УДК 519.876.5
doi:10.18720/SPBPU/2/id24-498

Шарков Илья Кириллович,
ведущий разработчик, исследователь

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ДЛЯ ПЛАНИРОВАНИЯ СТРУКТУРЫ БЕЗОПАСНОСТИ НА УРОВНЕ ФАКТИЧЕСКИХ ЧЕРТЕЖЕЙ

Россия, Санкт-Петербург, ООО «Комплексные системы»,
shark2.1@mail.ru

Аннотация. В данной статье рассматривается подход получения оценки эффективности систем физической защиты (СФЗ) на этапе их планирования. Оценивать эффективность предлагается с помощью моделей СФЗ, не описываемых графом атак и защиты. Подход предполагает построение модели в виде чертежа с помощью заранее заданных классов элементов системы и применения агентных моделей атакующих и защищающихся сил. Необходимо это для получения грамотно спланированных сложных технических систем защиты, соответствующих предъявляемым к системе требованиям.

Ключевые слова: анализ эффективности, система физической защиты, имитационное моделирование, агентное моделирование, графическое проектирование, оценка качества, техническое задание.

Ilya K. Sharkov,
Lead Developer, Researcher

MODELING AND PERFORMANCE ANALYSIS OF PHYSICAL PROTECTION SYSTEMS FOR PLANNING A SECURITY STRUCTURE AT THE BLUEPRINTS LEVEL

LLC “Complex Systems”, St. Petersburg, Russia, shark2.1@mail.ru

Abstract. This article reviewed problems of assessment of the effectiveness of Physical Protection Systems (PPS) at the stage before its implementation in real life. It is proposed to evaluate effectiveness using PPS models that are not described by graph of attacks and defenses. The approach assumes construction of the model in the form of a drawing with predetermined classes of system elements and application of agent-based models of attackers and defending forces. This is necessary to obtain competently planned complex technical defense systems that meet the requirements of the system.

Keywords: performance analysis, physical protection system, simulation modeling, agent-based models, graphic engineering, quality evaluation, terms of reference.

Введение

Для обеспечения высокой эффективности функционирования систем физической защиты (СФЗ) крайне важно уметь определять их способность противостоять внешнему вмешательству – атаке (проникновение, переброс предмета, пролет БПЛА и др.) – и оценивать их эффективность. Эффективность выражается в характеристиках *обнаруживающей* ($Р_{Обн}$) и *нейтрализующей* ($Р_{Нейтр}$) способностей системы (основные функции) по отношению к атаке. Чаще такие характеристики выражаются вероятностями.

Оценку эффективности СФЗ можно получать различными способами:

– натурные испытания,

– экспертная оценка,

– оценка с помощью компьютерного моделирования.

Для подхода оценки эффективности с применением компьютерного моделирования постоянно формируются различные методики, которые отражены в актуальной научной литературе [1]. Однако, не все разрабатываемые методики позволяют решить задачу оценки систем, находящихся на ранней стадии проектирования, без упрощения её модели. Кроме того, остается не решенным вопрос, как напрямую перенести полученные характеристики в практическую реализацию без применения отдельных методик.

В данной статье затрагивается методика оценки эффективности систем с применением имитационного моделирования на базе агентного подхода и конечных автоматов. Эта методика позволяет формировать цифровой двойник в виде фактического проекта (чертежа) с параметрами устройств на основе паспортных характеристик и физических величин. Такой подход формирования модели позволяет напрямую переносить характеристики эффективности в проектируемую систему.

1. Планирование системы с глубокой проработкой её структуры

На данный момент среди описанных методик оценки эффективности систем физической защиты (СФЗ) нет таких, которые позволили бы напрямую перенести желаемые характеристики защищенности планируемой системы из модели в проект её реализации. Для этого нужно, чтобы модель и реальная схема системы совпадали с высокой точностью и без упрощений.

Перенос этих характеристик из оцениваемой модели в реальную планируемую систему затруднителен. В некоторых подходах предлагается использовать дополнительные методики для размещения и выбора элементов инженерно-технических средств охраны на основе декомпозиции мультиграфа атак оцениваемой модели [1], с помощью которого оценивалась СФЗ.

Связано это с тем, что методики оценки, в которых СФЗ описывается заранее заданным графом атак, предлагают упрощение для модели планируемой системы [2]. Без такого упрощения необходимо увеличивать количество возможных состояний системы, что приводит к усложнению

структуры графа. Упрощение модели позволяет описать систему не в виде её фактической структуры, а в виде узлов состояний, обобщающих целые блоки и подсистемы в один узел графа.

Из-за этого свойства системы в модели неизбежно искажаются. В результате, перенос характеристик эффективности, полученных на основе такой модели, носит рекомендательный характер.

Чтобы не упрощать модель, требуется сменить подход при её формировании. Самым близким и точным приближением к объективной реальности может быть фактическая схема (чертеж) системы, где содержатся все её базовые блоки с их физическими и техническими (паспортными) характеристиками. Такую модель можно создавать на основе заранее заданного чертежа. Примером такого подхода служит реализация [3], которая позволяет на основе BIM-проектов опять же упростить систему в граф атак.

Альтернативой будет применить подход, в котором модель СФЗ сразу формируется в виде реальной схемы из всех её базовых элементов, что значительно упрощает задачу. Для реализации такого варианта потребуется разработка специального графического языка моделирования, с помощью которого будет задаваться параметрическая модель в виде чертежа из элементарных блоков. Над таким цифровым двойником должны проводиться эксперименты с имитацией движения агентов нарушителя и охранников, а накопленная статистика результатов испытаний будет ложиться в основу оценок эффективности. При этом, с такой имитационной моделью можно исключить задание заранее заданного графа атак, а строить атаки на основе специально подобранных или разработанных алгоритмов.

Таким образом, возможно планирование системы с подходящими характеристиками эффективности, которые могут быть перенесены в реальную жизнь напрямую в виде схемы. Это помогает добиться соответствия требованиям [4], предъявляемым к системам физической защиты, и повысить качество технических заданий на их реализацию.

Такой подход реализован в комплексе экспертного моделирования «АКИМ» [16].

2. Базовые элементы СФЗ как система классов в структуре её модели

В общем представлении исследуемую СФЗ можно представить как модель из набора подсистем, которые могут быть разложены на составляющие элементы:

$$\Sigma Модель = \{ ИТСО, Атака, Цель, Внешние\ условия \}, \quad (1)$$

где *ИТСО* – структура инженерно-технических средств охраны, *СБ* – служба безопасности (охранники, операторы и т. д.), *Атака* – акт незаконного вмешательства в систему (проникающий нарушитель, переброс предмета, атака БПЛА), *Цель* – задача, преследуемая атакующим на

территории СФЗ, *Внешние условия* – погодные условия и иные внешние факторы, влияющие на защищенность системы.

Каждая из этих подсистем может быть представлена набором типовых классов базовых элементов (например, извещатели различных типов, видеокамеры, препятствия с различными параметрическими свойствами), внешних условий, подвижных агентов атаки и защиты. Эти классы будут применяться для элементов на схеме планируемой СФЗ, в которой не будет упрощения структуры.

Такой подход формирования модели позволит избежать упрощения системы и задавать её свойства с на основе паспортных характеристик реальных устройств, применяемых для схемы СФЗ.

Представление структуры таких классов базовых элементов и агентов с их связями можно увидеть в примере на рисунке 1.

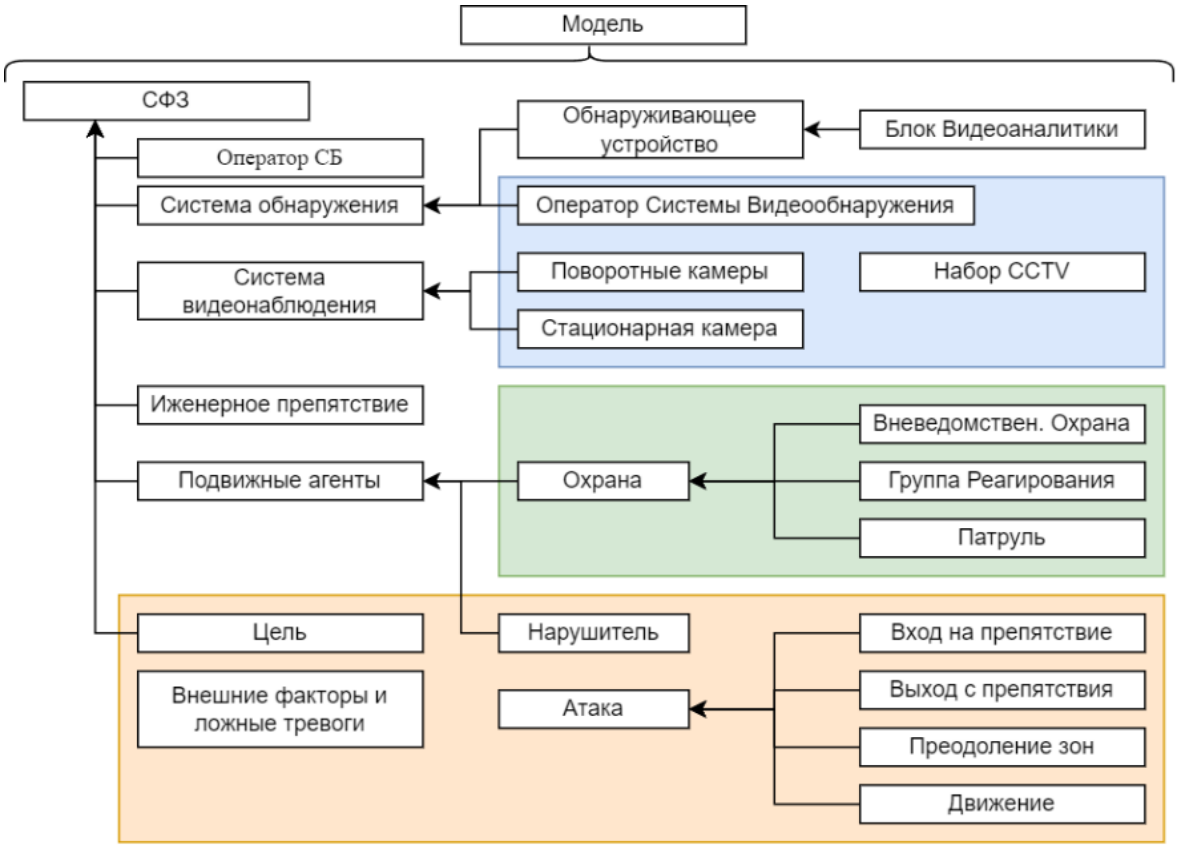

Рис. 1. Схема классов и их наследования

Такой подход реализован в ПО «АКИМ», модели элементов для которого разрабатывались в среде разработки многокомпонентных моделей сложных динамических систем AnyDynamics [5].

Модель СФЗ строится из описанных экземпляров базовых классов. В результате формируется план (2D и 3D), по которому будут двигаться модели агентов и охранников, имитируя реальные атаки и защиту. Классы элементов ИТСО содержат параметры, соответствующие техническим паспортам устройств. Благодаря этому возможно описывать их

функционирование и их геометрическую форму зон воздействия с привязкой к плану СФЗ, пример на рисунке 2.

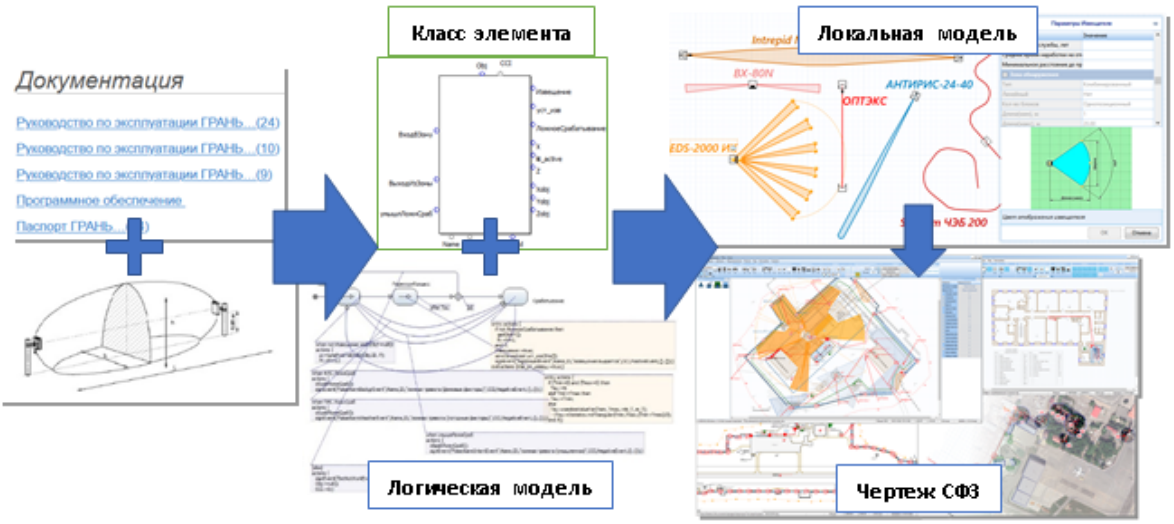

Рис. 2. Пример шагов задания элементов от паспортных данных до модели СФЗ в виде чертежа

3. Имитация движения нарушителя по плану СФЗ

Чтобы не описывать модель атаки на СФЗ с помощью заранее заданного графа, предлагается применять алгоритмы формирования событийно-управляемых траекторий (АСУТ) [6] и поиска путей «Polaris» [7]. 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 схему цифрового двойника СФЗ.

Для прокладки локального отрезка пути используется специально разработанный эвристический алгоритм поиска пути между двумя точками на плане без графа. Для построения каждого локального участка пути генерируется простейший граф видимости.

Алгоритм формирования событийно-управляемых траекторий (АСУТ) «расставляет» случайные события на локальном отрезке пути и возникает событийно-управляемая траектория, формируемая с помощью гибридных автоматов. Это позволяет автоматически строить динамические сценарии экспериментов и исключать необходимость привлечения эксперта на этапе подготовки модели СФЗ. Случайные события влияют на выбор агентом очередной достижимой точки (смена локального отрезка пути под воздействием событий), что вносит случайные изменения в сценарий.

Взаимодействие прокладчика пути и АСУТ можно представить в виде схемы на рисунке 3.

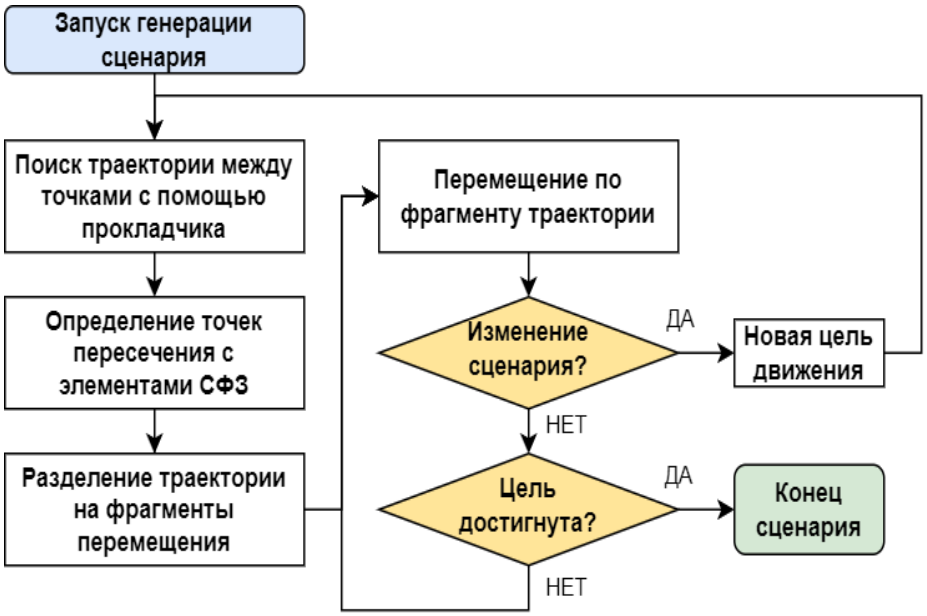

Рис. 3. Схема взаимодействия прокладчика пути и АСУТ для формирования динамически изменяемого сценария эксперимента

4. Отличия подхода от моделирования по заранее заданному графу

Объективное практическое сравнение для большинства методик анализа защищенности систем затруднено из-за отличающейся специфики (например, защита компьютерных систем и систем управления) или ввиду закрытости доступа к практическим реализациям (например, государственная или коммерческая тайна). Однако научные публикации методик позволяют провести как аналитическое сравнение, так и реализацию аналогичных моделей доступными способами.

Если аналитические различия могут быть очевидны по публикациям (подчеркиваются авторами), то различие результатов удается определить при интерпретации моделей. Для простоты сравнения разобьем модели систем для оценки эффективности их защищенности, описанные в различных подходах, на три основных типа [8]:

1) «одномерные» модели – модели атаки на систему, описанные детерминированной последовательностью вероятностных событий (сценарием) [9];

2) модели защиты на основе заранее заданных графов атак и реакций;

3) модели с имитацией движения атакующих и защищающих агентов по трехмерному плану.

Первые два типа обобщают в себе группы методик, в основе которых лежит моделирование систем, в которых новые события зависят только от предыдущего, но не от всех событий в системе.

Первый тип можно представить как расчет вероятности обнаружения атаки на систему и последующий расчет времени реакции системы (своевременность прибытия охраны к месту обнаружения).

Очевидно, что расчет вероятностей (2, 3, 4) опирается на экспертные исходные данные, а результат будет зависеть от общего качества и подробности каждой конкретной модели системы. В случае имитационной модели (предлагаемый подход) исходные данные – это характеристики инженерных и технических средств охраны (паспортные данные) и экспертные вероятности для физических и вероятностных характеристик агентов охраны и нарушителей (интервалы скорости движения, времени преодоления препятствий, вероятности реакции и выполнений определенных действий, и т. д.).

Предлагаемый подход позволяет с помощью параметрической модели не ограничиваться одними вербальными описаниями нарушителей [1] («случайный», «дилетант», «профессионал» и т. д.), применяемым в «одномерных» моделях и системах, описанных графом. В такой параметрической модели за вербальным описанием стоит множество физических и вероятностных характеристик. Такие характеристики могут быть взяты как из реальной статистики (если таковая есть и не засекречена), так и экспертным способом.

Таким образом, модель на реальной схеме объекта с имитацией движения агентов и сбором статистики может вовсе не зависеть от экспертных данных для элементов самой схемы и в меньшей степени для моделей службы безопасности и нарушителя.

Описанная в ранее (1) кортежная модель системы, включающая множество подсистем, позволяет оценивать характеристики на основе возникающих событий в ходе эксперимента: срабатывание датчиков, факт достижения цели или нейтрализация охраной, общее время движение до цели и до нейтрализации (зависят от скорости и задержек на препятствиях) и т. д. На основе собранной статистики формируется вероятностная оценка для тех или иных характеристик системы, например:

– вероятность обнаружения с помощью ТСО ($P_{обн}$);

– вероятность нейтрализации нарушителя агентами защиты ($P_{нейтр}$);

– уязвимые траектории (пути и координаты);

– время задержки нарушителя на ИСО (t) и т. д.

Такие характеристики подходят под рекомендации РБ-157-19.

Точность результатов зависит от количества проведенных испытаний над системой. Для того чтобы ограничить количество экспериментов N для формирования оценки с необходимой точностью, выбран подход с использованием доверительного интервала.

Второй тип упомянутых моделей с графом может быть представлен как расчет марковской цепи. В таком случае нет сложности для реализации простой модели СФЗ. Все узловые точки являются ТК на пути атаки к КЭ. При этом система может иметь одно состояние провала защиты (успешная атака).

Ключевые различия подходов для моделей СФЗ:

1) количество сценариев для одинаковых исходных условий:

1.1) У марковской цепи ограничено количество состояний графа, для которых может быть зарегистрирован исход эксперимента [10]. При увеличении количества состояний или переходов многократно увеличивается количество уравнений Колмогорова [11].

1.2) У предлагаемой имитационной модели нет прямого ограничения на количество сценариев и зависит от качества ГСЧ и прокладчика траекторий (каждый эксперимент может быть уникальным). Предлагаемый подход покрывает значительно большее количество сценариев, что позволяет повысить точность оценки. Оценка формируется на основе собранной статистики – чем больше экспериментов, тем она точнее. Для ограничения количества экспериментов можно применять метод доверительных интервалов с заданной надежностью.

2) ограничение для направлений возникновения атак и стартового состояния системы:

2.1) В случае с графами исходные условия привязаны к стартовому узлу (состоянию системы) и описывают варианты атак только оттуда.

2.2) В предлагаемом подходе стартовая позиция возникновения и направление атаки нарушителя может задаваться множеством точечных координат в пространстве схемы системы или областью, где случайным образом будет возникать нарушитель, а направление и варианты атак будут зависеть от количества целей проникновения на плане и возникающих во время атаки событий, влияющих на ход испытания.

3) возможности расчета параллельных атак:

3.1) Для марковских моделей такой расчёт затруднителен. Множество различных состояний системы экспоненциально увеличивается с ростом числа параллельных атак [12], а учитывая п. 1.1 лавинообразно увеличивается количество уравнений.

3.2) В предлагаемом подходе ограничение количества параллельных атак может быть связано только с ограничениями мощности вычислительной машины, на которой проводятся эксперименты. В настоящий момент с помощью предлагаемого подхода в комплексе «АКИМ» реализованы две параллельные атаки на систему по множеству различных направлений, и возможна доработка для реализации большего числа одновременных атак.

Очевидно, что модели второго типа требует упрощения структуры СФЗ до графа состояний её укрупненных блоков, что не подходит для адекватной оценки крупномасштабных сложно структурированных (реальных) систем, где есть множество уникальных вариантов воздействия на систему.

Однако если попытаться построить марковскую модель для примитивных структур, где реально учесть основные варианты сценариев атаки, то при сравнении с имитационной моделью предлагаемого подхода становится очевидным ещё одно различие: изменения физических масштабов схемы (карты) системы требуют переопределения значений всех вероятностей в матрице переходов, опираясь на личный опыт эксперта.

Сравнительный анализ таких моделей и результатов их расчета можно будет увидеть в планируемых публикациях автора.

К третьему типу моделей относится предлагаемый подход, подробнее описанный в других публикациях автора, с реализацией в ПО «АКИМ». Но кроме него существует подход с построением схемы последовательности действий нарушителя (СПДН) [13], который так же представляет из себя схему системы, расчерченную наложенной на него отредактированной сеткой (клеткой), преобразуемой далее в граф для любых доступных алгоритмов поиска пути. То есть всё сводится к анализу большого графа с упомянутыми ранее упрощениями и ограничениями.

Существенным недостатками СПДН являются: сложность задания графа (топологии объекта), которая не позволяет легко менять план и структуру СФЗ; ограничения алгоритмов поиска пути на графах, которые требуют значительной вычислительной мощности для крупномасштабных схем и значительного времени для расчета множество экспериментов с целью сбора статистики.

Во втором случае, проведен сравнительный анализ [7] известных прокладчиков и алгоритма Polaris, не использующего заранее заданные графы и применяемого в предлагаемом подходе вместе с АСУТ. Сравнения результатов работы применяемого в подходе алгоритма Polaris и алгоритма поиска пути JPS [13] проводилось по быстродействию расчета одной отдельной и тысяче параллельных траекторий для одинаковых топологических схем СФЗ, а также по длине найденного пути. Примеры результатов можно увидеть в таблице 1.

Таблица 1

Примеры результатов

Алгоритм	*T* генерации для 1 траектории, с	Длина пути, м	*T* параллельной генерации[1] для 10^3 траекторий, с
Схема СФЗ в виде лабиринта			
JPS	0,039	62,9	28,4
Polaris	0,176	60,2	48,8
Крупномасштабная хаотичная схема СФЗ			
JPS	0,33	1607	260,3
Polaris	0,29	1553	48,6

[1] Шесть потоков на ПК с процессором Intel i5-8400 и памятью 7,86 Гб.

5. Объективные и субъективные параметры модели при графическом проектировании

Планирование системы и анализ её уязвимости в виде приближенной к реальности схемы возможен с помощью графического конструктора. Такой конструктор должен позволять из базовых блоков СФЗ (реальных элементов), описанных модельными классами (см. п 2), описывать её структуру на локальном уровне. В результате этого получается схема (чертеж) реальной системы, которая и будет являться её математической моделью с подробностью, приближенной к жизни. Анализ этой модели подразумевает проведение имитационных экспериментов с участием атакующих и защищающихся агентов, в результате исходов которых формируется математическая статистика.

Исходными данными для каждого структурного элемента системы являются реальные рабочие параметры (вероятность срабатывания датчика, геометрическая зона обнаружения, правила действий охранников из их должностных инструкций) и графическая информация: координаты места установки устройства, габариты препятствия и так далее. Всё это можно назвать объективными данными.

При этом при графическом проектировании такой модели субъективные экспертные параметры относятся к выбору значений параметров, описывающих человеческую деятельность: диапазоны скоростей движения, времени выполнения действий и задержек на препятствиях и т. д. Некоторые из таких данных можно найти в научных публикациях [15].

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.

Заключение

В этой статье приведен краткий обзор проблематика планирования и оценки эффективности систем физической защиты на ранних этапах до их реализации, а также описана методика с применением имитационного моделирования на базе агентного подхода и конечных автоматов. Эта методика позволяет формировать цифровой двойник в виде фактического проекта (чертежа) с параметрами устройств на основе паспортных характеристик и физических величин. Такой подход формирования модели позволяет напрямую переносить характеристики эффективности в проектируемую систему.

В описанном подходе модель СФЗ не упрощается до графа, как это делается в других методиках, а описывается с учётом полноты структуры, важной для оценки. Атаки и защита имитируются движением агентных

моделей по карте без использования заданного графа атак и возможно динамическое изменение сценариев из-за вероятностных событий.

Список литературы

1. Костин В. Н. Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов: автореф. дис. … д-ра техн. наук: 05.13.01. – Оренбург: ОГУ, 2021.

2. Тарасов А. Д. Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: дис. … канд. техн. наук: 05.13.19: защищена 15.12.2017. – Уфа: УГАТУ, 2017. – 144 с.

3. Čakija D., Ban Ž., Golub M., Čakija D. Optimizing physical protection system using domain experienced exploration method // Automatika. Journal for Control, Measurement, Electronics, Computing and Communications. – 2020. – Vol. 61. – Iss. 2. – Pp. 207–218. – DOI:10.1080/00051144.2019.1698192.

4. РБ-157-19. Рекомендации по проведению оценки эффективности систем физической защиты объектов использования атомной энергии. – ФБУ «НТЦ ЯРБ», 2019.

5. Колесов Ю. Б., Сениченков Ю. Б. Объектно-ориентированное моделирование в среде Rand Model Designer 7. – М.: Изд. Проспект, 2016. – 256 с.

6. Шарков И. К., Сениченков Ю. Б., Колесов Ю. Б. Моделирование и оценка качества систем физической защиты на основе агентного подхода и алгоритма событийно-управляемых траекторий // Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021). Труды конференции (электронное издание), г. Санкт-Петербург, 20–22 октября 2021 г. – СПб.: АО «ЦТСС», 2021. – С. 503–510. – ISBN 978-5-905526-05-3.

7. 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.

8. Шанаев Г. Ф., Леус А. В. Системы защиты периметра. – М.: Security Focus, 2011. – 280 с.

9. Bennett H. A. EASI approach to physical security evaluation: Technical Report / Research Organization: Sandia Labs., Albuquerque, NM (USA). – January 1, 1977. – Report Numbers: SAND-76-0500; NUREG-760145; TRN: 77-010086. – U.S. Department of Energy, Office of Scientific and Technical Information, 1977.

10. Костин В. Н. Оценка эффективности физической защиты информации критически важных объектов на основе марковских цепей // Информационные технологии. – 2019. – Т. 25. – № 12. – С. 757–765.

11. Минаев В. А., Королев И. Д., Мухортов В. В. Марковские модели защиты информационных систем беспилотных робототехнических объектов // Интернет-журнал «Технологии техносферной безопасности» (http://ipb.mos.ru/ttb). – 2016. – Вып. № 6(70).

12. Горохова В. Ф. «Математические модели, численно-аналитические методы и программы для оценки эффективности и оптимизации систем защиты информации на основе поглощающих цепей Маркова»: автореф. дис. … канд. техн. наук: 05.13.18: защищена 20.09.2022. – Омск: ОмГТУ, 2022.

13. Боряринцев В. Н., Бражник А. Н., Зуев А. Г. Проблемы антитеррористма: категорирование и анализ уязвимости объектов. – СПб.: ЗАО «НПП «ИСТА-Системс», 2006.

14. Harabor D., Grastien A. The JPS pathfinding system. // 26th National Conference on Artificial Intelligence. AAAI. – 2012.

15. Keval H., Sasse A. “Not the usual suspects”: A study of factors reducing the effectiveness of CCTV // Security Journal. – 2010. – Vol. 23(2). – DOI: 10.1057/sj.2008.2.

16. Экспертный комплекс «АКИМ»: обоснование требований ТЗ к системе защиты периметра; оптимизация проектных решений; экспертиза проектов по существу [Электронный ресурс] // ООО «Пентакон»: сайт. – URL: https://www.cctv.ru/vebinar-ekspertnyij-kompleks-akim.html (дата обращения: 30.05.2024).