (1.12)$$

где *n* – число столбцов матрицы сравнений (число альтернатив).

Для первого этапа (таблица 1.2)

$$S=(a_{11}+a_{21}+a_{31}; a_{12}+a_{22}+a_{23}; a_{13}+a_{23}+a_{33})=(S_1; S_2: S_3) \qquad (1.13)$$

$$\lambda_{max}= S_1 k_1^1+ S_2 k_2^1+S_3 k_3^1. \qquad (1.14)$$

Значение λ_{max} используется для оценки согласованности обратно-симметричной матрицы и мнений экспертов. Чем ближе значение λ_{max} к числу *n*, тем выше согласованность результата. Еще одним критерием согласованности является отношение:

$$ОС = \frac{ИС}{СИ} \quad (1.15)$$

где ИС - индекс согласованности (отклонение от согласованности):

$$ИС = \frac{\lambda_{\max} - n}{n-1}. \quad (1.16)$$

СИ - среднестатистическое значение ИС «сгенерированных случайным образом по шкале от 1 до 9 обратно-симметричных матриц с соответствующими обратными величинами» [56].

Значения СИ для матриц порядка от 1 до 10 представлены в таблице 1.5.

Таблица 1.5 Значения случайного индекса

Порядок матрицы *n*	1	2	3	4	5	6	7	8	9	10
Случайная согласованность СС	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Значение ОС ≤ 0,1 считается приемлемым. В противном случае рекомендуется повторное заполнение матрицы парных сравнений.

На следующем этапе иерархии матрицы парных сравнений строятся для каждого типа нарушителей по степени их подготовленности. Так как рассматриваются три типа нарушителей, то строятся три матрицы и, соответственно, вычисляются три вектора приоритетов (таблицы 1.6 – 1.8).

Таблица 1.6 Вычисление вектора приоритетов k_1^1

k_1^1	Хорошо подготовлен и оснащен	Средне подготовлен и оснащен	Плохо подготовлен и оснащен	Приоритеты
хорошо подготовлен и оснащен	$a_{11}=1$	a_{12}	a_{13}	k_1^{21}
средне подготовлен и оснащен	$a_{21}=1/a_{12}$	$a_{22}=1$	a_{23}	k_2^{21}
плохо подготовлен и оснащен	$a_{31}=1/a_{13}$	$a_{32}=1/ a_{23}$	$a_{33}=1$	k_3^{21}

Таблица 1.7 Вычисление вектора приоритетов k_2^1

k_2^1	Хорошо подготовлен и оснащен	Средне подготовлен и оснащен	Плохо подготовлен и оснащен	Приоритеты
хорошо подготовлен и оснащен	$a_{11}=1$	a_{12}	a_{13}	k_1^{22}
средне подготовлен и оснащен	$a_{21}=1/a_{12}$	$a_{22}=1$	a_{23}	k_2^{22}
плохо подготовлен и оснащен	$a_{31}=1/a_{13}$	$a_{32}=1/ a_{23}$	$a_{33}=1$	k_3^{22}

Таблица 1.8 Вычисление вектора приоритетов k_3^1

k_3^1	Хорошо подготовлен и оснащен	Средне подготовлен и оснащен	Плохо подготовлен и оснащен	Приоритеты
хорошо подготовлен и оснащен	$a_{11}=1$	a_{12}	a_{13}	k_1^{23}
средне подготовлен и оснащен	$a_{21}=1/a_{12}$	$a_{22}=1$	a_{23}	k_2^{23}
плохо подготовлен и оснащен	$a_{31}=1/a_{13}$	$a_{32}=1/ a_{23}$	$a_{33}=1$	k_3^{23}

На основе векторов локальных приоритетов (таблицы 1.6 – 1.8), получаем вектор глобальных (обобщенных) приоритетов.

$$k^2 = \begin{pmatrix} k_1^{21} & k_1^{22} & k_1^{23} \\ k_2^{21} & k_2^{22} & k_2^{23} \\ k_3^{21} & k_3^{22} & k_3^{23} \end{pmatrix} \cdot \begin{pmatrix} k_1^1 \\ k_2^1 \\ k_3^1 \end{pmatrix} = \begin{pmatrix} k_1^2 \\ k_2^2 \\ k_3^2 \end{pmatrix}. \qquad (1.17)$$

Аналогичные анализ и вычисления проводятся на следующих уровнях иерархии. Синтез глобальных приоритетов на последнем уровне определяет возможность СФЗ противостоять угрозам (таблица 1.9).

Таблица 1.9 Интерпретация значений коэффициента k^6

Значение k^6	<0,05	[0,05; 0,1)	[0,1; 0,2)	[0,2; 0,4)	≥0,4
степень уязвимости объекта	абсолютная уязвимость	сильная уязвимость	умеренная уязвимость	слабая уязвимость	абсолютная неуязвимость

Исходные данные: составленные экспертами на каждом уровне иерархии матрицы парных сравнений.

Выходные данные: полученное значение приоритета k^6 и его словесное описание (таблица 1.9) являются результатом оценки эффективности, т.е. критерием эффективности СФЗ.

Основной областью применения являются СФЗ небольших типовых объектов, например, квартир, магазинов, офисов.

Достоинства метода:

- построение содержательной модели нарушителя;
- анализ возможных угроз; оценка эффективности элементов СФЗ, учитывающая угрозы и модели нарушителя;
- возможность рассмотреть альтернативы построения СФЗ ещё на этапе её проектирования.

Недостатки метода:

- отсутствие учета реальных характеристик нарушителя и СФЗ;
- зависимость достоверности оценки от компетентности аналитиков (экспертов);
- показатель эффективности является относительной, а не абсолютной величиной, так как вычисляется вследствие сравнения объектов между собой и отражает предпочтения аналитиков (экспертов);
- недостатки математического аппарата: возможна некорректная оценка при определенных наборах входных данных.

1.2.5 Метод вероятностно-временного анализа

Основой метода вероятностно-временного анализа (ВВА) является принцип своевременного обнаружения, согласно которому эффективность СФЗ определяется вероятностью обнаружения нарушителя в тот момент, когда у сил реагирования достаточно времени для перехвата нарушителя на пути к цели [17].

Исходные данные: вероятность обнаружения нарушителя, время задержки нарушителя, время реакции сил реагирования.

Выходные данные: вероятность своевременного обнаружения нарушителя.

Применяется для оценки СФЗ критически важных объектов, в частности, в области энергетики.

Исследование эффективности СФЗ происходит последовательно, на основе последовательных оценок показателей эффективности функций СФЗ:

1) обнаружение:

- вероятность обнаружения нарушителя;

- время, необходимое для сообщения о нападении и анализа полученной информации

2) задержка:

время, требуемое нарушителю (после обнаружения) для того, чтобы обойти каждый элемент задержки

3)реагирование:

- вероятность своевременного развертывания сил реагирования в районе расположения нарушителя и время, необходимое для этого [17]

Достоинства метода:

- обоснованная оценка эффективности СФЗ, вычисленная на её реальных характеристиках;

- возможность обнаружить критические элементы СФЗ: критическую точку обнаружения, критический маршрут нарушителя;

- позволяет определить пути улучшения СФЗ

Недостатки метода:

- проблема исходных данных: определение вероятности обнаружения, времени задержки, времени реагирования;

- необходимость совершенствования метода с учетом угрозы внутреннего нарушителя;

- высокая трудоёмкость анализа СФЗ для крупных объектов (необходимо рассмотреть большое количество возможных маршрутов нарушителей)

(устраняется применением программного обеспечения, использующих алгоритм метода ВВА).

В дальнейшем, под эффективностью СФЗ будет пониматься, являющаяся приоритетной, результативная оценка эффективности СФЗ. Для её исследования на основе анализа достоинств и недостатков каждого подхода выбран метод вероятностно-временного анализа.

1.3 Степень разработанности темы исследования

Данное диссертационное исследование направлено на разработку технологических решений задачи принятия обоснованных решений, направленных на повышение эффективности СФЗ. Проблемой исследования эффективности СФЗ занимались многие отечественные и зарубежные ученые. В их научных работах можно выделить следующие направления исследований: разработка методик оценки эффективности сложных систем, в том числе СФЗ, оценка эффективности конкретных категорий объектов; проектирование и совершенствование СФЗ, повышение эффективности работы ТСО.

Разработкой логико-вероятностного исчисления, являющегося основой одного из подходов к оценке эффективности СФЗ, занимались Ю.И. Журавлев, С.В. Макаров, Ю.В. Мерекин, И.А. Рябинин, L.Fratta, U.G.Montanari [58-61] и др.. На основе логики развития событий формализуются структурно-сложные системы более компактным способом, чем при словесном изложении, что позволило применить его для оценки эффективности сложных систем, в том числе, СФЗ [61].

В.Н. Бурков, Б.Н. Брук, Т. Саати [56, 62-64] разработали математический аппарат принятия решений в сложных задачах на основе системного подхода - метод анализа иерархий (МАИ). В ходе анализа задачи происходит структурирование проблемы в виде иерархии, на основе которой происходит сравнение и количественная оценка альтернативных вариантов решения. МАИ получил широкое применение для принятия решений в различных задачах, одной из которых является оценка эффективности СФЗ. Применение методик

логико-вероятностного моделирования и анализа иерархий к оценке эффективности СФЗ подробно изложено в параграфе 1.2.

Вопросы проектирования СФЗ и оценки эффективности СФЗ в целом рассматриваются в работах: М. Гарсиа, Джеймс Ф. Бродера, А.В. Бояринцева, А.Н. Бражника, А.Г. Зуева, И.М. Янникова, В.А. Куделькина и др.

М. Гарсиа на основе двадцатипятилетнего опыта работы в Национальной лаборатории «Сандия» Министерства энергетики США разработала концептуальную методологию проектирования СФЗ. В работе [17] описан вероятностно-временной подход, основанный на анализе эффективности отдельных компонентов для определения эффективности СФЗ ядерных объектов. Вероятностно-временной метод реализован в компьютерной модели EASI (Estimate of Adversary Sequence Interruption), целью которой является прогнозирование поведения системы защиты на заданном пути при определенных угрозах и состоянии самой системы.

Джеймс Ф. Бродер в работе [65] описывает процедуры, необходимые для оценки безопасности: вопросы оценки риска (понятия: риск угрозы, риск уязвимости), разработана модель количественной оценки безопасного состояния объекта [66].

Леус А.В. [67, 68] предложил «методику оценки эффективности СФЗ крупных распределённых объектов со сложной топологией». Её основой является «формализованная математическая модель СФЗ охраняемого объекта на основе клеточного поля с целыми значениями анализируемых параметров».

В монографии [69] А.В. Бояринцева, А.Н. Бражника, А.Г. Зуева изложены вопросы оценки и анализа эффективности СФЗ: предложена методика общегосударственного категорирования объектов независимо от их типа и ведомственной принадлежности. Авторы выделяют 10 категорий объектов. Категория присваивается объекту на основе «интегральной свертки» шести типов потерь: политических, людских, финансовых, экологических, культурных, экономических. [69]

Научными интересами Звежинского С.С., Волхонского В.В. являются вопросы, связанные с проектированием СФЗ, выработка технологических решений организации охраны ОО различных типов категорий [70 -73].

Вопросы повышения эффективности СФЗ с позиции функций компонентов системы: исследование способов повышения вероятности обнаружения техническими средствами обнаружения представлены в работах П.А. Воробьева, С.Ю. Быстрова, Р.Р. Трапш, В.И. Воловач и др..

Воробьев П.А. [74] провел анализ вероятности обнаружения нарушителя при радиальном и тангенциальном направлениях движения последнего относительно лучей диаграммы направленности (ДН) пассивного инфракрасного излучателя (ПИК). Для повышения вероятности обнаружения нарушителя автором разработан «алгоритм ортогональной обработки сигналов пироэлектрического приемника, структурная схема ПИК которые позволяют получить практически равномерную вероятность обнаружения нарушителя при различных способах его перемещения». Автор применяет «методы, позволяющие адаптивно менять форму ДН за счет использования многоэлементного пироэлектрического приемника с раздельными выходами».

Воловач В.И. в работе [75] на основе статистического анализа сигналов радиотехнических систем и устройств охраны получил математические модели адекватные реальным физическим процессам в данных технических средствах обнаружения. Воловач В.И. разработаны критерии, учитывающие: протяженный характер обнаруживаемых объектов, мгновенную вероятность обнаружения, законы непрерывно меняющейся дальности, условия априорной неопределенности относительно положения обнаруживаемого протяженного объекта и его параметров движения для оценки эффективности радиотехнических устройств охраны на открытых пространствах.

В рамках диссертационной работы Трапш Р.Р. [76] предлагает методы анализа уязвимостей и оценки эффективности пассивных инфракрасных (ПИК) извещателей, а также дает рекомендации по разработке структуры системы обнаружения на объекте. Для повышения надежности обнаружения в

исследовании использован метод разнесения каналов обнаружения извещателей, обеспечивающий инвариантность к направлению движении нарушителя.

О.А. Паниным сформулированы следующие требования к методикам категорирования объектов: относительная простота, непротиворечивость результатов категорирования, полнота учета различных видов потерь, универсальность, оптимальность выбора числа категорий. [77]

Разработкой математических моделей СФЗ занимались С.Ю. Быстров, А.С. Олейник, Т.Р. Гайнулин и др. Так, в работе [78] Быстров С.Ю. для особо важных объектов, имеющих сложную топологию, предложил математическую модель СФЗ на основе сети с кратными дугами, что позволяет получить интегральный показатель эффективности без применения операции редукции. Оценка эффективности СФЗ особо важных объектов проводится на основе разработанных автором функционально-стоимостных показателей, обеспечивающих выполнение оптимизации с учетом принципов равнопрочности и адекватности защиты.

Олейник А.С. [79, 80], используя аппарат теории игр, разработал математическую модель боевых столкновений сил охраны и нарушителей. В ходе моделирования происходит выбор наилучшей стратегии поведения сил защиты и проведения анализа возможных действий сил нападения.

Бесединым И.И. [81] на основе анализа показателей эффективности синтеза и состава комплекса инженерно-технических средств (КИТС) СФЗ сделан вывод о том, что «оценка эффективности должна учитывать соотношение между конечным эффектом $Э_{\Sigma}$ и затратами материальных ресурсов С, необходимых для его достижения: $Э_{\Sigma}/С \rightarrow max$. Конечный эффект представляет собой защищенность объекта, характеризуемую обратной величиной суммарного риска, получение которого за определенное время τ является целью мероприятия по нахождению структуры и состава КИТС СФЗ, где $\tau \leq \tau_{доп}$,. а $\tau_{доп}$, - допустимое время решения задачи по определению рациональной структуры и состава КИТС СФЗ промышленного объекта».

Малышкиным С.Л. [16] предложена «методика анализа эффективности средств обнаружения СФЗ объектов информатизации на основе последовательного применения методов структурирования диаграммы направленности, оценки формы и размеров зон обнаружения и анализа вероятности обнаружения».

Результатом исследования Тарасова А.Д. является «метод создания концептуального проекта СФЗ объектов информатизации. Основой метода является адаптивный генетический алгоритм, использующий многокритериальную оптимизацию взвешенных сумм целевых функций, процедуру поиска всех возможных путей перемещения нарушителя по территории объекта, отсеивающую нерациональные пути, в которой используется математический аппарат обработка графов и нечетких чисел» [82].

Гайнулин Т.Р. [83] «предложил формализовать процесс защиты на основе модели системы с полным перекрытием (модель Клементса-Хофмана); разработал алгоритмы автоматизированного проектирования СФЗ с применением формализованных методов выбора средств физической защиты на основе анализа критериев их эффективности». В работе использован математический аппарат «теории графов (для представления системы защиты), теории нечетких множеств (для определения значений вероятностных величин) и теории вероятностей (для расчета интегральных вероятностных показателей)».

Предметом исследования Востоковой О.В. [84] являются «математические модели функционирования и методы оценки эффективности пожарно-охранной системы безопасности (ПОСБ)». На примере объекта культуры «Русский музей» предложены: методики категорирования музея по величине потенциальных угроз и определения уязвимых мест музея. Автором при разработке модели функционирования охранной составляющей ПОСБ музея за основу взята модель EASI. Категорирование объектов проводилось по методике общегосударственного категорирования объектов «НПП «ИСТА-

Системс»» [69]. В качестве «показателем эффективности пожарно-охранной системы безопасности принята вероятность верификации несанкционированных действий нарушителя при передвижении маршруту, имеющему наименьшую защищенность» [84].

В работе Белова С.В. [85] выполнено теоретическое исследование процессов физической защищенности объектов обработки информации. На его основе разработаны принципы и технологии построения автоматизированной системы для анализа физической защищенности объекта обработки информации. Предложены методы решения задач:

- уточнение терминологии в области СФЗ;
- анализ методик оценки эффективности СФЗ;
- анализ ПО в области СФЗ;
- разработка методики определения угроз для конкретных типов охраняемых объектов (объектов культуры, объектов информатизации и т.д.);
- формирование требований к СФЗ;
- методика анализа эффективности технических средств обнаружения.

Практические методы управления рисками критических инфраструктур представили в своей работе Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л. [14]. Авторами также изложены формальная теория, методологические основания расчета рисков нарушения безопасности критически важных объектов на примере транспортной инфраструктуры с учетом неопределенности исходной информации высокой степени.

Таким образом, обзор исследований выявил: учеными разработаны методы проектирования и оценки эффективности СФЗ, предложены методики категорирования и анализа уязвимости объектов, рассмотрены способы повышения вероятности обнаружения нарушителей техническими средствами обнаружения (ТСО). Однако, вопросы анализа СФЗ на основе декомпозиции её структуры, технологии разработки решений по обеспечению заданной эффективности СФЗ разработаны не достаточно и слабо отвечают современным тенденциям изменения внешних условий, а также, внутренней среды ОО.

Следовательно, существуют противоречия между изменяющимися внешними и внутренними средами объекта (многообразие типов объектов охраны и структур СФЗ, совершенствование технических возможностей нарушителей, изменения характеристик ОО, влияющих на требования к его безопасности) и оперативной оценкой эффективности СФЗ и выработкой решений повышения эффективности до требуемого уровня. Это обусловило научную и практическую актуальность темы исследования: «Методика принятия решений по обеспечению требуемой эффективности СФЗ на основе многомерных статистических методов».

1.4 Постановка цели и задач исследования

Целью диссертационной работы является повышение эффективности принятия решений для систем физической защиты на основе многомерных статистических методов.

Для достижения поставленной цели предполагается решение следующих задач:

1. На основе системного анализа предметной области разработать концептуальную модель, позволяющую исследовать пути повышения эффективности СФЗ.

2. Разработать методику идентификации потенциальных нарушителей для каждой категории ОО.

3. Построить имитационную модель оценки эффективности функционирования СФЗ.

4. Разработать методику принятия решений по изменению структуры СФЗ для повышения ее эффективности с целью обеспечения требуемой безопасности ОО.

Выводы по первой главе

В главе представлен системный анализ процессов оценки и повышения эффективности СФЗ; рассмотрены основные методы исследования эффективности СФЗ (натурный эксперимент; логико-вероятностное моделирование; детерминистический метод; анализ иерархий; вероятностно-

временной анализ). От качества функционирования СФЗ зависит безопасность ОО, следовательно, оценка эффективности является необходимым процессом жизнедеятельности СФЗ. Она производится не только на этапе проектирования, но и в течение всего жизненного цикла СФЗ. В исследованиях и нормативно-правовых актах принято рассматривать эффективность с позиции «соотношения между вложенными ресурсами и результатом (потенциальными потерями)» и как «соответствие требуемого и достигнутого результатов». В нашем исследовании под эффективностью СФЗ понимается способность системы физической защиты обеспечить безопасное состояние ОО. На основе анализа сущности, достоинств и недостатков основных методов оценки эффективности СФЗ в работе выбран метод вероятностно-временного анализа. Критерием эффективности выступает вероятность нахождения ОО в безопасном состоянии $P_{бс}$ – показатель, характеризующий степень выполнения СФЗ своих основных функций: обнаружения, задержки, реагирования и нейтрализации нарушителя. Опираясь на отечественную и международную практику, принято решение придерживаться следующей стратегии оптимизации эффективности: СФЗ должна обеспечивать уровень безопасности не ниже допустимого (требуемого) при минимальных затратах на ресурсы, не превышающих величину потенциального ущерба ОО.

Анализ научных работ в области оценки и повышения эффективности СФЗ показал что, разработаны методы оценки эффективности СФЗ, рассмотрены способы повышения вероятности обнаружения нарушителей техническими средствами обнаружения (ТСО). Однако, вопросы анализа СФЗ на основе декомпозиции её структуры, технологии разработки решений по обеспечению заданной эффективности СФЗ разработаны не достаточно и слабо отвечают современным тенденциям изменения внешних условий, а также, внутренней среды ОО. Это позволило сформировать цель и задачи исследования.

Глава 2 Исследование путей повышения эффективности СФЗ

2.1 Системный анализ процесса повышения эффективности СФЗ

Разработка методики принятия решений повышения эффективности СФЗ до требуемого уровня требует формализации самого процесса оценки эффективности СФЗ. Методологической основой формализованной модели (оценки эффективности) СФЗ является модель с полным перекрытием, в основе которой лежит задача исключения (минимизации) всех возможных воздействий (угроз), направленных на защищаемые объекты (модель Клементса-Хоффмана) [14, 83].

Процесс обеспечения безопасности можно представить в виде кортежа:

$$S = <O, U, Y, M, V> \qquad (2.1)$$

Представим охраняемый объект конечным множеством прогнозируемых возможных (потенциальных) целей нарушителя (объектов защиты) $O = \{o_k | \ k = 1, \ldots, K\}$, определяющих потенциал опасности объекта.

$U = \{u_i | \ i = 1, \ldots, I\}$ - множество угроз и способов их реализации, которое характеризуется потенциалом опасности (угрозы) - величиной ожидаемого максимального ущерба при ее реализации.

Под уязвимостью понимается внутреннее свойство объекта, характеризующее возможность осуществления u_i–ой угрозы o_k-му объекту. В данной трактовке множество уязвимостей объекта Y является подмножеством декартового произведения $U \times O$:

$$Y \subseteq U \times O = \{y_r : y_r = < u_i; o_k >, r = 1, \ldots, R\} \qquad (2.2)$$

Матрица бинарного отношения Y представляет собой формальное представление требований по обеспечению безопасного состояния ОО, например:

$$Y = \begin{array}{c|cccc} & o_1 & o_2 & \ldots & o_K \\ u_1 & 1 & 0 & \ldots & 1 \\ u_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u_I & 1 & 1 & \cdots & 0 \end{array} \qquad (2.3)$$

$M = \{m_j | \ j = 1, \ ..., \ J\}$ - множество механизмов (средств) защиты, характеризующихся вероятностью нейтрализации уязвимостей y_r для обеспечения безопасного состояния ОО и материальными затратами (стоимостью) Z.

Для предотвращения наступления угроз необходимо каждой уязвимости поставить в соответствие элемент из множества M, т.е. пути реализации угроз перекрываются средствами защиты, что является задачей синтеза СФЗ для ОО. Формальная постановка которой представлена множеством V, являющимся декартовым произведением множеств Y, M:

$$V = Y \times M = \{s_l: \ s_l = < y_r; \ m_j > = < u_i; \ o_k \ ; \ m_j >, \ l = 1, \ ..., \ L\}, \qquad (2.4)$$

где каждой уязвимости y_r (или u_i угрозе o_k объекту) поставлен в соответствие механизм (средств) защиты m_j,.

Безопасное состояние объекта обеспечивается R-местным отношением подмножества M:

$$M_i = \{m_{ji}; \ m_j \in M, j = 1, \ ..., \ R\}, \ i = 1, \ldots, I \qquad (2.5)$$

где I - количество вариантов реализации СФЗ;

R - количество уязвимостей объекта.

$M_i = \{m_1, \ m_2, \ \ldots, \ m_R\}$ представляет собой i-ый вариант реализации СФЗ. Выбор варианта M_i осуществляется на основе оценки его эффективности.

Территория каждого объекта разделена на рубежи (зоны) охраны. Рубежи охраны неоднородны, так как отличаются друг от друга количеством и расположением зданий, инфраструктурой, персоналом, протяженностью (размерами), т.е. имеют различный потенциал опасности, а, следовательно, - различный уровень защищенности. Для нейтрализации нарушителя СФЗ последовательно выполняются функции обнаружения и задержки. Рубеж охраны, на котором произошло обнаружение нарушителя, является зоной обнаружения нарушителя. Последующие рубежи охраны, на пути нарушителя к цели будут являться зонами задержки. Таким образом, каждый рубеж может являться либо зоной обнаружения, либо зоной задержки и характеризуется следующими показателями: вероятностью обнаружения нарушителя P_o и

временем преодоления зоны - временем задержки $T_з$. Различный уровень защищенности рубежей охраны определяет неоднородность СФЗ.

«Путь нарушителя по территории объекта с момента проникновения до достижения цели» принято называть маршрутом [86]. Маршрут нарушителя проходит через различные рубежи охраны. Модель проникновения нарушителя на ОО представляется в виде ориентированного мультиграфа: $G=(V, E)$, где множество вершин графа V - рубежи охраны, через которые проходит маршрут нарушителя на пути к цели. Множество ребер графа E - варианты перемещения через рубежи охраны (рисунок 2.1).

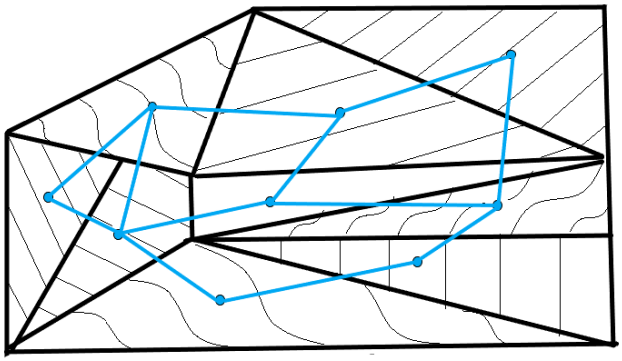


Рисунок 2.1 - Модель проникновения нарушителя

Неоднородность рубежей охраны влечет за собой неоднородность, проходящих через них, маршрутов нарушителей. [87]

Конечной целью любой СФЗ является обеспечение нахождения ОО в безопасном состоянии. Поэтому в качестве критерия эффективности СФЗ выступает вероятность нахождения ОО в безопасном состоянии $P_{бс}$ – показатель, характеризующий степень выполнения СФЗ своих основных функций: обнаружения, задержки, реагирования и нейтрализации нарушителя [13, 34, 88]:

$$P_{бс} = P_о \cdot P_{свп} \cdot P_н, \qquad (2.6)$$

где $P_о$ - вероятность обнаружения нарушителя,

$P_{свп}$ - вероятность своевременного прибытия сил реагирования (СР) в точку перехвата при условии обнаружения нарушителя,

$P_н$ - вероятность нейтрализации нарушителя при условии своевременного прибытия СР.

Будем считать, что в случае своевременного прибытия СР нейтрализация нарушителя является достоверным событием, т.е. $P_н$=1. Безопасность объекта определяется вариантом реализации СФЗ M_i (формула 2.5). $P_{свп}$ определяется соотношением времени своевременного прибытия сил реагирования ($T_{реаг}$) и времени задержки нарушителя на пути достижения им цели $T_з$. Т.е.

$$P_{бс}(M_i) = f(P_o, T_з, T_{реаг}) \qquad (2.7)$$

$P_{бс}$ обеспечивается значениями P_o и $P_{свп}$. P_o можно увеличить за счет более эффективных ТСО или их эшелонированием. Рост $P_{свп}$ обеспечивается увеличением времени задержки нарушителя $T_з$ (при не возрастающем времени своевременного прибытия СР $T_{реаг}$), которое можно осуществить за счет дополнительных средств задержки нарушителя. Все эти варианты характеризуются определенными материальными затратами Z. Формальное описание стратегии повышения эффективности СФЗ (параграф 1.2), являющейся приоритетной в нашем исследовании сформулировано следующим образом. Определить множество $M_i = \{m_1, m_2, \ldots, m_R\} \subset M$, обеспечивающее вероятность безопасного состояния ОО не меньше требуемого при минимуме затрат:

$$P_{бс}(P_{oi}, T_{зi}) \rightarrow P_{бс\ треб}, Z \leq Z_{\min} \qquad (2.8)$$

где P_{oi}, - вероятность обнаружения нарушителя на i-том маршруте;

$T_{зi}$ - время задержки нарушителя на i-том маршруте.

Оценка эффективности СФЗ определяется для каждого маршрута нарушителя. Для маршрутов, на которых эффективность СФЗ не соответствует требуемому уровню необходимо выработать решения для её повышения, которые должны учитывать его неоднородность. Различные маршруты требуют различных мероприятий по повышению эффективности СФЗ, имеющие разные градиенты направленности.

2.2 Концептуальная модель исследования путей повышения эффективности СФЗ

Для принятия решений по обеспечению требуемой эффективности СФЗ необходимо решить следующие задачи:

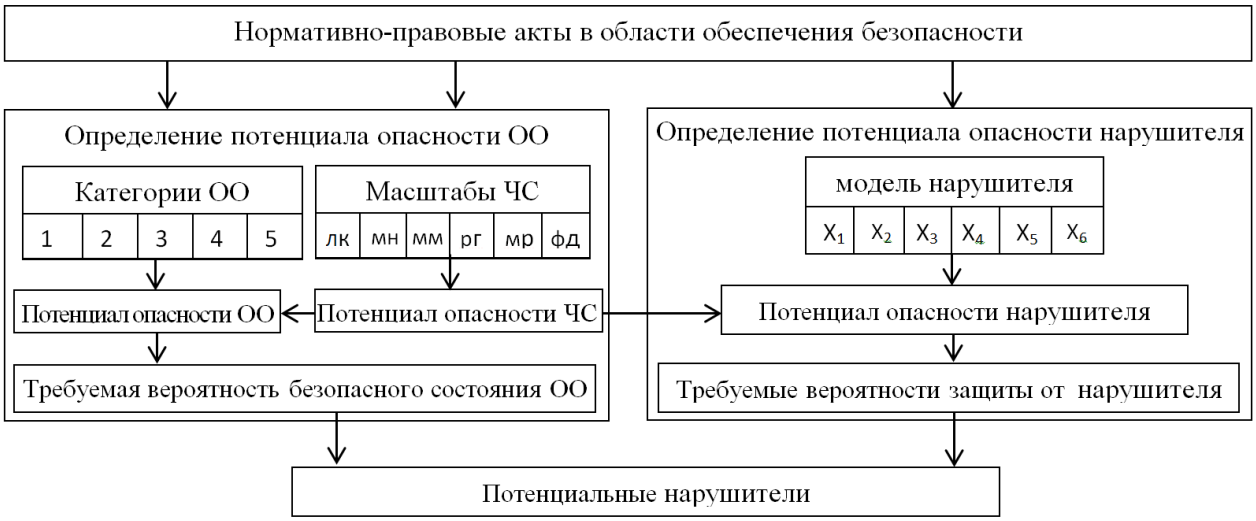
1. Определить цели СФЗ и требуемый уровень эффективности СФЗ;
2. Исследовать текущий уровень эффективности СФЗ;
3. Принять решения повышения эффективности СФЗ (в случае необходимости).

Обеспечение требуемой эффективности СФЗ начинается с определения значения требуемого уровня эффективности (уровня требуемой эффективности). Требуемый уровень эффективности СФЗ определяется величиной допустимого риска, т.е. величиной потенциальной опасности ОО. Потенциальная опасность ОО зависит от комплексной оценки его значимости: экологической, научно-технической, общественной, экономической, культурной, и др. Классификация объектов по степени их значимости – категорирование позволяет выработать общие требования безопасности для групп объектов, объединенных в одну категорию. Категория объекту присваивается по его наиболее опасному структурному элементу, поражение которого несет максимальный потенциальный (возможный) ущерб по сравнению с другими его структурными элементами [14].

Решение первой задачи можно разложить на следующие основные подзадачи:

- определение количества категорий объектов;
- определение критерия категорирования объектов, вычисление его количественных значений;
- вычисление диапазонов вероятностей безопасного состояния для каждой категории ОО;
- идентификация потенциальных нарушителей, как субъектов угроз, для каждой категории ОО.

Последовательность решения выделенных подзадач объединена в методику идентификации потенциальных нарушителей (рисунок 2.2).



ОО – охраняемые объекты, ЧС – чрезвычайные ситуации,

ЛК – локальный масштаб ЧС, МН - муниципальный масштаб ЧС, ММ - межмуниципальный масштаб ЧС,

РГ – региональный масштаб ЧС, МР - межрегиональный масштаб ЧС, ФД – федеральный масштаб ЧС

Рисунок 2.2 Методика идентификации потенциальных нарушителей

Входными данными являются нормативно-правовые документы в области обеспечения безопасности [89, 90, 91]. На основе анализа документа [89] выделены пять категорий ОО. Для определения значений критерия категорирования ОО и дальнейших вычислений диапазонов вероятностей безопасного состояния для каждой категории рассматривается наиболее опасный сценарий развития угроз объекту [14, с. 67], результатом которых являются чрезвычайные ситуации. Количественные характеристики масштабов чрезвычайных ситуаций [90]: материальный и территориальный ущербы, людские потери используются для определения потенциала опасности чрезвычайных ситуаций. Значения потенциалов опасности чрезвычайных ситуаций применяются в дальнейшем, при вычислении диапазонов требуемой вероятности безопасного состояния ОО, принятой в качестве критерия эффективности СФЗ, а также для вычисления диапазонов требуемой вероятности защиты от нарушителя. Перекрытие указанных диапазонов позволяет получить модели потенциальных нарушителей для каждой категории ОО.

Согласно международной и отечественной практике, организация безопасности на основе категорирования ОО позволяет наиболее оптимально распределить выделяемые на ее обеспечение затраты [14].

Для решения второй задачи применяется имитационная модель оценки эффективности СФЗ. Имитационное моделирование является удобным исследовательским инструментом, имеющим высокую прогностичность. Последовательная имитация основных функций СФЗ: обнаружения, задержки, нейтрализации не подвергает риску персонал и не нарушает процесс функционирования ОО, занимает меньше времени и ресурсов, т.е. имеет преимущества перед натурным экспериментом. Входные данные имитационной модели: время реагирования, количество маршрутов, для каждого маршрута: количество рубежей охраны, через которые проходит маршрут нарушителя, вероятность обнаружения и время задержки нарушителя на каждом рубеже. Выходные данные – вероятность безопасного состояния на каждом маршруте, получаемая как относительная частота пресечения несанкционированных действий нарушителя (число пресеченных атак нарушителя на объект к общему числу генерируемых атак нарушителя).

В случае, если полученные значения вероятности безопасного состояния меньше требуемого уровня решается третья задача. Первоначально производится декомпозиция маршрутов нарушителя, на основе выявленных между ними латентных связей, с помощью факторного анализа характеристик маршрутов проникновения. Для групп маршрутов нарушителей, имеющих вероятность безопасного состояния ниже требуемой, строятся уравнения регрессии с помощью полного факторного эксперимента. Анализ коэффициентов уравнения регрессии позволит принять решения по повышению вероятности безопасного состояния до требуемого уровня. Перечисленные действия решения третьей задачи объединены в методику принятия решений по повышению эффективности СФЗ (рисунок 2.3).

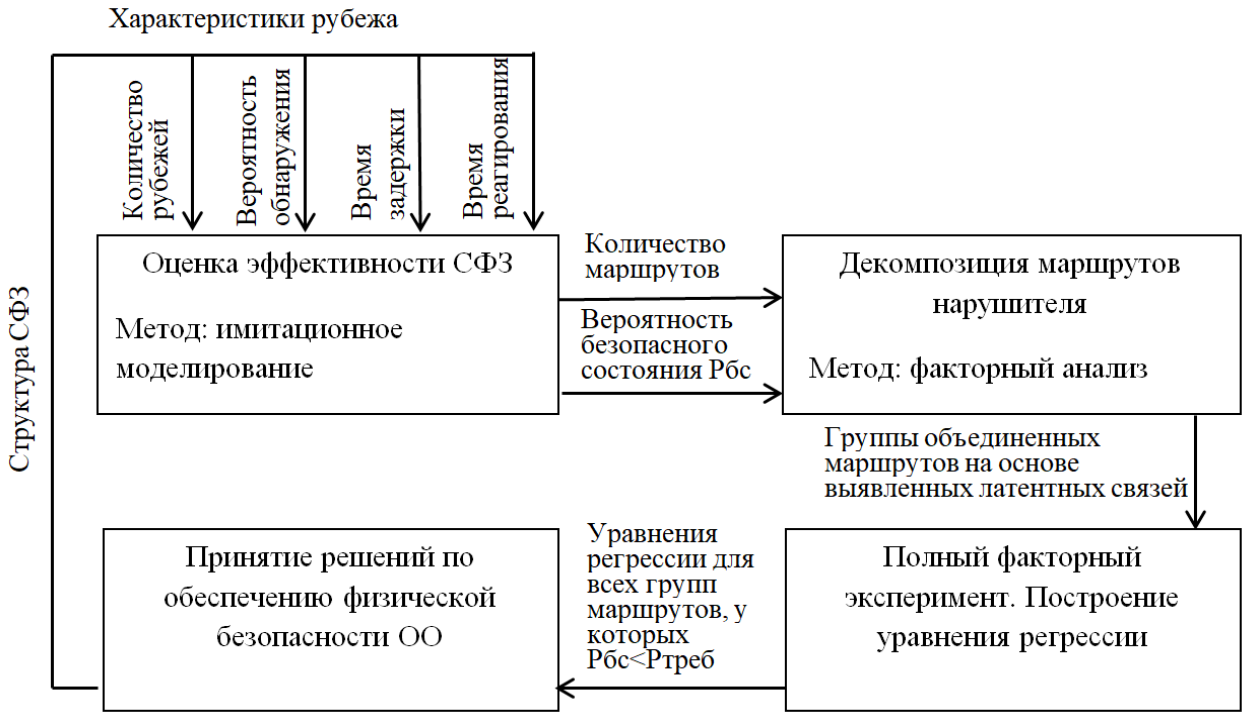


Рисунок 2.3 Методика принятия решений по повышению эффективности СФЗ

Методики решения поставленных задач объединены в концептуальную модель, представленную на рисунке 2.4.

Достоинства концептуальной модели заключаются в возможности определять латентные связи маршрутов проникновения, на их основе производить декомпозицию сложной задачи управления физической безопасностью ОО для получения более достоверных зависимостей вероятности безопасного состояния объекта от параметров (характеристик и структуры) СФЗ. Принятие решений учитывает разнородность маршрутов нарушителя и разнородность СФЗ.

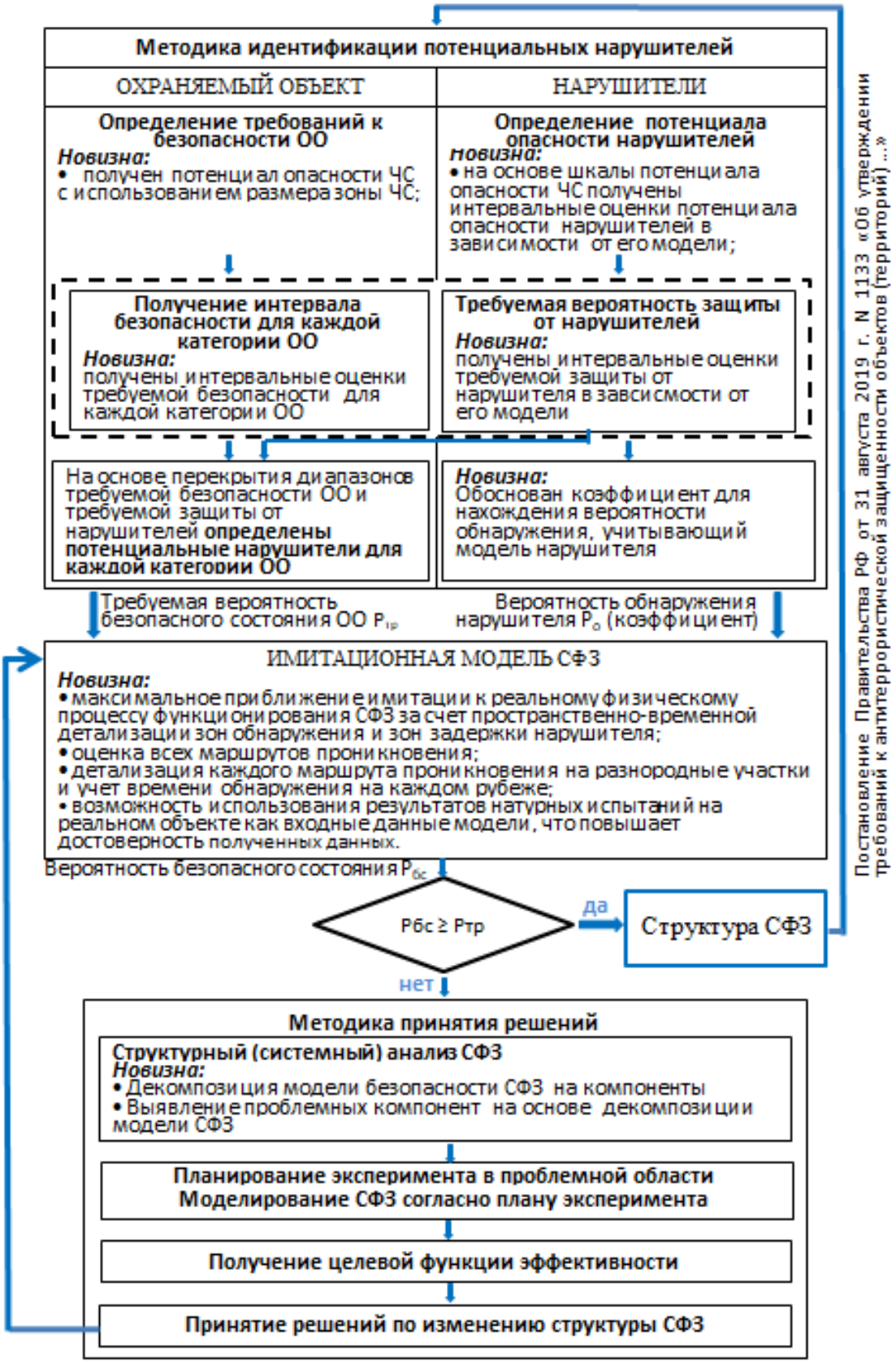


Рисунок 2.4 - Концептуальная модель исследования путей повышения эффективности СФЗ

Выводы по второй главе

В главе выполнена формализация процесса эффективности СФЗ. Процесс обеспечения безопасности можно представить в виде кортежа:

$$S = <O, U, Y, M, V>,$$

где O - множество прогнозируемых возможных (потенциальных) целей нарушителя (объектов защиты). U - множество угроз, M - множество механизмов (средств) защиты, Y - множество уязвимостей объекта, являющееся подмножеством декартового произведения $U \times O$:

Формальная постановка задачи синтеза СФЗ для ОО представлена множеством V, являющимся декартовым произведением множеств Y, M:

$$V = Y \times M = \{s_l: s_l = < y_r; m_j > = < u_i; o_k ; m_j >, l = 1, \ldots, L\},$$

где каждой уязвимости y_r (или u_i угрозе o_k объекту) поставлен в соответствие механизм (средств) защиты m_j,.

Формальное описание стратегии повышения эффективности СФЗ являющейся приоритетной в нашем исследовании сформулировано следующим образом. Определить множество $M_i = \{m_1, m_2, \ldots, m_R\} \subset M$ (вариант реализации СФЗ M_i, являющийся подмножеством множества механизмов защиты M), обеспечивающее вероятность безопасного состояния ОО не меньше требуемого при минимуме затрат:

$$P_{бс}(P_{oi}, T_{зі}) \rightarrow P_{бс\ треб}, Z \leq Z_{\min}$$

Показана сложная структура объекта, имеющая разнородные рубежи охраны по доступности к проникновению нарушителей. Как следствие, структура СФЗ также будет являться неоднородной, а именно, модель безопасности ОО как совокупность маршрутов проникновения через неоднородные рубежи охраняемых объектов также будут неоднородны. Поэтому мероприятия по оценке и повышению эффективности СФЗ будут иметь разные градиенты направленности, т.е. управление эффективностью распадается (разделяется) на отдельные компоненты.

Для решения задачи повышения эффективности СФЗ до требуемого уровня разработана концептуальная модель повышения эффективности СФЗ, включающая в себя: методику идентификации потенциальных нарушителей; имитационное моделирование; методику принятия решений.

Достоинствами модели являются возможность производить декомпозицию сложной задачи управления физической безопасностью ОО, учет разнородности маршрутов нарушителя и разнородность СФЗ, что позволяет увеличить достоверность зависимостей вероятности безопасного состояния объекта от параметров СФЗ.

Глава 3 Методика определения потенциальных нарушителей для категорируемых объектов

3.1 Определение необходимой безопасности для каждой категории охраняемого объекта

Оценка эффективности СФЗ начинается с определения целей СФЗ, которые формулируются на основе анализа характеристик охраняемого объекта (значимости и условий его функционирования), типов потенциальных угроз и ущерба в случае их успешной реализации. Так как основным субъектом угроз, нейтрализуемых СФЗ, является нарушитель, то основой определения потенциальных угроз для конкретного объекта является идентификация его потенциальных нарушителей.

Идентификацию потенциальных нарушителей представим последовательностью этапов: 1) определение необходимой безопасности для ОО; 2) определение требуемого уровня защиты от типовых нарушителей; 3) определение потенциальных нарушителей.

Согласно используемой в законодательных документах [35, 92-96] терминологии:

объект – «комплекс технологически и технически связанных между собой зданий, строений, сооружений и систем, отдельное здание, строение и сооружение, размещенные на обособленной территории (акватории), границы которой установлены в соответствии с законодательством РФ, и принадлежащие на праве собственности, аренды или ином законном основании физическим и юридическим лицам, которые осуществляют деятельность на территории РФ и иных территориях, над которыми РФ осуществляет юрисдикцию в соответствии с законодательством Российской Федерации и нормами международного права»;

охраняемый объект (ОО) – «отдельное помещение или несколько помещений в одном здании, объединенные единым периметром, здания, строения, сооружения, прилегающие к ним территории и акватории,

помещения, транспортные средства, а также грузы, денежные средства и иное имущество, подлежащее защите от противоправных посягательств».

ГОСТ Р 78.36.032-2013 [89] определяет следующие типы охраняемых объектов: критически важный объект, потенциально опасный объект, особо важный объект, объект с массовым пребыванием граждан, объект жизнеобеспечения (таблица 3.1) .

Таблица 3.1 – Типы охраняемых объектов

Тип объекта	Описание объекта
критически важный объект (КВО)	«это объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой РФ, субъекта РФ или административно-территориальной единицы субъекта РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения, проживающего на этой территории, на длительный период времени» [35, 89]
потенциально опасный объект (ПОО)	«это объект, на котором расположены здания и сооружения повышенного уровня ответственности, либо объект, на котором возможно одновременное пребывание более пяти тысяч человек» [89]
особо важный объект (ОВО)	«техногенный, природный, природно-техногенный объект, подверженный риску криминальных угроз нанесения неприемлемого ущерба самому объекту, природе и обществу, а также подверженный угрозам возникновения чрезвычайных обстоятельств» [36, 89]
объект с массовым пребыванием граждан (ОМПГ)	«здание или сооружение с одновременным пребыванием 50 и более человек (зрительные, обеденные, культовые и другие залы)» [89]
объект жизнеобеспечения (ОЖ)	«объект, на котором сконцентрирована совокупность жизненно важных материальных и финансовых средств, сгруппированных по функциональному предназначению и используемых для удовлетворения жизненно необходимых потребностей населения (например, в виде продуктов питания, жилья, предметов первой необходимости, а также в медицинском, санитарно-эпидемиологическом, информационном, транспортном, коммунально-бытовом обеспечении и др.)» [89]

Наиболее распространённой отечественной и международной практикой является зависимость предъявляемых к СФЗ требований от категории объекта [14, 97-104]. Категория объекта, согласно Национальному стандарту РФ «Системы охраны и безопасности» [35], представляет собой «комплексную оценку состояния опасности объекта, учитывающую его значимость (экономическую, научно-техническую, технологическую, культурную,

общественную и др.), последствий от возможных преступных посягательств на них, сложности требуемой надежности охраны» [35].

Категории КВО и ПОО представлены в таблице 3.2.

Таблица 3.2 - Категории КВО и ПОО и их характеристики

<table>
<tr><td colspan="6">критически важный объект [93]</td></tr>
<tr><td colspan="2">критически важные объекты федерального уровня значимости</td><td colspan="2">критически важные объекты регионального уровня значимости</td><td colspan="2">критически важные объекты муниципального уровня значимости</td></tr>
<tr><td colspan="2">объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой 2 и более субъектов РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения 2 и более субъектов РФ</td><td colspan="2">объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой субъекта РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения субъекта РФ</td><td colspan="2">объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой административно-территориальной единицы субъекта РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения административно-территориальной единицы субъекта РФ</td></tr>
<tr><td colspan="6">потенциально опасный объект [92]</td></tr>
<tr><td>1 категория опасности (особо высокий уровень опасности)</td><td>2 категория опасности (чрезвычайно высокий уровень опасности)</td><td>3 категория опасности (высокий уровень опасности)</td><td>4 категория опасности (повышенный уровень опасности)</td><td>5 категория опасности (средний уровень опасности)</td><td>6 категория опасности (низкий уровень опасности)</td></tr>
<tr><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации федерального характера</td><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации межрегионального характера</td><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации регионального характера</td><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации межмуниципального характера</td><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации муниципального характера</td><td>объекты, аварии на которых могут стать источником возникновения чрезвычайной ситуации не выше локального характера</td></tr>
</table>

В зависимости от ущерба, охраняемые объекты (таблица 3.1), ГОСТ Р 78.36.032-2013 [89] разделяет на две основные категории:

- А – объекты Государственной Власти, критически важные объекты, особо важные объекты, потенциально опасные объекты и объекты жизнеобеспечения, государственные, а также коммерческие объекты, преступные посягательства на которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества и иметь широкий международный и общественный резонанс;

- Б - объекты организаций различных форм собственности, преступные посягательства на которые могут привести к крупному и значительному материальному ущербу предприятию или собственнику.

В категории А выделяют в свою очередь, три группы: $А_1$, $А_2$, $А_3$, в категории Б – две: $Б_1$, $Б_2$ (рисунок 3.1).

Категория присваивается ОО по такому его элементу, поражение которого в случае наихудшего сценария развития угрозы несет максимальный ущерб [14]. Несанкционированное проникновение на ОО физических лиц: террористов, диверсантов, преступников, экстремистов инициализирует соответствующие объекту потенциальные угрозы безопасности, наиболее опасный вариант развития которых приводит к чрезвычайным ситуациям различного характера и масштаба.

Согласно Государственному стандарту РФ ГОСТ Р 22.0.02-2016 «Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий» чрезвычайная ситуация (ЧС) – «обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которая может повлечь или повлекла за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей» [96].

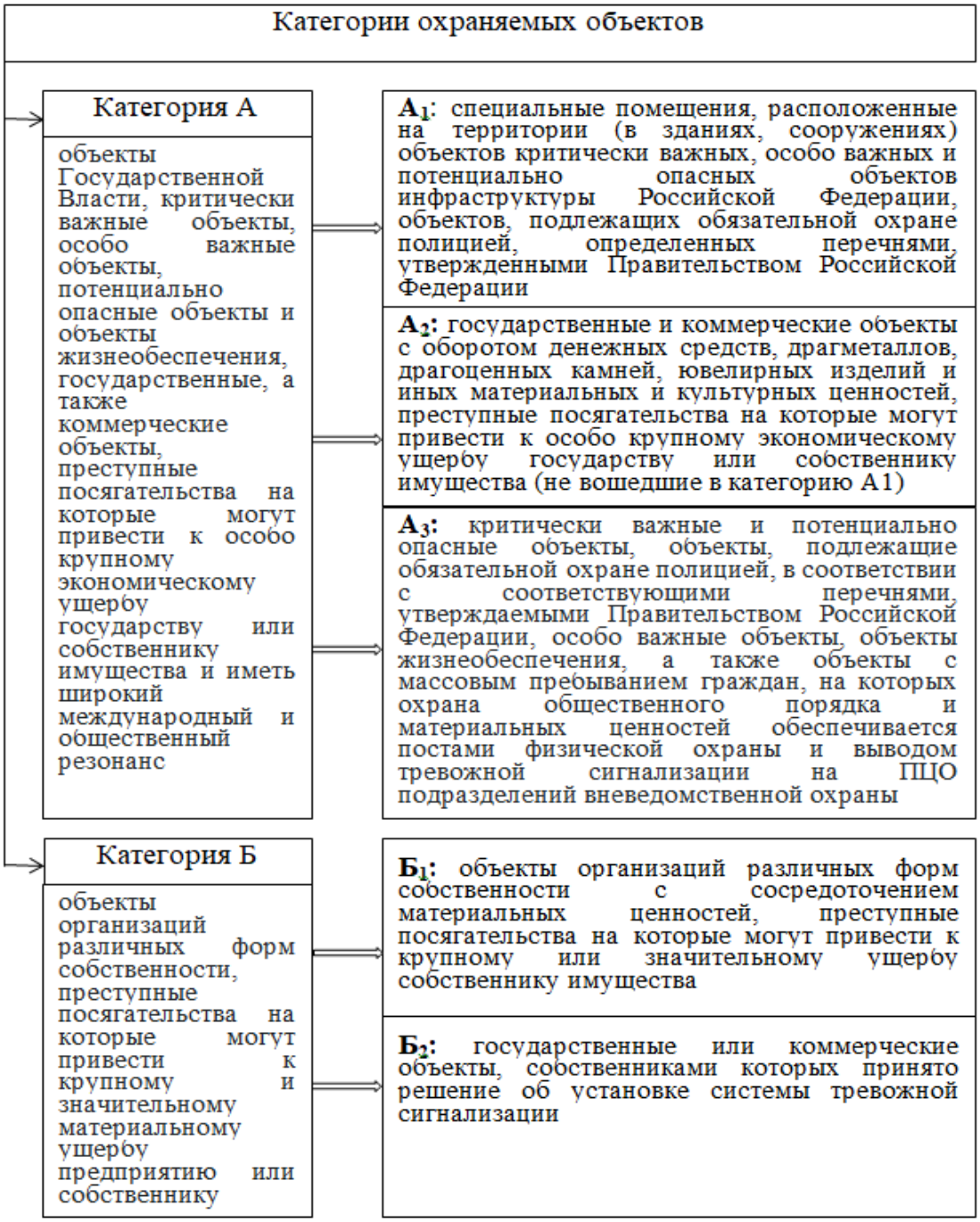


Рисунок 3.1 - Категории охраняемых объектов в зависимости от ущерба

Постановлением Правительства РФ от 21 мая 2007 №304 «О классификации чрезвычайных ситуаций природного и техногенного характера» [103] «чрезвычайные ситуации природного и техногенного характера подразделяются на:

а) чрезвычайную ситуацию локального характера;

б) чрезвычайную ситуацию муниципального характера;

в) чрезвычайную ситуацию межмуниципального характера;

г) чрезвычайную ситуацию регионального характера;

д) чрезвычайную ситуацию межрегионального характера;

е) чрезвычайную ситуацию федерального характера.»

С учетом изменений и поправок от 20 декабря 2019 г. № 1743 [90] их характеристика приведена в таблице 3.3.

Оценка масштаба ЧС производится по каждому из критериев (людские, финансовые потери, размер зоны ЧС), и присваивается по наивысшему значению любого из них [90].

Таблица 3.3 – Классификация и признаки ЧС

Масштаб ЧС	Количество людей, погибших и (или) получивших ущерб здоровью	Размер материального ущерба (млн. руб.)	Размер зоны ЧС
Локальный	не более 10	не более 0,24	территория организации (объекта) производственного или социального назначения
Муниципальный	10 - 50	0,24 - 12	территория одного муниципального образования
Межмуниципальный	10 - 50	0,24 - 12	территория двух и более муниципальных районов, муниципальных округов, городских округов, расположенных на территории одного субъекта РФ, или внутригородских территорий города федерального значения
Региональный	50 - 500	12 - 1200	территория одного субъекта РФ
Межрегиональный	50 - 500	12 - 1200	территория двух и более субъектов РФ
Федеральный	свыше 500	свыше 1200	Выходит за пределы территории РФ

Масштаб ЧС (как наихудший сценарий проникновения нарушителей) выступает качественным критерием категорирования объектов [99, 100]. Категория присваивается объекту по наибольшему значению любого признака масштаба ЧС. Анализ нормативно-правовых документов [89] (рисунок 3.1)

показал, что выделяют 5 категорий объектов, подлежащих физической защите. Объекты первой категории, с самой высокой степенью защищенности - объекты, проникновение нарушителей на которые могут привести к ЧС федерального характера. Объекты пятой категории, с самой низкой степенью защищенности - объекты, проникновение нарушителей на которые могут привести к ЧС муниципального или локального характера [105]. Качественный критерий и соответствующие каждой категории типы охраняемых объектов представлены в таблице 3.4

Таблица 3.4 - Категории охраняемых объектов и качественные критерии категорирования охраняемых объектов

Категория ОО	Аналог категории ОО согласно [89]	Тип охраняемого объекта	Критерий категорирования/ характеристика объекта в зависимости от возможного максимального размера ущерба
1	$А_1$	КВО федерального уровня значимости; ПОО особо высокого уровня опасности; ОВО	Объекты, проникновение нарушителей на которые могут привести к ЧС федерального характера
2	$А_2$	КВО регионального уровня значимости; ПОО чрезвычайно высокого уровня опасности	Объекты, проникновение нарушителей на которые могут привести к ЧС межрегионального характера
3	$А_3$	КВО муниципального уровня значимости; ПОО высокого уровня опасности; ОМПГ	Объекты, проникновение нарушителей на которые могут привести к ЧС регионального характера
4	$Б_1$	ПОО повышенного и среднего уровней опасности; ОЖ	Объекты, проникновение нарушителей на которые могут привести к ЧС межмуниципального характера
5	$Б_2$	ПОО низкого уровня опасности	Объекты, проникновение нарушителей на которые могут привести к ЧС муниципального или локального характера

Таким образом, потенциал опасности каждой категории ОО определяется через потенциал опасности масштаба ЧС.

Используя данные таблицы 3.3, оценим потенциал опасности каждого масштаба ЧС методом Хоменюка. Основная идея этого метода заключается в том, что при формировании оценочного потенциала не вызывающим сомнение

является тот факт, что различные признаки имеют различное долевое вложение в его значение [106, 107, 108].

Для проведения вычислений масштабы ЧС и их признаки (таблица 3.3), являющиеся входными данными, представим в виде двумерного пространства (таблица 3.5), описывающего:

- множество *n* чрезвычайных ситуаций;

- множество *m* признаков чрезвычайных ситуаций.

Таблица 3.5 – Структура входных данных

Признаки ЧС	Множество ЧС				
	$\{A_1\}$	...	$\{A_i\}$	…	$\{A_n\}$
X_1	X_{11}	…	X_{1i}	…	X_{1n}
…	…	…	…	…	…
X_j	X_{j1}	…	X_{ji}	…	X_{jn}
…	…	…	…	…	…
X_m	X_{m1}	…	X_{mi}	…	X_{mn}

Каждому признаку ЧС задаётся максимально возможное значение, определяемое масштабом ЧС (таблица 3.3). Входные (исходные) данные для вычислений потенциала опасности ЧС представлены в таблице 3.6.

Таблица 3.6 - Входные данные

Признаки ЧС (*j=1,2,3*)	Масштаб ЧС (*i=1, .., 6*)					
	локальный	муниципальный	межмуниципальный	региональный	межрегиональный	федеральный
	1	2	3	4	5	6
людские потери, ч.	10	25	50	250	500	1000
материальный ущерб, млн. руб.	0,24	6	12	600	1200	2400
зона ЧС, км^2	13,04	2561	3963	3083523	6914493	17098246

Для приведения характеристик $\{x_{ji}\}$ к единой шкале воспользуется нормализация типа (3.1):

$$r_{ji} = \frac{x_{ji}}{x_{\max j}}, \qquad (3.1)$$

отображающей $x_{ji} \to r \in [0;1]$. Полученные результаты представлены в таблице 3.7.

Таблица 3.7 - Нормализованные входные данные

Признаки ЧС	ЧС локального характера	ЧС муниципального характера	ЧС межмуниципального характера	ЧС регионального характера	ЧС межрегионального характера	ЧС федерального характера
	1	2	3	4	5	6
людские потери, ч.	0,01	0,025	0,05	0,25	0,5	1
материальный ущерб, млн. руб.	0,0001	0,0025	0,005	0,25	0,5	1
зона ЧС, км^2	$7{,}63 \cdot 10^{-7}$	0,0001498	0,0002318	0,18034148	0,404398	1

Нормированная мера r_{ji} применяется для вычислений формирующей оценочный потенциал, вероятности *p(r)*. Зависимость для определения величины *p(r)*, являющейся нормированной мерой на элементарных событиях *{r}*, основана на утверждениях:

- события, реальные прообразы которых (на одном иерархическом уровне) причинно независимы, независимы в вероятностном смысле;

- понятие оценочного потенциала заданного комплекса элементарных событий можно отождествить с функцией принадлежности, которая ставит в соответствие каждому *r* действительное число на отрезке [0; 1]. Искомая функция принадлежности представляется в форме [106, 107, 108]:

$$p_{ji}(r) = \frac{r_{ji}}{\sum_{i=1}^{n} r_{ji}} \qquad (3.2)$$

Значения $p_{ji}(r)$, вычисленные по формуле (3.2), приведены в таблице 3.8.

Таблица 3.8 - Значения функции принадлежности $p_{ji}(r)$

Признаки ЧС	ЧС локального характера	ЧС муниципального характера	ЧС межмуниципального характера	ЧС регионального характера	ЧС межрегионального характера	ЧС федерального характера
	1	2	3	4	5	6
людские потери, ч.	0,0054496	0,013624	0,02725	0,13624	0,2724796	0,544959
материальный ущерб, млн. руб.	$5{,}69\cdot10^{-5}$	0,001422	0,00284	0,142239	0,2844788	0,568958
зона ЧС, км^2	$4{,}811\cdot10^{-7}$	$9{,}45\cdot10^{-5}$	0,00015	0,113771	0,255121	0,630866

Фоменюк В.В. ввёл понятие «потенциального распределения вероятности» в качестве одного из методов расчета вероятности проявления j-ой характеристики сравниваемых вариантов на формирование оценочного потенциала, которое определяется по формуле [106, 107, 108]:

$$\hat{p}_j(r) = \frac{\sum_{i=1}^{n} r_{ji}}{\sum_{j=1}^{m}\sum_{i=1}^{n} r_{ji}} \qquad (3.3)$$

Вычисленные по формуле (3.3) потенциальные распределения вероятности равны:

$\hat{p}_1(r) = 0{,}354, \quad \hat{p}_2(r) = 0{,}339, \quad \hat{p}_3(r) = 0{,}306.$

Следующим этапом метода является получение вероятностных оценок проявления j-характеристики i-го варианта для формирования оценочного потенциала (таблица 3.9), вычисляемого по формуле:

$$p_i(ЧС) = \sum_{j=1}^{m} p_{ji}(r) \cdot \hat{p}_j(r) \qquad (3.4)$$

Таблица 3.9 - Вычисление оценочного потенциала

Признаки ЧС	ЧС локального характера	ЧС муниципального характера	ЧС межмуниципального характера	ЧС регионального характера	ЧС межрегионального характера	ЧС федерального характера
	1	2	3	4	5	6
людские потери, ч.	0,0019314	0,0048284	0,00965676	0,048284	0,096568	0,193135
материальный ущерб, млн. руб.	$1{,}9314 \cdot 10^{-5}$	0,0004828	0,00096568	0,048284	0,096568	0,193135
зона ЧС, км^2	$1{,}4729 \cdot 10^{-7}$	$2{,}893 \cdot 10^{-5}$	$4{,}4765 \cdot 10^{-5}$	0,03483	0,078103	0,193135
$P_i(ЧС)$	0,0019508	0,0053401	0,0106672	0,131398	0,271239	0,579405

Представим полученные в таблице 3.9 значения потенциала опасности ЧС в зависимости от её масштаба в более удобной форме, путём использования кратной величины, большей полученного значения в 1000 раз и округлённой до целых значений (таблица 3.10).

Таблица 3.10 - Итоговое значение оценочного потенциала опасности ЧС

Признак	Масштаб ЧС					
	локальный	муниципальный	межмуниципальный	региональный	межрегиональный	федеральный
Потенциал опасности	2	5	11	131	271	580

Потенциал опасностей объектов, относящихся к каждой из пяти категорий, оценивается на основе полученной нелинейной шкалы потенциалов опасностей масштабов ЧС. Поэтому следующим этапом является сопоставление категорий объектов и масштабов ЧС. В качестве характеристик объектов используются шесть видов потерь, рекомендованных «НПП «ИСТА-Системс»» в методике общегосударственного категорирования объектов [69]:

- политические (оценивается ущерб обороноспособности и безопасности государства, государственно-политической системе, заключающийся в снижении авторитета уровней власти и нестабильности, возникающей в результате этого);

- людские (оценивается ущерб здоровью и/или жизни людей);

- экологические (оцениваются затраты от потери природных ресурсов, приводящих к ухудшению экологической обстановки в регионе);

- финансовые (оценивается ущерб от утраты материальных ценностей, стоимость их восстановления);

- экономические (оцениваются затраты на переселение людей из зоны ЧС, страховые выплаты, компенсирующие населению нанесённый ущерб.);

- информационные (оценивается ущерб от утраты конфиденциальной информации и передовых технологий) [69, 105].

Значения потенциалов опасности, представленные в таблице 3.10, распределяются по перечисленным видам потерь ОО (таблица 3.11). Формируется генеральную совокупность опасности охраняемых объектов, представляющая собой монотонное увеличение её величины от минимального до максимального значений. Полученные данные представим в виде таблицы, имеющей 31 столбец и 6 строк. Количество столбцов соответствует количеству вариантов различных объектов, число строк - числу потерь, выбранных в качестве признаков категорирования ОО (таблица 3.11).

Таблица 3.11 - Генеральная совокупность опасности ОО

	номер варианта из генеральной совокупности опасности ОО											
Виды потерь	1	2	3	4	5	6	7	…	28	29	30	31
Политические	2	2	2	2	2	2	5	…	271	271	271	580
Людские	2	2	2	2	2	5	5	…	271	271	580	580
Финансовые	2	2	2	2	5	5	5	…	271	580	580	580
Экономические	2	2	2	5	5	5	5	…	580	580	580	580
Экологические	2	2	5	5	5	5	5	…	580	580	580	580
Информационные	2	5	5	5	5	5	5	…	580	580	580	580

Используя метод k-средних кластерного анализа и руководствуясь постановлением ГОСТ Р 78.36.032-2013 полученная совокупность разделяется на 5 классов (соответствующих пяти категориям ОО). Вычисления проведены в программе Statistica 10. Пятую категорию определяют объекты, для которых характерно распределение потенциала опасности, соответствующее 1 - 14 столбцам таблицы. В четвертую категорию вошли объекты, для которых характерно распределение потенциала опасности, соответствующее 15 - 20 столбцам таблицы, в третью – соответствующее 21 - 25 столбцам таблицы, во

вторую – соответствующее 26 - 28 столбцам таблицы. Первую категорию составили объекты, определяемые потенциалом опасности столбцов с номерами 29 - 31. Граничные значения классов, интерпретируемых как категории ОО, представлены в таблице 3.12.

Таблица 3.12 - Граничные значения категорий ОО

Виды потерь	Границы категорий ОО									
	5 ($Б_2$)		4 ($Б_1$)		3 ($А_3$)		2 ($А_2$)		1 ($А_1$)	
Политические	2	11	11	131	131	201	201	271	271	580
Людские	2	11	11	131	131	271	271	271	271	580
Финансовые	2	11	11	131	131	271	271	271	271	580
Экономические	2	11	11	131	131	271	271	426	426	580
Экологические	2	71	71	201	201	271	271	580	580	580
Информационные	2	131	131	271	271	271	271	580	580	580

Методом Хоменюка (формулы (3.1)-(3.4)), используя данные таблицы 3.13, определён диапазон опасности для каждой из пяти категорий. Нормализация входных данных таблицы 3.12, вычисленная по формуле (3.1) представлена в таблице 3.13.

Таблица 3.13 - Нормализация входных данных

Виды потерь	5 категория	4 категория	3 категория	2 категория	1 категория
Политические	0,0034483	0,018966	0,22586	0,346552	0,4672414
Людские	0,0034483	0,018966	0,22586	0,467241	0,4672414
Финансовые	0,0034483	0,018966	0,22586	0,467241	0,4672414
Экономические	0,0034483	0,018966	0,22586	0,467241	0,7344828
Экологические	0,0034483	0,122414	0,34655	0,467241	1
Информационные	0,0034483	0,225862	0,46724	0,467241	1

Результаты вычислений, выполненных по формуле (3.2) представлены в таблице 3.14.

Таблица 3.14 - Значения функции принадлежности $p_{ji}(r)$

Виды потерь	5 категория	4 категория	3 категория	2 категория	1 категория
Политические	0,0016722	0,00919732	0,109532	0,16806	0,226589
Людские	0,0015798	0,00868878	0,103476	0,21406	0,21406
Финансовые	0,0015798	0,00868878	0,103476	0,21406	0,21406
Экономические	0,0014075	0,00774103	0,092189	0,190711	0,299789
Экологические	0,001173	0,04164223	0,117889	0,158944	0,340176
Информационные	0,0010899	0,07138965	0,147684	0,147684	0,316076

Вычисленные по формуле (3.3) потенциальные распределения вероятности для ОО равны:

$\hat{p}_1(r) = 0{,}138,\ \hat{p}_2(r) = 0{,}146,\ \hat{p}_3(r) = 0{,}146,\ \hat{p}_4(r) = 0{,}164,\ \hat{p}_2(r) = 0{,}196,\ \hat{p}_3(r) = 0{,}212.$

Значения оценочного потенциала для каждой категории объектов (формула (3.4)) приведены в таблице 3.15.

Таблица 3.15 - Значения оценочного потенциала

Виды потерь	5 категория	4 категория	3 категория	2 категория	1 категория
Политические	0,0002302	0,001265968	0,015076534	0,023133	0,031189
Людские	0,0002302	0,001265968	0,015076534	0,031189	0,031189
Финансовые	0,0002302	0,001265968	0,015076534	0,031189	0,031189
Экономические	0,0002302	0,001265968	0,015076534	0,031189	0,049028
Экологические	0,0002302	0,008171251	0,023132697	0,031189	0,066751
Информационные	0,0002302	0,015076534	0,031188859	0,031189	0,066751
$P_i(OO)$	0,0013811	0,028311658	0,11462769	0,179077	0,276096

Итоговые значения потенциала опасности для каждой категории ОО представим в виде диапазонов (таблица 3.16).

Таблица 3.16 - Распределение потенциала опасности по категориям ОО

Признак	Категория ОО				
	5 ($Б_2$)	4 ($Б_1$)	3 ($А_3$)	2 ($А_2$)	1 ($А_1$)
Диапазон значений потенциала опасности	1-28	28-115	115-179	179-276	276-401

На основе полученных диапазонов потенциалов опасности формулируются требования к вероятности безопасного состояния для каждой категории ОО. Вероятность безопасного состояния ОО $P_{бс}$, является вероятностью наступления совместных событий (формула 2.6): обнаружением нарушителя датчиком (характеризующееся вероятностью $P_д$), своевременным прибытием СР в точку перехвата (характеризующееся вероятностью $P_{свп}$) и нейтрализацией нарушителя (характеризуется вероятностью $Р_н$). Перечисленные события являются независимыми а значит, $P_{бс}$ равно произведению вероятностей их наступления. Принимая $P_н$=1, формула (2.6) имеет вид:

$$P_{бс} = P_д \cdot P_{свп}. \quad (3.5)$$

Минимальными значениями вероятности безопасного состояния обладают ОО, относящиеся к пятой категории ($Б_2$). Для определения нижней границы вероятности безопасного состояния объектов, относящихся к пятой категории, примем $P_д$=0,7 - значение вероятности обнаружения ультразвуковых извещателей, вероятность реакции СР $P_{свп}$ = 0,9. Таким образом, получаем значение:

$$Р_{бс} = 0,9 \cdot 0,7 = 0,63.$$

Примем верхнюю границу вероятности безопасного состояния для ОО, относящихся к первой категории равной 0,999. Множество значений потенциала опасности объекта [1; 401] отображается на множество диапазона [0,63; 0,999]. Вычислим сжимающий коэффициент:

$$k = \frac{0,999 - 0,63}{401 - 1} \approx 0,000923$$

Тогда внутренние границы вероятностей безопасного состояния:

$$0,63 + (28 - 1) \cdot 0,000923 = 0,655$$

$$0,655 + (115 - 28) \cdot 0,000923 = 0,735$$

$$0,735 + (179 - 115) \cdot 0,000923 = 0,794$$

$$0,794 + (276 - 179) \cdot 0,000923 = 0,884$$

$$0,884 + (401 - 276) \cdot 0,000923 = 0,999$$

Полученные оценки интервалов требуемых вероятностей безопасного состояния для каждой категории объектов оформлены в таблицу 3.17.

Таблица 3.17 – Диапазоны вероятностей безопасного состояния, вычисленные методом Хоменюка

	Категория объекта				
	5 ($Б_2$)	4 ($Б_1$)	3 ($А_3$)	2 ($А_2$)	1 ($А_1$)
Вероятность безопасного состояния	0,63 – 0,655	0,655 – 0,735	0,735 – 0,794	0,794 – 0,884	0,884 – 0,999

Представление значений вероятности безопасного состояния не в виде точечных оценок, а в виде интервалов позволяет:

- получить непрерывные вероятностные функции (функции вероятностей безопасного состояния объекта) в заданном диапазоне значений. Значит, любое полученное значение $P_{бс}$ гарантировано принадлежит какому-нибудь интервалу и может быть однозначно определена достаточность защиты объекта, относящегося к определенной (конкретной) категории.

- определить нижние и верхние границы интервалов требуемой (необходимой) вероятности безопасного состояния объекта для каждой категории ОО и требуемых вероятностей защиты от нарушителя. Это даёт возможность: 1) избежать избыточности или недостаточности СФЗ; 2) расширить варианты реализации СФЗ.

Для подтверждения достоверности полученных результатов выбран метод расчетов декомпозиции генеральной совокупности (метод многомерной классификации) – дискриминантный анализ. Дискриминантный анализ проводится на основе линейной «классифицирующей функции» Фишера, которая максимизирует различия между классами, но минимизирует дисперсию внутри классов [109]:

$$D_k=b_{ko}+b_{k1}X_1+b_{k2}X_2+\ldots+b_{kp}X_p, \qquad (3.5)$$

где $k = 1,\ldots, 5$ - номер класса: множество объектов разбито на 5 подмножеств (классов) – категорий ОО (таблица 3.12);

b_{kj} - коэффициенты дискриминантной «классифицирующей» функции. Отличительными признаками каждой категории являются виды потерь. Таким образом, дискриминантные функции характеризуются шестью переменными: политическими, людскими, экономическими, финансовыми, экологическими, информационными потерями (т.е. $i = 1,\ldots, 6$). Коэффициенты для классифицирующих функций определяются с помощью формул [109]:

$$b_{ki} = (n-g)\sum_{j=1}^{p} a_{ij} X_{jk}^{*} \qquad (3.6)$$

где $\underset{*}{n}$ - общее число наблюдений по всем классам, g – число классов, $\underset{*}{X}_{jk}$ - среднее значение переменной j в k-ом классе, a_{ij} - элемент матрицы, обратной к внутригрупповой матрице сумм попарных произведений W [109].

$$W_{ij} = \sum_{k=1}^{g} \sum_{j=1}^{n_k} (X_{ikm} - \underset{*}{X}_{ik})(X_{jkm} - \underset{*}{X}_{jk}) \quad (3.7)$$

где n_k – число наблюдений в k-ом классе, X_{ikm} – величина переменной i для m-го наблюдения в k-м классе. Постоянный член – разделительный коэффициент (константа дискриминации) определяется по формуле [109]:

$$b_{k0} = -0{,}5 \sum_{j=1}^{p} b_{kj} \underset{*}{X}_{jk} \quad (3.8)$$

Для вычислений использовалось «Программное средство классификации объектов», свидетельство регистрации [110] (Приложение А). Диапазон вероятностей безопасного состояния ОО определяется на основе значений границ, разделяющих группы объектов – констант дискриминации (таблица 3.18).

Таблица 3.18 - Значения констант дискриминации

Дискриминантная функция	D_1	D_{12}	D_{23}	D_{34}	D_{45}	D_5
Значение разделительного коэффициента (модуль)	0,4	1,84	6,5	8,4	12,9	18,4

Отобразим диапазон значений констант дискриминации [0,4; 18,4] на определенный ранее отрезок вероятности безопасного состояния объектов [0,63; 0,999]. Значение сжимающего для отображения коэффициента вычисляется как:

$$k = \frac{0{,}999 - 0{,}63}{18{,}4 - 0{,}4} = 0{,}0205$$

На основе данных таблицы 3.18, используя значения k=0,0205, вычислены диапазоны вероятности безопасного состояния объектов (таблица 3.19).

Таблица 3.19 - Диапазоны вероятностей безопасного состояния, вычисленные на основе дискриминантного анализа

	Категория объекта				
	5 ($Б_2$)	4 ($Б_1$)	3 ($А_3$)	2 ($А_2$)	1 ($А_1$)
Вероятность безопасного состояния	0,63 – 0,659	0,659 – 0,755	0,755 – 0,794	0,794 – 0,886	0,886 – 0,999

Совпадение значений диапазонов вероятностей безопасного состояния, представленных в таблицах3.17 и 3.19 показывает правильность и адекватность приведенных рассуждений и выполненных на их основе вычислений. Полученные результаты не противоречат имеющимся разработкам в области категорирования ОО и обеспечения требований к их безопасности.

3.2 Определение требуемой вероятности (требуемого уровня) защиты от потенциальных нарушителей

Отсутствие единой терминологии делает необходимым уточнение понятия «нарушитель». Анализ нормативно-правовой документации [35, 111 - 114], научных источников [17, 86] позволил выделить следующие основные подходы в его определении (его трактовки).

Так, согласно М. Гарсиа [17, с. 358] «нарушитель, злоумышленник (adversary) - лицо, совершающее противоправные действия, направленные на причинение ущерба охраняемому объекту. Нарушитель может быть сотрудником фирмы или посторонним лицом».

Магауенов Р.Г. в кратком толковом словаре «Охранная сигнализация и другие элементы систем физической защиты» даёт следующую трактовку: «нарушитель – лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищённое системой охранной или пожарно-охранной сигнализации, без разрешения ответственного лица (владельца).» [86, с. 45]

В Постановлении Правительства РФ от 19.07.2007 № 456 (ред. от 28.08.2012) "Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов" указано: «… «нарушитель» - лицо, совершившее или пытающееся совершить несанкционированное действие, а также лицо, оказывающее ему содействие в

этом; … [111].» Аналогичная трактовка «нарушителя» даётся в проекте Постановления Правительства РФ «Об антитеррористической защищенности объектов Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций» (по состоянию на 15.05.2014) [112].

РД 78.36.003-2002. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств (утв. МВД РФ 06.11.2002) использует следующую терминологию: «нарушитель: лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя или жильца» [113, с.4]. Схожая терминология используется в ГОСТ Р 53195.1-2008 [113]: нарушитель – «лицо, осуществляющее попытку вторжения или несанкционированного действия либо осуществившее такие действия.»

ГОСТ Р 52551-2016 [35] определяет нарушителя как «лицо, создающее криминальную угрозу охраняемому объекту и/или имуществу».

Анализируя перечисленные определения, можно выделить два подхода трактовки термина «нарушитель». Таким образом, нарушитель – лицо, 1) совершившее или пытающееся совершить несанкционированное действие (криминальную угрозу), а также лицо, оказывающее ему содействие в этом [17, с. 358, 5]; 2) пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя или жильца [86, 113].

«Совокупность качественных и количественных характеристик нарушителю, определяющих его вероятные действия» [114] формирует модель нарушителя. Перечень характеристик, определяющих модель нарушителя, представлен в таблице 3.20.

Таблица 3.20 - Характеристики, определяющие модель нарушителя

Характеристика	Описание
тип нарушителя	внешний (лица, не входящие в состав персонала объекта, и не имеющие права доступа на его территорию) [17, 115]; внутренний (лица из числа персонала объекта и другие лица, пропущенные на территорию объекта установленным порядком) [17, 115]
численность	террористическая группа (6-20 человек); групповой нарушитель (2-5 человек); одиночный нарушитель
Цель и мотив	причинение вреда жизни или здоровью конкретным лицам или неопределенному кругу лиц; порча или уничтожение имущества; демонстрации собственной значимости и серьёзности намерений путём совершения опасных действий (поджога, стрельбы, взрыва) без причинения существенного ущерба людям и имуществу; совершение хищения, кражи; выдвижений требований к органам власти и/или конкретным должностным лицам; захват заложников; совершение суицида на основе мотивов: политических (несогласие с политикой государства, выражение поддержки деятельности экстремистских и террористически ориентированных организаций и групп в стране и за рубежом); идеологических (личностные качества нарушителя, укреплённые пропагандой идеологии экстремизма и терроризма); личных. [116,]
Последствия действий нарушителя	Потери масштабов: локального; муниципального; межмуниципального; регионального; межрегионального; федерального
Уровень осведомленности	знание системы и работы технических средств охраны; наличие сговора внешнего нарушителя с внутренним; оценка времени осуществления противоправной акции; разработка тактики осуществления противоправных действий;

Владение и оснащение холодным и огнестрельным оружием	уровень боевых навыков нарушителей; наличие: стрелкового и/или холодного оружия; горючих веществ, пиротехники, дымовых шашек; защитных жилетов и шлемов (балаклав); взрывчатых веществ, взрывных устройств
Техническая оснащенность; уровень подготовки по преодолению барьеров	наличие навыков и необходимого оборудования для отключения или блокировки работы средств сигнализации, связи, оповещения, видеонаблюдения, наличие транспортного средства, лестницы и/или альпинистского и иного оборудования; наличие навыков и профессиональных средств для проникновения на объект через КПП: поддельных документов и/или формы работников коммунальных служб или правоохранительных органов

Исходя из различного уровня подготовленности внешних нарушителей, Шепитько Г.Е. выделяет среди них следующие группы: случайный нарушитель, подготовленный нарушитель, квалифицированный нарушитель, высококвалифицированный нарушитель [117]. Мальцев А. [118] по степени осведомленности выделяет также четыре типа нарушителей: случайные (непреднамеренные), подготовленные неквалифицированные, подготовленные квалифицированные, подготовленные высококвалифицированные.

В нашей работе рассматриваются шесть основных моделей нарушителей: четыре модели внешних и две модели внутренних нарушителей. К моделям внешних нарушителей относятся: террористические группы (высококвалифицированный групповой нарушитель), групповой нарушитель (квалифицированный групповой нарушитель), одиночные террористы (подготовленный одиночный нарушитель), уголовные элементы («случайный» одиночный нарушитель). Среди моделей внутренних нарушителей выделены: рядовой сотрудник объекта (не имеющий доступа к СФЗ), персонал подразделения охраны, принуждаемый к содействию нарушителям путем подкупа, шантажа или угрозы применения силы [119,120] (таблица 3.21).

Таблица 3.21 - Характеристики основных моделей нарушителей

Характеристика	Модель нарушителя					
тип	внешние				внутренние	
обозначение	X_1	X_2	X_3	X_4	X_5	X_6
численность	6 – 20	3 – 5	1	1	1	1
описание	террористическая группа	групповой нарушитель	террорист-смертник, наемник	«случайный», неподготовленный	рядовой сотрудник объекта	сотрудник объекта, имеющий доступ к СФЗ
цель	террористический акт	террористический акт, хищение, уничтожение	террористический акт, порча, уничтожение	кража, порча, уничтожение	хищение	террористический акт
последствия действий нарушителя (масштаб ЧС)	федеральный, межрегиональный	межрегиональный, региональный	локальный, муниципальный	локальный	локальный	федеральный - региональный
уровень осведомленности	средний	средний	низкий	низкий	высокий	высокий
владение и оснащение холодным и огнестрельным оружием	хорошо вооружен	хорошо вооружен	средний уровень	отсутствует	отсутствует	вооружен
уровень подготовки по преодолению барьеров	высокий	высокий/ средний	средний	низкий	низкий	средний/ высокий

Исходя из того, что нарушитель является субъектом угроз, выполним оценку его действий, приводящих к самым опасным последствиям: возникновению чрезвычайных ситуаций на ОО. В зависимости от характеристик каждой модели нарушителей (таблица 3.21) экспертами распределяется количественная оценка последствий ЧС (таблица 3.10) по шести видам потерь: политических, людских, финансовых, экономических, экологических, информационных/культурных (таблица 3.22).

Таблица № 3.22 - Масштаб ЧС, распределенный по видам потерь в зависимости от модели нарушителя

Виды потерь (от действий нарушителей)	Модель нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	580	271	131	2	5	11
Людские	580	271	131	2	5	11
Финансовые	11	5	5	11	271	131
Экономические	580	271	131	5	5	11
Экологические	580	271	2	2	11	5
Информационные	11	5	2	5	271	271

Оценка последствий нарушителя определена методом Хоменюка (формулы (3.1)-(3.4)). Вычисления приведены в таблицах 3.23 – 3.24.

Нормализуем входные данные таблица (3.22) по формуле (3.1) (таблица 3.23).

Таблица 3.23 - Нормализованные масштабы потерь каждой модели нарушителя

Виды потерь (от действий нарушителей)	Модель нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	1	0,4672	0,2259	0,0034	0,0086	0,019
Людские	1	0,4672	0,2259	0,0034	0,0086	0,019
Финансовые	0,0406	0,0185	0,0185	0,0406	1	0,4834
Экономические	1	0,4672	0,2259	0,0086	0,0086	0,019
Экологические	1	0,4672	0,0034	0,0034	0,019	0,0086
Информационные	0,0406	0,0185	0,0074	0,0185	1	1

Значение функции принадлежности $p_{ji}(r)$, вычисленные по формуле (3.2) представлены в таблице 3.24.

Таблица 3.24. - Значения функции принадлежности $p_{ji}(r)$

Виды потерь (от действий нарушителей)	Модель нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	0,58	0,271	0,131	0,002	0,005	0,011
Людские	0,58	0,271	0,131	0,002	0,005	0,011
Финансовые	0,0253	0,0115	0,0115	0,0253	0,6244	0,3018
Экономические	0,5783	0,2702	0,1306	0,005	0,005	0,011
Экологические	0,6659	0,3111	0,0023	0,0023	0,0126	0,0057
Информационные	0,0195	0,0088	0,0035	0,0088	0,4796	0,4796

Вычисленные по формуле (3.3) потенциальные распределения вероятности равны:

$\hat{p}_1(r) = 0{,}166, \quad \hat{p}_2(r) = 0{,}166, \quad \hat{p}_3(r) = 0{,}154, \quad p_4(r) = 0{,}167, \quad \hat{p}_5(r) = 0{,}145,$
$\hat{p}_6(r) = 0{,}201.$

Вычисление оценочного потенциала масштабов потерь нарушителей по формуле (3.4) представлено в таблице 3.25.

Таблица 3.25 Вычисление оценочных потенциалов масштабов потерь нарушителей

Виды потерь (от действий нарушителей)	Модель нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	0,0965	0,04508	0,02179	0,00033	0,00083	0,00183
Людские	0,0965	0,04508	0,02179	0,00033	0,00083	0,00183
Финансовые	0,0039	0,00178	0,00178	0,00392	0,09647	0,04663
Экономические	0,0965	0,04508	0,02179	0,00083	0,00083	0,00183
Экологические	0,0965	0,04508	0,00033	0,00033	0,00183	0,00083
Информационные	0,0039	0,00178	0,00071	0,00178	0,09647	0,09647
$P_i(МП)$	0,3937	0,18386	0,06819	0,00753	0,19727	0,14943

Полученные значения интерпретируются как оценка последствия действий нарушителя.

Следующим шагом является вычисление потенциала опасности нарушителей. Качественным показателям моделей нарушителя (таблица 3.21): уровень осведомленности, владение и оснащение холодным и огнестрельным оружием, уровень подготовки по преодолению барьеров, заданы числовые значения, которые определяются методом экспертных оценок на основе вербально-числовой шкалы Харрингтона. Последствия действий нарушителя представляют собой значения функции неопределенности масштабов потерь в случае успешной реализации ими своих целей (таблица 3.25). Числовые значения характеристик моделей потенциальных нарушителей представлены в таблице 3.26.

Таблица 3.26 - Характеристики моделей потенциальных нарушителей

Характеристика	Модель потенциального нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Численность	11	4	1	1	1	1
Цель и мотив	10	9	8	2	2	5
последствия действий нарушителя	0,3937	0,18386	0,06819	0,00753	0,19727	0,14943
уровень осведомленности	0,7	0,6	0,4	0,3	0,9	1
владение и оснащение холодным и огнестрельным оружием	0,9	0,8	0,7	0,3	0,3	1
уровень подготовки по преодолению барьеров	1	0,9	0,8	0,3	0,3	0,6

Оценка потенциала опасности моделей нарушителя определяется методом потенциалов Хоменюка (формулы (3.1)-(3.4)), аналогично, как в случае оценки потенциала опасностей ОО. Нормализованные характеристики моделей потенциальных нарушителей, вычисленные по формуле (3.1) представлены в таблице 3.27.

Таблица 3.27. - Нормализованные входные данные

Характеристика	Модель потенциального нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
численность	1	0,3636	0,0909	0,0909	0,0909	0,0909
Цель и мотив	1	0,9	0,8	0,2	0,2	0,5
последствия действий нарушителя	1	0,46699	0,1732	0,0191	0,5010	0,3795
владение и оснащение холодным и огнестрельным оружием	0,9	0,8	0,7	0,3	0,3	1
уровень подготовки по преодолению барьеров	1	0,9	0,8	0,3	0,3	0,6
уровень осведомленности	0,7	0,6	0,4	0,3	0,9	1

Значения функции принадлежности, вычисленные по формуле (3.2), представлены в таблице 3.28.

Таблица 3.28 - Значения функции принадлежности $p_{ji}(r)$

Характеристика	Модель потенциального нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
численность	0,57895	0,21053	0,05263	0,05263	0,05263	0,05262
мотив/цель	0,2778	0,25	0,2222	0,0556	0,0556	0,1389
последствия действий нарушителя	0,39372	0,18386	0,06819	0,00753	0,19727	0,14943
владение и оснащение холодным и огнестрельным оружием	0,225	0,2	0,175	0,075	0,075	0,25
уровень подготовки по преодолению барьеров	0,25641	0,23077	0,20513	0,07692	0,07692	0,15385
уровень осведомленности	0,17949	0,15385	0,10256	0,07692	0,23077	0,25641

Потенциальные распределения вероятности, вычисленные по формуле (3.3), равны:

$$\hat{p}_1(r) = 0{,}0878, \quad \hat{p}_2(r) = 0{,}1830, \quad \hat{p}_3(r) = 0{,}1291, \quad \hat{p}_4(r) = 0{,}2034,$$
$$\hat{p}_5(r) = 0{,}1983, \quad \hat{p}_6(r) = 0{,}1983.$$

Вычисленные по формуле (3.4) и округлённые до целого значения величины потенциалов опасности, соответствующие каждой модели нарушителя представлены в таблице 3.29.

Таблица 3.29 - Итоговое значение потенциала опасности нарушителей

	Модель потенциального нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Потенциал опасности	285	205	151	61	116	182

Далее, на основе полученного диапазона потенциала опасности определим значения требуемых вероятностей защиты для каждой модели нарушителя. Отобразим диапазон значений констант дискриминации [61; 285] на определенный ранее отрезок вероятности безопасного состояния объектов [0,63; 0,999]. Вычислим сжимающий коэффициент:

$$k = \frac{0{,}999 - 0{,}63}{285 - 61} \approx 0{,}0016$$

Вычислим внутренние границы вероятностей для всех моделей нарушителей:

$$0{,}63 + (116 - 61) \cdot 0{,}0016 = 0{,}718$$

$$0{,}718 + (151 - 116) \cdot 0{,}0016 = 0{,}774$$

$$0{,}774 + (182 - 151) \cdot 0{,}0016 = 0{,}824$$

$$0{,}824 + (205 - 182) \cdot 0{,}0016 = 0{,}860$$

$$0{,}860 + (285 - 205) \cdot 0{,}0016 = 0{,}988$$

Результаты вычислений представлены в таблице 3.30.

Таблица 3.30 - Значение требуемых вероятностей защиты от нарушителей

	Модель потенциального нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Требуемая вероятность защиты	0,988-0,999	0,860–0,988	0,774-0,824	0,63 – 0,718	0,718 - 0,774	0,824–0,860

3.3 Идентификация потенциальных нарушителей для категорируемых объектов

Согласно разработанной концептуальной модели, первоочередной задачей оценки эффективности СФЗ является идентификация потенциальных нарушителей для заданной категории ОО. Для решения данной задачи необходимо описание разнородных объектов исследования (ОО и нарушителей) привести к одинаковым шкалам. Для этого, первоначально определены потенциалы опасности категорий ОО и моделей нарушителя. На основе потенциалов опасности ОО (таблица 3.16) и нарушителей (таблица 3.29) переходим к вероятности безопасного состояния ОО (таблица 3.17) и значениям требуемых вероятностей защиты от нарушителей (таблица 3.30). Т.О. множества ОО и потенциальных нарушителей сведены к единой шкале [0;1], интерпретируемой как вероятность (рисунок 3.2). Опираясь на аксиому, о возможности сравнения любых событий в вероятностном смысле [108], это позволило определить потенциальных нарушителей по результатам пересечения диапазонов значений полученных оценочных шкал.

Категории охраняемых объектов				
1	2	3	4	5
⇓				
Потенциал опасности				
276-401	179-276	115-179	28-115	1-28
⇓				
Вероятность безопасного состояния ОО				
0,884 - 0,999	0,794 - 0,884	0,735 – 0,794	0,655 - 0,735	0,63 - 0,655

0,988 - 0,999	0,860 - 0,988	0,774 - 0,824	0,63 - 0,718	0,718 - 0,774	0,824 - 0,860
Значение требуемых вероятностей защиты от нарушителей					
⇑					
285	205	151	61	116	182
Потенциал опасности					
⇑					
1	2	3	4	5	6
Модель нарушителя					

Рисунок 3.2 - Схема идентификации потенциальных нарушителей

Перечень потенциальных нарушителей для каждой категории ОО представлен в таблице 3.31.

Таблица 3.31 - Потенциальные нарушители для категорий ОО

Категория объекта	1 ($А_1$)	2 ($А_2$)	3 ($А_3$)	4 ($Б_1$)	5 ($Б_2$)
Потенциальные нарушители	X_1 , X_2	X_2 , X_3 , X_6	X_3 , X_5	X_4, X_5	X_4

Анализируя результаты, представленные в таблице 3.21, получаем, что для первой категории ОО потенциальными нарушителями являются групповые, высоко подготовленные и осведомленные нарушители, основной целью которых является террористический акт. Потенциальные нарушители для второй категории объектов представляют собой как групповых, так и одиночных нарушителей (смертников) вступающих в сговор с хорошо осведомленными о СФЗ объекта сотрудниками (внутренние нарушители). К потенциальным нарушителям объектов третьей категории относятся одиночные террористы-смертники и вступающие с ними в сговор сотрудники объекта. Потенциальными нарушителями объектов четвертой и пятой категорий являются нарушители, с низким уровнем подготовленности и осведомленности, так называемые «случайные нарушители». К потенциальным нарушителям четвертой категории относятся также внутренние нарушители - сотрудники, имеющие цель кражи или хищения.

3.4 Вероятность обнаружения нарушителя

Обеспечение безопасности ОО начинается с момента обнаружения нарушителя. Факт обнаружения нарушителя инициализирует процессы его задержки и нейтрализации.

Обнаружение нарушителей обеспечивается датчиками охранной сигнализации (внешними - использующимися снаружи помещений и внутренними - использующимися внутри помещений), контролем на КПП, видеосистемами оценки сигнала тревоги, сбором и обработкой сигналов тревоги. Важным показателем эффективности процесса обнаружения нарушителя является вероятность обнаружения, зависящая от технических

характеристик и условий эксплуатации аппаратуры, а также цели обнаружения (модели потенциальных нарушителей)[121].

Очевидно, что обнаружение нарушителя зависит от его типа (внешний, внутренний). Выявление внутренних нарушителей зависит от уровня всей системы обеспечения безопасности, а именно от состояния режимной и кадровой работы, проводимой на ОО. Для внешних нарушителей вероятность обнаружения определяется уровнем отличительных свойств, соответствующих определенной модели нарушителя (таблица 3.21) и характеристиками комплексов технических средств охраны [122, с. 12, с. 31]. Одной из важных характеристик внешнего нарушителя, влияющей на его обнаружение является тактика действий при проникновении на территорию ОО. Она может быть: насильственная (с применением насилия по отношению к людям и с повреждением ИТСО); обманная (создающая видимость санкционированных действий путём использования поддельных документов, ключей, идентификаторов личности и т.п.); скрытная (когда нарушитель стремится остаться незамеченным); комбинированная (различные сочетания вышеуказанных видов тактик). Когда проникновение на объект осуществляется с помощью насильственной тактики с использованием фактического разрушения заграждений, применения огнестрельного вооружения, т.е. носит явный характер проникновения на объект, вероятность обнаружения нарушителя равна единице. В остальных случаях, значение вероятности обнаружения является неизвестной величиной.

Согласно [71], ТСФЗ, а именно системы обнаружения (СО) разрабатываются и проверяются на предмет соответствия заявленной в технической документации вероятности обнаружения для наименее опасной модели нарушителя (x_4), которая характеризуется низким уровнем осведомленности об ОО и его СФЗ, и низким уровнем подготовленности. Чем выше осведомленность нарушителей об ОО, тем ниже становится вероятность его обнаружения [71]. Так, обнаружение злоумышленников, относящихся к третьей модели x_3 происходит уже с меньшей сигнализационной надежностью,

а для второй x_2 и первой x_1 моделей сигнализационная надежность любой СО снижается существенно.

Отечественные и зарубежные исследователи [17, 71, 123-126], сходятся во мнении, что вероятность обнаружения нарушителей, пропорциональна уровню их осведомленности (подготовленности). Учитывая данные обстоятельства, пусть *k* – коэффициент, определяемый осведомленностью (подготовленностью) нарушителя, тогда

$$P_o = k \cdot P_{ктсо}. \qquad (3.9)$$

где $P_{ктсо}$ – вероятность комплекса технических средств обнаружения, определяемая технической документацией ТСО и их комбинацией в конкретной зоне обнаружения. Вычислим значение коэффициента *k*, опираясь на уровень осведомленности каждой модели нарушителя (таблица 3.26). Методом экспертных оценок на основе вербально-числовой шкалы Харрингтона характеристикам уровню осведомленности для каждой модели нарушителя задаются числовые значения: x_1 – 7; x_2 – 6; x_3 – 4; x_4 – 3; x_5 – 9; x_6 – 10 (увеличенное в 10 раз для выполнения требований к значению коэффициента). Отобразим диапазон значений экспертных оценок, характеризующих модели нарушителей [3; 10] на отрезок [0; 1] – диапазон значений коэффициента *k*. Оценим сжимающий коэффициент Δ:

$$\Delta = \frac{k_{\max} - k_{\min}}{y_{\max} - y_{\min}} \qquad (3.10)$$

Зададим максимальное значение коэффициента $k_{max}= 1$ для нарушителей, относящихся к модели x_4, Минимальное значение $k_{min}= 0$ для внутренних нарушителей.$y_{max} = 10$ – максимальное значение осведомленности и подготовленности нарушителя. $y_{mim} = 3$ – соответственно минимальное значение осведомленности и подготовленности нарушителя. Тогда:

$$\Delta = \frac{1}{7}$$

Для X_1 значение $k=0+\Delta(10-9)=0,43$. Полученные значения коэффициентов представлены в таблице 3.32.

Таблица 3.32 – Значение коэффициента k

	Модель нарушителя			
	X_1	X_2	X_3	X_4
k	0,43	0,57	0,86	1

Вычисленные значения коэффициента k согласуются с результатами, представленными в исследованиях [71, 122, 123].

Выводы по третьей главе

В главе представлена методика определения потенциальных нарушителей для каждой категории ОО. Основными этапами которой являются: 1) определение требований к безопасности ОО; 2) определение потенциала опасности нарушителей 3) идентификация потенциальных нарушителей для каждой категории ОО.

Критерием категорирования ОО выбран масштаб ЧС, являющийся наихудшим результатом несанкционированного проникновения на ОО нарушителя. Введена нелинейная шкала оценки ЧС для формирования генеральной совокупности. При формировании данной шкалы учитываются три признака ЧС: людские потери, материальный ущерб, зона ЧС. На основании данной шкалы сформирована генеральная совокупность опасности ОО. Используя метод k-средних кластерного анализа и руководствуясь постановлением ГОСТ Р 78.36.032-2013 полученная совокупность разделяется на 5 классов (соответствующих пяти категориям ОО).

Используя метод Хоменюка и дискриминантный анализ, определена интервальная оценка безопасного состояния ОО.

На основе анализа научных источников и нормативно-правовых актов выделены 6 моделей нарушителей. Для каждой модели нарушителей методом Хоменюка вычислены диапазоны вероятности требуемой защиты.

Представление значений вероятностей безопасного состояния ОО и защиты от нарушителей не в виде точечных оценок, а в виде интервалов позволяет:

- получить непрерывные вероятностные функции в заданном диапазоне значений. Следовательно, любое полученное значение вероятности гарантировано принадлежит какому-нибудь интервалу и может быть однозначно определена достаточность защиты объекта, относящегося к определенной (конкретной) категории;

- определить нижние и верхние границы интервалов требуемой (необходимой) вероятности безопасного состояния объекта для каждой категории ОО и требуемых вероятностей защиты от нарушителя. Это даёт возможность: 1) избежать избыточности или недостаточности СФЗ; 2) расширить варианты реализации СФЗ.

На основе перекрытия диапазонов вероятности безопасного состояния ОО и требуемой вероятности защиты от нарушителя, определены потенциальные нарушители каждой категории объекта.

Полученные результаты апробированы и используются специалистами ОРО ОО «Российское научное общество анализа риска» для повышения достоверности результатов риска КВО, что подтверждается соответствующим актом (Приложение Б).

Глава 4 Имитационная модель оценки эффективности систем физической защиты объектов

4.1 Математическое описание имитационной модели оценки эффективности СФЗ

Для решения задачи оценки эффективности СФЗ разработана имитационная модель, целью которой является определение вероятности безопасного состояния ОО. Вероятность безопасного состояния определяется вероятностью устранения угрозы, под которой понимается вероятность своевременного прибытия сил реагирования при обнаружении проникновения нарушителя на объект.

Имитационная модель учитывает неоднородность ОО и маршрутов проникновения нарушителя. Вся территория объекта состоит из множества связанных охраняемых зон различной важности, и соответственно, различного уровня защищенности – рубежей охраны. Рубежи (зоны) охраны оснащены различными техническими системами защиты (ТСЗ), к которым относятся средства обнаружения и средства задержки нарушителей (рисунок 2.1 глава 2). Маршрут нарушителя характеризуется количеством рубежей охраны, через который он проходит, вероятностью обнаружения и временем задержки на каждом из них.

Поставленная перед имитационной моделью цель достигается имитацией основных функций СФЗ в последовательности, происходящей в реальности: обнаружение нарушителя, задержка продвижения нарушителя на следующих рубежах охраны, которые после обнаружения преодолевает нарушитель до достижения им своей цели и реакция сил реагирования и нейтрализации на проникновение [17].

Обнаружение - выявление явных или скрытых действий нарушителя [17] на территории ОО, является важнейшей функцией СФЗ. Так как в случае отсутствия обнаружения, отсутствует реакция СФЗ на проникновение. Оценка эффективности СФЗ должна быть выполнена при любом развитии сценария действий нарушителя. Обнаружение нарушителя не должно иметь

предпочтительный характер относительно сценария действий нарушителя. (Каждый сценарий проникновения нарушителя является равновозможным). В этом случае вводится допущение, что генерирование случайной величины x - вероятности обнаружения нарушителя на пересекаемом им рубеже обнаружения зоны охраны осуществляется по равномерному закону распределения. Функция равномерного распределения в нашем случае на отрезке [0; 1] имеет вид:

$$F(x)=\begin{cases} 0, \ при\ x \le 0 \\ \dfrac{x-0}{1-0}, \ при\ 0 < x \le 1 \\ 1, \ при\ x > 1 \end{cases} \qquad (4.1)$$

В выражении (3.1) величина x равномерно распределена в интервале от 0 до 1, в соответствии с заданной функцией [127, с.119].

$$F(x)=\begin{cases} 0, \ при\ x \le 0 \\ x, \ при\ 0 < x \le 1 \\ 1, \ при\ x > 1 \end{cases} \qquad (4.2)$$

Величина x разыгрывает в модели вероятность обнаружения нарушителя на пересекаемом им j-том рубеже, где j =1,…, n, n – количество рубежей на маршруте. Её значение генерируется в диапазоне от 0 до 1 и сравнивается с заданной величиной P_{oj}. В случае, если её значение принадлежит интервалу $[P_{0j}; 1]$, то событие интерпретируется как пропуск нарушителя на j-том рубеже и нарушитель переходит на j+1 рубеж. Если $x \in [0; P_{oj})$, то событие интерпретируется как обнаружение нарушителя. В этом случае j-ый рубеж является зоной обнаружения нарушителя, а последующие рубежи, начиная с j+1 и до n (последнего рубежа маршрута), являются зонами задержки нарушителя.

В этом случае, моделируются время задержки нарушителя $t_з$ и время реакции группы реагирования и нейтрализации t_p. Задержка нарушителя – одна из функций СФЗ, заключающаяся в замедлении продвижения нарушителя по территории ОО после его обнаружения. Время задержки $t_з$ представляет собой сумму:

$$t_з = t_{зоj} + \sum_{k=j+1}^{n} t_{зk}\,, \tag{4.3}$$

где $t_{зоj}$ – время задержки нарушителя на j-том рубеже обнаружения – рубеже, на котором он был обнаружен;

$t_{зk}$ - время задержки нарушителя на *k*-ом рубеже задержки, где *k= j+1,…, n*.

Обе величины: $t_{зоj}$, $t_{зk}$ являются случайными. Рассмотрим алгоритм генерирования каждой из них.

Пусть нарушитель обнаружен (находится) на *j*-том рубеже охраны. Дальнейшие рассуждения аналогичны для каждого рубежа охраны, поэтому для удобства опустим в формулах индекс *j*. Вероятность обнаружения нарушителя зависит от длительности времени его движения на *j*-том рубеже охраны и подчиняется экспоненциальному закону распределения [128]:

$$\mathrm{P_o} = 1 - \mathrm{e}^{-\lambda_o t}. \tag{4.4}$$

В формуле (4.4) λ_o - параметр закона распределения, характеризует эффективность системы обнаружения [128]. Графическая интерпретация зависимости (4.4) представлена на рисунке 4.1.

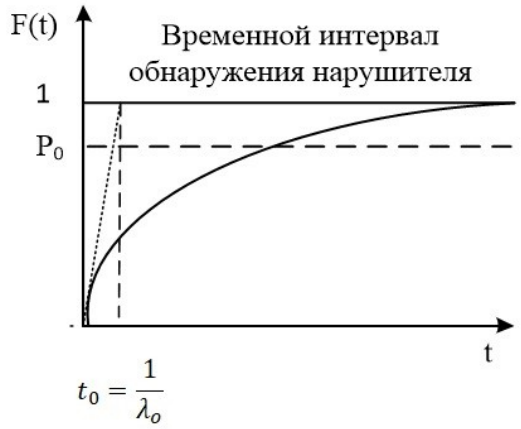


Рисунок 4.1 Функция распределения вероятности

Следовательно, чем дольше нарушитель находится в зоне обнаружения, тем выше вероятность его обнаружения. Выразим из формулы (4.4) величину λ_o:

$$\lambda_o = -\frac{\ln(1-P_o)}{t}. \tag{4.5}$$

Время обнаружения является случайной величиной и определяется выражением:

$$t_o = -\frac{1}{\lambda_o}\ln(1-x), \tag{4.6}$$

где x – случайная величина, распределённая равномерно в интервале (0, 1) и интерпретируемая, как обнаружение или пропуск нарушителя.

Подставляя в формулу (4.6) значение λ_o из (4.5), получим случайное время обнаружения t_o нарушителя в зоне ответственности (контроля) средств обнаружения:

$$t_o = \frac{\ln(1-x)}{\ln(1-P_o)}t, \tag{4.7}$$

где t - математическое ожидание времени перемещения в зоне контроля средства обнаружения на данном рубеже обнаружения, являющееся его технической характеристикой и входным параметром имитационной модели для каждого рубежа. Тогда время $t_{зо}$:

$$t_{зо} = t - t_o. \tag{4.8}$$

Таким образом, формула (4.8) с учетом (4.7) на каждом j-том рубеже охраны примет вид:

$$\mathrm{t_{зоj}} = \mathrm{t_j} - \frac{\ln(1-\mathrm{x_j})}{\ln(1-\mathrm{P_{oj}})}\mathrm{t_j} \tag{4.9}$$

Время задержки на остальных рубежах охраны маршрута, по которым движутся нарушители $t_{зk}$, генерируется по нормальному закону распределения на каждом k-том рубеже (где $k=j+1,\ldots, n$) .

Формирование нормально распределенной случайной величины основано на использовании центральной предельной теоремой Ляпунова: если случайная величина представляет собой сумму большого числа взаимно независимых случайных величин, влияние каждой из которых на всю сумму ничтожно мало, то случайная величина имеет распределение близкое к нормальному [129]. Последовательность нормально распределенных случайных величин со значениями математического ожидания и дисперсии, строится с помощью нормально распределенной случайной величины Z_i с параметрами $N(0, 1)$:

$$x_i = M(x) + \sigma(x)Z_i. \tag{4.10}$$

Пусть ξ_1, ξ_2,..., ξ_m – m независимых случайных величин, равномерно распределенных в диапазоне [0; 1], для которых математическое ожидание и дисперсия равны:

$$M(x) = \frac{1}{2}, \quad \sigma^2(x) = \frac{1}{12}. \tag{4.11}$$

Их сумма равна:

$$\sum_{i=1}^{m} \xi_i = \frac{m}{2} + \sqrt{\frac{m}{12}} \cdot z_i \,. \tag{4.12}$$

Тогда величина Z_i имеет вид:

$$z_i = \sqrt{\frac{12}{m}} \cdot \left(\sum_{i=1}^{m} \xi_i - \frac{m}{2} \right), \tag{4.13}$$

где m – количество реализаций. При $m \to \infty$ случайная величина Z_i стремится к стандартной нормально распределенной случайной величине с нулевым математическим ожиданием и дисперсией равной 1 [129]. На практике обычно берут $m = 12$, тогда:

$$z_i = \sum_{i=1}^{m} \xi_i - 6. \tag{4.14}$$

Время реагирования – время, которое группе реагирования и нейтрализации необходимо для своевременного прибытия с целью нейтрализации нарушителя. Согласно исследованиям автора М. Гарсиа [17] время реагирования - это аддитивная величина, представляющая собой сумму времен, требуемых на выполнение задач, возникающих после обнаружения нарушителя. К ним относятся:

- передача сигнала тревоги оператору и его оценка;
- передача сигнала тревоги силам реагирования;
- подготовка сил реагирования (время сборов охраны);
- движение сил реагирования до цели;
- развертывание сил реагирования.

В общем случае, для выполнения перечисленных задач требуется неодинаковое время. При разных попытках, оно представляет собой случайную величину, генерируемую по закону нормального распределения.

Для генерации времени реагирования t_{pj} с значениями *M(x)* и σ, которые являются входными данными и задаются по результатам натурных испытаний на реальном физическом объекте защиты. Условием задержки нарушителя является выполнение неравенства $t_{\text{р}} \leq t_{\text{з}}$. Количество случаев задержки нарушителя (успешного функционирования СФЗ) определяет величину *M*. Моделируются *N* попыток проникновения на объект и вычисляется величина:

$$W = \frac{M}{N}, \tag{4.15}$$

которая при стремлении *N* к бесконечности определяет величину $P_{бс}$ - вероятность безопасного состояния объекта. Моделируя движение нарушителя на каждом маршруте *N*=100000 раз, получаем информацию о безопасности ОО. Таким образом, эффективность СФЗ определяется числом пресеченных атак нарушителя на объект к общему числу генерируемых атак нарушителя.

Пространственно-временная схема имитационной модели представлена на рисунке 4.2.

Достоинствами имитационной модели является:

- максимальное приближение имитации к реальному физическому процессу функционирования СФЗ за счет пространственно-временной детализации зоны обнаружения и зоны задержки нарушителя;

- оценка всех маршрутов проникновения;

- детализация каждого маршрута проникновения на разнородные участки и учет времени обнаружения на каждом рубеже обнаружения;

- возможность использования результатов натурных испытаний на реальном объекте как входные данные модели, что повышает достоверность полученных данных.

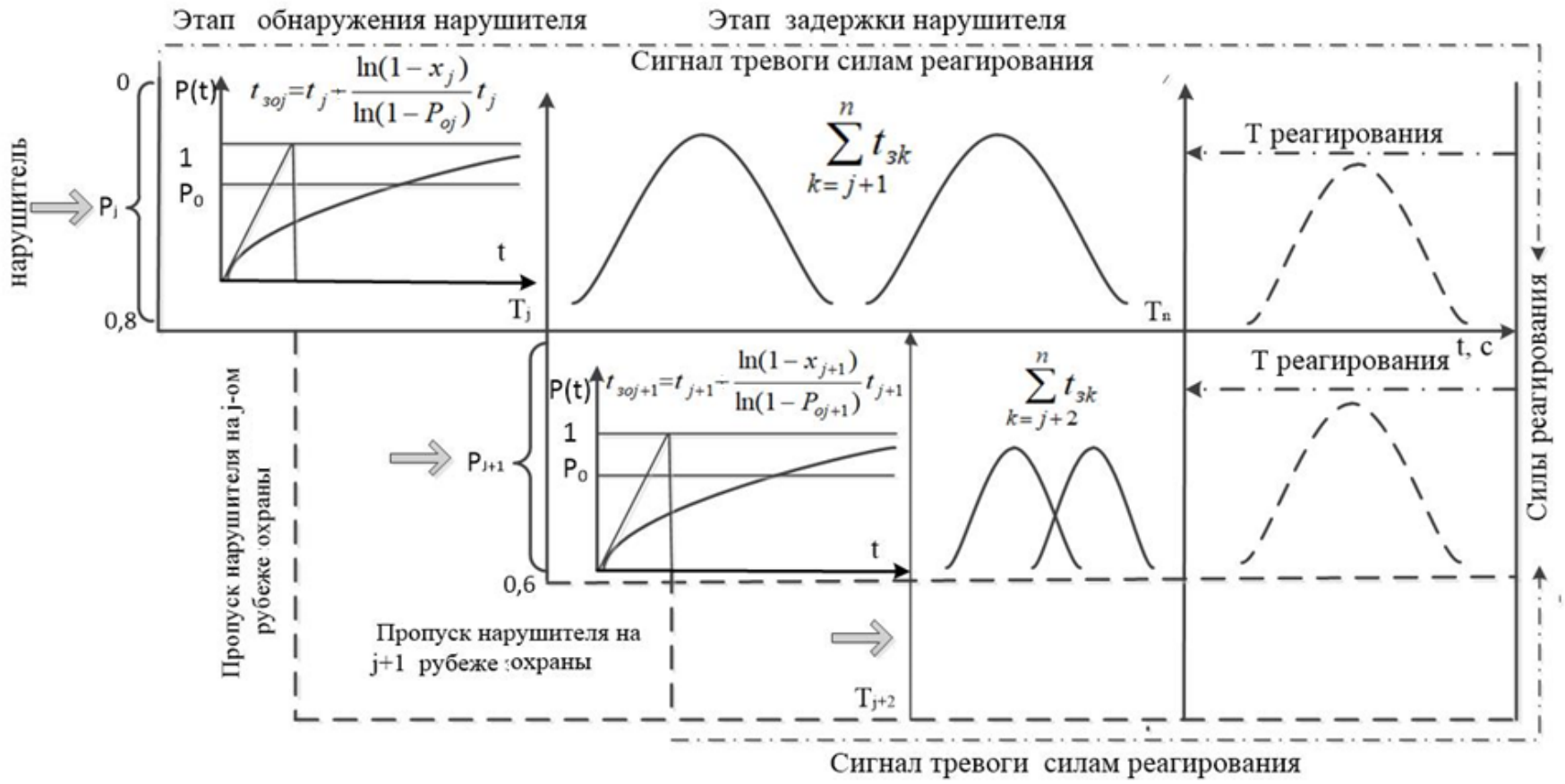


Рисунок 4.2. Пространственно-временная схема имитационной модели

4.2 Описание программного средства имитационной модели

Завершающим этапом разработки имитационной модели оценки эффективности СФЗ [130] является её программная реализация. Алгоритм описанной модели реализован в программном средстве (ПС) «Имитационная модель функционирования системы физической защиты объекта» [131] (Приложение А). Для написания программного средства использовался язык программирования C# (Приложение В).

Движение нарушителя по территории объекта может быть различным и заранее неизвестно. Однако, зная структуры объекта и СФЗ, можно определить все маршруты проникновения и рассчитать вероятность нейтрализации нарушителя на каждом из них. Имитационная модель учитывает разнородность маршрутов нарушителя: количество рубежей защиты, через которые проходит маршрут, вероятность обнаружения на каждом рубеже и время прохождения рубежей нарушителем. Перечисленные параметры являются основными входными данными имитационной модели. Вероятности обнаружения нарушителя определяются исходя из характеристик технических систем защиты (ТСЗ), действий оператора и степени надежности системы оповещения. Время преодоления нарушителем каждого рубежа определяется расчетным путем методом экспертных оценок или проведением натурного эксперимента на физическом объекте защиты.

Результатом работы имитации обнаружения является случайная величина P, сгенерированная по равномерному закону в диапазоне (0; 1). Имитация функции задержки использует два типа распределения: экспоненциальный (формула 4.9) и нормальный (формулы 4.10 - 4.14). Основной характеристикой функции задержки является время задержки (T – время преодоления рубежа). Для реализации экспоненциального закона распределения пользователем указывается ожидаемое время срабатывания устройства (T*). Реализация нормального закона распределения осуществляется с помощью величины σ (стандартное отклонение) времени преодоления рубежа.

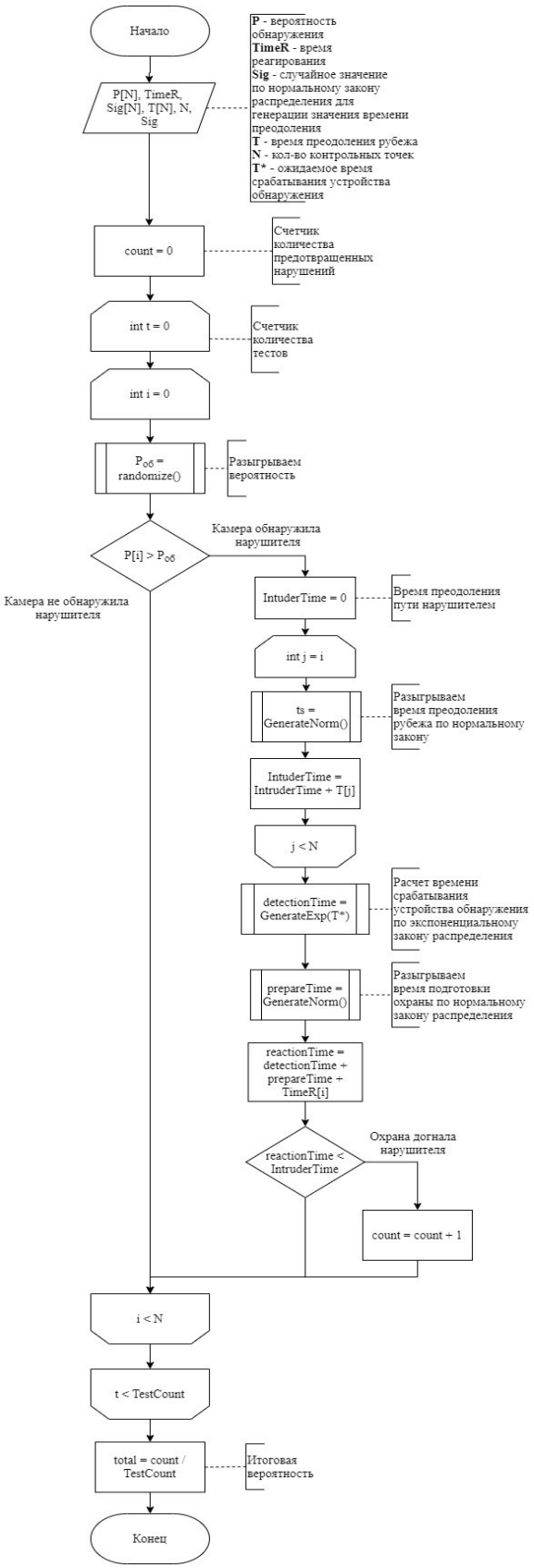


Рисунок 4.3 Схема имитационной модели оценки эффективности СФЗ

Функция СФЗ - реагирование имитируется также на основе нормального закона распределения. Входными данными для ее реализации являются время реагирования (TimeR) и σ (стандартное отклонение) времени реагирования (Sig).

Эффективность СФЗ определяется числом пресеченных атак нарушителя на объект к общему числу генерируемых атак нарушителя (формула 4.15). Схема имитационной модели оценки эффективности СФЗ представлена на рисунке 4.3.

Функции ПС:

- вычисление вероятности безопасного состояния объекта для каждого маршрута нарушителя;

- вывод статических данных (количество обнаружений нарушителя по каждому рубежу, количество пропусков и пресечений в случае обнаружения) для каждого маршрута нарушителя.

Учитывая, что в вопросах обеспечения безопасности ОО экспертные оценки могут являться единственной информацией [14, с. 98] для принятия решений, то проверка

имитационной модели на адекватность (валидация) представляет собой оценку степени отражения экспертного прогноза и результатов имитации. Для этого экспертами разработаны десять вариантов тестов, представленных в таблице 4.1.

Таблица 4.1 - Набор тестов для проверки адекватности имитационной модели

№ теста	P_1	T_1, с	σ для T_1	P_2	T_2,с	σ для T_2	Ожидаемое $P_{бс}$
1	1	0	0	0	300	90	0,5
2	1	300	90	0	0	0	0,5
3	1	150	45	0	150	45	0,5
4	1	100	30	0	200	60	0,5
5	0,5	0	0	0	300	90	0,25
6	0,5	300	90	0	0	0	0,25
7	0,5	150	45	0	150	45	0,25
8	0,5	100	30	0	200	60	0,25
9	0	любое		1	300	90	0,5
10	0	любое		0,5	300	90	0,25

Тестирование осуществляется на маршрутах, имеющих 2 рубежа задержки. Ожидаемое время срабатывания устройства принимается равным нулю. Время реагирования задано 300 с., σ = 90 с. Проверка адекватности модели состоит в сравнении выходных данных модели и тестов, разработанных экспертами. При одинаковых значениях входных данных, результаты имитационной модели считаются выборочными данными. Используя статистические методы проверки гипотез, выскажем предположение несущественности различий между средними величинами откликов модели и экспертными значениями откликов СФЗ [131]. Следовательно, нулевая гипотеза

$$H_0: M(X) = m \qquad (4.16)$$

где M(X) –математическое ожидание вычислительного эксперимента, проведенного с помощью имитационной модели,

m - экспертное значение вероятности безопасного состояния.

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{4.17}$$

Несмещённая оценка дисперсии:

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{X})^2 \tag{4.18}$$

t-статистика вычисляется:

$$t = \frac{\overline{X} - m}{S}\sqrt{n} \tag{4.19}$$

Пример работы программы для тестового варианта №8 представлен на рисунке 4.4.

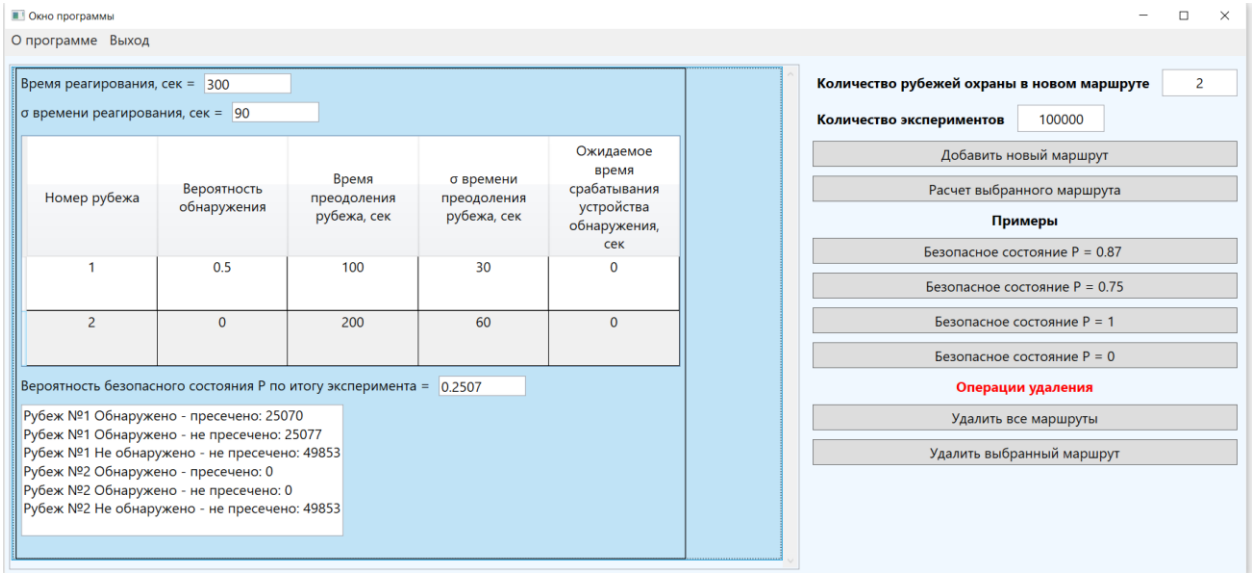


Рисунок 4.4 Пример работы программы тестового варианта №8

Для каждого варианта теста проводилось по 10 вычислительных экспериментов, результаты представлены в таблице 4.2.

Табличное значение при n=9 и уровня значимости суждений a = 0,05 критическое значение t-критерия Стьюдента равно 2,62. Результаты вычислений, представленные в таблице 4.2, показывают, что для каждого тестового набора выполняется условие $r \leq t_{табл}$. Что говорит, об адекватности имитационной модели оценки эффективности СФЗ.

В таблице 4.3 представлены результаты вычислений абсолютной и относительной погрешности вычислений. Появление данных ошибок связано с погрешностями алгоритмов генерирования случайных величин.

Таблица 4.2 Результаты вычислительного эксперимента

№ теста	1	2	3	4	5	6	7	8	9	10	$\bar{X}$	S^2	t
1	0,50197	0,50298	0,50307	0,50204	0,50443	0,50371	0,50218	0,49288	0,50209	0,50171	0,501706	$1{,}037\cdot10^{-5}$	1,67
2	0,50357	0,49958	0,50101	0,504	0,50005	0,50214	0,50112	0,49753	0,50149	0,50161	0,50121	$3{,}56\cdot10^{-6}$	2,03
3	0,50006	0,50009	0,49975	0,50029	0,50307	0,49922	0,49863	0,50215	0,50008	0,50063	0,500397	$1{,}72\cdot10^{-6}$	0,96
4	0,50055	0,50331	0,50216	0,49843	0,50012	0,50048	0,49988	0,49971	0,50053	0,5005	0,500567	$1{,}78\cdot10^{-6}$	1,34
5	0,25089	0,24973	0,25148	0,25159	0,25032	0,25081	0,24894	0,24977	0,25085	0,25125	0,250563	$7{,}37\cdot10^{-7}$	2,07
6	0,25001	0,2506	0,25012	0,25197	0,25054	0,24941	0,25296	0,25043	0,25312	0,24948	0,250864	$1{,}82\cdot10^{-6}$	2,03
7	0,25053	0,25083	0,25018	0,24973	0,24917	0,2502	0,24812	0,24984	0,25282	0,24974	0,250116	$1{,}47\cdot10^{-6}$	0,30
8	0,25067	0,24949	0,2507	0,2492	0,25115	0,25297	0,24841	0,24907	0,24878	0,25012	0,250056	$1{,}47\cdot10^{-6}$	0,15
9	0,50373	0,5005	0,49944	0,49955	0,50291	0,50132	0,49828	0,50447	0,50196	0,50152	0,501368	$3{,}92\cdot10^{-6}$	2,19
10	0,24938	0,25035	0,25089	0,25119	0,25205	0,25265	0,25061	0,25083	0,24843	0,25178	0,250816	$1{,}56\cdot10^{-6}$	2,07

Таблица 4.3 Анализ погрешности/ точности имитационной модели

№ теста	$\bar{X}$	m	абсолютная погрешность	относительная погрешность, %
1	0,501706	0,5	0,001706	0,3412
2	0,50121	0,5	0,00121	0,242
3	0,500397	0,5	0,000397	0,0794
4	0,500567	0,5	0,000567	0,1134
5	0,250563	0,25	0,000563	0,2252
6	0,250864	0,25	0,000864	0,3456
7	0,250116	0,25	0,000116	0,0464
8	0,250056	0,25	$5{,}6\cdot10^{-5}$	0,0224
9	0,501368	0,5	0,001368	0,2736
10	0,250816	0,25	0,000816	0,3264

Исходя из этого, можно полагать, что разработанная имитационная модель действительно отображает СФЗ ОО.

Выводы по четвертой главе

В главе представлено описание разработанной имитационной модели оценки эффективности СФЗ. Поставленная перед имитационной моделью цель: определение вероятности безопасного состояния ОО достигается имитацией основных функций СФЗ в последовательности, происходящей в реальности: обнаружение нарушителя, задержка продвижения нарушителя на следующих рубежах охраны, которые после обнаружения преодолевает нарушитель до достижения им своей цели и реакция сил реагирования и нейтрализации на проникновение. Эффективность СФЗ определяется числом пресеченных атак нарушителя на объект к общему числу генерируемых атак нарушителя (статистическая вероятность).

Алгоритм имитационной модели реализован в программном средстве (ПС) «Имитационная модель функционирования системы физической защиты объекта».

Адекватность имитационной модели подтверждена с помощью отражения степени соответствия результатов ее работы с результатами тестов, разработанными экспертами. Оценка проверки статистической гипотезы выполнена с использованием t-критерия Стьюдента.

Достоинствами имитационной модели являются: возможность за счет пространственно-временной детализации зоны обнаружения и зоны задержки нарушителя максимально приблизить результаты имитации к реальному физическому процессу функционирования СФЗ; оценка всех возможных маршрутов проникновения нарушителя на ОО; детализация каждого маршрута проникновения на разнородные участки и учет времени обнаружения на каждом рубеже обнаружения; возможность использования результатов натурных испытаний на реальном объекте как входные данные модели. Что позволяет повысить достоверность оценки эффективности СФЗ.

Глава 5 Методика принятия решений по обеспечению требуемого уровня объектов

5.1 Оценка эффективности СФЗ охраняемых объектов

Методика принятия решений по обеспечению физической безопасности ОО состоит из 4 этапов:

1. Оценка эффективности СФЗ ОО;
2. Декомпозиция маршрутов нарушителя;
3. Полный факторный эксперимент. Построение уравнения регрессии;
4. Принятие решений по обеспечению физической безопасности ОО;

и представляет собой комплексное исследование СФЗ [132].

Первый этап заключается в оценке вероятности безопасного состояния ОО с помощью имитационной модели, описанной в главе 4. Исследование полученных результатов имитации с помощью многомерных статистических методов даёт количественную зависимость вероятности безопасного состояния ОО от характеристик СФЗ в виде уравнения отклика системы (уравнения регрессии). Анализ коэффициентов которого позволяет вырабатывать решения по повышению эффективности до требуемого уровня.

Рассмотрим гипотетичный модельный объект – цех подготовки и перекачки нефти (ЦППН), который является взрыво-пожароопасным объектом. Структура объекта соответствует структуре реального ОО. На территории объекта располагаются: насосная товарной нефти – 2 шт, концевые сепараторные установки (КСУ) - 1,2; печи трубчатые блочные (ПТБ), отстойники, электроподстанция, операторная, резервуар вертикальный стальной (для уловленной нефти); резервуарный парк нефти РВС, узел учета нефти, узел учета газа и т.д.

На объекте организована защита по периметру: полоса отчуждения, основное ограждение оборудовано охранным освещением, системой охранной сигнализации (ОС). Частично ограждение усилено сверху спиральным барьером безопасности (СББ) «Егоза».

Три контрольно-пропускных пункта (КПП), используя систему СКУД и электромеханические ворота и дорожные блокираторы, организуют санкционированный доступ на объект персоналу и транспорту. Двое запасных ворот оснащены мягкими шлагбаумами, дорожными блокираторами и оборонительными сооружениями. (рисунок 5.1)

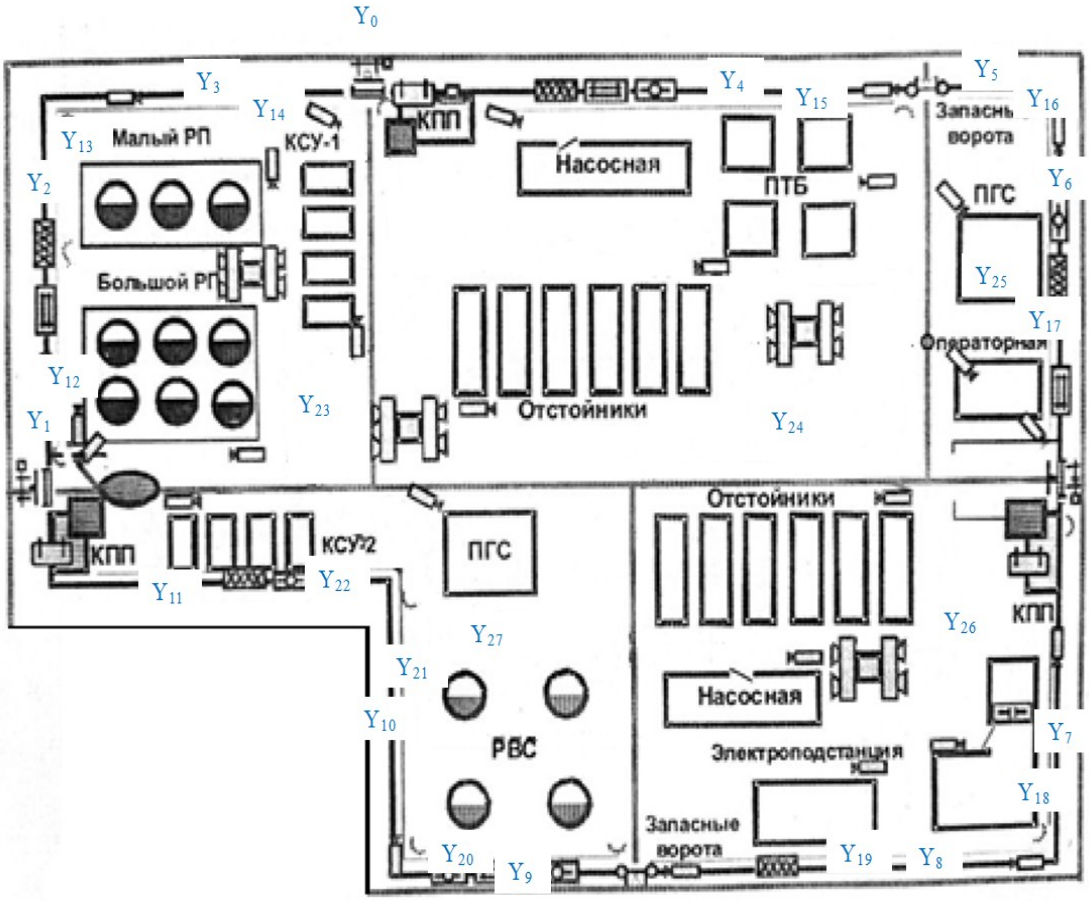


Рисунок 5.1 Рубежи охраны ЦППН [133, с.123]

Численность персонала на ЦППН достигает 300 человек. Вокруг объекта степной ландшафт у северо-восточной границы находится федеральная трасса. На расстоянии 2 км на северо-запад расположен населенный пункт.

Модельный объект относится ко второй категории. Потенциальные нарушители: X_2 (групповой нарушитель), X_3 (террорист-смертник, наемник), X_6 (сотрудник объекта, имеющий доступ к СФЗ). Основными угрозами объекту являются: теракты, диверсии, хищения товарно-материальных ценностей (нефтепродуктов, аппаратуры, оборудования, лома цветных

металлов). Наихудший сценарий реализации целей нарушителей может привести к ЧС межрегионального масштаба.

На объекте выделены 27 рубежей охраны: Y_0 – Y_{27}. Y_0 – рубеж за периметром объекта Y_1 – Y_{11} - ограждение, Y_{12} – Y_{22} – рубежи, находящиеся на полосе отчуждения, Y_{23} – Y_{27} - рубежи, находящиеся внутри объекта. Цель нарушителей - совершение противозаконных действий в отношении элементов, находящихся на внутренних зонах охраны Y_{23} – Y_{27}.

Для оценки действительного состояния безопасности объекта формируется модель (сценарии) проникновения нарушителя на объект. Модель проникновения нарушителя формируется в виде разветвленного ориентированного графа (рисунок 5.2), который является графом достижимости нарушителем своей цели. Вершины графа – рубежи охраны (Y_0 - Y_{27}), дуги (x_1 - x_{33}) – способы перемещения между рубежами охраны.

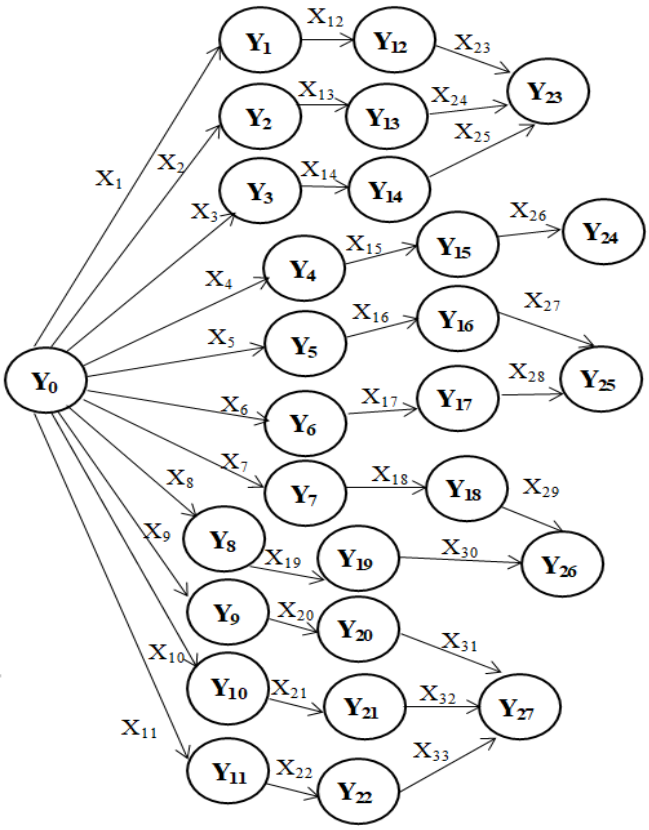


Рисунок 5.2 Граф достижимости нарушителем цели

Вероятности нахождения нарушителя в нулевой вершине Y_0 в начальный момент времени присваивается значение 1, это событие интерпретируется как инициализация противоправных действий нарушителя.

Равенство единице вероятности нахождения нарушителя в любой из вершин $Y_{23} - Y_{27}$ означает факт достижения им своей цели. Вероятность того, что нарушитель не достиг вершин (рубежей охраны) $Y_{23} - Y_{27}$ есть показатель эффективности СФЗ.

Используя алгоритм обхода графа в глубину (Depth First Search, DFS), получили 11 маршрутов проникновения (рисунок 5.2):

$Y_1\ Y_{12}\ Y_{23}$;	$Y_4\ Y_{15}\ Y_{24}$;	$Y_7\ Y_{18}\ Y_{26}$;	$Y_{10}\ Y_{21}\ Y_{27}$;
$Y_2\ Y_{13}\ Y_{23}$;	$Y_5\ Y_{16}\ Y_{25}$;	$Y_8\ Y_{19}\ Y_{26}$;	$Y_{11}\ Y_{22}\ Y_{27}$
$Y_3\ Y_{14}\ Y_{23}$;	$Y_6\ Y_{17}\ Y_{25}$;	$Y_9\ Y_{20}\ Y_{27}$;	

Внутри объекта, начиная с рубежей охраны $Y_{11} - Y_{22}$, до цели – рубежей Y_{23} - Y_{27} нарушителю необходимо преодолеть два рубежа. Каждый рубеж характеризуется вероятностью обнаружения и временем преодоления рубежа (временем задержки).

Входные данные и результаты работы имитационной модели оценки вероятности безопасного состояния для модельного объекта по каждому маршруту нарушителя представлены в таблице 5.1. Математическое ожидание времени реакции на проникновение группы реагирования и нейтрализации составляет 300 с., среднеквадратическое отклонение - $\sigma = 30$ с. Значение времени задержки получены как отношение расстояний между рубежами к средней скорости перемещения нарушителя на данном участке. Вероятность обнаружения определяется характеристиками технических средств обнаружения и уровнем подготовки нарушителя.

Таблица 5.1 Результаты имитационного моделирования безопасного состояния модельного ЦППН*

Номер маршрута	P_1	T_1, с.	P_2	T_2, с.	$P_{бс}$
1	0,6	270	0,8	240	0,602
2	0,6	240	0,8	260	0,584
3	0,6	270	0,8	270	0,607
4	0,6	240	0,8	240	0,615
5	0,6	180	0,8	180	0,586
6	0,6	190	0,8	180	0,599
7	0,6	220	0,8	120	0,550
8	0,6	240	0,8	180	0,595
9	0,8	150	0,6	270	0,813
10	0,8	180	0,6	240	0,807
11	0,8	150	0,6	300	0,817

* P_1 - вероятность обнаружения нарушителя на первом рубеже;
T_1 – время задержки нарушителя на первом рубеже, с;
P_2 - вероятность обнаружения нарушителя на втором рубеже;
T_2 – время задержки нарушителя на втором рубеже, с;
$P_{бс}$ – вероятность безопасного состояния.

Модельный ЦППН относится ко второй категории. Диапазон вероятностей безопасного состояния для ОО второй категории, вычисленный в главе 3, равен [0,794; 0,884]. Анализ результатов имитационного моделирования (таблица 5.1), показал, что на рубежах охраны, через которые проходят маршруты нарушителя №1 – 8, СФЗ не обеспечивает требуемый уровень вероятности безопасного состояния. Следовательно, необходимо повысить вероятность безопасного состояния ЦППН на данных рубежах охраны. Для этого переходим ко второму этапу: декомпозиции маршрутов.

5.2 Декомпозиция маршрутов нарушителя

Задачей данного этапа является определение латентных связей характеристик и маршрутов проникновения, на основе этого произвести декомпозицию сложной структуры СФЗ на более простые элементы, что позволит получить более достоверные зависимости вероятности безопасного состояния объекта от параметров СФЗ [87]. Для решения поставленной

задачи используется факторный анализ данных, представленных в таблице 4.4. Методы факторного анализа делятся на две основные группы: метод главных компонент, методы факторного анализа. Обе группы методов имеют общую схему решения, представленную на рисунке 5.3. [135].

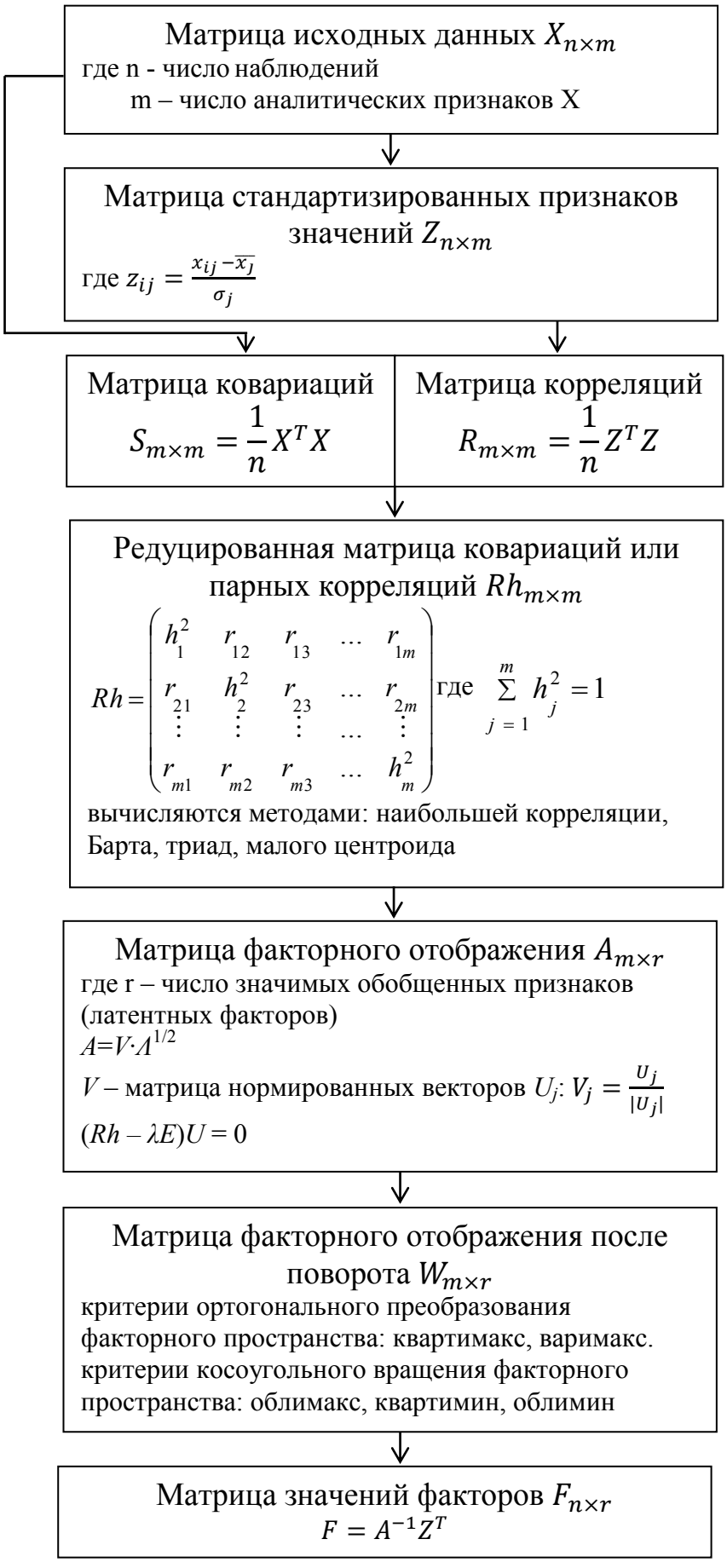


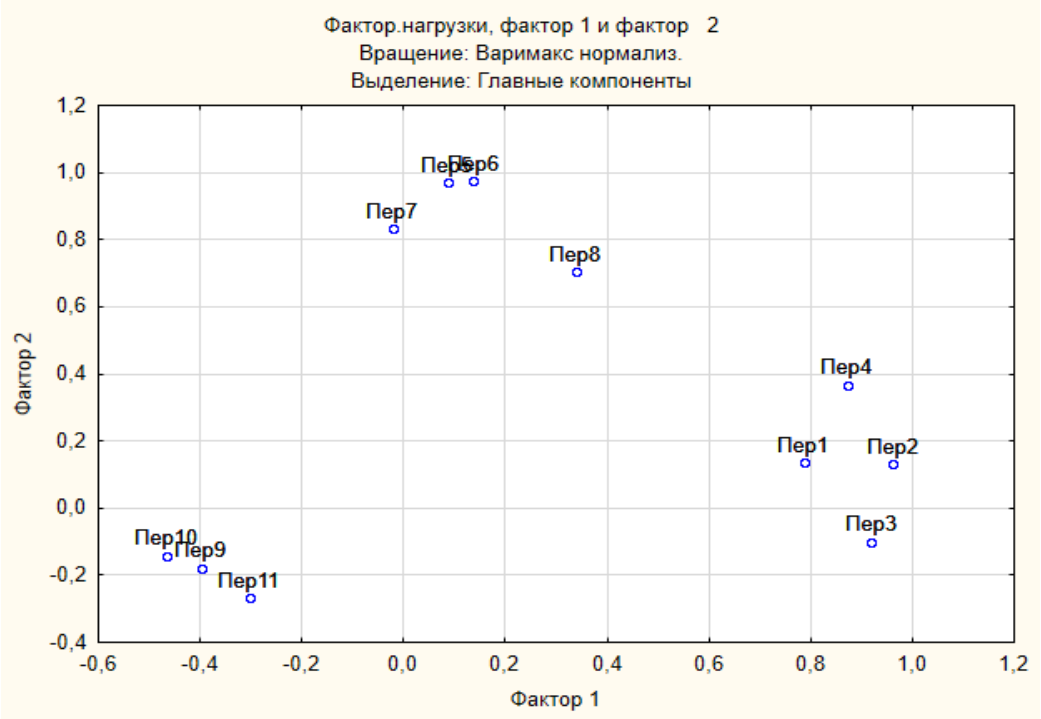
Рисунок 5.3 Схема реализации методов факторного анализа

Наблюдениями являются маршруты проникновения нарушителя (n=11), аналитическими признаками выступают вероятности обнаружения нарушителя (P_1, P_2) и время задержки на всех рубежах (T_1, T_2) маршрутов.

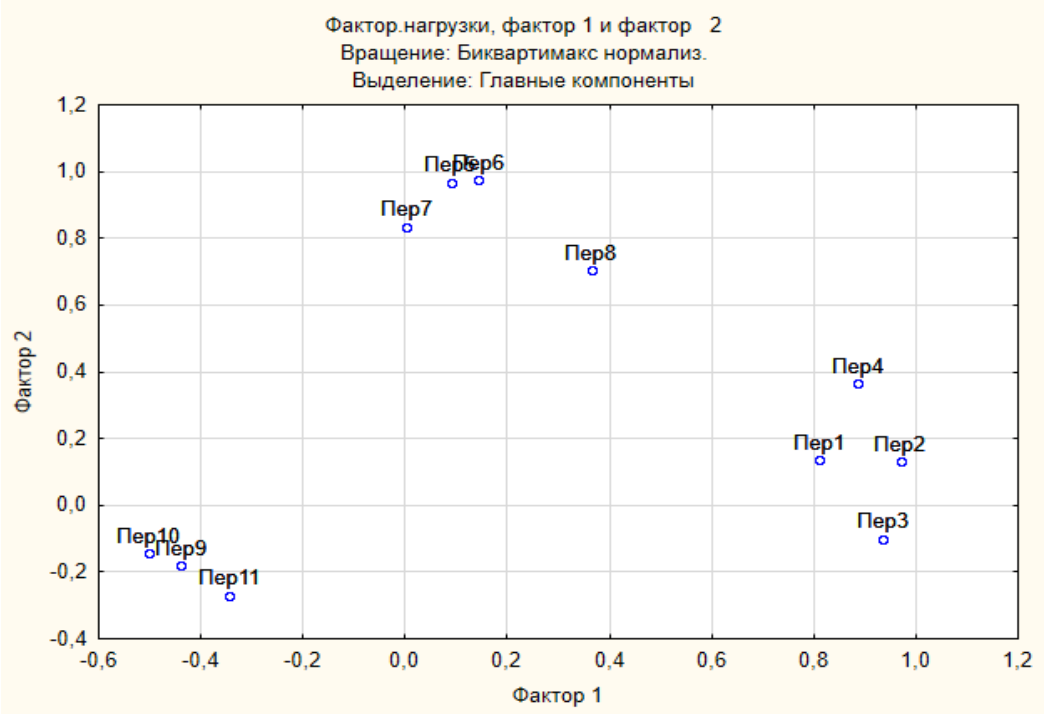
Вычисления проведены в программе Statistica 10. Декомпозиция маршрутов выполнена с применением ортогонального вращения факторного пространства методами: варимакс, биквартимакс. Вычисления, проведенные разными методами вращения дали схожие результаты (таблица 5.2, рисунок 5.4).

Таблица 5.2 - Результат анализа характеристик маршрутов проникновения

Номер маршрута нарушителя	Варимакс (нормализированные факторные нагрузки)			Биквартимакс(нормализированные факторные нагрузки)		
	F_1	F_2	F_3	F_1	F_2	F_3
1	***0,787427***	0,135136	0,534017	***0,811330***	0,135591	0,496826
2	***0,962409***	0,132058	0,186409	***0,970275***	0,130103	0,141628
3	***0,920045***	-0,100090	0,360976	***0,935257***	-0,100971	0,319223
4	***0,871927***	0,366832	0,324310	***0,886836***	0,365893	0,282211
5	0,085857	***0,968640***	0,013745	0,089128	***0,968431***	0,004472
6	0,136876	***0,973952***	0,104997	0,144269	***0,974079***	0,093273
7	-0,021290	***0,832327***	0,474900	0,002730	***0,834934***	0,470775
8	0,338245	***0,703246***	0,548822	0,364896	***0,705149***	0,528948
9	-0,398051	-0,178075	***-0,892288***	-0,438813	-0,181654	***-0,872226***
10	-0,464964	-0,141090	***-0,784644***	-0,500645	-0,143884	***-0,761850***
11	-0,302294	-0,267173	***-0,914123***	-0,344403	-0,271162	***-0,897910***



а) вращение методом варимакс



б) вращение методом биквартимакс

Рисунок 5.4 - Графическая интерпретация результатов факторного анализа

Маршруты проникновения нарушителя распределились на три главных фактора F_1, F_2, F_3. Количество факторов определено критерием Кайзера (отбираются только факторы, с собственными значениями, большими или

равными 1): для F_1 λ=6,97, для F_2 λ=2,48, для F_3 λ=1,03. Выбранные факторы объясняют 95,25% разброса. Факторы интерпретируются как группы, в которые объединяются маршруты нарушителя, между которыми выявлена латентная связь. Первую группу составляют маршруты №1-№4, вторую – №5-№8, третью - №9-№11. Вероятность безопасного состояния объекта в случаях, когда нарушители, совершают движение по территории объекта по маршрутам, относящимся в первой и второй группам (таблица 5.2), не удовлетворяет требованиям безопасного состояния ОО. После детализации маршрутов проникновения нарушителя, для первой и второй групп, имеющих недостаточный показатель эффективности СФЗ, исследуется зависимость вероятности безопасного состояния от её характеристик.

Далее, для каждой группы, обладающей недостаточным уровнем вероятности безопасного состояния, вырабатываются соответствующие решения для повышения эффективности СФЗ.

5.3 Полный факторный эксперимент. Построение уравнения регрессии

Исследование зависимости вероятности безопасного состояния ОО от характеристик СФЗ для первой и второй групп маршрутов проводится с помощью полного факторного эксперимента с количеством факторов равным четырём [135].

Входными параметрами (факторами) являются характеристики маршрутов: вероятности обнаружения и время задержки на двух рубежах, преодолеваемых нарушителем для достижения цели. Выходная характеристика: вероятность безопасного состояния ОО. Целью многофакторного эксперимента является установление зависимости: $f(x_1, x_2, \ldots, x_n)$, описывающей поведение объекта исследования.

Для маршрутов, объединённых в первую группу значения: P_1=0,6; P_2=0,8; T_1=255 с.; T_2=253 с. задают базовый (основной) уровень. Интервалы варьирования для P_1 и P_2 выбраны равными 0,03, а для T_1 и T_2 - 15 с.

Для маршрутов, объединённых во вторую группу базовый (основной) уровень задают значения: P_1=0,6; P_2=0,8; T_1=210 с.; T_2=150 с. Интервалы варьирования для P_1 и P_2 выбраны равными 0,03, а для T_1 и T_2 - 15 с.

Значения $Рбс_1$, $Рбс_2$, $Рбс_3$, являющиеся выходными параметрами эксперимента, получены с помощью имитационной модели, описанной в главе 4 [130]. Матрица планирования вычислительного эксперимента для первой группы маршрутов приведена в таблице 5.3.

Таблица 5.3 Описание результатов полного факторного эксперимента для первой группы маршрутов*

N	X_0	X_1	X_2	X_3	X_4	$Рбс_1$	$Рбс_2$	$Рбс_3$
1	1	0,57	240	0,77	238	0,552	0,555	0,556
2	1	0,63	240	0,77	238	0,637	0,634	0,611
3	1	0,57	270	0,77	238	0,558	0,569	0,575
4	1	0,63	270	0,77	238	0,635	0,639	0,653
5	1	0,57	240	0,83	238	0,575	0,584	0,58
6	1	0,63	240	0,83	238	0,631	0,633	0,642
7	1	0,57	270	0,83	238	0,593	0,564	0,577
8	1	0,63	270	0,83	238	0,649	0,628	0,634
9	1	0,57	240	0,77	268	0,566	0,572	0,566
10	1	0,63	240	0,77	268	0,634	0,65	0,624
11	1	0,57	270	0,77	268	0,572	0,582	0,596
12	1	0,63	270	0,77	268	0,641	0,648	0,655
13	1	0,57	240	0,83	268	0,6	0,567	0,587
14	1	0,63	240	0,83	268	0,653	0,633	0,638
15	1	0,57	270	0,83	268	0,577	0,612	0,58
16	1	0,63	270	0,83	268	0,657	0,653	0,661

* в таблицах 5.3 и 5.5

N – номер опыта;

X_0, X_1, X_2, X_3, X_4 – входные параметры эксперимента, где

X_0 – используется для оценки свободного члена уравнения регрессии

X_1 - P_1, вероятность обнаружения нарушителя на первом рубеже,

X_2 - T_1, время задержки нарушителя на первом рубеже, с,

X_3 - P_2 , вероятность обнаружения нарушителя на втором рубеже,

X_4 - T_2, время задержки нарушителя на втором рубеже, с;

$Рбс_1$, $Рбс_2$, $Рбс_3$ – выходные данные эксперимента,

$Рбс_{средзнач}$ – среднее значение $Рбс_1$, $Рбс_2$, $Рбс_3$

Проверка на однородность дисперсии выходного параметра выполняется по критерию Кохрена:

$$G_{расч.} = \frac{S_j^2 \max}{\sum_{j=1}^{N} S_j^2} \qquad (5.1)$$

где N=16 – количество опытов для полного факторного эксперимента с количеством факторов равным четырём;

S_j^2 – оценка дисперсии выходного параметра для *j*-го опыта, вычисляемая по формуле:

$$S_j^2 = \frac{\sum_{\gamma=1}^{l} (y_{jэ\gamma} - \bar{y}_{jэ})}{l-1} \qquad (5.2)$$

В формуле (5.2) *l*=3 количество выходных параметров Рбс; $y_{iэ\gamma}$ - значения каждого из трех выходных параметров Рбс на каждом опыте; $\overline{y_{jэ}}$ - средние значения выходных параметров Рбс:

$$\bar{y}_{jэ} = \frac{\sum_{\gamma=1}^{l} y_{jэ\gamma}}{l} \qquad (5.3)$$

Вычисления, выполненные по формулам (5.2), (5.3) для первой группы маршрутов приведены в таблице 5.4

Таблица 5.4 Вычисления, выполненные для первой группы маршрутов

$Рбс_{средзнач}$	S_i^2
0,5543	$4{,}33 \cdot 10^{-6}$
0,6273	0,000202333
0,5673	$7{,}43 \cdot 10^{-5}$
0,6423	$8{,}93 \cdot 10^{-5}$
0,5797	$2{,}033 \cdot 10^{-5}$
0,6353	$3{,}43 \cdot 10^{-5}$
0,578	0,000211
0,637	0,000117
0,568	0,000012
0,636	0,000172
0,5833	0,000145333
0,648	$4{,}9 \cdot 10^{-5}$
0,5847	0,000276333

0,6413	0,000108333
0,5897	0,000376333
0,657	0,000016
Итого S^2	0,001908333
$S_j^2 \max$	0,000376333

Используя значения таблицы 5.4, по формуле (5.1) вычислено G*расч*= 0,197. Критическое значение критерия G для уровня значимости α = 0,05, числа степеней свободы $f = l - 1 = 2$ и числа суммируемых оценок дисперсий, равного N:

$$G_{табл}(0{,}05;\, N = 16;\, f = 2) = 0{,}3346 \quad \Rightarrow \quad \text{G } расч < \text{G } табл$$

По результатам сравнения расчетного и табличного значений G–критерия гипотеза об однородности ряда выборочных дисперсии выходного параметра не отвергается и в качестве оценки дисперсии воспроизводимости эксперимента берётся средняя дисперсия:

$$S^2_{воспр} = \frac{\sum_{j=1}^{N} S_j^2}{N}, \tag{5.4}$$

$$S^2_{воспр} = \frac{0{,}0019083}{16} = 0{,}00011927$$

$$f_{воспр} = N(l-1) = 16(3-1) = 32. \tag{5.5}$$

Таким образом, все предпосылки для проведения множественного регрессионного анализа выполняются. Расчет коэффициентов уравнения регрессии производится по формуле:

$$b_i = \frac{1}{N}\sum_{j=1}^{N} x_{ji}\,\overline{y}_{iэ}. \tag{5.6}$$

На основе вычисленных по формуле (5.6) коэффициентов, уравнение приближенной линейной регрессии будет иметь вид:

$$\overline{y} = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + \ldots + b_Nx_N. \tag{5.7}$$

Проверка адекватности уравнения регрессии результатам эксперимента, осуществляется по критерию Фишера:

$$F_{расч} = \frac{S^2_{ад}}{S^2_{воспр.}}; \quad (5.8)$$

$$S^2_{ад} = \frac{l\sum_{j=1}^{N}(\bar{y}_{jэ} - \bar{y}_j)^2}{N-h} = \frac{3\sum_{j=1}^{8}(\bar{y}_{jэ} - \bar{y}_j)^2}{16-4} \quad (5.9)$$

где $\bar{y}_j$ - оценка выходного параметра по результатам вычислений с использованием полученного уравнения приближенной регрессии.

Уравнение регрессии, построенное для первой группы маршрутов, имеет вид:

$$P_{бс} = - 0{,}340 + 1{,}082 \cdot P_1 + 3{,}17 \cdot 10^{-4} \cdot T_1 + 0{,}158 \cdot P_2 + 3{,}61 \cdot 10^{-4} \cdot T_2. \quad (5.10)$$

Матрица планирования вычислительного эксперимента для второй группы маршрутов приведена в таблице 5.5.

Таблица 5.5 Описание результатов полного факторного эксперимента для второй группы маршрутов

N	X_0	X_1	X_2	X_3	X_4	$Рбс_1$	$Рбс_2$	$Рбс_3$	$Рбс_{средзнач}$
1	1	0,57	195	0,77	135	0,56852	0,5685	0,56792	0,5683
2	1	0,63	195	0,77	135	0,62793	0,62909	0,63047	0,6292
3	1	0,57	225	0,77	135	0,56946	0,57017	0,56948	0,5697
4	1	0,63	225	0,77	135	0,62968	0,63074	0,63169	0,6307
5	1	0,57	195	0,83	135	0,57237	0,56917	0,56931	0,5703
6	1	0,63	195	0,83	135	0,63146	0,62993	0,62973	0,6304
7	1	0,57	225	0,83	135	0,57124	0,57291	0,57175	0,57197
8	1	0,63	225	0,83	135	0,63118	0,63164	0,63089	0,6312
9	1	0,57	195	0,77	165	0,57201	0,57374	0,5715	0,5724
10	1	0,63	195	0,77	165	0,63029	0,62953	0,63028	0,6300
11	1	0,57	225	0,77	165	0,56993	0,57114	0,56983	0,5703
12	1	0,63	225	0,77	165	0,63048	0,62983	0,63234	0,6309
13	1	0,57	195	0,83	165	0,57053	0,57026	0,57195	0,5709
14	1	0,63	195	0,83	165	0,63214	0,63024	0,63114	0,63117
15	1	0,57	225	0,83	165	0,57176	0,56847	0,57355	0,5713
16	1	0,63	225	0,83	165	0,63152	0,63113	0,63102	0,63122

Вычисления, выполненные по формулам (5.2), (5.3) для второй группы маршрутов приведены в таблице 5.6.

Таблица 5.6 Вычисления, выполненные для второй группы маршрутов

$Рбс_{средзнач}$	S_j^2
0,5683	$1{,}1613 \cdot 10^{-7}$
0,6292	$1{,}6169E \cdot 10^{-6}$
0,5697	$1{,}6343 \cdot 10^{-7}$
0,6307	$1{,}011 \cdot 10^{-6}$
0,5703	$3{,}2705 \cdot 10^{-6}$
0,6304	$8{,}9563 \cdot 10^{-7}$
0,57197	$7{,}3243 \cdot 10^{-7}$
0,6312	$1{,}4303 \cdot 10^{-7}$
0,5724	$1{,}3784 \cdot 10^{-6}$
0,6300	$1{,}9003 \cdot 10^{-7}$
0,5703	$5{,}317 \cdot 10^{-7}$
0,6309	$1{,}697 \cdot 10^{-6}$
0,5709	$8{,}2423 \cdot 10^{-7}$
0,63117	$9{,}0333 \cdot 10^{-7}$
0,5713	$6{,}6391 \cdot 10^{-6}$
0,63122	$6{,}9033 \cdot 10^{-8}$
Итого S^2	$2{,}0182 \cdot 10^{-5}$
$S_j^2 \max$	$6{,}6391 \cdot 10^{-6}$

Для второй группы маршрутов, вычисленное по формуле (5.1) на основе данных таблицы 5.5, G*расч*= 0,329. Как, и для первой группы маршрутов:

$$G_{табл}(0{,}05;\ N = 16;\ f = 2) = 0{,}3346 \quad \Rightarrow \quad G\ расч < G\ табл$$

Следовательно, для маршрутов второй группы гипотеза об однородности ряда выборочных дисперсии выходного параметра также не отвергается.

Уравнение регрессии второй группы маршрутов имеет вид:

$$Р_{бс} = -\ 0{,}019 + 0{,}999 \cdot Р_1 + 1{,}92 \cdot 10^{-5} \cdot Т_1 + 0{,}014 \cdot Р_2 + 2{,}69 \cdot 10^{-5} \cdot Т_2. \qquad (5.11)$$

Адекватность уравнений регрессии для первой и второй групп маршрутов проверена с использованием табличного значения критерия Фишера (выбранного при доверительной вероятности равной 0,95). Для первой группы маршрутов дисперсия адекватности $S^2_{ад}=7{,}85 \cdot 10^{-5}$, дисперсия воспроизводимости $S^2_{воспр}= 1{,}19 \cdot 10^{-4}$. Рассчитанное значение критерия Фишера F=0,66. Для второй группы маршрутов дисперсия адекватности $S^2_{ад}= 2{,}16 \cdot 10^{-6}$, дисперсия воспроизводимости $S^2_{воспр}= 1{,}26 \cdot 10^{-6}$. Рассчитанное

значение критерия Фишера F=1,71. В обоих случаях рассчитанные значения меньше табличного значений критерия Фишера F=2,1. Что позволяет сделать вывод об адекватности полученных уравнений регрессии для первой и второй групп маршрутов.

5.4 Принятие решений по обеспечению требуемой безопасности охраняемых объектов

Принятие решений по обеспечению требуемой безопасности ОО проводится на основе анализа уравнений регрессии.

В уравнениях регрессии для рассмотренных групп маршрутов (5.10), (5.11) наибольшее значение имеют коэффициенты вероятности обнаружения нарушителя на первом рубеже P_1. Далее по значимости расположены коэффициенты вероятности обнаружения нарушителя на втором рубеже P_2, времени движения нарушителя на втором рубеже T_2. Наименьшее значение у коэффициентов T_1. Коэффициенты каждой характеристики маршрутов положительные, это значит, что увеличивая их значения, будет расти вероятность безопасного состояния объекта, а, следовательно, эффективность СФЗ ОО. Наибольшее влияние на вероятность безопасного состояния объекта оказывает вероятность обнаружения нарушителя на первом рубеже. Второй по значимости является вероятность обнаружения нарушителя на следующем рубеже. Для рассматриваемого модельного ОО – это второй и последний рубеж, являющийся фактически критической точкой обнаружения нарушителя. В случае, если нарушитель обнаружен на данном рубеже, то вероятность безопасного состояния ОО будет определяться временем задержки в этой зоне. Коэффициент характеристики T_2 больше коэффициента T_1, это показывает, что время задержки нарушителя на последнем рубеже более значимо для вероятности безопасного состояния ОО, чем время задержки нарушителя на ранних рубежах. Коэффициенты при T_1 и T_2 значительно меньше коэффициентов при P_1 и P_2, это показывает нецелесообразность увеличения времени задержки нарушителя, в случае, если он не будет выявлен средствами обнаружения СФЗ [136].

По результатам анализа уравнений регрессии можно выработать два направления решений повышения эффективности СФЗ:

1) повышение вероятности обнаружения путём установки технических средств обнаружения (ТСО), имеющих улучшенные технические характеристики (по сравнению с установленными) и/ или повышения надежности работы персонала СФЗ;

2) увеличение времени задержки при проникновении нарушителя на территорию ОО для совершения деструктивных действий.

В первом случае, исходя из наибольшего значения коэффициента вероятности обнаружения P_1 в уравнениях (5.10) и (5.11), для обеспечения превентивности, необходимо проводить модернизацию ТСО на внешнем рубеже. Надежность работы персонала можно повысить за счет введения дополнительного оператора для одновременного наблюдения за ситуацией.

Во втором случае, так как коэффициент у T_2 в уравнениях регрессии выше чем у T_1, увеличивать время задержки целесообразно после критической точки обнаружения.

Значения коэффициентов при P_1 в уравнениях (5.10) и (5.11) примерно равны единице. Для достижения $P_{бс}$ равным 0,8 необходимо повысить значение P_1 до 0,8. Так как значение P_2 на рассматриваемых маршрутах равно 0,8 вторым способом увеличения вероятности $P_{бс}$ является повышение T_2 на 47 с. (от базового уровня) в первой группе и на 190 с. (от базового уровня) во второй группе маршрутов, т.е. до значения $T_2 = 300$ с. Указанные значения характеристик маршрутов выходят из областей, для которых построены уравнения регрессии, в этом случае необходимо движение по градиенту. Подстановка указанных данных, в имитационную модель СФЗ показала, что необходимая вероятность безопасного состояния ОО будет достигнута.

Гипотетический модельный ЦППН имеет периметр 4500 м. По периметру установлено ограждение из металлической сетки высотой 2,5 м, усиленное сверху СББ «Егоза». По периметру расположена полоса отчуждения шириной 5 м. На некоторых рубежах установлены

оборонительные сооружения. Рекомендуемые способы повышения времени задержки для второго рубежа охраны:

- увеличение ширины полосы отчуждения до 10 м – от 10 с;
- установка дополнительного инженерного заграждения из трех спиралей из армированной скрученной колючей ленты (АСКЛ) диаметром 860 мм в три ряда два яруса – от 50 с;
- установка дополнительного оборонительного сооружения "Шиповник-1" и "Шиповник-2" модификация М4 – от 180 с [137].

Рубежи охраны периметра ОО, для которых P_1=0,6 оснащены двумя вибрационными точечными пьезоэлектрическими извещателями с вероятностью обнаружения 0,65. Для увеличения значения P_1 до 0,8 необходимо установить два ТСО с вероятностью обнаружения не менее 0,95.

Окончательное решение по способу повышения эффективности принимается после экономических (стоимостных) расчетов по реализации предложенных направлений решений и выбирается наиболее приемлемый для ОО способ.

5.5 Оценка эффективности концептуальной модели исследования СФЗ

Чтобы провести оценку эффективности разработанной концептуальной модели исследования СФЗ: методик и имитационной модели, представленных в ней, нужно сравнить эффективность работы оценки эффективности СФЗ ОО и принятия решений для ее повышения, в случае необходимости без их помощи и с их помощью. Для этого необходимо сравнить два процесса:

1) оценка эффективности СФЗ ОО и принятие решений для ее повышения, в случае необходимости, без использования разработанных методик и программного средства;

2) оценка эффективности СФЗ ОО и принятие решений для ее повышения, в случае необходимости, с использованием разработанных методик и программного средства.

По информации экспертов, наибольшее влияние на принятие решений для повышения эффективности СФЗ, имеют временные и экономические затраты следующих процессов:

- сбор необходимой информации об ОО;

- оценка эффективности СФЗ;

- анализ результатов оценки эффективности СФЗ и принятие решений по её повышению.

Временные и экономические затраты на внедрение программного средства, обучение оператора и обслуживание аппаратного обеспечения были определены экспертами как несущественные. Одно рабочее место оператора можно использовать оценки эффективности СФЗ для нескольких объектов информатизации.

Так как сбор необходимой информации об ОО походит одинаково как с использованием разработанной концептуальной модели, то временные и экономические затраты этого процесса являются одинаковыми. Использование ПС «Имитационная модель функционирования системы физической защиты объекта» позволяет снизить оценки эффективности СФЗ до 60 мин. Итоговое время на весь процесс с использованием концептуальной модели составляет 9 часов, без использования - 16 часов.

Анализ СФЗ модельного ОО экспертами выявил следующие недостатки: рубежи охраны $Y_3 – Y_{11}$ оснащены ТСО, имеющими технические характеристики; недостаточность средств задержки рубежей охраны $Y_{15} – Y_{21}$. Экспертами рекомендовано установить датчики обнаружения (системы видеонаблюдения), вероятность которых (согласно технической документации) составляет 0,99. По мнению экспертов, время задержки необходимо увеличить примерно от 50 до 180 с. Таким образом, результаты оценки эффективности СФЗ, полученной на основе концептуальной модели, согласуются с результатами экспертов.

Экспертами выделены 5 критериев оценки эффективности использования разработанной концептуальной модели (таблица 5.7).

Таблица 5.7 – Количественные критерии оценки приращения эффективности

Критерии оценка эффективности	Оценка эффективности без применения концептуальной модели	Оценка эффективности с применением концептуальной модели	Весовые коэффициенты
Количество параметров оценки потенциала опасности ЧС	2	3	0,08
Весовой коэффициент приращения обоснованности	0,6	1	0,12
Учет подготовленности нарушителя при оценке вероятности его обнаружения	0,6	0,85	0,09
Сужение области принятия решения	3	2	0,12
Временные затраты, ч.	16	9	0,12

Применяя метод ранга (Хоменюка) для принятия решений выявлено, что каждый критерий вносит примерно одинаковый вклад на принятие решений о целесообразности применения концептуальной модели. Также на основе полученных значений оценочных потенциалов: для альтернативы без применения концептуальной модели – 0,47 и для альтернативы с применением концептуальной модели – 0,53 делаем вывод об эффективности представленных в исследовании разработок. Следовательно, относительное приращение эффективности составляет 12,8%.

Выводы по пятой главе

В главе представлена методика принятия решений по обеспечению физической безопасности, с помощью которой проведена оценка эффективности на гипотетическом модельном ОО (ЦППН).

Обработка матрицы характеристик маршрутов проникновения с помощью факторного анализа, позволяет понять латентные связи в структуре характеристик маршрутов. Для модельного ОО получены три разнородные

группы маршрутов проникновения. Для каждой группы маршрутов, обладающих вероятностью безопасного состояния ниже требуемой для ОО, относящихся к заданной категории, получены уравнение связи эффективности СФЗ от характеристик ИТСО на данном маршруте проникновения. Градиенты этих уравнений показывают направления изменения параметров для максимального приращения эффективности. Анализ уравнений показывает, что коэффициенты в уравнениях различаются, следовательно, для каждой части системы безопасности надо использовать разные изменения структуры СФЗ. Анализ значений коэффициентов уравнений позволил сформировать решения по повышению вероятности безопасного состояния на рубежах, через которых проходят маршруты выделенных групп, до требуемого уровня.

Достоинством разработанного метода является повышение достоверности результатов оценки из-за возможности детализировать маршрут проникновения нарушителя на группы разнородных маршрутов, и вырабатывать для каждой группы соответствующие решения для повышения эффективности СФЗ.

Заключение

Интенсивно и непрерывно изменяющие внешние и внутренние условия функционирования ОО приводят к изменению требований к их безопасности, обеспечиваемой СФЗ. Следовательно, оценка эффективности является необходимым процессом их жизнедеятельности СФЗ.

Анализ научных работ в области оценки и повышения эффективности СФЗ показал, что учеными разработаны методы проектирования СФЗ и оценки их эффективности, предложены методики категорирования и анализа уязвимости объектов, рассмотрены способы повышения вероятности обнаружения нарушителей техническими средствами обнаружения (ТСО). При этом, существует необходимость разработки методики принятия обоснованных решений, направленных обеспечение требуемого уровня эффективности СФЗ.

В рамках исследования проведен системный анализ процесса повышения эффективности СФЗ, под которой понимается способность системы физической защиты обеспечить безопасное состояние ОО. На его основе разработана концептуальная модель повышения эффективности СФЗ, состоящая из этапов: определение требуемого уровня эффективности СФЗ и потенциальных нарушителей для различных категорий ОО; имитационное моделирование; принятие решений по повышению эффективности СФЗ. Критерием эффективности выступает вероятность нахождения ОО в безопасном состоянии $P_{бс}$ – показатель, характеризующий степень выполнения СФЗ своих основных функций: обнаружения, задержки, реагирования и нейтрализации нарушителя. Приоритетной стратегией оптимизации эффективности СФЗ является требование обеспечения уровня безопасности не ниже допустимого при минимальных затратах на ресурсы, не превышающих величину потенциального ущерба ОО.

Для определения критериев безопасного состояния и потенциальных нарушителей для каждой категории ОО разработана методика, основными этапами которой являются: 1) определение требований к безопасности в

зависимости от категории ОО; 2) определение потенциала опасности нарушителей 3) идентификация потенциальных нарушителей для каждой категории ОО.

На основе анализа соответствующих научных источников и нормативно-правовых актов выделены пять категорий ОО и шесть моделей нарушителей.

Критерием категорирования ОО выбран масштаб ЧС, являющийся наихудшим результатом несанкционированного проникновения на ОО нарушителя. Введена нелинейная шкала оценки ЧС для формирования генеральной совокупности. При формировании данной шкалы учитываются три признака ЧС: людские потери, материальный ущерб, зона ЧС. Используя данную шкалу, получены интервальные оценки требуемой вероятности безопасного состояния для каждой категории ОО и вероятности требуемой защиты для каждой модели нарушителей. Перекрытие диапазонов вероятности безопасного состояния ОО и требуемой вероятности защиты от нарушителя позволило определить потенциальных нарушителей для каждой категории объекта.

Для определения вероятности безопасного состояния ОО разработана имитационная модель функционирования системы физической защиты объекта. Поставленная перед имитационной моделью цель: достигается имитацией основных функций СФЗ в последовательности, происходящей в реальности. Эффективность СФЗ определяется как статистическая вероятность пресеченных атак нарушителя на объект.

Принятие решений по обеспечению требуемого уровня физической безопасности осуществляется с помощью разработанной методики, представляющей собой комплексное исследование СФЗ. Методика состоит из этапов: оценка эффективности СФЗ ОО (имитационное моделирование); декомпозиция маршрутов нарушителя; построение уравнения регрессии на основе полного факторного эксперимента; принятие решений по обеспечению физической безопасности ОО. На этапе декомпозиции матрица

характеристик маршрутов проникновения исследуется метолом факторного анализа, что позволяет выявить латентные связи, на основе которых группируются маршруты. Для каждой группы маршрутов, обладающих вероятностью безопасного состояния ниже требуемой для ОО, относящихся к заданной категории, строятся уравнения регрессии. Анализ значений коэффициентов уравнений позволяет сформировать решения по повышению вероятности безопасного состояния на рубежах, через которых проходят маршруты выделенных групп, до требуемого уровня.

Основные выводы и результаты работы:

1. В ходе системного анализа СФЗ ОО разработана концептуальная модель исследования путей повышения эффективности СФЗ, которая позволяет формировать оптимальную структуру СФЗ. Достоинствами модели являются возможность производить декомпозицию сложной задачи управления физической безопасностью ОО, учет разнородности маршрутов нарушителя и разнородность СФЗ, что позволяет увеличить достоверность зависимостей вероятности безопасного состояния объекта от параметров СФЗ.

2. Разработана методика определения потенциальных нарушителей для категорий ОО на основе оценки и сопоставления потенциалов опасности ОО и нарушителей.

3. Предложены критерии безопасного состояния каждой категории ОО. Использование интервальных оценок безопасного состояния позволяет однозначно определить достаточность защиты объекта, избежать избыточности или недостаточности СФЗ и расширить варианты реализации СФЗ.

4. Предложен алгоритм вычисления коэффициента снижения вероятности обнаружения, учитывающий уровень подготовленности потенциального нарушителя.

5. Разработана имитационная модель оценки эффективности СФЗ ОО. Достоинствами которой являются: возможность за счет пространственно-

временной детализации зоны обнаружения и зоны задержки нарушителя максимально приблизить результаты имитации к реальному физическому процессу функционирования СФЗ; оценка всех возможных маршрутов проникновения нарушителя на ОО; детализация каждого маршрута проникновения на разнородные участки и учет времени обнаружения на каждом рубеже обнаружения; возможность использования результатов натурных испытаний на реальном объекте как входные данные модели. Что позволяет повысить достоверность оценки эффективности СФЗ.

6. Разработана методика принятия решений по обеспечению физической безопасности ОО.

7. Реализованная концептуальная модель по изменению структуры СФЗ для повышения ее эффективности позволила сократить временные затраты на принятие решений на 44%. Относительное приращение эффективности применения концептуальной модели исследования СФЗ составляет 12,8%.

Перспективы дальнейших исследований

Приоритетными направлениями дальнейших исследований являются:

1. Разработка методики оценки эффективности СФЗ, направленной на обнаружение и предотвращение угроз, субъектом которых являются внутренние нарушители.

2. Разработка методики оценки эффективности СФЗ, направленной на предотвращение угроз субъектами которых являются управляемые технические устройства (роботы, беспилотные летательные аппараты и т.д…).

3. Изучение возможностей применения методов машинного обучения и искусственного интеллекта в вопросах поддержки принятия решений по повышению эффективности СФЗ.

Список использованных источников

1. Конституция Российской Федерации [Электронный ресурс].: принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года, с изменениями на 4 октября 2022 года// Электронный фонд правовых и нормативно-технических документов АО «Кодекс». - URL: **https://docs.cntd.ru/document/9004937**. – 15.04.2024.
2. О Стратегии научно-технологического развития Российской Федерации [Электронный ресурс].: Указ Президента Российской Федерации от 01.12.2016 г. № 642// Президент России, 2025 - URL: **http://static.kremlin.ru/media/acts/files/0001201612010007.pdf**. – 15.04.2024.
3. О Стратегии национальной безопасности Российской Федерации [Электронный ресурс].: Указ Президента Российской Федерации от 02.07.2021г. № 400// Президент России - URL: http://www.kremlin.ru/acts/bank/47046/page/1. -– 15.04.2024
4. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс].: Федеральный закон от 31.07.2023 № 398-ФЗ// Президент России - URL: http://www.kremlin.ru/acts/news/copy/71871. – 15.04.2024
5. Даль В.И. Толковый словарь живого великорусского языка В.И. Даля. – Санкт-Петербург: Весь, 2004. - 735 с
6. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений. - М.: Азбуковник, 1999. - 944 с.
7. Кузнецов С.А. Большой толковый словарь русского языка/ С.А. Кузнецов - Санкт-Петербург: Норинт, 1998. - 1535 с.
8. Ушаков Д.Н. Большой толковый словарь русского языка: современная редакция/ Д.Н. Ушаков – М.: Дом Славянской кн., 2008. - 959 с.
9. Чикунов, И. А. Анализ дефиниции термина "безопасность"/ И. А. Чикунов, Н. В. Сербиновская// Вестник науки и образования Северо-Запада России. – 2021. – Т. 7, № 1. – С. 53-59. – EDN BPCCNC.
10. Термины МЧС России [Электронный ресурс].: словарь// МЧС России. - URL: https://www.mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/3180. - 15.03.2021.
11. ГОСТ Р 12.3.047-98 Пожарная безопасность технологических процессов. Общие требования. Методы контроля [Электронный ресурс].: Система стандартов безопасности труда// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: http://docs.cntd.ru/document/1200003311 - 15.03.2021.
12. ГОСТ Р МЭК 61508-4-2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью [Электронный ресурс].: Национальный стандарт РФ//

Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: http://docs.cntd.ru/document/1200063224. - 16.03.2021.

13. Костин В. Н. Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов: дис. …д-ра техн. наук: 05.13.01: защищена 16.09.2021: утв. 21.02.2022/ В.Н. Костин.- Оренбург, 2021. – 249 с.

14. Цыгично В.Н. Безопасность критических инфраструктур/ В.Н. Цыгичко, Д.С. Черешкин, Г.Л. Смолян. – М.: ЛЕНАРД. – 2021. – 200 с.

15. Боровский А.С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации дисс. … д-ра техн. наук 05.13.19: защищена 24.06.2015/ А.С. Боровский – Оренбург, 2015 г. - 344с.

16. Малышкин С.Л. Модель и методы вероятностного анализа процесса обнаружения нарушителя средствами систем физической защиты объектов информатизации. дисс. … канд. тех. наук: 29.12.15: защищена 16.09.2021/ С.Л. Малышкин – Санкт- Петербург, 2015 г. – 123 с.

17. Гарсиа М. Проектирование и оценка систем физической защиты. Пер. с англ. – М.: ООО «Издательство АСТ», 2002. – 386 с.

18. РД 78.36.003-2002. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств. [Электронный ресурс].: Утвержден МВД РФ 6 ноября 2002 г. - Введен с 01.01.2003 взамен РД 78.143-92 и РД 78.147-93// Юридическая информационная система "Легалакт - законы, кодексы и нормативно-правовые акты Российской Федерации". – 2015-2025. – URL: https://legalacts.ru/doc/rd-7836003-2002-inzhenerno-tekhnicheskaja-ukreplennost-tekhnicheskie-sredstva-okhrany/. – 23.05.2023

19. Свод правил СВ 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования». Введен 20.09.2011. - М.: Министерство регионального развития России, 2011. - 6с.

20. Рекомендации Р 78.36.007-99 «Выбор и применение средств охранно- пожарной сигнализации и средств технической укреплённости для оборудования объектов». [Электронный ресурс].: Утв. ГУВО МВД РФ 27 июня 1998 г.// Охрана труда в России. – URL: https://ohranatruda.ru/ot_biblio/norma/246642/. – 25.03.2023

21. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации. Часть 1. Общие требования». Введен в действие постановлением Госстандарта РФ от 22 мая 1995 г. № 256. – М.: Госстандарт России, 1995. – 11 с.

22. ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» [Электронный ресурс].: Разработан ФГУ НИЦ "ОХРАНА" МВД России, Центром оперативного руководства деятельностью вневедомственной охраны (ЦОРДВО) МВД России// Электронный фонд

правовых и нормативно-технических документов АО «Кодекс». - URL: https://docs.cntd.ru/document/1200071688. – 25.03.2023

23. ГОСТ Р 51558-2008 «Средства и системы охранные телевизионные». Разработан ФГУ НИЦ "ОХРАНА" МВД России, Центром оперативного руководства деятельностью вневедомственной охраны (ЦОРДВО) МВД России. – М.: Стандартинформ, 2009. – 15 с.

24. ГОСТ 53704-2009 «Системы безопасности комплексные интегрированные». Разработан ФГУ НИЦ "ОХРАНА" МВД России. – М.: Стандартинформ, 2010. – 30 с.

25. ГОСТ 12.1.004-91 ССБТ. «Пожарная безопасность. Общие требования». Разработан МВД СССР, Министерством химической промышленности СССР. – М.: Стандартинформ, 2006. – 64 с.

26. ГОСТ Р 22.1.12-2005 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений». Разработан ФГУ ВНИИ по проблемам гражданской обороны и чрезвычайных ситуаций. – М.: Стандартинформ, 2005. – 9 с.

27. ГОСТ Р 50862-2012 «Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2012 г. № 1031-ст. – М.: Стандартинформ, 2014. – 27 с.

28. РД 25.952-90 «Системы автоматические пожаротушения, пожарной, охранной и охраннопожарной сигнализации. Порядок разработки задания на проектирование». [Электронный ресурс].: Утвержден Министерством электротехнической промышленности и СССР// Электронный фонд правовых и нормативно-технических документов АО «Кодекс». – URL: https://docs.cntd.ru/document/1200004289– 25.03.2023

29. РД 78.148-94 «Защитное остекление Классификация, методы испытаний» [Электронный документ].: Утвержден МВД СССР// Гост Ассистент. – URL https://gostassistent.ru/doc/6c12a64f-8ce4-4294-884b-224f7ca255a1 - 23.03.2023

30. Технический регламент о требованиях пожарной безопасности [Электронный документ].: Федеральный закон № 117-ФЗ от 10 июля 2012 г.// Электронный фонд правовых и нормативно-технических документов АО «Кодекс». - URL: https://docs.cntd.ru/document/902111644. – 25.03.2023

31. ГОСТ 26342-84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры. [Электронный документ].: Межгосударственный стандарт. Введ. 01.01.1986// Электронный фонд правовых и нормативно-технических документов АО «Кодекс». - URL: https://docs.cntd.ru/document/1200031059. – 25.03.2023

32. РД-07-01-2004 «Методические указания по проведению оценки состояния физической защиты ядерно- и радиационно-опасных объектов по результатам проведенной инспекции». [Электронный документ].:

Межгосударственный стандарт. Введ. 1.01.2005// Электронный фонд правовых и нормативно-технических документов АО «Кодекс». - URL: https://docs.cntd.ru/document/1200039725 - 25.03.2023

33. Алаухов, С. Ф. Концепция безопасности и принципы создания систем физической защиты важных промышленных объектов/ С. Ф. Алаухов, С. Ф. Коцеруба. – НИКИРЭТ, 2005. – 96 с.

34. Боровский А.С. Концептуальное проектирование и анализ систем физической защиты [Электронный ресурс]: учебное пособие/ А.С. Боровский, А.Д. Тарасов, М.Ю. Шрейдер; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2022. – 177 с. URL: http://artlib.osu.ru/web/books/metod_all/164779_20220331.pdf – 15.05.2023

35. ГОСТ Р 52551-2016 Системы охраны и безопасности. Термины и определения [Электронный ресурс].: Национальный стандарт РФ// Электронный фонд правовых и нормативно-технических документов – АС «Кодекс». – 2025. - URL: https://docs.cntd.ru/document/1200141714 - 20.03.2023

36. Интеллектуальная интегрированная система безопасности критически важных и потенциально опасных объектов: монография/ Янников И.М. [и др.] – Самара: Изд-во СамНЦ РАН, 2019. – 182 с.

37. Бурькова Е.В. Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова; – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 157 с.

38. Определение критериев эффективности систем физической защиты ядерных объектов / А. В. Жуков, А. В. Бояринцев, Н. И. Гераскин, А. А. Краснобородько// Ядерная физика и инжиниринг. – 2014. – Т. 5, № 5. – С. 373. – DOI 10.1134/S2079562914050091. – EDN STHXXJ.

39. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, его территориальных органов и подведомственных ему организаций, а также формы паспорта безопасности этих объектов (территорий) [Электронный ресурс].: Постановление Правительства от 31 августа 2019 г. №1133// Официальный интернет-портал правовой информации. 2005-2025 гг. - 05.09.2019. – URL: http://publication.pravo.gov.ru/Document/View/0001201909050032?index=13&rangeSize=1 – 5.03.2024

40. ГОСТ 12.0.230.3-2016. Система стандартов безопасности труда. Системы управления охраной труда. Оценка результативности и эффективности (введен в действие Приказом Росстандарта от 31.05.2017 N 471-ст) [Электронный ресурс].: Межгосударственный стандарт// Консультант URL: https://www.consultant.ru/document/cons_doc_LAW_294354/74f283c8ba88587ab702c6e4f95cde93a4e1acf5/ - 5.03.2024.

41. Системный анализ и принятие решений: словарь-справочник/ под редакцией В.Н. Волковой, В.Н. Козлова. – М.: Высшая школа, 2004. – 616 с.

42. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения [Электронный ресурс].: Межгосударственный стандарт// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/1200006979. – 11.03.1014

43. Cooper, W. W. Data Envelopment Analysis: A Comprehensive Text with Models, Applications, References, and DEA-Solver Software / W. W. Cooper, L. M. Seiford, K. Tone.– Boston : Kluwer Academic Publishers, 2000. – 318 p.

44. Боровский А.С., Тарасов А.Д. Автоматизированное проектирование и оценка систем физической защиты потенциально опасных (структурно-сложных) объектов: монография в 3 ч. – М.: Омега-Л, 2013, 248 с.

45. Определение критериев эффективности систем физической защиты ядерных объектов/ А. В. Жуков, А. В. Бояринцев, Н. И. Гераскин, А. А. Краснобородько// Ядерная физика и инжиниринг. – 2014. – Т. 5, № 5. – С. 373. – DOI 10.1134/S2079562914050091. – EDN STHXXJ

46. ГОСТ ISO/IEC 27014—2021 Информационные технологии. Информационная безопасность. Кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению безопасности Межгосударственный стандарт. Введ 30.11.2021 – М. Стандартинформ, 2021. – 17 с.

47. Царькова Е. Г. Чем измерить эффективность: методы оценки эффективности систем физической защиты охраняемых объектов УИС//Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: Сборник материалов круглого стола, Тверь, 24 июня 2019 года. – Тверь: Федеральное казенное учреждение "Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний", 2019. - С. 189-202. - EDN HHGMRK

48. Шнякина, Е. А. Методы оценки эффективности систем физической защиты объектов/ Е. А. Шнякина, В. Н. Костин // Современные научно-исследовательские и технологические аспекты программной инженерии: Материалы Всероссийской научно-технической конференции, Оренбург, 14–15 сентября 2023 года. – Оренбург: Оренбургский государственный университет, 2023. – С. 138-141. – EDN COZLCF

49. Истомин А. Л. Математические модели задач построения эффективной системы физической защиты охраняемого объекта/ А.Л. Истомин, А.В. Баденков. А. А Истомина// Информатика и системы управления - 2019. - № 1(59) - С. 58-70. – DOI 10.22250/isu.2019.59.58-70.

50. Олейник А.С. Методы оценки эффективности защиты критически важных объектов/ А.С. Олейник // Вестник Московского университета МВД России. -2017. - №4. – С. 280-286

51. РД-07-01-2004 «Методические указания по проведению оценки состояния физической защиты ядерно- и радиационно-опасных объектов по результатам проведенной инспекции» [Электронный ресурс].: Введ 01.01.2025// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/1200039725. – 11.10.2024

52. Панин О. Как измерить эффективность? Логико-вероятностное моделирование в задачах оценки систем физической защиты/ О. Панин// Безопасность. Достоверность. Информация. - 2008. - № 77. - С. 20-24. - EDN KTOSBR

53. Рябинин И. А. Логико-вероятностные методы исследования надежности структурно-сложных систем/ И.А. Рябинин, Г.Н. Черкесов – М.: Радио и связь, 1981. – 264 с.

54. Можаев А.С. Общий логико-вероятностный метод анализа надежности сложных систем/ А.С. Можаев – Ленинград: Изд.Военно-Морская Академия имени Маршала СССР Гречко А.А., 1988 г. - 68 с.

55. Бочков А. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход/ А. Бочков// Безопасность. Достоверность. Информация. – 2009. – № 82. – С. 22-24. - EDN MUJJBN

56. Саати Т. Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. – М.: URSS, 2021. – 360 с.

57. Применение метода анализа иерархий для обеспечения безопасности объектов / Е. Д. Жужа, А. П. Жужа, Е. В. Дяговец, Т. В. Огнева // Актуальные проблемы развития вертикальной интеграции системы образования, науки и бизнеса: экономические, правовые и социальные аспекты : материалы XI Международной научно-практической конференции, Воронеж, 29–30 декабря 2022 года. – Воронеж: Воронежский экономико-правовой институт, 2022. – С. 257-265. – EDN YLSHAB.

58. Рябинин И.А. Логико-вероятностный метод и его современные возможности/ И.А. Рябинин //БИОСФЕРА. Международный научный и практический журнал. 2010. - Том 2.№1. - С.23-38.

59. Логико-вероятностный метод расчета надежности судовых энергетических установок/ С.В. Кондрашоа [и др.] // Вычислительные системы. Сборник трудов. Институт математики СО АН СССР. – 1964. - Вып.13. - С. 45-57.

60. L.Fratta, U.G.Montanari," A Boolean Algebra Method for Computing the Terminal Reliability in a Communication Network," IEEE Trans. Circuit Theory, vol CT-20, 1973 May, pp 203-211

61. Козарь В.Б. Использование имитационно-логико-вероятностных моделей для оценки эффективности сложных систем/ В.Б. Козарь// Вестник Концерна ВКО «Алмаз – Антей». – 2015. - №2. – С. 16-20. https://doi.org/10.38013/2542-0542-2015-2-16-20

62. Брук Б.Н. Методы экспертных оценок в задачах упорядочения объектов/ Б.Н. Брук, В.Н. Бурков// Известия АН СССР. Техническая кибернетика. - 1972. - № 3. - С. 29 – 39.

63. Saaty T.L. The analytic hierarchy process. – N.-Y.: McGraw Hill, 1980. – 288 p.

64. Saaty, T. L. Decision Making with Dependence and Feedback: The Analytic Network Process (Second ed.). Pittsburgh, USA, 2001, 350 p.

65. Broder, J. F. Risk Analysis and the Security Survey / J. F. Broder. – Butterworth-Heinemann, 2006. – 393 p.

66. Огородников П. И. Системный анализ обеспечения стабильности эффективного функционирования инновационной и цифровой экономики на основе интеллектуализации системы комплексной безопасности/ П.И. Огородников, Г.М. Залозная, А.С. Боровский // Экономика региона. — 2018. — Т. 14, вып. 4. — С. 1221-1231

67. Леус А. В. Оценка эффективности систем безопасности с помощью моделирования перемещения субъектов движения по охраняемому объекту: автореф. дис. … канд. техн. наук/ А.В. Леус. - Москва. - 2012 г. - 22 с.

68. Леус А. В. Математическая модель оценки эффективности систем физической защиты/ А.В. Леус // T-Comm - Телекоммуникации и Транспорт. 2010. №6. С. 46-49.

69. Бояринцев, А. В. Проблемы антитерроризма: Категорирование и анализ уязвимости объектов / А. В. Бояринцев, А. Н. Бражник, А. Г. Зуев. – Санкт-Петербург: ИСТА-Системс, 2006. – 252 с.

70. Интеллектуализация принятия решений в системах физической защиты объектов/ С. С. Звежинский, А. Е. Духан, Е. И. Духан, И. В. Парфенцев// T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 1. С. 40-43. DOI 10.24411/2072-8735-2018-10008.

71. Звежинский С., Козлов С.. Львов Д. Что остановит подготовленного нарушителя? Технические, финансовые и психологические барьеры/ С. Звежинский, С. Козлов, Д. Львов// Системы безопасности. – 2018. - №4. – URL: http://lib.secuteck.ru/articles2/kompleks_sys_sec/chto-ostanovit-podgotovlennogo-narushitelyatehnicheskie--finansovye-i-psihologicheskie-barery . - 15.04.2025

72. Звежинский С.С. Особенности организации охраны периметра крупных городских объектов 2019 г/ С.С. Звежинсткий [Электронный ресурс].: статья// Интернет-магазин Актив-СБ. 2004-2025 - URL: https://www.aktivsb.ru/statii/osobennosti_organizatsii_okhrany_perimetra_krupnykh_gorodskikh_obektov.html. – 16.04.2025

73. Волхонский В.В. Основные положения концепции обеспечения безопасности объектов/ В.В. Волхонский// Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. - № 3 (73) - С.116-121

74. Воробьев П.А. Модель и метод анализа вероятности обнаружения нарушителя пассивными инфракрасными извещателями систем физической

защиты объектов информатизации: автореф. дис. … канд. техн. наук/ П.А. Воробьев–Санкт-Петербург, 2015 г. – 19 с.

75. Воловач В.И. Развитие теории, принципов построения и средств реализации эффективных радиотехничесих систем обнаружения и контроля протяженных объектов: автореф. дис. … канд. техн. наук/ В.И. Воловач - Самара 2015 - 18 с.

76. Трапш Р.Р. Разработка методов повышения эффективности средств обнаружения нарушителя в системах физической защиты объектов информатизации автореф. дис. … канд. техн. наук/ Р.Р. Трапп – Санкт-Петербург, 2014 г. – 18 с.

77. Панин, О. Категорирование объектов для создания эффективных систем физической защиты/ О. Панин // Безопасность. Достоверность. Информация. – 2007. – № 70. – С. 20-24. – EDN JVRZPH.]

78. Быстров С.Ю. Анализ и оптимизация систем физической защиты особо важных объектов: автореф. дис. … канд. техн. наук/ С.Ю. Быстров – Пенза, 2004 г. – 24 с.

79. Олейник А. С. Методы оценки эффективности защиты критически важных объектов// Вестник Московского университета МВД России. 2017. № 4. – С. 280-286.

80. Олейник А.С. Совершенствование управления системой физической защиты важных государственных объектов на основе применения математических моделей: автореф. дис. … канд. техн. наук/ А.С. Олейник –Москва, 2012 г. – 24 с.

81. Беседин И.И. Математическое моделирование и синтез комплекса инженерно-технических средств системы физической защиты промышленного объекта: автореф. дис. … канд. техн. наук/ ИИ. Беседин. – Брянск, 2013. -20 с.

82. Тарасов А.Д. Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: автореф. дис. … канд. техн. наук/.А.Д. Тарасов -Уфа, 2017. - 18 с.

83. Гайнулин Т.Р. Моделирование процесса выбора состава технических средств системы физической защиты: автореф. дис. … канд. техн. наук/. - Брянск. - 2008. - 19 с.

84. Востокова О.В. Модели и методы оценки пожарно-охранной системы безопасности учреждений культуры (на примере Федерального государственного учреждения культуры «Русский музей»): автореф. дис. … канд. техн. наук/ О.В. Востокова - Санкт- Петербург. - 2011. - 22 с.

85. Белов С.В. Автоматизированная система анализа физической защищенности объектов обработки информации: автореф. дис. … канд. техн. наук/.С.В. Белов - Астрахань. - 2005 г. - 24 с.

86. Магауенов Р.Г. Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь/ Р.Г. Магауенов – М.: Горячая линия – Телеком, 2007. – 97 с.

87. Шнякина Е. А. Принятие управляющих решений по структурным изменениям системы физической защиты объекта для повышения её эффективности/ Е.А. Шнякина, В.Н. Костин// Информационные технологии. – 2022. – Том 28. - №11. – С. 607-615. - DOI: 10.17587/it.28.607-615. - EDN: LLIZUJ

88. Никитин, В.В. Телевидение в системах физической защиты: учеб. пособие /.В. Никитин, А.К. Цыпулин. – СПб: СПбГЭТУ «ЛЭТИ», 2001. – 132

89. ГОСТ Р 78.36.032-2013 Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1. Методические рекомендации" [Электронный ресурс].: утв. МВД России 11.12.2013// Юридическая информационная система "Легалакт - законы, кодексы и нормативно-правовые акты Российской Федерации" - ООО "Инфра-Бит", г. Москва – URL: https://legalacts.ru/doc/r-7836032-2013-inzhenerno-tekhnicheskaja-ukreplennost-i-osnashchenie-tekhnicheskimi/

90. О классификации чрезвычайных ситуаций природного и техногенного характера [Электронный ресурс].: изменения и поправки от 20 декабря 2019 г. № 1743 к Постановлению Правительства РФ от 21 мая 2007№304// Система ГАРАНТ. Энциклопедия Российского законодательства - URL: https://base.garant.ru/73324523/#block_1003. – 15.10.2024

91. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций и формы паспорта безопасности этих объектов (территорий) [Электронный ресурс].: Постановление Правительства РФ № 875 от 29.08.2014// Официальное опубликование правовых актов. - 03.09.2014. - URL: http://publication.pravo.gov.ru/Document/View/0001201409030012. – 15.10.2024

92. Об утверждении Правил разработки критериев отнесения объектов всех форм собственности к потенциально опасным объектам [Электронный ресурс].: Постановление Правительства РФ от 14 августа 2020 г. № 1226// МЧС России– URL: https://mchs.gov.ru/uploads/document/2023-02-13/1b80f0f7a7935e7e5a5bf3d6e8be7a88.pdf.- 1.02.2024

93. Об утверждении Правил разработки критериев отнесения объектов всех форм собственности к критически важным объектам [Электронный ресурс].: Постановление Правительства РФ от 14 августа 2020 г. № 1225// Система Гарант – URL: http://ivo.garant.ru/#/document/74523898/paragraph/1:0. - 1.02.2024

94. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций и формы паспорта безопасности этих объектов (территорий) [Электронный ресурс].: Постановление Правительства РФ от 29.08.2014 №

875// – URL: https://rossafety.ru/media/uploads/law/postanovlenie-pravitelstva-875.pdf. - 1.02.2024

95. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера [Электронный ресурс].: Федеральный закон от 21.12.1994 г. № 68-ФЗ, последняя редакция от 14.04.2023 № 131-ФЗ // Президент России. - URL: http://www.kremlin.ru/acts/bank/7352. - 3.08.2022

96. ГОСТ Р 22.0.02-2016 Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий. Государственный стандарт РФ. Введ. 12.09.2016 – М.: Стандартинформ, 2016. – 7 с.

97. Назаренко, Е. К. К вопросу о трактовке термина "критически важный объект" / Е. К. Назаренко // Проблемы безопасности и чрезвычайных ситуаций. – 2021. – № 5. – С. 5-10. – DOI 10.36535/0869-4179-2021-05-1. – EDN PEWQZE.

98. Ранжирование критически важных объектов и объектов критической информационной инфраструктуры системы связи / О. М. Лепешкин, О. А. Остроумов, М. В. Митрофанов, А. Д. Синюк // Нейрокомпьютеры и их применение: XIX Всероссийская научная конференция: тезисы докладов, Москва, 30 марта 2021 года. – Москва: Московский государственный психолого-педагогический университет, 2021. – С. 237-239. – EDN JYFYAA.

99. Оленин Ю.А., Алаухов С.Ф. К вопросу категорирования объектов с позиции охранной безопасности/ Ю.А Оленин, С.Ф. Алаухов// Системы безопасности, связи и телекоммуникаций, - 1999. - № 30, - С. 26.

100. Панин, О. Категорирование объектов для создания эффективных систем физической защиты/ О. Панин // Безопасность. Достоверность. Информация. – 2007. – № 70. – С. 20-24. – EDN JVRZPH.

101. Глебов, В. Ю. К проблеме разработки критериев отнесения объектов всех форм собственности к критически важным объектам и их категорированию/ В. Ю. Глебов // Проблемы безопасности и чрезвычайных ситуаций. – 2021. – № 5. – С. 45-49. – DOI 10.36535/0869-4179-2021-05-6. – EDN JOLEDA.

102. Об утверждении Правил разработки обязательных для выполнения требований к критически важным объектам в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера [Электронный ресурс].: Постановление Правительства Российской Федерации от 11 сентября 2021 г. № 1537// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/608609335. – 1.02.2024

103. О классификации чрезвычайных ситуаций природного и техногенного характера [Электронный ресурс].: Постановление Правительства Российской Федерации от 21 мая 2007 №304// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/902043525. - 1.02.2024

104. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [Электронный ресурс].: Постановление Правительства Российской Федерации от 8 февраля 2018 года №127// Правительство РФ, 2025. - URL: http://static.government.ru/media/files/uPA03V4BfqknJWNExcfX3gSlDZi4zuas.pdf. - 1.02.2024

105. Шнякина Е. А. К вопросу о трактовке термина «категорирование охраняемого объекта/ Е.А. Шнякина// Актуальные проблемы науки и образования в условиях современных вызовов: мат. XXX Междунар. науч.-практ. конф. - 2024. - С. 20-27. - doi: 10.62994/7858.2024.11.71.050.

106. Андреев Г.И. Методология моделирования сложных технических систем. Основа системных исследований/ Г.И. Андреев, П.А. Созинов, В.А. Тихомиров. - Москва: Радиотехника; 2020. 512 с.

107. Андреев Г.И.. Основы теории принятия решений/ Г.И. Андреев, П.А. Созинов, В.А. Тихомиров. - Москва: Радиотехника; 2017: 648 с.

108. Тихомиров, В. А. Принципы конструирования информационно-вероятностного метода осуществления долгосрочного прогноза/ В. А. Тихомиров, В. А. Тихомиров, А. В. Макушкин// Программные продукты и системы. – 2004. – № 2. – С. 2. – EDN IYPYLR.

109. Факторный, дискриминантный и кластерный анализ/ Дж.-О. Ким, Ч. У. Мьюллер, У.Р. Клекка и др.; под ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.

110. Программное средство классификации объектов: свидетельство о гос. регистрации программы для ЭВМ 2024667798/ О.А. Капустина, Е. А. Шнякина, В.А. Мироненко, В.Н. Костин; правообладатель Оренбург. Федеральный исслед. центр УОРАН.- № 2024666167 заявл. 09.07.2024 опубл. 30.07.2024, 2024. - 1 с. - EDN: PRISCL

111. Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов [Электронный ресурс].: Постановлении Правительства РФ от 19.07.2007 № 456 (ред. от 28.08.2012)// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/902053152.- 08.05.2025

112. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций и формы паспорта безопасности этих объектов (территорий) [Электронный ресурс].: постановление Правительства РФ от 29 авг. 2014 г. № 875// Гарант.ру : информ.-правовое обеспечение. - 1990-2025. – URL: https://base.garant.ru/70731274/. - 08.05.2025.

113. РД 78.36.003-2002. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по

защите объектов от преступных посягательств" [Электронный ресурс].: утв. МВД РФ 06.11.2002// Охрана труда в России. – Москва, 2001-2025. - URL: https://ohranatruda.ru/upload/iblock/710/4294816400.pdf. - 08.05.2025.

114. ГОСТ Р 53195.1-2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем [Электронный ресурс].: Национальный стандарт РФ от 01.01.2010// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/1200071028 - 08.05.2025.

115. Петров Н. В. Задачи построения систем физической защиты. Оценка эффективности СФЗ/ Н. В. Петров, С. Б. Титков// Защита информации. Инсайд. – 2006. – № 1(7). – С. 58-67. – EDN TRMPPV.

116. Олейник А. С. Определение и ранжирование целей нарушителя при нападении на важный государственный объект/ А. С. Олейник // Инженерный вестник Дона. – 2023. – № 5(101). – С. 185-193. – EDN VDXYEU.

117. Шепитько Г. Е. Идентификация угроз безопасности объектов от внутренних нарушителей/ Г. Е. Шепитько// Технологии техносферной безопасности. – 2010. – № 5(33). – С. 111-115. – EDN NTEXDH.

118. Мальцев А. Подход к обоснованию вероятностных характеристик периметральных средств обнаружения/ А. Мальцев// Технологии защиты. - 2015. - № 5. - URL: http://www.tzmagazine.ru/jpage.php?uid1=1348&uid2=1450&uid3=1461. - 10.04.2025

119. Шнякина Е. А. Модель нарушителя/ Е.А. Шнякина //Проблемы техники и технологий телекоммуникаций ПТиТТ-2024: XXVI Международная научно-техническая конференция, VII Научный форум «Телекоммуникации: теория и технологии ТТТ-2024», Самара, 06–08 ноября 2024 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2024. - С. 426-427

120. Шнякина Е. А. Разработка алгоритмического обеспечения принятия решений по идентификации типовых нарушителей категорируемых объектов/ Е. А. Шнякина, В. Н. Костин // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2023. – № 3(67). – С. 72-82. – DOI 10.21685/2072-3059-2023-3-5. – EDN YDSNAN.

121. Шнякина Е.А., Костин В.Н. Оценка вероятности обнаружения нарушителя в зависимости от его модели// Научно-технический вестник Поволжья. – 2025. - № 7. - С. 206-208.

122. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие/ Р.Г. Магауенов – М.: Горячая линия. –Телеком, 2004. – 367 с.

123. Журин С. Сертификация наполовину Кто гарантирует обнаружение подготовленного нарушителя?/ С. Журин// Безопасность. Достоверность. Информация. – 2005. – № 60. – С. 32-36.

124. Обоймов А.С. Оценка эффективности систем физической защиты. Обнаружение наиболее вероятных и опасных сценариев атак на СФЗ/ А.С. Обоймов// Успехи современной науки. – 2016. – Т.8. - №12. - С. – 52-58

125. Герлинг Е. Ю., Ахрамеева К.А. Формирование моделей нарушителей систем контроля и управления доступом на объекте/ Е. Ю. Герлинг, К. А. Ахрамеева// Инновационные технологии и вопросы обеспечения безопасности реальной экономики: сборник научных трудов по итогам Всероссийской научно-практической конференции, Санкт-Петербург, 27 марта 2020 года/ Под редакцией Г.В. Лепеша, О.Д. Угольниковой, С.Ю. Александровой. – СПб: Санкт-Петербургский государственный экономический университет, 2020. – С. 58-65.

126. Олейник А. С. Формирование модели нарушителя при нападении на важный государственный объект/ А. С. Олейник // Инженерный вестник Дона. – 2023. – № 6(102). – С. 691-704.

127. Гмурман В.Е. Теория вероятностей и математическая статистика: учебное пособие для вузов./ В.Е. Гмкрман – М.: Высш.шк., 1999. – 479 с.

128. Костин В.Н. Методика формирования требований к системе физической защиты на основе концептуальной имитационной модели/ В.Н. Костин, С.Н. Шевченко// Инфокоммуникационные технологии. – 2013. – Т.12. - №2. – С. 91- 98.

129. Костин В.Н. Статистические методы и модели: учебное пособие/ В.Н. Костин, Н.А. Тишина – Оренбург: ИПК ГОУ ОГУ, 2004. – 138 с.

130. Шнякина Е.А. Имитационная модель оценки эффективности систем физической защиты объектов// Автоматизация. Современные технологии. – 2023.- Т.77. - №6. С. 263-268. - DOI: 10.36652/0869-4931-2023-77-6-263-268. - EDN: LVJLXB

131. Имитационная модель функционирования системы физической защиты объекта: свидетельство о гос. регистрации программы для ЭВМ 2022684010/ Е. А. Шнякина, М. А. Школин, А. Д. Попов; правообладатель Оренбург. гос. ун-т.- № 2022683828 заявл. 07.12.2022 опубл. 09.12.2022, 2022. - 1 с. - EDN: RWUCIS.

132. Ильин В.А. Метод проверки тренажерных моделей на адекватность/ В.А. Ильин, Н.П. Кирюшов // Программные продукты и системы. - 2021. - Т. 34. - № 1. - С. 061–066. DOI: 10.15827/0236-235X.133.061-066.

133. Шнякина Е. А. Методика принятия эффективных управленческих решений по обеспечению физической безопасности критически важных объектов/ Е. А. Шнякина, В. Н. Костин/ Вестник компьютерных и информационных технологий. – 2023. – Т. 20, № 10 (232). – С. 46-55. – DOI 10.14489/vkit.2023.10.pp.046-055. – EDN JMLFKS.

134. Бабиков В.Г. Защита объектов нефнятной промышленности. Справочное пособие/ В.Г. Бабиков – М.: НОУ ШО «Барс», 2005 г. – 512 с.

135. Многомерный статистический анализ в экономике/ Л.А. Сошникова, В.Н. Тамашевич, Г. Уебе, М. Шефер – М.: ЮНИТИ-ДАНА, 1999. – 598 с.

136. Шнякина Е.А. Исследование эффективности системы физической защиты критически важных объектов/ Е.А. Шнякина, В.Н. Костин// Приоритетные направления развития науки и технологий: доклады XXXII шмеждународной научно-практической конференции, Тула, 15 марта 2023 года/ под общ. ред. В.М. Панарина. – Тула: Инновационные технологии, 2023, С. 103-107, EDN ANHYHY

137. Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы [Электронный ресурс].: Приказ Минюста России от 04.09.2006 № 279 (ред. от 17.06.2013)// Электронный фонд правовых и нормативно-технических документов АО «Кодекс», 2025. - URL: https://docs.cntd.ru/document/456017757. – 18.05.2025

138. Архиреев А.В. Генезис понятия эффективности. Структура, состояние, оценка/ А.В. Архиреев// Контекст и рефлексия: философия о мире и человеке. 2023. Том 12. № 10А. С. 36-49. DOI: 10.34670/AR.2024.43.45.004

Приложение А

(*обязательное*)

Свидетельства о государственной регистрации программ на ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024667798

Программное средство классификации объектов

Правообладатели: ***Федеральное государственное бюджетное учреждение науки Оренбургский федеральный исследовательский центр Уральского отделения Российской академии наук (RU), Общество с ограниченной ответственностью «Научно-производственное предприятие «ЭКОТЕХНОЛОГИИ» (RU)***

Авторы: ***Капустина Оксана Александровна (RU), Шнякина Елена Александровна (RU), Мироненко Владимир Андреевич (RU), Костин Владимир Николаевич (RU)***

Заявка № **2024666167**

Дата поступления **09 июля 2024 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***30 июля 2024 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022684010

Имитационная модель функционирования системы физической защиты объекта

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» (RU)***

Авторы: ***Шнякина Елена Александровна (RU), Школин Максим Аркадьевич (RU), Попов Алексей Дмитриевич (RU)***

Заявка № **2022683828**

Дата поступления **07 декабря 2022 г.**

Дата государственной регистрации

в Реестре программ для ЭВМ ***09 декабря 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Ю.С. Зубов

Приложение Б

(*обязательное*)

Акты о внедрении результатов исследования

УТВЕРЖДАЮ
Заместитель начальника
испытательного полигона (пос. Первомайский)
3 «Центрального научно-исследовательского
института» Минобороны России по научно-
исследовательской и испытательной работе
кандидат технических наук

О.Бобков

«25» 08 2025 г.

Акт реализации

Мы нижеподписавшиеся представители ИП (пос. Первомайский) 3 «ЦНИИ» Минобороны России, начальник 7 отдела научно-исследовательского испытательного к.т.н. Серегин А.М. и старший научный сотрудник 7 отдела научно-исследовательского испытательного Сергеев С.В., составили настоящий акт о том, что: имитационная модель оценки эффективности систем физической защиты и методика принятия решения по повышению эффективности систем физической защиты, разработанные в ходе выполнения диссертационной работы Шнякиной Еленой Александровной на тему «Методика принятия решения по обеспечению требуемой эффективности систем физической защиты на основе многомерных статистических методов», были использованы при проведении оценки эффективности имеющихся систем физической защиты охраняемых объектов, разработке технического задания на проектировку перспективных систем физической защиты и выработке оптимальных управленческих решений по повышению эффективности систем физической защиты.

Начальник 7 отдела НИИ
кандидат технических наук
А.Серегин

Старший научный сотрудник 7 отдела НИИ
С.Сергеев

ОРЕНБУРГСКОЕ РЕГИОНАЛЬНОЕ ОТДЕЛЕНИЕ
ОБЩЕРОССИЙСКОЙ ОБЩЕСТВЕННОЙ ОРГАНИЗАЦИИ
«РОССИЙСКОЕ НАУЧНОЕ ОБЩЕСТВО АНАЛИЗА РИСКА»

460021, г. Оренбург, ул. Луговая, д. 78 а; тел.: (3532) 770660

УТВЕРЖДАЮ
Председатель правления ОРО ООО «Российское научное общество анализа риска», к.т.н., доцент
О.А. Капустина
«29» августа 2025 г.

АКТ

о рассмотрении результатов диссертационной работы «Методика принятия решений по обеспечению требуемой эффективности систем физической защиты на основе многомерных статистических методов» Шнякиной Елены Александровны на соискание ученой степени кандидата технических наук

Комиссия в составе председателя правления ОРО ООО «Российское научное общество анализа риска» О.А. Капустиной, и членов комиссии М.Ю. Нестеренко и В.Д. Павлидис, рассмотрела вопрос об использовании результатов диссертационной работы и установила следующее.

Разработанная в рамках диссертационного исследования имитационная модель оценки эффективности функционирования системы физической защиты, внедрена и используется специалистами ОРО ООО «Российское научное общество анализа риска» для повышения достоверности результатов оценки риска критически важных объектов, рассчитанных по существующим классическим методам и методикам.

Члены комиссии:
д-р геол.-минерал. наук,
канд. техн. наук, доцент М.Ю. Нестеренко

д-р пед. наук,
канд. физ.-мат. наук, профессор В.Д. Павлидис

УТВЕРЖДАЮ
Проректор по научной работе
ФГБОУ ВО «Оренбургский
государственный университет»,
д-р физ.-мат. наук, профессор

_____ С.Н. Летута
«02» 09 2025

АКТ
внедрения результатов диссертационной работы
«Методика принятия решений по обеспечению требуемой эффективности систем физической защиты на основе многомерных статистических методов» Шнякиной Елены Александровны на соискание ученой степени кандидата технических наук

Мы, нижеподписавшиеся, заведующий кафедрой вычислительной техники и защиты информации, доктор технических наук, доцент Тугов Виталий Валерьевич, и доцент кафедры вычислительной техники и защиты информации, кандидат технических наук, доцент Галимов Ринат Равилевич, настоящим актом подтверждаем, что результаты диссертационной работы Шнякиной Е.А. используются в учебном процессе ФГБОУ ВО «Оренбургский государственный университет».

Результаты научных исследований, полученных Шнякиной Е.А., используются преподавателями кафедры вычислительной техники и защиты информации при ведении занятий по дисциплинам образовательной программы направления подготовки 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации»: «Системы охранной и пожарной сигнализации», «Защита и обработка конфиденциальных документов».

Успешный опыт использования результатов диссертационного исследования, проведенного Шнякиной Е.А. в учебном процессе ФГБОУ ВО «Оренбургский государственный университет» подтверждает практическую значимость результатов её научных исследований.

Заведующий кафедрой
вычислительной техники
и защиты информации,
д-р техн. наук, доцент В.В. Тугов

доцент кафедры
вычислительной техники
и защиты информации,
канд. техн. наук, доцент Р.Р. Галимов

Приложение В

Листинг программы «Имитационная модель функционирования системы физической защиты объекта»

```
public class RouteViewModel : INotifyPropertyChanged
  {
    public class DataSet : INotifyPropertyChanged
    {
      private ObservableCollection<Route> _routes;
      public ObservableCollection<Route> routes
      {
        get { return _routes; }
        set { _routes = value; OnPropertyChanged("routes"); }
      }
      private double _ReactionTime;
      public double ReactionTime
      {
        get { return _ReactionTime; }
        set { _ReactionTime = value; OnPropertyChanged("ReactionTime"); }
      }
      private int _Sigma;
      public int Sigma
      {
        get { return _Sigma; }
        set { _Sigma = value; OnPropertyChanged("Sigma"); }
      }
      private double _Answer;
      public double Answer
      {
        get { return _Answer; }
```

```
        set { _Answer = value; OnPropertyChanged("Answer"); }
    }
    public event PropertyChangedEventHandler PropertyChanged;
    public void OnPropertyChanged([CallerMemberName] string prop = "")
    {
        if (PropertyChanged != null)
            PropertyChanged(this, new PropertyChangedEventArgs(prop));
    }
}
private int testCount = 1000;
private double detectionTimeLimit = 12;
private ObservableCollection<DataSet> _dataSets;
public ObservableCollection<DataSet> dataSets
{
    get { return _dataSets; }
    set
    {
        _dataSets = value;
        OnPropertyChanged("dataSets");
    }
}
private int _AddingCount;
public int AddingCount
{
    get { return _AddingCount; }
    set { _AddingCount = value; OnPropertyChanged("AddingCount"); }
}
private DataSet _SelectedDataSet;
public DataSet SelectedDataSet
{
```

```
    get { return _SelectedDataSet; }
    set
    {
        _SelectedDataSet = value;
        OnPropertyChanged("SelectedDataSet");
    }
}
#region examples
private RelayCommand _ExampleP05Command;
public RelayCommand ExampleP05Command
{
    get
    {
        return _ExampleP05Command ??
          (_ExampleP05Command = new RelayCommand(obj =>
          {
              DataSet dataset = new DataSet();
              dataset.routes = new ObservableCollection<Route>();
              dataset.Answer = 0;
              for (int i = 0; i < 4; i++)
              {
                  Route route = new Route();
                  route.Id = i + 1;
                  route.P = 0.5;
                  dataset.Sigma = 10;
                  route.SigmaIntruder = 2;
                  route.T = 100;
                  route.deltaT = 12;
                  //route.ReactionTime = 408 - 100 * i;
                  dataset.ReactionTime = 400;
```

```
                dataset.routes.Add(route);
            }
            dataSets.Add(dataset);
            SelectedDataSet = dataset;
            CalculateCurrentCommand.Execute(obj);
            SelectedDataSet = null;
        }));
    }
}
private RelayCommand _ExampleP075Command;
public RelayCommand ExampleP075Command
{
    get
    {
        return _ExampleP075Command ??
         (_ExampleP075Command = new RelayCommand(obj =>
         {
            DataSet dataset = new DataSet();
            dataset.routes = new ObservableCollection<Route>();
            dataset.Answer = 0;
            for (int i = 0; i < 2; i++)
            {
                Route route = new Route();
                route.Id = i + 1;
                route.P = 0.5;
                dataset.Sigma = 20;
                route.SigmaIntruder = 20;
                route.T = 1000;
                route.deltaT = 12;
                //route.ReactionT = 200;
```

```
                dataset.ReactionTime = 200;
                dataset.routes.Add(route);
            }
            dataSets.Add(dataset);
            SelectedDataSet = dataset;
            CalculateCurrentCommand.Execute(obj);
            SelectedDataSet = null;
        }));
    }
}
private RelayCommand _ExampleP0Command;
public RelayCommand ExampleP0Command
{
    get
    {
        return _ExampleP0Command ??
          (_ExampleP0Command = new RelayCommand(obj =>
          {
            DataSet dataset = new DataSet();
            dataset.routes = new ObservableCollection<Route>();
            dataset.Answer = 0;
            for (int i = 0; i < 2; i++)
            {
                Route route = new Route();
                route.Id = i + 1;
                route.P = 0.5 + 0.1*i;
                dataset.Sigma = 20;
                route.SigmaIntruder = 10;
                route.T = 200;
                // route.ReactionT = 1000;
```

```
                route.deltaT = 12;
                dataset.ReactionTime = 1000;
                dataset.routes.Add(route);
            }
            dataSets.Add(dataset);
            SelectedDataSet = dataset;
            CalculateCurrentCommand.Execute(obj);
            SelectedDataSet = null;
        }));
    }
}
private RelayCommand _ExampleP1Command;
public RelayCommand ExampleP1Command
{
    get
    {
        return _ExampleP1Command ??
         (_ExampleP1Command = new RelayCommand(obj =>
         {
            DataSet dataset = new DataSet();
            dataset.routes = new ObservableCollection<Route>();
            dataset.Answer = 0;
            for (int i = 0; i < 2; i++)
            {
                Route route = new Route();
                route.Id = i + 1;
                route.P = 1;
                dataset.Sigma = 20;
                route.SigmaIntruder = 10;
                route.T = 1000;
```

```
                route.deltaT = 12;
                //route.ReactionT = 200;
                dataset.ReactionTime = 200;
                dataset.routes.Add(route);
            }
            dataSets.Add(dataset);
            SelectedDataSet = dataset;
            CalculateCurrentCommand.Execute(obj);
            SelectedDataSet = null;
        }));
    }
}
#endregion
private RelayCommand addCommand;
public RelayCommand AddCommand
{
    get
    {
        return addCommand ??
          (addCommand = new RelayCommand(obj =>
          {
              if (AddingCount > 0 && AddingCount < 5)
              {
                  DataSet dataset = new DataSet();
                  dataset.routes = new ObservableCollection<Route>();
                  dataset.Answer = 0;
                  for (int i = 0; i < AddingCount; i++)
                  {
                      Route route = new Route();
                      route.Id = i + 1;
```

```
                    route.deltaT = 12;
                    dataset.routes.Add(route);
                }
                dataSets.Add(dataset);
            }
            else MessageBox.Show("Введите число от 1 до 4", "Внимание");
        }));
    }
}
private RelayCommand removeCommand;
public RelayCommand RemoveCommand
{
    get
    {
        return removeCommand ??
          (removeCommand = new RelayCommand(obj =>
          {
            if (SelectedDataSet != null)
                dataSets.Remove(SelectedDataSet);
            else MessageBox.Show("Сначала выберите эксперимент для удаления!",
"Внимание");
        }));
    }
}
private RelayCommand removeAllCommand;
public RelayCommand RemoveAllCommand
{
    get
    {
        return removeAllCommand ??
          (removeAllCommand = new RelayCommand(obj =>
```

```
            {
                if (dataSets != null && dataSets.Count > 0)
                    dataSets.Clear();
                else MessageBox.Show("Экспериментов нет!", "Внимание");
            }));
        }
    }
    private RelayCommand calculateAllCommand;
    public RelayCommand CalculateAllCommand
    {
        get
        {
            return calculateAllCommand ??
              (calculateAllCommand = new RelayCommand(obj =>
              {
                  if (dataSets.Count > 0)
                  {
                      try
                      {
                          foreach (var dataSet in dataSets) {
                              SelectedDataSet = dataSet;
                              calculateCurrentCommand.Execute(dataSet);
                              }
                          SelectedDataSet = null;
                      }
                      catch
                      {
                          MessageBox.Show("Заполните все поля в экспериментах и проверьте данные на корректность ввода!", "Ошибка");
                      }
                  }
```

```
            else MessageBox.Show("Сначала создайте эксперимент!", "Внимание");
        }));
    }
}
private RelayCommand calculateCurrentCommand;
public RelayCommand CalculateCurrentCommand
{
    get
    {
        return calculateCurrentCommand ??
         (calculateCurrentCommand = new RelayCommand(obj =>
         {
            if (SelectedDataSet != null)
            {
               bool check = true;
               foreach (var item in SelectedDataSet.routes)
               {
                  if (item.P < 0 || item.P > 1)
                  {
                     MessageBox.Show("Вероятность должна быть в пределах от 0 до 1");
                     check = true;
                     break;
                  }
               }
               if (check)
               {
                  Random random = new Random();
                  ///10000
                  double AnswerBuf = 0;
                  for (int count = 0; count < testCount; count++)
```

```
                {
                    double intruderTime = 0;
                    for (int i = 0; i < SelectedDataSet.routes.Count; i++)
                    {
                        double randP = random.NextDouble();
                        if (SelectedDataSet.routes[i].P > randP)
                        {
                            var normalRnd = new NormalRaspred(SelectedDataSet.Sigma, false);
                            double IntruderSumT = 0;
                            for (int j = i; j < SelectedDataSet.routes.Count; j++)
                            {
                                var normalRndIntruder = new
NormalRaspred(SelectedDataSet.routes[i].SigmaIntruder, false);
                                IntruderSumT += SelectedDataSet.routes[j].T +
normalRndIntruder.GetNext();
                            }
                            var normalRndDetection = new
NormalRaspred(Convert.ToInt32(detectionTimeLimit), true);
                            double detectionTime =
GetExponentValue(SelectedDataSet.routes[i].P, SelectedDataSet.routes[i].deltaT);
                            double ReactionTimeSum = detectionTime +
                                                //SelectedDataSet.routes[i].ReactionT + //Старое
говно
                                                SelectedDataSet.ReactionTime +
                                                normalRnd.GetNext();
                            if (ReactionTimeSum < IntruderSumT)
                                AnswerBuf++;
                            break;
                        }
                    }
                    SelectedDataSet.Answer = Math.Round(AnswerBuf / testCount, 4);
                }
```

```
                }
            }
            else MessageBox.Show("Сначала выберите эксперимент!", "Внимание");
        }));
    }
  }
  private double GetExponentValue(double Po, double deltaT)
    => (Math.Log(1.0d - NextDoubleRnd()) / Math.Log(1.0d - Po)) * deltaT;
  private double NextDoubleRnd()
    => new Random().NextDouble();
  public RouteViewModel()
  {
    dataSets = new ObservableCollection<DataSet>();
    AddingCount = 2;
  }
  public event PropertyChangedEventHandler PropertyChanged;
  public void OnPropertyChanged([CallerMemberName] string prop = "")
  {
    if (PropertyChanged != null)
      PropertyChanged(this, new PropertyChangedEventArgs(prop));
  }
}
public class Route : INotifyPropertyChanged
{
  public int Id { get; set; }
  private double _P;
  public double P
  {
    get { return _P; }
    set
```

```
    {
        _P = value;
        OnPropertyChanged("P");
    }
}
private double _T;
public double T
{
    get { return _T; }
    set
    {
        _T = value;
        OnPropertyChanged("T");
    }
}
private double _deltaT;
public double deltaT
{
    get { return _deltaT; }
    set
    {
        _deltaT = value;
        OnPropertyChanged("deltaT");
    }
}
private int _SigmaIntruder;
public int SigmaIntruder
{
    get { return _SigmaIntruder; }
    set
```

```
            {
                _SigmaIntruder = value;
                OnPropertyChanged("SigmaIntruder");
            }
        }
        public event PropertyChangedEventHandler PropertyChanged;
        public void OnPropertyChanged([CallerMemberName] string prop = "")
        {
            if (PropertyChanged != null)
                PropertyChanged(this, new PropertyChangedEventArgs(prop));
        }
    }
}
public class DotConverter : IValueConverter
    {
        public object Convert(object value, Type targetType, object parameter, CultureInfo culture)
        {
            try
            {
                if (System.Convert.ToDouble(value) < 0)
                {
                    value = 0;
                    return value;
                }
                if (System.Convert.ToDouble(value) > 1)
                {
                    value = 1;
                    return value;
                }
            }
```

```
            catch { }
            return value.ToString().Replace(",", ".");
        }
        public object ConvertBack(object value, Type targetType, object parameter, CultureInfo
culture)
        {
            try
            {
                if (System.Convert.ToDouble(value) < 0)
                {
                    value = 0;
                    return value;
                }
                if (System.Convert.ToDouble(value) > 1)
                {
                    value = 1;
                    return value;
                }
            }
            catch { }
            return value.ToString().Replace(",", ".");
        }
    }
    public class DotConverterSimple : IValueConverter
    {
        public object Convert(object value, Type targetType, object parameter, CultureInfo culture)
        {
            try
            {
                if (System.Convert.ToDouble(value) < 0)
                {
```

```
                value = 0;
                return value;
            }
        }
        catch { }
        return value.ToString().Replace(",", ".");
    }
    public object ConvertBack(object value, Type targetType, object parameter, CultureInfo
culture)
    {
        try
        {
            if (System.Convert.ToDouble(value) < 0)
            {
                value = 0;
                return value;
            }
        }
        catch { }
        return value.ToString().Replace(",", ".");
    }
}
public class NormalRaspred
{
    private List<int> _numbers;
    private int _current = 0;
    public int GetNext()
    {
        if (_numbers.Count == 1) return 0;
        var num = _numbers[_current];
        _current++;
```

```
            if(_current >= _numbers.Count)
                _current = 0;
            return num;
        }
        /// <param name="sigma">Сигма</param>
        /// <param name="isPositive">Только положительные</param>
        public NormalRaspred(int sigma, bool isPositive)
        {
            if (isPositive)
            {
                _numbers = new List<int>(sigma );
                for (int n = 1; n <= sigma; n++)
                    _numbers.Add(n);
            }
            else
            {
                _numbers = new List<int>(sigma * 2);
                for (int n = -sigma; n <= sigma; n++)
                    _numbers.Add(n);
            }
        }
    }
public class RelayCommand : ICommand
    {
        private Action<object> execute;
        private Func<object, bool> canExecute;
        public event EventHandler CanExecuteChanged
        {
            add { CommandManager.RequerySuggested += value; }
            remove { CommandManager.RequerySuggested -= value; }
```

```
    }
    public RelayCommand(Action<object> execute, Func<object, bool> canExecute = null)
    {
        this.execute = execute;
        this.canExecute = canExecute;
    }
    public bool CanExecute(object parameter)
    {
        return this.canExecute == null || this.canExecute(parameter);
    }
    public void Execute(object parameter)
    {
        this.execute(parameter);
    }
}
```