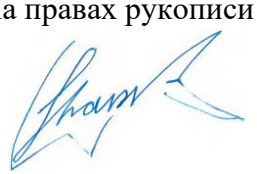
ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

На правах рукописи



Шарков Илья Кириллович

Методы оценки эффективности систем физической защиты объектов на основе агентного моделирования и гибридных автоматов

2.3.1. Системный анализ, управление и обработка информации, статистика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург
2025

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Научный руководитель: **Сениченков Юрий Борисович**
доктор технических наук, доцент

Официальные оппоненты: **Шорников Юрий Владимирович**
профессор, доктор технических наук, профессор кафедры автоматизированных систем управления ФГБОУ ВО «Новосибирский государственный технический университет», г.Новосибирск

Маликов Рамиль Фарукович
профессор, доктор физико-математических наук, руководитель научно-исследовательской лаборатории «Системного анализа математического и моделирования», профессор кафедры информационных технологий ФГБОУ ВО «Башкирский государственный педагогический университет им. М. Акмуллы», г. Уфа

Ведущая организация: Акционерное общество "Научно-производственное объединение "Импульс", г. Санкт-Петербург

Защита диссертации состоится «22» октября 2025 г. в 16 часов 00 минут на заседании диссертационного совета У.2.3.1.29 при Санкт-Петербургском политехническом университете Петра Великого по адресу: Россия, 195251, г. Санкт-Петербург, ул. Политехническая, дом 29, корпус 3, аудитория 506.

С диссертацией можно ознакомиться в библиотеке библиотеки Санкт-Петербургского политехнического университета Петра Великого, на сайте Электронной библиотеки СПбПУ по адресу: http://elib.spbstu.ru.

Автореферат разослан «___» _____ 2025 г.

Ученый секретарь диссертационного совета,
доцент, кандидат технических наук Сараджишвили Сергей Эрикович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Обеспечение физической безопасности на важных территориальных объектах – крайне важная задача, усложняющаяся с годами. Для её решения создаются и совершенствуются Системы Физической Защиты (СФЗ), позволяющие обеспечить заданный адекватный уровень безопасности. Это крайне сложные комплексные киберфизические системы, представленные наборами связанных подсистем инженерно-технических средств охраны, организационных мер защиты (правил) и автоматизированного и человеческого управления. Каждая из таких подсистем на территории может быть представлена комбинациями десятков или сотен технических устройств (видеокамеры, датчики, устройства оповещения и т.д.), связанными в единую управляемую сеть (автоматизированную и под ручным управлением), человеческими ресурсами (служба безопасности объекта с различными задачами и правилами функционирования для каждой единицы от операторов до групп реагирования), инженерными средствами обеспечения безопасности (ограждения и пр.).

Из всего этого комплекса многообразных мер и технических решений формируется уникальная СФЗ для каждого охраняемого объекта. Структура системы зависит от уникальных свойств, структуры, целей и задач защиты таких объектов: частный объект (банк, склад), гражданский аэропорт или сложный топливно-энергетический комплекс – все защищаются различными образами и от различных внешних и внутренних угроз со стороны нарушителей (люди, перебрасывание предмета, воздушные виды актов незаконного вмешательства и иные).

При разработке таких систем, как проектируемых, так и существующих, важную роль играет оценка их эффективности. Причем, как уже существующих (построенных) систем, так и планируемых (проектируемых) новых. Под эффективностью СФЗ подразумевается способность системы противостоять внешнему вмешательству, а её оценка эффективности должна формироваться в виде понятной количественной характеристики с высокой точностью.

Такие методики оценки эффективности важны в связи увеличением сложности систем защиты из-за появления новых видов угроз (в т.ч. усилением угроз терроризма) и появлением новых технологий обеспечения безопасности. Количество, сложность и разнообразие новых объектов физической безопасности также увеличивается. Интерес ученых и инженеров к проблеме оценки эффективности систем защиты критических объектов усилился после появления жестких требований к обеспечению физической защиты объектов ядерной промышленности в конце 20 века. Кроме того, тенденция подкрепляется формируемыми законодательными мерами в свете реакций на актуальные угрозы.

Степень разработанности темы исследования. Решению этих задач посвящены работы многих авторов: М. Гарсия, А.Д. Тарасов, З. Винтр, Х.А. Беннет., Дж. К. Мэттер, Г.В. Шанаев, А.В. Леус, А.С. Молосов, А.М. Омельянчук, В.Н. Костин, А.В. Бояринцев, А.С. Боровский, Г.А.

Попов, И.Н. Петров, В.И. Балута, И.В. Котенко, А. Н. Бражник, Б.П. Степанов, А.В. Годовых, Э.И. Абалмазов, А.В. Измайлов, А.С. Олейник, А. В. Бояринцев, Н.Н. Радаев, В.В. Лесных, А.В. Бочков и множество других. В первую очередь можно выделить монографию М. Гарсиа «Проектирование и оценка систем физической защиты» и диссертации отечественных ученых (В. Н. Костин, А.Д. Тарасов).

О практической значимости методик и способов получения оценок эффективности СФЗ говорит то, что многие работы упомянутых исследователей были доведены до программной реализации: ВЕГА-2, СПРУТ (НПП «ИСТА-Системс»), Полигон (СНПО «Элерон»), Итерация-СФЗ (АО «Итерация»), САПР СИТЗО «Амулет» (АО Производственно-внедренческое предприятие «Амулет»), EASI, ASSESS, SAVI («Сандийские национальные лаборатории», США), КонтрФорс (МВД РФ), IPAD («Харбинский инженерный университет», Китай) и другие.

Среди предлагавшихся ранее подходов, с помощью которых формируются оценки эффективности, следует отметить следующие варианты:

1. Анализ реакций системы с помощью заранее предопределенного сценария-алгоритма, строящего последовательность дискретных воздействий на систему (атака на объект по заданному сценарию).
2. Анализ реакций пространственной модели СФЗ на воздействия со стороны нарушителя в случайных точках (координатах), получаемых методом Монте-Карло.
3. Анализ реакций СФЗ, модель которой описана в виде заранее известного графа возможных путей атак нарушителя;
4. Анализ характеристик СФЗ с помощью теории игр – антагонистические игры, симуляторы с участием человека-исследователя, др.
5. Анализ СФЗ с помощью имитационного моделирования, где модель и эксперимент приближены к реальности.

Наряду с достигнутыми результатами предложенные варианты, однако, имеют недостатки и противоречия: исследование проводится для уже окончательно сформированных (построенных) СФЗ или для их упрощений; с помощью графов затруднительно описать крупномасштабные системы без их упрощения; применяются заранее заданные сценарии или ограничивается возможность их генерации; используются преимущественно субъективные экспертные параметры для описания моделей. Анализ систем с применением имитационного моделирования в качестве инструмента исследования является современным, но, одновременно, слабо проработанным и многообещающим направлением, которое практически не применяется для задач проектирования и оценки эффективности СФЗ.

В соответствии с этим, тема диссертационной работы, посвященной устранению этих недостатков и разработке методов для оценки эффективности систем физической защиты

объектов на основе агентного моделирования и гибридных автоматов, представляется актуальной.

Объект исследования. Компьютерные системы анализа и разработки систем физической защиты, представляющих собой комплекс киберфизических систем с учетом планирования, координации человеческих ресурсов, контроля и реализации инженерно-технических систем и организационных мер для осуществления физической безопасности на большой площади.

Предмет научного исследования. Методы оценки эффективности планируемых или уже построенных систем физической защиты с помощью их цифровых двойников и имитационного моделирования.

Цель диссертационной работы и задачи исследования. Целью диссертационной работы является разработка методов планирования и оценки эффективности систем физической защиты объектов на основе агентного моделирования, гибридных автоматов и алгоритмов автоматизированного формирования сценариев атак для оценки уязвимости СФЗ с помощью имитационного моделирования.

В работе решались следующие задачи:

1. **Разработка методики** построения модели СФЗ и оценки её эффективности с помощью имитационного моделирования на базе агентных моделей и гибридных автоматов.
2. **Разработка подхода** автоматизированной генерации сценариев испытаний СФЗ с помощью предложенных **методов формирования событийно-управляемых траекторий** и эвристического **поиска эффективного пути** атак без использования заранее созданного графа.
3. Разработка графического языка моделирования Систем Физической Защиты, который позволяет создать цифровой двойник системы, её управляющие компоненты, а также логику локального взаимодействия её базовых элементов на уровне схем и чертежей для специалистов по безопасности.
4. Создание специального проблемно-ориентированного ПО для проектирования структуры СФЗ в виде чертежа (цифрового двойника объекта) и исследования её эффективности, принятия решений и повышения эффективности.

Соответствие диссертации паспорту научной специальности. Диссертация удовлетворяет п.5, п.9 и п.11 паспорта специальности 2.3.1. «Системный анализ, управление и обработка информации, статистика»:

П.5. Разработка специального математического и алгоритмического обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта;

П.9. Разработка проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов.

П.11. Методы и алгоритмы прогнозирования и оценки эффективности, качества, надежности функционирования сложных систем управления и их элементов.

Научная новизна. В диссертационной работе предложена методика исследования и анализа эффективности СФЗ, которую можно представить положениями научной новизны:

1. **Предложена и реализована методика** проектирования, анализа и количественной оценки эффективности сложно-структурированных СФЗ на базе имитационного моделирования с применением агентного подхода и гибридных автоматов, **отличающаяся** подходом интерпретации модели всей системы и атакующих агентов структурой базовых элементов без её сведения к графу и набору уравнений с экспертными параметрами, **что позволяет исследовать** сложно-структурированные системы физической защиты без их упрощения, отказаться от применения заранее заданных графов для формирования сценариев исследования, получить готовую рабочую схему системы в виде чертежа и функциональных параметров.
2. **Предложен и реализован на практике метод** формирования имитационной модели Систем Физической Защиты для средств проектирования и количественной оценки эффективности таких систем с применением специально разработанного графического языка моделирования, **отличающийся** тем, что каждый структурный элемент системы представляется настраиваемым модельным классом, размещаемым на плане, а не объединяется группа элементов и подсистем до узлов графа, **что позволяет** рассматривать СФЗ в виде её фактической схемы без упрощения, что дает более полное представление системы для адекватной оценки её эффективности, где осуществляется взаимодействие базовых элементов с моделями подвижных агентов охранников и атакующих нарушителей (люди, переброс и иные акты незаконного вмешательства) на локальном уровне.
3. **Предложен метод** формирования событийно-управляемых траекторий сценариев атак и защиты на базе гибридных автоматов и логико-вероятностных характеристик, **отличающийся** бóльшим покрытием возможных вариантов сценария, чем у других подходов, за счет сохранения стохастической природы атаки и защиты, а также возможностью усложнения моделей поведения агентов без изменения модели всей системы, **что позволяет** без участия эксперта формировать бóльшое число уникальных сценариев действий и взаимодействий с окружением агентов в условиях СФЗ, а также автоматизирует процесс создания таких сценариев.

4. **Для предлагаемой методики разработан эвристический метод** поиска эффективного пути (Polaris) для пространственной модели СФЗ, **отличающийся тем**, что не зависит от заранее заготовленного графа возможных путей атак или состояний системы, как это делается в большинстве существующих системах проектирования СФЗ, **что позволяет** существенно выигрывать в скорости генерации траекторий и характере внешней формы при параллельном проведении множества экспериментов.

Теоретическая значимость работы. Предлагаемые методы могут быть использованы для решения задач формирования и исследования стохастических моделей, а также оценки эффективности в иных областях исследования, где возможно описание крупномасштабной системы с помощью её отдельных локальных модулей и их реакций на плохо предсказуемые воздействие со стороны подвижных агентов. Кроме того, становится возможным исследование не только уже существующих (построенных) систем, но и находящихся на стадии планирования, при этом исследование касается фактических технических решений, готовых без применения сторонних или вспомогательных методик к реализации, как это решается у других подходов.

Особенностями предлагаемой методики и алгоритмов являются:

- Удобство формирования технически сложных крупномасштабных СФЗ с помощью графического языка моделирования в виде чертежей для эскизного проекта (технического задания на создание);
- Высокая скорость получения статистической оценки эффективности СФЗ за счет проведения множества параллельных экспериментов;
- Способ формирования исходных данных на основе паспортных характеристик устройств и экспертных вероятностей для повышения их объективности;
- Возможность сравнения результатов анализа для различных конфигураций систем с целью выбора наиболее дешевой и эффективной.

Таким образом, становится возможным формирование моделей крупномасштабных систем, исследование их свойств и принятие структурных решений для повышения их эффективности.

Исследуемая система представляется в виде чертежа со всей полнотой структуры (до каждого базового элемента), пригодного для создания проекта реальной системы напрямую без применения сторонних методик. Это служит основой для более широкого применения в подобных разработках.

Практическая значимость работы в первую очередь, определяется реализацией разработанных методов и алгоритмов в рамках специального проблемно-ориентированного ПО (комплекс экспертного моделирования «АКИМ»). Результаты диссертационного исследования и разработанное ПО апробированы на практике ООО «Делетрон» (документ о применении от 22.09.2022 № 02/177, акт о внедрении р-тов дис. исследования от 14.05.2025), пробная опытная

эксплуатация в МДВ Республики Беларусь (документ о применении от 15.07.2024 № 28/3/70396, акт о внедрении р-тов дис. исследования № 24-2025), применяются ООО «ПЕНТАКОН» для решения практических задач в области проектирования СФЗ различных объектов (аэропорт Пашковский) и исследования эффективности выбранных решений (ООО «Автотор» – акт № ИШ100420 от 10.04.2020, ЗАО «ТАМАНЬНЕФТЕГАЗ» - акт № ИШ150121 от 15.01.2021).

Методология и методы диссертационного исследования. В работе использованы методы системного анализа, теория графов, имитационное моделирование, теория вероятности, математическая статистика, метод доверительных интервалов и различные подходы к оценке эффективности разрабатываемой системы.

Положения, выносимые на защиту:

1. **Методика проектирования, анализа и оценки эффективности** СФЗ с применением имитационного моделирования в качестве инструмента исследования;
2. **Метод проектирования**, исследования и статистической оценки эффективности цифрового двойника СФЗ с помощью имитационного моделирования на базе агентного подхода;
3. **Метод формирования** событийно-управляемых траекторий на базе гибридных автоматов и логико-вероятностных характеристик для описания сложного поведения элементов в системе и автоматизации создания сценариев исследования.
4. **Разработанный на основе предложенной методики эвристический метод** поиска эффективного пути (Polaris) движения агентов для пространственной модели СФЗ без заранее заданных графа путей атак.

Реализация и внедрение результатов. Разработанные методы данной научной работы были успешно применены в ПО для моделирования и оценки эффективности СФЗ и использованы для исследования крупных объектов Российской Федерации, Республики Беларусь и Республики Казахстан, использовались в проектных работах в компаниях ООО «ПЕНТАКОН», ООО «Делетрон» и др.

Были получены два свидетельства о регистрации ПО: №2019664336 от 12 ноября 2019 г. и №2022683804 от 06 декабря 2022 г. с указанным коллективом авторов (Шарков И.К., Крылов В.М, Квачадзе В.Р., Колесов Ю.Б., Инихов Д.Б.).

Получены патенты:

1) Российская Федерация: RU 2 755 775 C1. Дата регистрации: 21.09.2021
2) Израиль: № 262628. Date of Application: 23/08/2018

Апробация. Результаты работы докладывались и обсуждались на семинарах и конференциях различного уровня:

- Национальная научно-техническая конференция «КоМод-2017» (Санкт-Петербург);
- 13 апреля 2019 года – SEIM-2019 (Санкт-Петербург);
- 30-31 мая 2019 года пройдет IX Международный форум «Безопасность на транспорте» (Санкт-Петербург);
- 21-22 апреля 2020 Skolkovo – STARTUP VILLAGE (Красноярск);

- 20-22 октября 2021 года – Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021);
- 16 апреля 2024 года – Всероссийский инженерный форум PROпроект-2024 (в рамках программы выставки Securika Moscow 2024);

Обоснованность и достоверность подтверждены строгостью математического аппарата, общепринятыми методами компьютерного моделирования, корректным использованием теории системного анализа, математической статистики, актами о внедрении результатов диссертационного исследования, апробацией разработанного программного средства «АКИМ», использующего описанный подход. Также проверена на базе исследования заданных экспертных траекторий со сравнением оценок эффективности СФЗ, полученных в программе EASI по тем же траекториям. Основные результаты представлялись на международных конференциях, публиковались в научных изданиях Перечня ВАК и были отмечены премиями.

Личный вклад автора. Все результаты, отображенные в научной новизне и положениях, выносимых на защиту, принадлежат лично автору, были выполнены в период обучения в аспирантуре в «Политехническом университете Петра Великого» и внедрены в активно развиваемый программный комплекс (ПО «АКИМ» ООО ПЕНТАКОН), созданный коллективом авторов, к которому относится автор.

Публикации. По теме диссертации опубликовано 13 научных работ. Из них в ведущих рецензируемых журналах, входящих в перечень, утвержденный ВАК – 3, в том числе в журнале К1, 2 авторских свидетельства о регистрации программы для ЭВМ. Без соавторов 6 работ.

Структура работы. Основа диссертационной работы состоит из введения, четырех глав и заключения. Список использованной литературы включает 76 наименований. Основной текст работы содержит 171 страниц машинописного текста (12 кегль), включая 72 рисунка, 7 таблиц и 9 приложений.

СОДЕРЖАНИЕ РАБОТЫ

В **первой главе** рассматривается степень разработанности проблематики и перечисляются недостатки существующих подходов, которые ложатся в основу постановки задачи для диссертационного исследования. Так поднимается проблема количественной оценки эффективности систем физической защиты (СФЗ), их состав, существующие методики анализа и ключевые недостатки современных подходов.

Критически важной задачей является оценка эффективности СФЗ через количественные характеристики, чаще выражаемые вероятностями обнаружения ($P_{Обн.}$) и нейтрализации ($P_{Нейтр.}$) нарушителя, а также временем задержки ($T_{Проник.}$). Однако, традиционные методы (натурные испытания, экспертные оценки) обладают ограничениями: высокая стоимость, субъективность, невозможность применения на этапе проектирования системы.

Для получения таких оценок используются различные методы системного анализа и оценки СФЗ с помощью компьютерного моделирования. В большинстве случаев, чтобы провести анализ СФЗ для исследования её уязвимости с помощью компьютерного моделирования необходимо рассматривать минимальный набор математических моделей, куда включены модели объекта, тестирующего воздействия (проникновения), внешних условий и расчет конечного результата (исход). Всё это можно представить в виде кортежа:

$$\sum Модель = \{Объект,\ Проникновение,\ Внешние\ условия,\ Исход\} \quad (1)$$

Основные существующие методики компьютерного моделирования, выработанные для оценки эффективности системы, можно разделить на четыре основных группы:

- ***Предопределенные сценарии*** (EASI, ASSESS): оценка по жестко заданным маршрутам, но ограниченная гибкостью;
- ***Случайные точечные воздействия*** (метод Монте-Карло): оценка обнаруживающей способности по площади объекта, но без учета динамики взаимодействий;
- ***Графы путей проникновения***: поиск уязвимых маршрутов через алгоритмы (JPS и пр.), но с ростом сложности системы увеличивается вычислительная нагрузка;
- ***Имитационное моделирование***: динамический анализ с агентными моделями, позволяющий учитывать поведение нарушителя и охраны в реальном времени.

Основными, хотя и не единственными приведенными в главе, недостатками описанных методов и подходов являются:

- ***Упрощение моделей:*** абстракция сложных СФЗ до графов снижает реалистичность;
- ***Субъективность исходных параметров:*** зависимость от экспертных значений для количественных характеристик укрупненных компонент системы (время реакции, задержка и пр.);
- ***Ограниченность сценариев анализа:*** невозможность учета всех потенциальных угроз и их путей атак, особенно для крупных объектов (аэропорты, ТЭК и пр.);
- ***Ориентация на построенные системы:*** сложность применения методов на этапе проектирования для заблаговременного исключения уязвимостей в реализации.

Для преодоления этих недостатков, необходимо, чтобы методика оценки СФЗ могла:

Решение 1. Состоять из отдельных структурных элементов системы (например, ограждение, датчик, видеоаналитика), описанных их пространственными, физическими и вероятностными параметрами и способных взаимодействовать друг с другом на локальном и общем уровне;

Решение 2. Использовать паспортные данные отдельных технических и инженерных устройств системы или диапазоны экспертных значений для формирования

статистически случайных событий и характеристик (например, время преодоления ограждения, скорость движения);

Решение 3. Формировать сценарии атак без какого-либо заранее заданного графа или детерминированных траекторий и учитывать вероятностную природу событий для динамического изменения сценария;

Решение 4. Описываться с помощью графического языка для формирования достаточно точного цифрового двойника в виде чертежа (2D, 3D). Это позволит не только переносить существующие объекты в виртуальное пространство для их системного анализа, но и составлять цифровые двойники для объектов, существующих еще на этапе технического задания.

Так предлагается разработка новой методики формирования количественной оценки эффективности СФЗ, сочетающей в себе: ***детализированное описание цифрового двойника системы*** (от геометрии, параметров устройств, поведенческие модели агентов) без упрощений, ***повышение объективности исходных данных*** за счет возможности задания паспортных характеристик элементам системы и использования интервальных характеристик с законами распределения для описания реальной человеческой деятельности, ***агентное моделирование*** для динамического анализа взаимодействий системы с силами атаки и защиты (нарушители различных видов и типов, охранники), ***автоматизированная генерация сценариев экспериментов с помощью гибридных автоматов для анализа системы*** без привязки к заранее построенным графам.

Во **второй главе** изложена разрабатываемая методика оценки эффективности систем физической защиты (СФЗ), ориентированная на преодоление ключевых ограничений традиционных подходов — избыточной абстракции в виде графов, зависимости от экспертных оценок и ограниченного охвата сценариев. Основу предложенного решения составляет использование имитационного моделирования с применением агентного подхода, гибридных автоматов и эвристических алгоритмов. Методика составлена из совокупности предлагаемых исследованием методов, отраженных в научной новизне диссертационного исследования.

Общей характерной чертой методики (***первый пункт научной новизны***) является задача оценки эффективности СФЗ с помощью исследования цифрового двойника, который должен быть приближен к реальности. Такое приближение становится возможным, если разложить СФЗ как более подробную модель ∑СФЗ (1), где каждая из подсистем (ИСО, ТСО, СБ, условия эксплуатации, цели защиты) могут быть разложена на множество связанных друг с другом функций и элементов. Как очевидно из описания СФЗ, представленной кортежем, такая декомпозиция осуществима разбиением системы на отдельные математические модели, каждая из которых представляет или базовый элемент (извещатель, камеру, охранника), или логическую

подсистему (правила обработки тревоги, логики поведения операторов видеонаблюдения). Кроме того, к таким моделям возможно добавление внешних условий: погода (различные модели), наработка на ложную тревогу, атакующее воздействие (человек, воздушный способ нарушения безопасности, переброс, иные акты незаконного вмешательства).

Ключевыми компонентами методики являются три метода, отраженные в 2-4 пунктах научной новизны: ***метод построения цифрового двойника*** за счет модифицируемой системы классов, ***метод автоматизированной генерации динамически изменяемых сценариев*** испытаний и ***эвристический метод поиска эффективного пути*** в условиях СФЗ для имитации движения агентных моделей.

С целью реализации этой методики был выбран крайне наукоёмкий отечественный продукт имитационного моделирования – AnyDynamics, в основу которого легли результаты двух докторских работ. Это высокопроизводительная среда для создания и отладки интерактивных многокомпонентных имитационных моделей сложных динамических систем. Составляющие их модели могут быть модифицированы или полностью изменены без необходимости доработки всей модели и программной оболочки. Последнее позволяет использовать эти модели в программных разработках других авторов.

Результирующей частью методики является применение метода доверительных интервалов, который нужен для определения необходимого и достаточного количества экспериментов над СФЗ, формирующих статистику. Результаты этой статистики ложатся в основу количественной оценки эффективности, выраженной как основными вероятностями ($P_{Обн}$, $P_{Нейтр.}$), так и множеством других количественных характеристик ($P_{Реакц}$,$T_{Задерж}$ и пр.).

В рамках ***второго пункта научной новизны*** разработан метод построения цифрового двойника с помощью системы классов. При этом строится комплексная модель системы, представленная совокупностью взаимодействия элементов (рис.1): инженерно-технических средств охраны, операторов и групп реагирования, нарушителей и внешних условий. Для повышения объективности результатов дальнейшего исследования предлагается использовать в качестве исходных данных паспортные характеристики базовых элементов и объекта в целом.

Суть метода состоит в первоначальной разработке совокупности системы классов моделей по принципу «от общего к частному» (родительские к дочерним) с заданием их параметрической сущности на каждом шаге и в конечном применении полученных моделей дочерних классов (базовых элементов) на практике по принципу «частное формирует общее» для каждой конкретной системы (например, элементы видеонаблюдения и операторы формируют систему видеонаблюдения). Это позволило формализовать сложные структуры функционирования СФЗ без сведения системы к упрощённому графу и избежать искажения пространственной логики объекта.

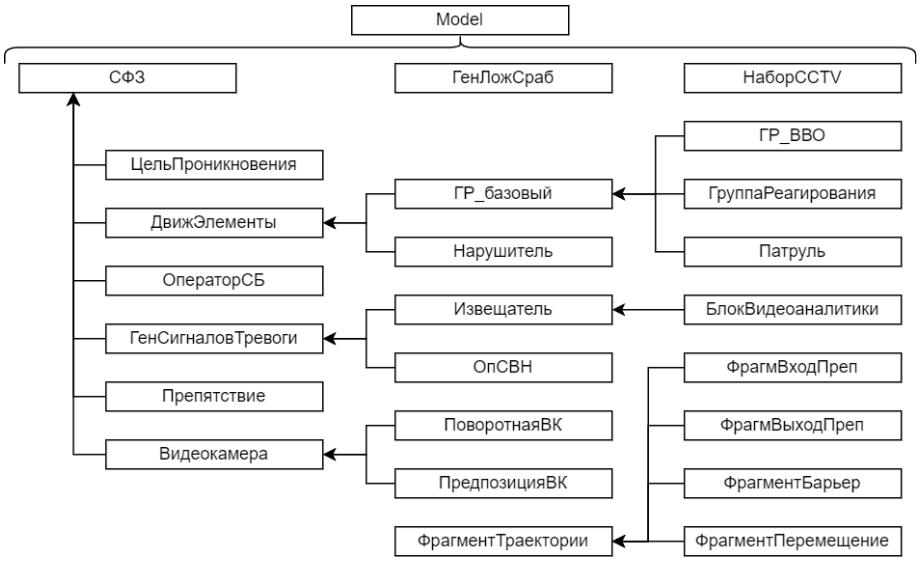


Рис. 1 – Предлагаемая структура классов и их наследование для ∑СФЗ

В ***рамках третьего пункта научной новизны*** разработан метод автоматизированного формирования динамических сценариев, необходимых для постановки экспериментов над цифровым двойником СФЗ с целью оценки её эффективности. Суть метода заключается в формировании событийно-управляемых траекторий (МФСУТ) на базе гибридных автоматов, что позволяет автоматизировано создавать гибкую динамически изменяемую модель поведения агента (атака, защит) в условиях СФЗ. Динамика такой модели зависит от стохастической природы цифрового двойника, где каждое событие может изменить ход действий в эксперименте, а значит и сценарий, представленный моделью поведения агента.

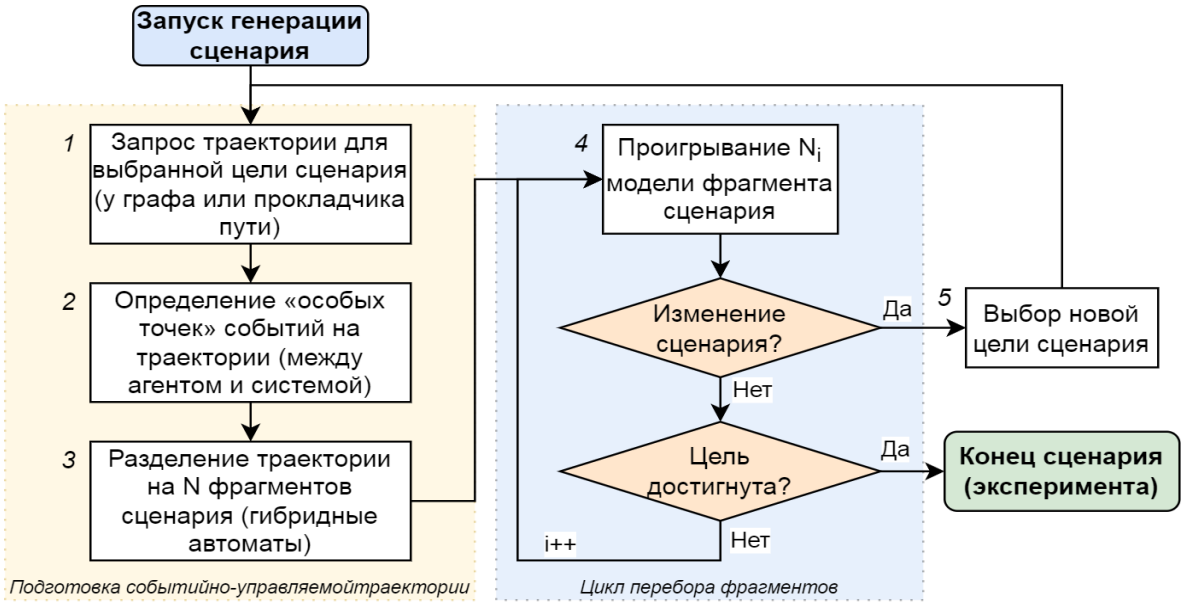


Рис. 2 – Укрупненная блок-схема работы метода формирования сценариев

Метод может быть представлен двумя положениями, где первое – способ формирования модели поведения агента в эксперименте с помощью событийно-управляемой траектории. Модель поведения агента (МФСУТ) строится из фрагментов сценария на основе точек взаимодействия агента (рис.2, блок 2-3) с базовыми элементами СФЗ (вход в зону действия

извещателя, преодоление барьера и др.), а также взаимодействия друг с другом. Второе положение – способ динамического изменения сценария из-за возникающих событий, когда меняется сама модель поведения агента (меняется скорость, направление движения, принятые решения и т.д.), так как поведение агентов формируется через гибридные автоматы с логико-вероятностной природой. Воспроизведение сценария на основе такой модели (блок 4) представляет собой циклический перебор фрагментов с генерацией случайных параметров и событий до тех пор, пока не будет достигнута или изменена цель сценария.

Такой подход позволяет отказаться от заранее заданных сценариев, часто описываемых с помощью графового метода, обеспечив динамическую генерацию разнообразных испытаний без вмешательства человека эксперта.

В ***рамках четвертого положения научной новизны*** разработан метод эвристического поиска пути в условиях СФЗ, необходимый для имитации движения агентов и проведения экспериментов без заранее заготовленных графов путей атак и защиты. Путь, получаемый этим методом, применяется при генерации событийно-управляемых траекторий (рис.2, блок 1). Алгоритмизация метода представлена на рис.3.

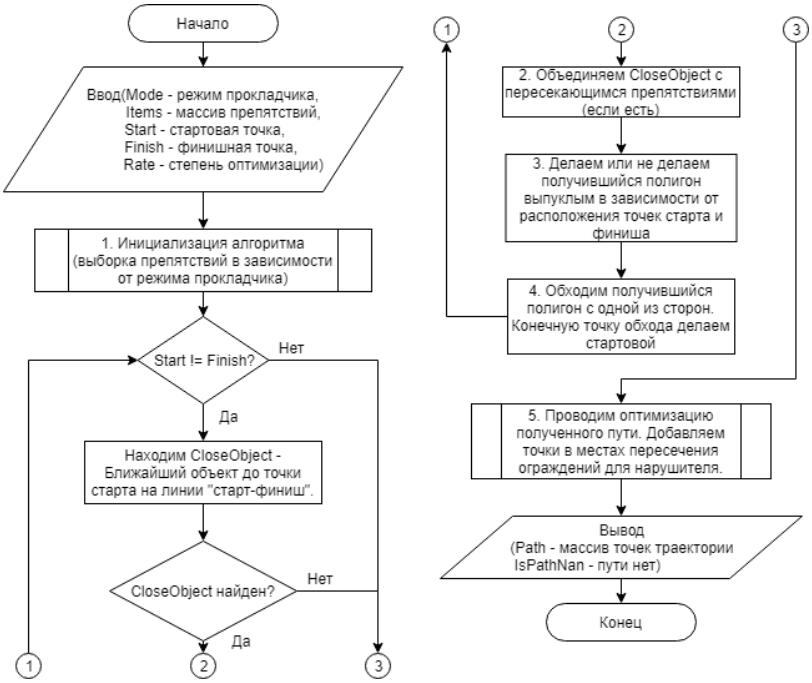


Рис. 3 – Алгоритм эвристического метода поиска эффективного пути для задач моделирования СФЗ

Метод поиска пути, названный «Polaris», не использует графовую модель и формирует траекторию напрямую по геометрии препятствий. Этот подход демонстрирует высокую вычислительную эффективность и реалистичность: обеспечивает быстрое построение множества уникальных траекторий на картах любой сложности, включая крупномасштабные объекты с плотным расположением элементов (аэропорт, город). В сравнении с классическими

алгоритмами (JPS, Ли, поиск по графу видимости) предложенный метод обеспечивает **до 100-кратного выигрыша** по времени при сопоставимом или лучшем качестве маршрутов (табл.1).

Таблица 1: Результаты генерации траекторий на разных картах СФЗ

Алгоритм/метод:	1. Малая простая карта			2. Малая сложная карта		
	t1	**t1000**	**L**	**t1**	**t1000**	**L**
JPS	0.002 с	0.8	144	7.2 с	33 с	64
Ли	0.006 с	0.78	170	34 с	58 с	74.3
«Polaris»	0.002 с	0.1	154	1.1 с	48 с	62
Выигрыш:	~	в 7-8 крат	~	до 30 раз	~	~
	3. Средняя сложная карта			4. Крупная хаотичная карта		
JPS	1.55 с	$>4\cdot10^3$	1343	17,3 с	–	1622
Ли	105.4 с	$>7\cdot10^3$	1677	27,8 с	–	1818
«Polaris»	0.167 с	44.19	1340	0,292 с	48,6	1553
Выигрыш:	в 10 крат	в 100 крат	~	в 10 крат	> 100 крат	на 4-10% короче
где **L** – длина (условная размерность, «юниты»), **t1** – время построения одной траектории от заданных точек старта и финиша, **t1000** – время генерации тысячи случайных траекторий с периметра карты до финиша.						

Примеры в таблице – результаты сравнения предложенного эвристического метода «Polaris» с альтернативными на примере для 4-х типов карт с разной топологией. Видно динамику, где затраты времени для объектов малой площади и простой структуры практически мало отличаются друг от друга. Уже для объектов средней сложности (ближе к реальным) выигрыш предложенного метода оказывается значительным (в десятки раз). При переходе к картам большой площади и сложной топологии выигрыш увеличивается экспоненциально. Важной составляющей этого выигрыша является хорошая распараллеливаемость вычислений, которые могут быть оптимизированы за счет GPU, а не только CPU.

Таким образом, в главе представлена методика, в которой методы формирования цифрового двойника СФЗ, эвристического поиска пути и событийно-управляемых траекторий образуют единую систему автоматизированного проектирования и анализа эффективности сложноструктурированных крупномасштабных систем. Это позволяет не только устранить ранее обозначенные недостатки существующих решений, но и реализовать гибкий, адаптивный инструмент количественной оценки эффективности СФЗ на стадии проектирования или модернизации.

В **третьей главе** для задачи сравнительного анализа предлагаемой методики оценки эффективности с альтернативными приводится обзор существующих реализаций, их критика и вывод общих черт – моделирование СФЗ на основе заранее заготовленного. Имеющиеся публикации о методах и информация о принципах, положенных в основу альтернативных программных решений, указывает на то, что они базируются на цепях Маркова. С целью получения количественных значений оценки эффективности сравнительный анализ осуществляется на одинаковых примерах систем для графовых методов (цепь Маркова) и для предлагаемой методики.

Упомянутые недостатки реализаций очевидно снижают точность и достоверность оценок эффективности, особенно при анализе сложных крупномасштабных систем, таких как аэропорт или объект топливно-энергетического комплекса. Кроме того, графовые методы требуют полного пересчёта матриц переходов при изменении конфигурации объекта (замена средств охраны, изменение правил, перенос постов и прочее), что ***делает их применение трудоёмким и неэффективным для реальных задач***. Предлагаемая методика позволяет параллельно с моделированием корректировать как конфигурацию системы, так и параметры её элементов – изменять цифровой двойник, преобразуя его в новую структуру. Кроме того, особенность подхода позволяет модифицировать и заменять математические модели базовых элементов, что позволяет сохранить функциональную гибкость практической реализации.

В программной реализации предлагаемой методики (ПО «АКИМ») используется параметрический чертеж, заданный специально разработанным для задач построения и анализа СФЗ графическим языком моделирования. Подход преодолевает все упомянутые недостатки (1 глава и начало 3 главы), позволяя:

- Графическим способом описывать 2D и 3D структуру (чертеж) объекта защиты (исследования), для чего достаточно только понимание основ работы СФЗ;
- Динамически генерировать уникальные сценарии атак с учётом нелинейных взаимодействий и случайных факторов;
- Детально моделировать поведение агентов (нарушителей и охранников) с заданием реалистичных параметров, таких как скорость, экипировка и тактика, описанных интервальными значениями (вместо точных экспертных) и законами распределения (PERT-распределение);
- Легко адаптироваться к изменениям масштаба или конфигурации объекта, корректируя лишь геометрические параметры плана и набор базовых элементов.

Для построения марковских моделей СФЗ применялся AnyDynamics. Для сравнительного анализа описываются два примера: «одномерная» и «двумерная» модель систем, которые вносятся в «АКИМ» и задаются в виде цепи Маркова. «Трехмерная» модель не рассматривалась ввиду её очевидной сложности для реализации графовым способом, хотя в предлагаемой методике любая модель СФЗ уже является трехмерной: элементы системы имеют трехмерные параметры форм и зон воздействия, можно задавать многоэтажные конструкции для перемещения, а движение агентов рассматривается в трехмерном пространстве как для человека, так и для альтернативных актов незаконного вмешательства (воздушный, переброс).

Необходимо отметить, что сравнение проводилось для оценки нейтрализации угрозы ($P_{Нейтр}$). Получаемая оценка любым методом не может быть «точнее» или «лучше», так как зависит от особенности способа задания и расчета модели. Потому сравнивается подробность и

достоверность (реалистичность) этих оценок, а также сложность их получения. Для каждого различия приводится обоснование. ***Оценки предлагаемого подхода формируются на основе полученной статистики экспериментов***.

Получение оценок может быть достигнуто точечной оценкой вероятности, где результат является суммой всех событий C_i, деленное на число испытаний N:

$$P = \frac{1}{N}\sum_{i=1}^{N} C_i \qquad (2)$$

Точность результатов зависит от количество проведенных испытаний над системой. Для того чтобы ограничить количество экспериментов N для формирования оценки с необходимой точностью, выбран подход с использованием доверительного интервала. Подход гласит, что вероятность того, что вероятность p и частота $\overline{P}$ будет отличаться не более чем на величину ε определяется по формуле:

$$P\left(\left|\overline{P} - p\right| < \varepsilon\right) = 2\Phi\left(\frac{\varepsilon\sqrt{N}}{\sqrt{p(1-p)}}\right), \qquad (3)$$

где Ф – функция Лапласа:

$$\Phi(x) = \frac{1}{2\pi}\int_0^x e^{-\frac{t^2}{2}}dt \qquad (4)$$

Так, например, вероятности нейтрализации нарушителя $P_{Нейтр.}$ силами службы безопасности определяется как частота $\overline{P_{\text{Нейтр}}}$ по формуле (5):

$$p_{\text{Нейтр}} \approx \overline{P_{\text{Нейтр}}} = {}^{M}/_{N}, \qquad (5)$$

где N – общее число всех экспериментов, а M – число испытаний, в которых нарушитель был нейтрализован. Вероятность достоверности результата определяется:

$$P\left(\left|\overline{P_{\text{Нейтр}}} - p_{\text{Нейтр}}\right| < \varepsilon\right) = 2\Phi\left(\frac{\varepsilon\sqrt{N}}{\sqrt{p_{\text{Нейтр}}(1-p_{\text{Нейтр}})}}\right) \qquad (6)$$

Для ***одномерной модели*** (имитация зоны досмотра в аэропорту, где нарушитель проходит строго заданную последовательность действий на маршруте) приводится подробный пример построения системы сравниваемыми способами. Для СФЗ заданной цепью Маркова оценка эффективности защиты ($P_{\text{Нейтр}}$) составила 84.4%. Результаты моделирования в среде «АКИМ» для 1000 испытаний дали 957 успешных нейтрализаций нарушителя, что попадает в ***доверительный интервал от 0.9444 до 0.9696***. Так становится известен худший и лучший прогноз системы и формируются различные способы прохождения «одномерного сценария». Кроме того, были получены дополнительные оценки – обнаружение ($P_{\text{Обн}}$=98.5%), временя движения, самые уязвимые сценарии событий в этой цепочке и т.д. – что потребовало бы у

альтернативных методов формирования новой матрицы переходов и появление новых связей между узлами (напр., обнаружение через несколько рубежей).

Анализ ***двумерной модели*** (объект с двумя рубежами охраны, тремя постами охраны, без технических средств) выявил значительные различия как по оценке, так и по свойствам получаемых результатов. Всего было выделено три существенных различия. Кроме очевидного ограничения количества вариантов сценария на примере цепи Маркова (1-ое отличие), где предлагаемый подход дает практически неограниченное количество, были получены различные варианты оценок в зависимости от типа нарушителя (2-ое отличие), описываемого физическими и вероятностными характеристиками. Так, для испытаний были сформированы параметрические модели «Дилетанта» и «Нарушителя с силовым методом проникновения», влияние которых сложно было бы описать в виде матрицы переходов (что, практически, вообще не осуществляется в альтернативных подходах).

3-е существенное отличие предлагаемого подхода проявляется в способности эффективно масштабироваться для анализа систем физической защиты различных размеров и конфигураций, в то время как традиционные методы на основе марковских цепей требуют полного пересмотра, как было описано на примере одномерной модели. Сравнение приводится для примеров одинаковой модели нарушителя «Дилетант», где площадь объекта меняется с 2 км^2 до 0.2 км^2 – уменьшается в 10 раз.

Модель, описанная графом, по сложности возросла многократно и потребовала длительной ручной оптимизации для повышения читаемости своих связей. Так, например, в левой части рис.4 отражен плохо читаемый граф до крайне трудоёмкой ручной обработки.

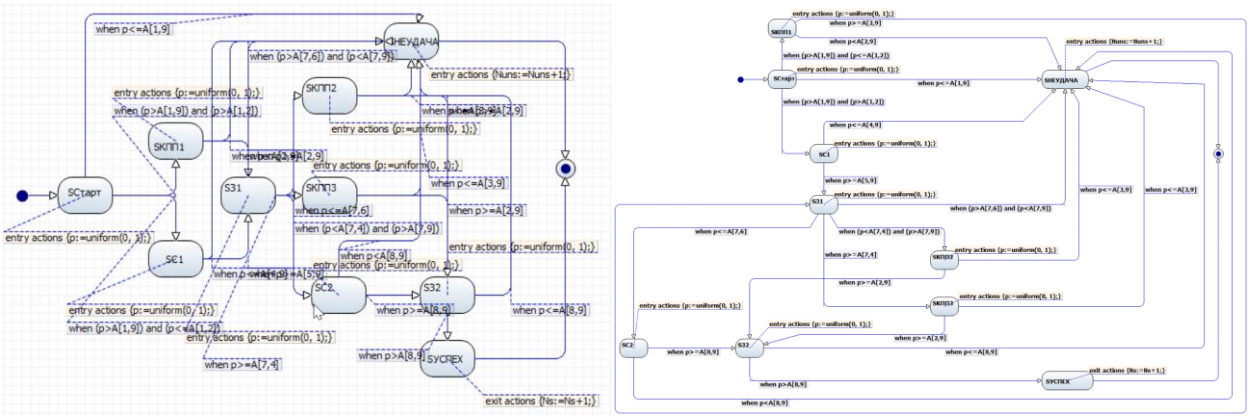


Рис. 4 – Цепь Маркова для описанной СФЗ на языке UML до и после оптимизации

Ещё одним выигрышным отличием предлагаемого подхода является возможность формировать сценарии не только из одной точки (одинаковые стартовые условия), но проанализировать систему с помощью атак со всех направлений вокруг объекта, например, разбив периметр на множество участков. Так становится возможным определение самых слабых

и сильных направлений атак, что повышает глубину оценки эффективности, не ограничивая её общей оценкой для всей системы, как у альтернативных подходов.

В табл. 2 приведены результаты, где для одного цифрового двойника без серьёзных трудозатрат получены результаты для трех различных ситуаций (простой нарушитель – 2 столбец, «нарушитель с силовым методом проникновения» – 3 столбец, простой нарушитель на аналогичном объекте в 10 раз меньшей площади – 4 столбец).

Таблица 2: Результаты оценки нейтрализации с предлагаемым подходом

Участки	**«Дилетант»**	**«Нар. с сил. метод. проник.»**	**«Дилетант» на об. 0.2 кв. км**
1	0.6836 – 0.7773	0.4540 – 0.5160	0.7335 – 0.7865
2	0.6867 – 0.7800	0.4231 – 0.4849	0.9186 – 0.9494
3	0.7602 – 0.8444	0.4971 – 0.5589	0.9787 – 0.9933
4	0.7383 – 0.8256	0.4640 – 0.5260	0.9665 – 0.9855
5	0.7298 – 0.8181	0.4251 – 0.4869	0.9906 – 0.9994
6	0.8763 – 0.9377	0.4023 – 0.4637	0.9878 – 0.9982
7	0.8174 – 0.8919	0.3894 – 0.4506	0.9865 – 0.9975
8	0.6827 – 0.7766	0.4202 – 0.4818	0.9851 – 0.9969
9	0.7609 – 0.8449	0.4470 – 0.5090	0.9892 – 0.9988
10	0.7950 – 0.8736	0.5111 – 0.5729	0.9825 – 0.9955
11	0.6562 – 0.7525	0.4321 – 0.4939	0.9354 – 0.9626
12	0.6723 – 0.7670	0.4351 – 0.4969	0.7658 – 0.8162
Общие:	**78.1%**	**47.3%**	**76%**
Минимальная вероятность нейтрализации		42% (участок: 7, «Нарушитель с силовым методом проникновения»)	

Оценка для марковской модели в ситуации 2 столбца составила **66.7%** для всей СФЗ. При этом отсутствует детализация по различным участкам или местам возникновения нарушителя и для ситуаций с изменением модели (меняем нарушителя, структуру объекта или его площадь) вся подготовка исходных данных должна производиться заново (матрица переходов, граф и пр.).

Кроме того, полученные статистические данные позволяют сформировать не только оценку нейтрализации, обнаружения и времени движения, но и практически любых других свойств системы, которые можно вывести на основе собранных данных. Например, рассчитать частоту срабатывания тех или иных технических средств, коэффициент задержки нарушителя на инженерных препятствиях, обнаружить избыточные элементы, не участвующие в задачах защиты. За счет замены моделей нарушителей или изменения конфигурации СФЗ без серьёзных трудозатрат можно сравнивать результаты различных условий и модификаций, что является полезным свойством предлагаемой методики.

В **четвертой главе** диссертации рассмотрены следующие вопросы: практическая реализация предложенной методики оценки эффективности СФЗ в составе программного комплекса «АКИМ», его архитектура, функциональные возможности и примеры применения, а также специально разработанный графический язык моделирования.

Ключевым результатом главы является описание программной реализации методики, включая:

- интеграцию математических моделей в виде динамической библиотеки (DLL) для взаимодействия с оболочкой «АКИМ»;
- разработку визуального языка для сборки моделей СФЗ, позволяющего формировать цифровые двойники объектов;
- реализацию методов прокладки траекторий движения агентов (нарушителей и охранников) с учетом стохастических факторов;
- механизм проведения имитационных экспериментов и анализа статистических данных.

Основная практическая ценность заключается в ***решении реальных практических задач***, что отражается в соответствующих актах. Так, подтверждается работоспособность предложенного подхода, включая корректность генерации сценариев, обработку событий и расчет оценок эффективности.

Кроме того, методика продемонстрировала свою ***универсальность в задачах планирования и оценки*** СФЗ. Специально разработанный графический язык моделирования и модульная архитектура «АКИМ» позволяют адаптировать комплекс для моделирования СФЗ объектов различной сложности и конфигурации, а также позволяют модифицировать и даже заменять модели без изменения (переписывания) остального программного продукта или изменения сути методики.

Репрезентативность результатов программной реализации позволяет повысить прозрачность методики. Использование доверительных интервалов и статистических методов обеспечивает достоверность оценок, что критически важно для принятия проектных решений.

Дальнейшее развитие работы может быть связано с расширением функциональности «АКИМ», добавлением новых видов актов незаконного вмешательства, новых подсистем и их функций, их базовых элементов, включая более сложные модели поведения агентов и интеграцию с системами проектирования (BIM), которой и является программная реализация. При этом нет зависимости от сторонних технологий, как в случае некоторых практических реализаций альтернативных методов оценки СФЗ.

ЗАКЛЮЧЕНИЕ

В диссертационной работе была предложена методика количественной оценки эффективности СФЗ с помощью имитационного моделирования, позволяющая устранить недостатки существующих подходов. Она включает в себя моделирование на базе агентного подхода и конечных автоматов, а также алгоритмы автоматизированного формирования сценариев и поиска пути атак без заранее заданных графов, что позволяет подробно описать систему на уровне её элементов для всестороннего исследования характеристика безопасности.

Были получены следующие результаты:

1) Предложена методика формирования модели и количественной оценки эффективности СФЗ с применением имитационного моделирования на базе конечных автоматов и агентных моделей;
2) Разработаны алгоритмы формирования событийно-управляемых траекторий и эвристического поиска пути для описания проникновения нарушителя и движения охранников без заранее созданного графа.
3) Разработан графический язык формирования моделей СФЗ, позволяющий описать структуру системы и логику взаимодействия её элементов на уровне схем и чертежей для специалистов по безопасности.
4) Создано проблемно-ориентированное ПО на основе предложенной методики и алгоритмов, применяемое в коммерческой практике.

Преимуществами предлагаемой методики формирования модели и оценки эффективности СФЗ в отличии от других подходов стали: автоматизация формирования моделей сложных систем и постановки экспериментов над ними; возможность моделирования крупномасштабных систем с включением сотен элементов киберфизических систем и человеческих ресурсов без серьёзных ограничений на вычислительные мощности; повышение объективности получаемых результатов за счет использования паспортных характеристик реальных устройств и применения стохастических моделей, описывающих человеческий фактор; возможность анализа как существующих (построенных), так и планируемых систем без применения сторонних методик; возможность моделирования множества параллельных агентов атак и защиты без увеличения количества состояний системы.

Для разработки моделей использовался наукоёмкий пакет математического моделирования AnyDynamics, а также были реализованы эвристический алгоритм поиска пути «Polaris» и программа графического редактора моделей, моделирования и анализа результатов «АКИМ».

Внедрение результатов. Результаты данной научной работы были успешно применены различными организациями (указаны в актах о внедрении и приложениях к диссертации) в практике моделирования и оценки эффективности СФЗ крупных объектов (аэропортов, объектов ТЭК и т.п.), а также при участии в тендерах и проектных работах.

Основные публикации по теме диссертации

1. Шарков И.К., Сениченков Ю.Б. Имитационное моделирование систем физической защиты в среде АКИМ // Научно-практический журнал "Программные продукты и системы". - 2025. - №1. - С. 77-88. **(РИНЦ, ВАК, К1)**.

2. Шарков И.К., Колесов Ю.Б. Метод формирования сценариев имитационного эксперимента для исследования систем с подвижными агентами // журнал "Перспективы науки". - 2025. - №3(186). - С. 36-41. **(РИНЦ, ВАК, К3)**.

3. Sharkov, I. Planning and Quality Evaluation of Physical Protection Systems Using Simulation Modeling / I. Sharkov, V. Krylov, Yu. Kolesov // Компьютерные инструменты в образовании. – 2022. – No. 2. – P. 32-40. – DOI 10.32603/2071-2340-2022-2-32-40. **(РИНЦ, ВАК, К2)**.

Свидетельства о государственной регистрации программы для ЭВМ

4. Шарков И.К. Программный комплекс «АКИМ-ОНЛАЙН» / Крылов В.М., В.Р. Квачадзе, И.К. Шарков, Ю.Б. Колесов, Д.Б. Инихов – Свидетельство о регистрации программы для ЭВМ RU 2019665127, 20.11.2019. Заявка № 2019664336 от 12.11.2019.

5. Шарков И.К. «АКИМ» / Крылов В.М., В.Р. Квачадзе, И.К. Шарков, Ю.Б. Колесов, Д.Б. Инихов – Свидетельство о регистрации программы для ЭВМ № 2023617480, 11.04.2023. Заявка No 2022683804 от 06 декабря 2022 г.

Статьи и материалы конференций

6. Шарков И.К., Желудков Е.А. Применимость эвристического алгоритма для задач поиска траекторий движения через систему физической защиты. В сборнике: SEIM-2019. 2019. С. 34-40.

7. Шарков, И.К. Моделирование и оценка качества систем физической защиты на основе агентного подхода и алгоритма событийно-управляемых траекторий / И.К. Шарков, Ю.Б. Сениченков, Ю.Б. Колесов // Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021). – Санкт-Петербург: АО «Центр технологии судостроения и судоремонта», 2021. – С. 503-510.

8. Шарков И.К. Имитационное моделирование средств физической защиты на охраняемом объекте в задачах оценки уязвимости / Шарков И.К. // В сборнике: Первая всероссийская научно-практическая конференция по имитационному моделированию и его применению в военной сфере "Имитационное моделирование систем военного назначения, действий войск и процессов их обеспечения" ("ИМСВН-2020"). Труды конференции. Санкт-Петербург, 2020. С. 254-264.

9. Крылов В.М., Шарков И.К. Генерация сценариев атак нарушителя с помощью алгоритма событийно-управляемых траекторий [Электронный ресурс] // Вторая всероссийская научно-практическая конференция по имитационному моделированию и его применению в военной сфере «Имитационное моделирование систем военного назначения, действий войск и процессов их обеспечения» («ИМСВН-2022»). Труды конференции, 20 октября 2022 г., Санкт-Петербург. – Санкт-Петербург: ВА МТО; Москва: РИОР, 2022. – 199 с. – ISBN 978-5-369-02106-4. С. 105-114.

10. Шарков, И.К., Сениченков, Ю.Б., Желудков, Е.А. Генерация траекторий для задач моделирования СФЗ. В сборнике: Молодежь и современные информационные технологии. Сборник трудов XVI Международной научно-практической конференции студентов, аспирантов и молодых ученых. Томский политехнический университет. 2019. С. 122-123.

11. Шарков И.К., Желудков Е.А. О построении траекторий движения на охраняемых объектах. В сборнике: НЕДЕЛЯ НАУКИ СПбПУ. материалы научной конференции с международным участием. 2019. С. 43-46.

12. Шарков, И.К. Планирование и оценка качества систем физической защиты с помощью имитационного моделирования / И.К. Шарков, В.М. Крылов // Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика». – Санкт-Петербург: АО «Центр технологии судостроения и судоремонта», 2021. С. 496-502.

13. Шарков И.К. Моделирование и анализ эффективности систем физической защиты для планирования структуры безопасности на уровне фактических чертежей. // Сборник научных трудов XXVIII международной научно-практической конференции «Системный анализ в проектировании и управлении (SAEC-2024)». СПб: Издательство Санкт-Петербургского Государственного Политехнического Университета. 2024. – С. 66-77. – DOI: 10.18720/SPBPU/2/id24-498.