ПЛАНИРОВАНИЕ И ОЦЕНКА КАЧЕСТВА СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ С ПОМОЩЬЮ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

И.К. Шарков, В.М. Крылов (Санкт-Петербург)

1. Оценка качества систем физической защиты на этапе планирования

В настоящий момент нет доступной информации об инструментах компьютерного моделирования и оценки качества систем физической защиты (СФЗ), использующих объектно-ориентированный подход, позволяющих на основе чертежа охраняемого объекта построить агентную модель, имитирующую атаки на объект, и с ее помощью оценить качество защиты проектируемой системы. Графический язык описания проектируемого объекта и имитационная модель системы защиты ускоряют процесс проектирования, позволяют исследовать свойства модели, добиться ее соответствия предъявляемым требованиям и, в результате, повысить качество технических заданий на реализацию СФЗ.

Существующие решения к моделированию СФЗ базируются на графах атак нарушителей и концептуальных представлениях о системе [1]. Используемые модели позволяют планировать размещение точек контроля (ТК) на пути до критических элементов (КЭ) и определять уровень вероятностей обнаружения $P_{Обн.}$ и нейтрализации $P_{Нетр.}$ нарушителя для обеспечения нужного уровня безопасности. Результаты моделирования становятся требованиями к структуре будущей СФЗ.

Для адекватной оценки планируемой СФЗ необходимо прозрачное и подробное представление её структуры. Таким представлением является чертеж в двухмерном или трехмерном электронном представлении (например, чертежи из программ AutoCAD, NanoCAD, Revit и т.п.). Существуют реализации [2], которые позволяют на основе BIM (Building Information Modeling) проектов формировать графы путей движения нарушителей через охраняемый объект. Ограничениями таких решений является достаточно высокий порог сложности для эскизного проектирования, а также необходимость строить графы путей на основе чертежей зданий, не включающих в себя описание охраны объекта на территории вокруг них. Такой подход возможно использовать для уже существующих объектов, которые имеют цифровое представление.

Если принять чертеж СФЗ как основу для формирования её математической модели, то можно применять программное средство моделирования, позволяющее из готовых компонентов (типовых элементов) инженерных и технических средств охраны и сил служб безопасности объекта собирать цифровой двойник планируемого объекта в виде чертежа. Кроме элементов СФЗ необходимы компоненты для задания внешних условий (погода, ложные тревоги) и модели нарушителей, учитывающих место и цели проникновения. Модель должна включать: модели инженерных (ИСО) и технических средства охраны (ТСО), модель службы безопасности (СБ). Целью моделирования являться оценка эффективности СФЗ, с помощью минимум двух количественных оценок безопасности:

- вероятность обнаружения ($P_{Обн.}$) нарушителя;
- вероятность нейтрализации ($P_{Нейтр.}$) нарушителя силами СБ.

Существуют различные методики компьютерного моделирования в задачах оценки качества СФЗ [2, 4], однако практически все они описывают структуру СФЗ с помощью графа путей. Чем подробнее описана система, тем сложнее модель СФЗ и труднее описывать её графом. Увеличение размерности графа (или использование наложенной сетки) влечет лавинообразный рост объема исходных данных для моделирования [3, 4]. По этой причине рационально использовать подход

имитационного моделирования для задач оценки качества. Благодаря высокой вычислительной мощности современных персональных компьютеров и возможности распараллеливания имитационных экспериментов становится возможным проведение достаточного числа испытаний, чтобы получить оценку качества с заданной необходимой точностью с помощью достаточно малых доверительных интервалов (порядка ε=0.01 и даже ниже).

2. Реализация математических моделей в AnyDynamics

Для задач разработки имитационных моделей СФЗ применимы множество различных инструментов: MATLAB, AnyDynamics, Dymola, MapleSim, AnyLogic, Scilab, Maxima [5]. Для создания моделей СФЗ была выбрана высокопроизводительная среда для разработки многокомпонентных моделей сложных динамических систем AnyDynamics, позволяющая создавать модели (dll), встраиваемые в приложения. Был выбран агентный подход к моделированию. Агентный подход позволил описать взаимодействия агентов на языке, понятном разработчикам систем СФЗ и оценивающих их экспертам.

Представление классов всех сущностей такой имитационной модели можно увидеть на рис. 1.

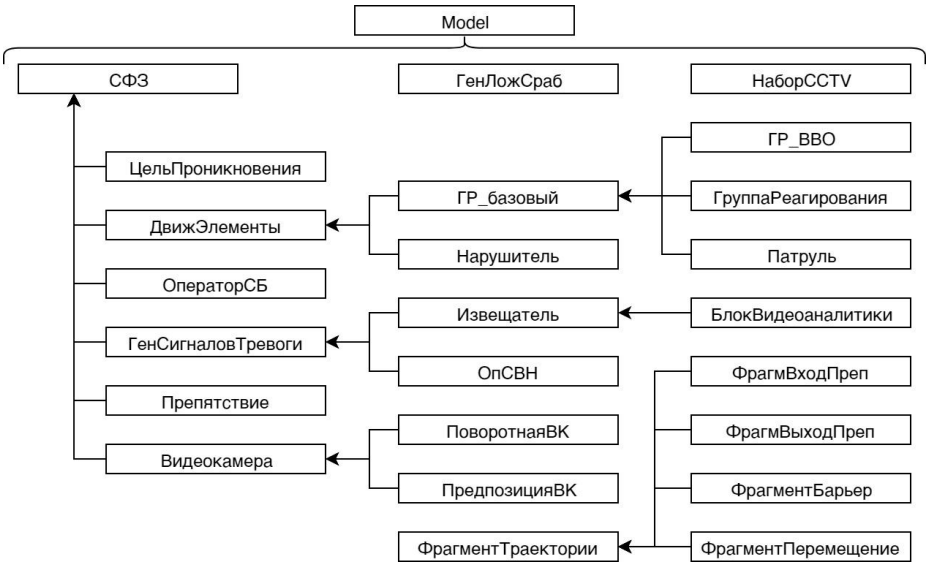

Рис. 1. Схема классов и их наследования разработанной модели

Создание сценария проникновения обеспечивается разработанными алгоритмами формирования событийно-управляемых траекторий с использованием карт поведения, а реализация сценария осуществляется с помощью алгоритма поиска путей «Polaris» [6].

Эти алгоритмы обеспечивают автоматизированный процесс формирования сценариев атак, для которых необходимы только начальные и конечные условия. Благодаря этому нет необходимости в использовании графов путей, проложенных через чертеж цифрового двойника СФЗ.

Моделирование взаимодействия нарушителя с элементами СФЗ позволяет собирать все необходимые данные о процессе и результатах каждого эксперимента. На основе полученных данных множества статистических испытаний можно получить количественные оценки качества эффективности моделируемой системы.

3. Среда графического проектирования и имитационного моделирования

Так как структура планируемой СФЗ описывается чертежом, то за каждым элементом чертежа должен быть закреплен свой уникальный компонент со своими

исходными данными. Исходными данными являются рабочие параметры (вероятность обнаружения, интервал времени задержки движения и т.д.), графическая информация: координаты места установки устройства, габариты препятствия, геометрическая форма зоны обнаружения и так далее. Таким образом, структуру цифрового двойника СФЗ становится возможным формировать с помощью специального графического конструктора.

Для полноценного описания СФЗ у графического редактора моделей должны быть следующие возможности:

1. СФЗ: создание плана территории объекта с помощью описания его инфраструктуры и топологии, влияющей на возможные маршруты движения нарушителя;
2. СФЗ: создание элементов ИСО с необходимыми характеристиками их пространственной геометрической формы и способности сдерживания нарушителя;
3. СФЗ: создание элементов ТСО с необходимыми характеристиками для задания пространственной геометрической формы их зон обнаружения, способа их работы и вероятности реакции на тот или иной тип воздействия нарушителя, описанный разработанной математической моделью;
4. СФЗ: создание структуры сил СБ на территории объекта – это как расположение постов охраны и количество охранников на них (группы реагирования), патрули и их траектории патрулирования, операторы и их функциональное назначение, так и параметры, отвечающие за образ поведения каждой единицы, тактику реакций, движения или образа принятия решений, описанный в разработанной математической модели;
5. Внешние условия: задание параметрических характеристик погодных условий, динамики их изменения, а так же параметры модели возникновения ложных тревог;
6. Нарушитель: Задание модели нарушителя в виде параметрического набора, описывающего его поведение и характеристики;
7. Путь проникновения: задание способа генерации траектории (в данной разработке использован собственный эвристический алгоритм поиска пути Polaris), а так же обозначение мест возникновения нарушителя и типов предпочитаемых им целей;
8. Исход: задание целей проникновения (защищаемых зон на территории СФЗ) с их характеристиками взаимодействия с нарушителем.

Для реализации такого подхода проектирования и моделирования планируемых СФЗ компанией ООО «ПЕНТАКОН» был разработан программный комплекс «АКИМ», включающий в себя разработанные в AnyDynamics модели и алгоритмы, прокладчик траекторий «Polaris», графический редактор цифровых двойников СФЗ и модуль сбора и анализа результатов статистических испытаний для формирования оценок качества охраны и программных отчетов с ними.

Программный комплекс «АКИМ» позволяет разрабатывать модели СФЗ и создавать в них условиях проведения имитационного эксперимента с проникновением нарушителя с помощью своего собственного графического языка. Данный графический язык представляет собой чертежный инструмент с элементом конструктора, который помогает собирать СФЗ из заранее подготовленных блоков-моделей.

Внешний вид программы и её графический редактор можно увидеть на коллаже рис. 2.

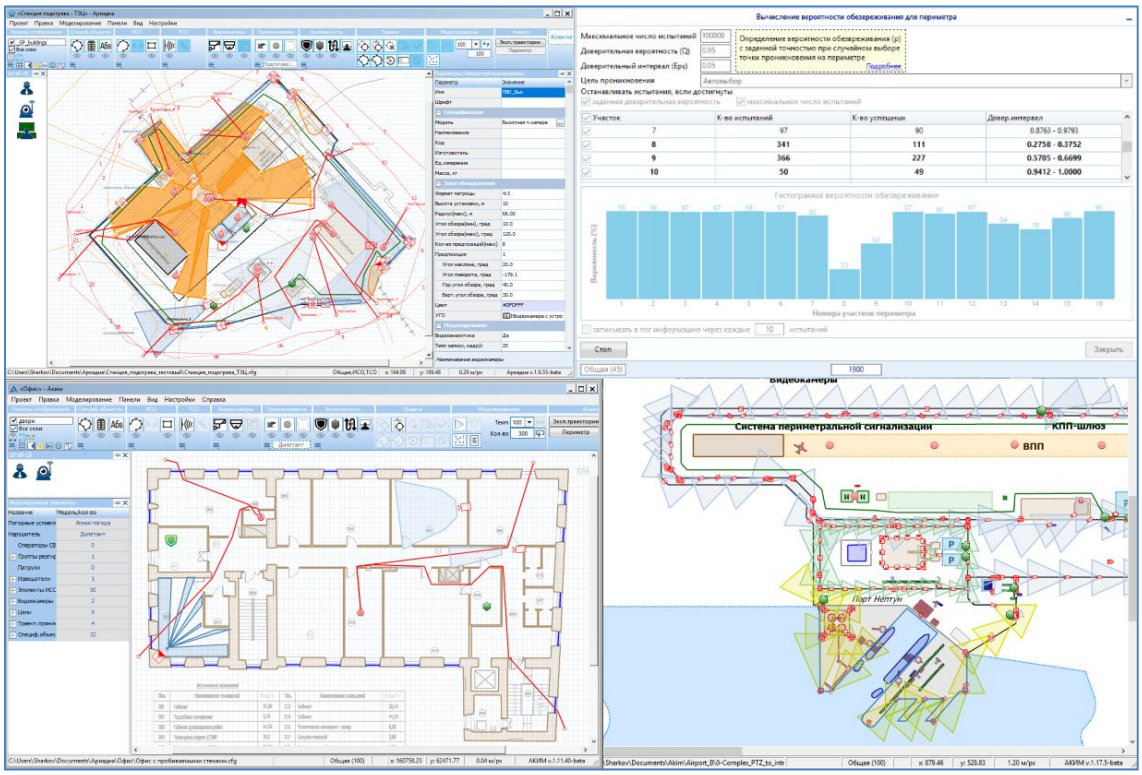

Рис. 2. Графическое представление моделей СФЗ охраняемых объектов в «АКИМ»

Для графического редактора цифровых двойников СФЗ были реализованы следующие моделируемые элементы, которые можно «нарисовать» в конструкторе:

· «Строение» (непреодолимое препятствие) – структура, ограничивающая движение нарушителя в пространстве, не позволяет сквозное прохождение и визирование; посредством элементов «строение» описываются стены зданий и иные препятствия;

· «Специфический участок» – участок особой зоны, которая влияет на скорость перемещения человека и дистанцию сквозной видимости; это может быть как водоем, так и кустарник;

· «Ограждение» – основной элемент ИСО, предназначенный для защиты объекта по периметру его зон охраны;

· «Препятствие» – дополнительный элемент ИСО, описывающий охранные препятствия большой площади (рвы, натянутую колючую проволоку и т.д.);

· «Барьер» – дополнительный элемент ИСО, описывающий широкий спектр элементов: от заградительной ленты до стекла в оконном проеме;

· «Извещатель» – элемент ТСО, предназначенный для обнаружения проникающего воздействия нарушителя. В «АКИМ» может быть представлен различными типам и геометриями зон обнаружения (см. рис. 3);

· «Стационарная» и «Поворотная» видеокамеры – элементы ТСО, позволяющие дистанционное слежение за территорией объекта со стороны операторов и видеоаналитики;

· «Группа реагирования» – подвижная единица сил службы безопасности (охранник), способная перемещаться по объекту в соответствии с приказами оператора или при преследовании нарушителя;

· «Патруль» – частный случай «Группы реагирования» – охранник, циклично обходящий территорию объекта по заданной траектории патрулирования с заданным расписанием;

· «Вневедомственная охрана» – частный случай «Группы реагирования» - охранник, прибывающий на территорию объекта извне в указанный промежуток времени в случае тревоги;

· «Оператор СБ» – сотрудник СБ, занимающийся мониторингом сигналов тревоги и отвечающий за принятие решений;

· «Оператор СВН» – сотрудник СБ, занимающийся мониторингом системы видеонаблюдения (видеокамер);

· «Зона охраны» – зона на территории объекта, в которой обеспечивается охрана; может иметь разные уровни доступа для разных охранников;

· «Периметр проникновения» – периметр вокруг объекта, разбитый на участки, описывающий места возникновения нарушителя;

· «Цель проникновения» – точка или зона на территории объекта, в которую будет стремиться проникающий нарушитель.

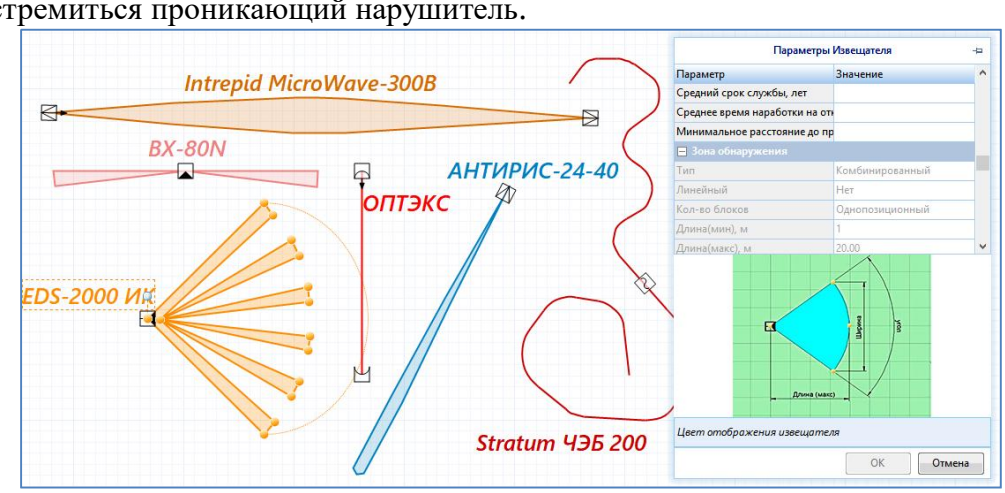

Рис. 3. Примеры извещателей в «АКИМ» с открытым окном параметров одного из них

Также в редакторе «АКИМ» указываются моделируемые условия:

· параметрическая модель нарушителя и его оснащения;

· модель погодных условий;

· модель ложных тревог и срабатываний.

Программный комплекс разработан в двух вариантах:

· программная оболочка, написанная на языке Delphi («АКИМ»);

· программная оболочка, написанная на языке C# («АКІМ+»).

Обе оболочки обладают схожим функционалом, но различными подходами в графическом проектировании моделей СФЗ.

4. Пример проведения экспериментов с проникновением

Вычислительные эксперименты с созданной имитационной моделью СФЗ (цифровым двойником охраняемого объекта) предполагают имитацию процесса реально возможного сценария проникновения нарушителя на территорию объекта. Моделирование начинается с задания цели проникновения нарушителя на объект: необходимо зафиксировать точку (зону) на территории объекта, куда стремится попасть нарушитель. В процессе такого эксперимента моделируются:

· движение нарушителя, его преодоление ИСО, воздействие на ТСО, осуществление преступной деятельности возле цели;

· работа ТСО;

· работа операторов службы безопасности;

· движение патрулей и групп реагирования, действующих в штатном режиме или по сигналу тревоги.

Один имитационный эксперимент позволяет получить данные о событиях в ходе испытания и его исход. Для получения оценок качества моделируемой СФЗ, как уже было сказано ранее, необходимо проведение множества экспериментов. Данные всех экспериментов складываются в статистику. Пример серии экспериментов над СФЗ можно увидеть на рис. 4, где зеленые линии – эксперимент завершен перехватом, а красные линии – нарушитель дошел до цели:

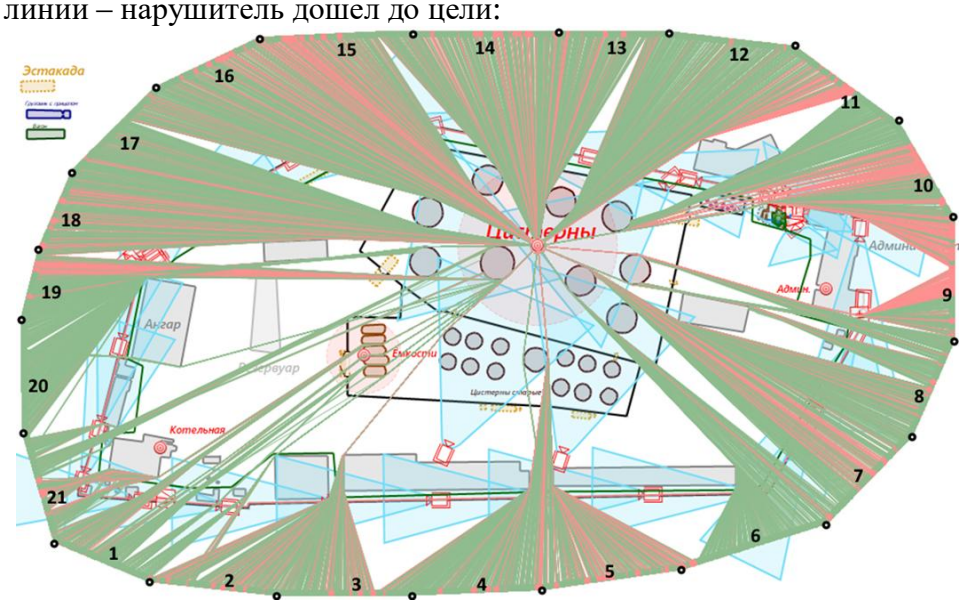

Рис. 4. Диаграмма траекторий проникновения по участкам периметра объекта

5. Результаты моделирования СФЗ

Результаты имитационного моделирования и оценки качества СФЗ в «АКИМ» представляются следующим образом;

· **вероятность обнаружения** ($P_{Обн.}$) нарушителя – общая оценка обнаруживающей способности для всей системы;

· **вероятность нейтрализации** ($P_{Нейтр.}$) нарушителя силами СБ – общая оценка нейтрализующей способности для всей СФЗ;

· **время сдерживания** ($T_{Сдерж.}$) нарушителя на ИСО – минимальное, среднее и максимальное время движения нарушителя до цели за всю историю экспериментов;

· **время выполнения процедуры нейтрализации** ($T_{Нейтр.}$) нарушителя с момента обнаружения – минимальное, среднее и максимальное время противодействия СБ в случаях успешного перехвата за всю историю экспериментов;

· **эффективность сдерживания** на ИСО – коэффициент отношения времени движения нарушителя к цели через существующие ИСО ко времени движения нарушителя к цели по тем же маршрутам с нулевой задержкой; позволяет определить эффективность сдерживания нарушителя на препятствиях – чем больше значение, тем выше эффективность, абсолютного предела нет; значения близкие к единице значат, что ИСО не справляется со своей задачей;

· **гистограмма вероятности обезвреживания по участкам периметра** СФЗ – оценка периметра СФЗ, разделенного на множество участков проникновения; позволяет определить самый слабый участок защиты объекта, а не усреднять оценку вероятностей для всей системы;

· **частота срабатывания элементов ТСО** – характеристика количества срабатываний тех или иных моделируемых ТСО за всю серию вычислительных экспериментов; позволяет определять эксплуатационную нагрузку на каждое устройство – выявляются элементы, не принимающие участие в экспериментах, которое может быть связано с неправильной установкой или избыточностью

структуры СФЗ.

Информация модели и результатах её исследования записывается в автоматически генерируемые отчеты, где указывается все оценки и промежуточные результаты. Результаты в отчетах представлены как в текстовой и табличной форме, так и в виде графической информации: диаграммы, гистограммы, лепестковые диаграммы вероятностей.

Скорость расчетов экспериментов зависит от сложности модели СФЗ и мощности компьютера, на котором производится расчет. Объект большой площади (несколько десятков квадратных километров) с длительной протяженностью ИСО, с большим количеством элементов ТСО (сотни элементов) и десятками сотрудников СБ может моделироваться со скорость порядка 330 экспериментов в минуту на процессоре AMD Ryzen 5 3600. Такая скорость достижима за счет возможности распараллеливания экспериментов по всем ядрам. Возможны и иные реализации оптимизации для распараллеленных расчетов.

Выводы

Описанный в статье подход имитационного моделирования и оценки качества СФЗ обеспечивает возможность анализа как уже существующей системы (или проекта), так и планируемой СФЗ на этапе её эскизного проектирования. Подход позволяет формирование детального технического задания, на основе графического чертежа, являющегося моделью планируемой СФЗ. Этим решается проблема переноса заявленных требований и качественных характеристик в фактическую реализацию СФЗ. Точность оценки может быть определена методом доверительных интервалов. Скорость вычислительных экспериментов без обращения к заранее известному сложному графу для поиска пути выше, чем у альтернативных алгоритмов, использующих поиск пути на сетке. Это позволяет провести большое количество имитационных экспериментов в короткий период.

Литература

1. **Тарасов А.Д.** Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: дис. на соиск. учен. степ. канд. тех. наук: 05.13.19: защищена 15.12.17 / Тарасов Андрей Дмитриевич. – Уфа, 2017. – 144 с.
2. **Dejan Čakija, Željko Ban, Marin Golub & Dino Čakija** (2020) Optimizing physical protection system using domain experienced exploration method, Automatika, 61:2, 207-218, DOI: 10.1080/00051144.2019.1698192.
3. **Степанов Б.П., Годовых А.В.** Основы проектирования систем физической защиты ядерных объектов: учебное пособие / Томский политехнический университет. – Томск: Изд-воТомского политехнического университета, 2009. – 118 с.
4. **Шанаев Г.Ф.** Системы защиты периметра / Г.Ф. Шанаев, А.В. Леус. – М.: Security Focus,. 2011. – 280 с.
5. **Петров И.Н.** Применение методов имитационного моделирования для оценки возможности осуществления актов незаконного вмешательства в деятельность гражданской авиации // Научный вестник ГосНИИ ГА. М.: ООО «Издательско-полиграфическое предприятие «ИНСОФТ», 2012. С. 126-129.
6. **Шарков И.К., Желудков Е.А.** Применимость эвристического алгоритма для задач поиска траекторий движения через систему физической защиты // SEIM-2019. СПб.: 2019. С. 34-40.