(19) Евразийское патентное ведомство

(11) 043326 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.05.15

(21) Номер заявки
201891899

(22) Дата подачи заявки
2018.08.23

(51) Int. Cl. ***G06F 17/50*** (2006.01)
G06Q 10/06 (2012.01)

(54) СПОСОБ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И АНАЛИЗА СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ И СИСТЕМ БЕЗОПАСНОСТИ В ЦЕЛОМ

(31) **2017133220**
(32) **2017.09.25**
(33) **RU**
(43) **2019.08.30**
(86) **PCT/RU2018/050102**
(87) **WO 2019/059816 2019.03.28**

(71)(73) Заявитель и патентовладелец:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "КОМПЛЕКСНЫЕ СИСТЕМЫ" (RU)

(72) Изобретатель:
Крылов Виктор Михайлович (RU)

(74) Представитель:
Котлов Д.В., Яшмолкина М.Л., Яремчук А.А. (RU)

(56) US-A1-20150106941
US-A1-20050080502
US-A1-20070016955

(57) Изобретение относится к области защиты объектов от несанкционированного проникновения, а именно к способам цифровых вычислений и обработки данных, специально предназначенным для проектирования и анализа систем физической защиты. Техническим результатом заявляемого изобретения является повышение эффективности проектирования и полноты анализа систем безопасности за счет комплексного подхода к моделированию максимально возможного количества факторов (элементов), влияющих на оценку эффективности защиты объектов от несанкционированного проникновения. При этом результат достигается путем математического моделирования без необходимости проведения натурных экспериментов на готовом объекте. В способе автоматизированного проектирования и анализа систем физической защиты и систем безопасности в целом формируют библиотеки динамических математических моделей технических средств охраны, инженерных средств охраны, нарушителей и службы безопасности, формируют модель территории охраняемого объекта, на территории охраняемого объекта формируют элементы технических средств охраны и инженерных средств охраны, настраивают динамическую математическую модель службы безопасности, формируют динамическую математическую модель угроз, в рамках которой настраивают динамические математические модели нарушителей, осуществляют моделирование, после чего формируют оценку уязвимости объекта.

043326 B1

043326 B1

Изобретение относится к области защиты объектов от несанкционированного проникновения, а именно к способам цифровых вычислений и обработки данных, специально предназначенным для проектирования и анализа систем физической защиты.

В описании использованы следующие термины и сокращения.

Динамическая математическая модель - математическая модель, которая дает описание возникновения действий, которые должны сменять друг друга в известной последовательности.

Средства защиты периметра (СЗП) - комплекс средств и методов по обеспечению физической защиты периметра от проникновения и обнаружения его нарушения. В СЗП входят системы видеонаблюдения, служба безопасности объекта, правила и регламенты работы её сотрудников, извещатели, оповещатели, препятствия, средства физической защиты (рвы, насыпи, ограждения, канавы, бетонные пилоны, колючая проволока и т.д.), системы сбора и обработки тревожных сигналов и множество других систем, направленных на обеспечение поставленной задачи по охране периметра.

Система безопасности объекта - это совокупность всех методов и средств, обеспечивающих поддержание безопасного состояния объекта внутри периметра, предотвращение, обнаружение и ликвидацию угроз жизни, здоровью, среде обитания, имуществу и информации, имеющая общие средства сбора и обработки информации и управления.

Системы физической защиты (СФЗ) - это совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту жизненно-важных интересов и ресурсов предприятия (объекта) от угроз, источниками которых являются злоумышленные (несанкционированные) физические воздействия физических лиц - нарушителей: террористов, преступников, экстремистов и т.д.

Комплексная система безопасности (КСБ) - это совокупность технических и программных средств поддержания безопасного состояния, предотвращения, обнаружения, противодействия и ликвидации комплекса угроз объекту обеспечения безопасности. Является составной частью СФЗ, но не полной.

Технические средства охраны (ТСО) - комплекс охранных технических средств. Находится в составе комплексов инженерно-технических средств охраны (КИТСО), предназначен для повышения эффективности охраны внешних рубежей объектов различного назначения. К ТСО относятся датчики, оповещатели, телекамеры системы видеонаблюдения (СВН), программные средства видеоаналитики (ВА) и т.д. ТСО напрямую относится к КСБ - является её структурной частью, описывающей технические средства.

Инженерные средства охраны (ИСО) - комплекс охранных инженерных средств, направленный на физическое сдерживание возникающих угроз. В состав ИСО входят ограждения, барьеры, рвы, противоподкопные фундаменты и иные физические препятствия, затрудняющие их незаконное преодоление.

Инженерно-технические средства охраны (ИТСО, комплекс ИТСО) - совокупность ТСО и ИСО в единой взаимодействующей системе.

Зона обслуживания датчика, зона обнаружения, зона чувствительности (ЗО) - зона, в которой датчик способен осуществлять детекцию вероятного нарушения. При появлении посторонних объектов или возмущающих воздействий в ЗО датчик способен с определенной вероятностью сформировать сигнал тревоги. Чем лучше датчик, тем достовернее и быстрее он дает тревожный сигнал.

Группа реагирования (ГР) - мобильная группа сотрудников службы безопасности объекта, которая выполняет нейтрализацию возникшей угрозы: перехват нарушителя, исследование зоны возникновения тревоги, физическое сдерживание нарушителей, охрана важных целей и т.д.

Патруль - группа сотрудников системы безопасности, занимающаяся цикличным патрулированием объекта, совершающие обход и проверку зон охраняемого объекта.

Оператор поста охраны (оператор ПО) - сотрудник (сотрудники) службы безопасности объекта, которые занимаются мониторингом систем оповещения на посту охраны. Оператор ПО может осуществлять идентификацию угрозы и принимать решение о возникновении тревоги: объявить тревогу или посчитать её ложной.

Оператор системы видеонаблюдения (оператор СВН) - сотрудник (сотрудники) службы безопасности объекта, которые просматривают территорию объекта через телекамеры (СВН). Могут осуществлять идентификацию угрозы, принимать решение о возникновении тревоги, отслеживать нарушителя через СВН, сообщать координаты нарушителя ГР для его нейтрализации.

Система видеонаблюдения (СВН) - это комплекс охранного оборудования, задачей которого является обеспечение постоянного визуального контроля над охватываемым системой видеонаблюдения пространством.

Видеоаналитика (ВА) - аппаратно-программное обеспечение или технология, использующие методы компьютерного зрения для автоматизированного сбора данных на основании анализа потокового видео (видеоанализа). В задачах систем охраны объекта: обнаружение, идентификация, слежение.

Нарушитель - человек, который незаконным образом проникает на охраняемую территорию объекта. Может быть случайным, дилетантом, подготовленным и т.д. Различные модели нарушителя описывают особенности его поведения и реакции на структуру КСБ.

API (англ. application programming interface - программный интерфейс приложения, интерфейс при-

кладного программирования) - набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах.

Program (Project) Evaluation and Review Technique (PERT) - метод оценки и анализа проектов, который используется в управлении проектами.

Для достижения целей обеспечения безопасности на охраняемом объекте необходимо решать следующий спектр задач.

Физическое воспрепятствование проникновению посторонних лиц на объект - задача по ограничению доступа на объект для посторонних лиц различными способами: предупреждающие знаки, ограждения, КПП и т.д. Позволяет избежать большинства случаев случайного или умышленного проникновения.

Максимально возможная задержка скорости проникновения нарушителя - задача различных средств защиты периметра по задержке скорости движения нарушителя по направлению к цели проникновения. Данная задача является одной из самых важнейших, так как от неё во многом зависит возможность перехвата злоумышленников. Чем больше время задержки на каждом элементе СФЗ, тем больше возможностей противодействия у всей системы в целом. Каждый элемент СФЗ способен противодействовать определенной совокупностью способов проникновению на охраняемый объект. Например, колючая проволока не спасет от тарана на машине, но бетонный забор может.

Обнаружение проникновения - задача, решаемая используемыми ТСО и службой безопасности объекта по фактическому обнаружению нарушителя на объекте. Задачами обнаружения занимаются извещатели (всевозможные датчики), телекамеры СВН с ВА, операторы СВН, патрули и т.д.

Идентификация - задача по определению угрозы, возникающей на объекте. Угроза может следовать из проникновения случайного нарушителя, неверного срабатывания датчиков на персонал, одиночного вора, террористической группы и т.д. Идентификация нарушителя и угрозы влияет на принятие решений и действий службы безопасности и ГР.

Выработка и принятие решения - задача по формированию выработки правильного решения о причинах возникновении тревоги на объекте. От принятого решения зависят последующие действия оператора поста охраны, группы реагирования, операторов СВН и т.д.

Доведение решения до исполнения - задача по фактической раздаче команд и распоряжений от поста охраны службы безопасности конечным исполнителям: техническим средствам, группе реагирования, патрулям и т.д. Правильность и своевременность исполнения команд зависят от множества факторов.

Предотвращение проникновения: задержание или иная нейтрализация угрозы - фундаментальная задача, от исполнения которой зависит реальный исход событий. В зависимости от качества исполнения всех предыдущих задач и реализации задачи предотвращения проникновения будут зависеть успешность задержания и защищенность охраняемого объекта.

В зависимости от качества реализации каждой задачи зависит формирование оценки уязвимости и защищенности объекта. Эту оценку можно получать различными способами: экспертной оценкой (субъективно), реальными экспериментами (нерационально, так как система уже построена), при помощи вычислительного эксперимента на этапе проектирования (заявляемый способ).

Наиболее близким аналогом заявляемого изобретения является техническое решение из патента RU 2219576, относящееся к способу проектирования системы комплексной безопасности объекта. В способе осуществляют размещение датчиков на территории объекта и формируют зону обнаружения для каждого датчика. Затем осуществляют моделирование, в рамках которого генерируют точки возникновения возмущающего события (появление нарушителя). При этом датчики реагируют или нет на возмущающее событие исходя из двух обстоятельств: первое - попадает или нет возмущающая точка в зону обнаружения датчика, и второе - в зависимости от вероятности срабатывания датчика. В заключение формируют результаты: вероятности обнаружения нарушителя по всей территории объекта.

Однако данное решение описывает выполнение задачи только частично, так как дается только статическая оценка работы системы датчиков. При этом не рассматривается природа происхождения воздействия (реальный нарушитель, погодные обстоятельства, ложная тревога или подобное), не описано взаимодействие датчиков с различными объектами, не описано взаимодействие гипотетических нарушителей с датчиками (попытка обойти видимый датчик, сломать и т.д.), не моделируются другие технические средства обнаружения (СВН, радиолокаторы и др.), не рассматривается вероятность обнаружения нарушителя сотрудниками службы безопасности, а так же не рассматриваются другие задачи. Оценка уязвимости и защищенности объекта, таким образом, полностью не может быть рассмотрена.

В патенте RU 2219576 описывается узкоспециализированная область по оцениванию качества функционирования сети датчиков, которые можно размещать на поле модели и менять в процессе изучения их зону обнаружения ("зоны обслуживания"). При этом учитывается, на каком объекте реализована данная сеть: комната, первый этаж, улица. Исследования созданного проекта производятся при помощи генерации псевдослучайных чисел для формирования возникновения тестирующих воздействий в произвольном месте в пространстве (в плоскости) модели. Это значит, что на территории объекта формируют плоские зоны обнаружения, в которых случайным образом появляются возмущающие воздействия. Та-

кое воздействие может появиться как в зонах чувствительности датчиков, так и за их пределами.

Таким образом, из списка задач, которые необходимо решить для обеспечения безопасности объекта и для формирования оценки защищенности объекта (оценки уязвимости объекта), в патенте RU 2219576 описан способ оценки только факта обнаружения нарушителя. При этом возникновение "возмущающего воздействия" может произойти не только на границе объекта, но и внутри него, что является в этом случае полным провалом службы безопасности, поскольку нарушитель обнаружен уже глубоко на территории объекта.

Техническая проблема, на решение которой направлено заявляемое изобретение, заключается в создании способа, обеспечивающего комплексное автоматизированное проектирование и анализ эффективности систем физической защиты и в целом системы безопасности, включающей не только технические средства, но и службу безопасности.

Техническим результатом заявляемого изобретения является повышение эффективности проектирования и полноты анализа систем безопасности за счёт комплексного подхода к моделированию максимально возможного количества факторов (элементов), влияющих на оценку эффективности защиты объектов от несанкционированного проникновения. При этом результат достигается путем математического моделирования без необходимости проведения натурных экспериментов на готовом объекте.

Указанный технический результат достигается за счёт того, что в способе автоматизированного проектирования и анализа систем физической защиты и систем безопасности в целом формируют библиотеки динамических математических моделей технических средств охраны, инженерных средств охраны, нарушителей и службы безопасности, формируют модель территории охраняемого объекта, на территории охраняемого объекта формируют элементы технических средств охраны и инженерных средств охраны, настраивают динамическую математическую модель службы безопасности, формируют динамическую математическую модель угроз, в рамках которой настраивают динамические математические модели нарушителей, осуществляют моделирование, после чего формируют оценку уязвимости объекта.

В способе после формирования оценки уязвимости объекта могут осуществлять доработку динамических математических моделей технических средств охраны, инженерных средств охраны и службы безопасности.

В способе могут осуществлять экспорт проекта плана объекта в элементы проектной документации.

В способе могут дополнительно формировать математические модели специфических областей и инфраструктуры.

В способе могут учитывать экспертные траектории и/или случайные траектории движения нарушителя и/или службы охраны.

В способе могут в качестве динамической математической модели технического средства охраны, инженерного средства охраны, нарушителя и службы безопасности использовать реально функционирующий элемент технического средства охраны, инженерного средства охраны, нарушителя и службы безопасности.

В отличие от точечной генерации воздействий на "поле зон обнаружения датчиков", используемой для получения статической картины обнаруживающей способности датчиков, как в наиболее близком аналоге, заявляемое изобретение предполагает полный комплекс исследования и оценки угроз, возникающих по различным причинам, причем исследования в динамике и во взаимодействии всех факторов друг с другом.

Заявляемое изобретение проиллюстрировано фиг. 1-44, на которых изображены:

фиг. 1 - траектория движения нарушителя;

фиг. 2 - интерфейс среды моделирования абстрактного гибридного класса "ФрагментТраектории";

фиг. 3 - интерфейс среды моделирования абстрактного гибридного класса "ФрагментПеремещение";

фиг. 4 - интерфейс среды моделирования локального класса "Перемещение";

фиг. 5 - интерфейс среды моделирования абстрактного гибридного класса "ФрагментПрепятствие";

фиг. 6 - представление траектории в виде последовательности состояний;

фиг. 7 - интерфейс среды моделирования абстрактного гибридного класса "Нарушитель";

фиг. 8 - интерфейс среды моделирования локального непрерывного класса "Динамика_i";

фиг. 9 - карта поведения класса "ГруппаРеагирования";

фиг. 10 - интерфейс среды моделирования абстрактного гибридного класса "Оператор";

фиг. 11 - карта поведения класса "Монитор";

фиг. 12 - интерфейс среды моделирования абстрактного гибридного класса "Извещатель";

фиг. 13 - интерфейс среды моделирования класса "Модель";

фиг. 14 - карта поведения класса "Модель";

фиг. 15 - интерфейс среды моделирования функции "нейтрализация";

фиг. 16 - окно создания нового проекта графического интерфейса пользователя;

фиг. 17 - окно настройки параметров модели графического интерфейса пользователя;

фиг. 18 - пример загруженного чертежа проекта "аэропорт";

фиг. 19 - план объекта;

фиг. 20 - графический интерфейс пользователя создания нового объекта;

фиг. 21 - графический интерфейс пользователя выставления настроек элемента;

фиг. 22-26 - графический интерфейс пользователя настройки элементов объекта;

фиг. 27 - графический интерфейс пользователя выбора модели нарушителя;

фиг. 28 - графический интерфейс пользователя процесса моделирования;

фиг. 29 - графический интерфейс пользователя окончания расчёта моделирования;

фиг. 30 - графический интерфейс пользователя, отображающий результат расчёта моделирования;

фиг. 31 - графический интерфейс пользователя, отображающий отчёт;

фиг. 32 - графический интерфейс пользователя с добавленным извещателем;

фиг. 33 - графический интерфейс пользователя, отображающий результат расчёта моделирования с добавленным извещателем;

фиг. 34 - графический интерфейс пользователя для учета случайных траекторий;

фиг. 35 - графический интерфейс пользователя построения большого периметра проникновения;

фиг. 36 - графический интерфейс пользователя большого периметра проникновения по секторам;

фиг. 37 - графический интерфейс пользователя моделирования большого периметра проникновения по секторам;

фиг. 38 - графический интерфейс пользователя, отображающий результат расчёта моделирования более 2 тысяч испытаний;

фиг. 39 - графический интерфейс пользователя, отображающий результат расчёта моделирования более 5 тысяч испытаний;

фиг. 40 - графический интерфейс пользователя, отображающий траектории проникновения;

фиг. 41 - графический интерфейс пользователя доработки объекта;

фиг. 42 - графический интерфейс пользователя, отображающий результат расчёта моделирования более 13 тысяч испытаний для доработанного объекта;

фиг. 43 - графический интерфейс пользователя, отображающий результат расчёта моделирования более 14 тысяч испытаний для доработанного объекта;

фиг. 44 - графический интерфейс пользователя отдельного редактора по настройке моделей элементов системы.

Способ осуществляют следующим образом.

Сначала проводят подготовительный этап, на котором формируют библиотеки динамических математических моделей различных ТСО (не только датчиков), ИСО, специфических областей, инфраструктуры, моделей нарушителей и т.д.

Затем осуществляют этап формирования территории охраняемого объекта в виде чертежа или плана при помощи доступных элементов проектирования: оригинальный чертеж, библиотечные элементы специфических областей и инфраструктуры.

Этап формирования на территории охраняемого объекта элементов ИСО подразумевает размещение ограждений, препятствий и т.д. На этапе формирования на территории охраняемого объекта охранной обнаруживающей системы располагают извещатели различных видов и назначения (датчики) на ограждениях, под землей, над землей с навеса и т.д. и телекамеры различных видов (поворотные, стационарные, с системой ВА или без).

Затем формируют системы оповещения и предупреждения: громкоговорители, прожекторы, знаки.

На этапе формирования структуры службы безопасности объекта осуществляют настройку моделей: оператор ПО; операторы СВН; ГР, их места расположения и приоритетные траектории движения до гипотетических целей проникновения; патрули и их траектории патрулирования.

На этапе формирования модели угроз осуществляют настройку моделей нарушителя, экспертных траекторий проникновения, областей и зон внешнего проникновения (возникновение нарушителя в случайно выбранной области за пределами объекта), областей и зоны внутреннего проникновения (возникновения внутреннего нарушителя в случайной выбранной области в зоне возникновения) и создают цели интереса и проникновения, т.е. места, куда могут стремиться нарушители.

На этапе моделирования осуществляют динамическое моделирование различных моделей движения различных моделей нарушителей по экспертным или случайным траекториям проникновения; исследование работы системы обнаружения; исследование задерживающей способности СЗП; исследование вероятности успешного задержания нарушителя до его достижения цели; формирование статистических данных по множеству экспериментов.

На этапе автоматизированного формирования и анализа оценки уязвимости объекта формируют оценку уязвимости объекта по различным критериям на основе полученных статистических данных, проводят анализ полученных оценок и составляют рекомендации.

Затем осуществляют исправления и доработки плана СФЗ и, в частности, СЗП на территории объекта на основе результатов оценки и рекомендаций анализа. Этот этап повторяют необходимое количество раз до момента создания удовлетворяющего всем требованиям проекта по защите объекта.

После чего следует этап принятия итогового проекта для создания проектной документации.

На этапе экспорта проекта плана объекта в элементы проектной документации готовят различные

чертежи плана объекта с нанесением необходимых элементов (ИСО, ТСО и т.д. вместе или по раздельности) и формируют спецификации использованных элементов для проектной документации.

Данный процесс может быть цикличным и иметь несколько вариантов решения.

Программный комплекс, реализованный с помощью заявляемого способа, состоит из двух независимо запускающихся программ: среды проектирования СФЗ и моделирования проникновений и редактора библиотек элементов.

В среду моделирования можно загрузить чертеж объекта в формате .dxf из AutoCAD. Этот чертеж является картой объекта, на котором как на рабочем поле можно чертить или размещать из библиотеки элементы ИСО, ТСО, инфраструктуру и т.д. Также на этом плане можно размещать пользовательские (экспертные) траектории проникновения нарушителей, зону возникновения нарушителей и т.д. Путем применения различных комбинаций элементов СФЗ (размещение ограждений разных типов, формирование рубежей охраны, расстановка камер и извещателей, т.п.) можно получить уникальную структуру на объекте. Эту структуру можно подвергнуть множеству вычислительных экспериментов на предмет изучения проникновения злоумышленника на территорию объекта в указанные точки. Все вычислительные эксперименты осуществляют внутри среды с использованием программного блока математического моделирования. Результаты моделирования выводят в виде визуализации движения нарушителя по карте объекта и записывают в программный лог событий.

Вычислительные эксперименты могут происходить по нескольким критериям и условиям: проникновения по экспертной траектории, проникновения с выбранной зоны периметра возникновения нарушителей, проникновения со всех направлений периметра возникновения нарушителей. Результаты всех экспериментов записывают в файл-историю. Выбранные интересующие эксперименты можно воспроизвести.

Результаты каждой серии вычислительных экспериментов выводят в файл-отчет с подробным анализом. На основе полученных результатов формируют оценки: оценка вероятности своевременной реакции ТСО, оценка задержки нарушителя при помощи ИСО, оценка вероятности перехвата нарушителя службой безопасности объекта. В зависимости от выбранного критерия исследования в отчет также могут выводиться гистограммы вероятности проникновения со всех участков периметра возникновения нарушителей.

Все элементы, размещенные на карте объекта в среде, используют в процессе вычислительных экспериментов и влияют на конечный результат. Элементы можно создавать на плане с нуля, например, чертить и задавать их параметры, а также можно использовать готовые элементы из библиотек и размещать их на плане. При этом сохраняется возможность изменения параметров, формы зоны обнаружения датчиков, их расположения.

Формировать библиотеку элементов помогает редактор библиотек элементов. В нем существует несколько категорий элементов: ТСО, ИСО, инфраструктура, нарушители и т.д. В каждой категории можно создать элемент с заданными пользователем физическими, геометрическими, вероятностными и логическими параметрами. Таким образом, формируется база данных часто используемых элементов с уникальными наборами параметров: различные типы телекамер, модели извещателей, виды ограждений.

Каждый элемент, создаваемый в базе данных, имеет свой собственный набор параметров. Для каждой категории элементов наборы параметров различаются. Таким образом, например, ограждение имеет временные характеристики преодоления, коэффициент прозрачности, свойства тараноустойчивости и т.д.

Примеры конкретной реализации.

В качестве среды моделирования использован программный продукт Rand Model Designer.

Предполагали одновременное проникновение только одного нарушителя типа "злоумышленник с единственной конкретной целью". В этом случае каждый запуск модели начинается в момент появления нарушителя на периметре и завершается в момент нейтрализации нарушителя или достижения им цели проникновения.

Для моделирования нарушителя необходимо было принять условие, что он может двигаться либо по заведомо известной траектории (экспертная траектория, проложенная пользователем), либо по наикратчайшей траектории из случайной точки появления по направлению к цели с условием огибания непреодолимых препятствий. При движении по такой случайной траектории и в случае попадания на экспертную траекторию нарушитель продолжает движение по ней.

Моделирование СФЗ проводилось в двух режимах: режим визуализации (режим "тренажера") и режим расчета показателей эффективности СФЗ.

В режиме визуализации все перемещения нарушителя и группы реагирования, а также возникающие в модели дискретные события (появление сигнала тревоги и т.п.) непрерывно отображаются на плане СФЗ с помощью визуального редактора. Есть также возможность интерактивного вмешательства пользователя в работу модели. Результатом моделирования в этом режиме является субъективная оценка пользователем правильности построения и эффективности исследуемого варианта СФЗ.

В режиме расчета показателей эффективности СФЗ проводится вычислительный стохастический эксперимент, в котором по методу Монте-Карло путем многократных прогонов модели определяется

доверительный интервал [p_{min}, p_{max}]. в котором с вероятностью P находится значение величины p - вероятности успешной работы (эффективности) исследуемой СФЗ. Проведя вычисления в данном режиме для различных значений параметров СФЗ, можно получить зависимости эффективности СФЗ от значений параметров ее элементов. Предполагается также возможность автоматического построения параметрических зависимостей, а также оценка чувствительности эффективности СФЗ к значениям параметров.

Имитационная модель включает в себя как минимум четыре параллельных процесса, независимо развивающихся в модельном времени и взаимодействующих между собой: модель действий нарушителя, модель действий оператора, модель действий монитора (оператора, циклически просматривающего картинки камер), модель действий группы реагирования.

Кроме того, для каждого элемента СФЗ, используемого в данном прогоне и обладающего собственной функциональностью, например извещатель с переходным процессом выработки сигнала тревоги, запускается свой независимый процесс, развивающийся во времени.

Модель действий нарушителя.

Траектория движения нарушителя задается ломаной линией. Движение нарушителя завершается в следующих случаях: если нарушитель достигает цели - конечной точки траектории, если нарушителя перехватывает группа реагирования. Принято, что успешный перехват происходит при сближении нарушителя и группы реагирования на расстояние, меньшее заданного R.

Все точки траектории движения, соединяющие её в ломаную линию, являются точками смены направления движения или, если находятся на отрезке прямой линии, являются точкой пересечения границы особой области. Под точкой пересечения границы особой области подразумеваются: вхождение и выход из зоны чувствительности извещателя или камеры, начало и окончание пересечения препятствия, пересечение границы участков местности с ограничениями скорости и достижение цели следования.

Траектория движения нарушителя (фиг. 1) содержит 14 особых точек: 0 - начало траектории, 14 - конец траектории (достижение цели), точки 1 и 2 - точки входа и выхода из зоны чувствительности линейного извещателя, точки 4 и 5 - точки начала и конца преодоления ограждения, точки 6, 8 и 11 - точки смены направления движения, точки 9 и 10 - точки перехода с одного участка на другой. Таким образом, траектория движения состоит из фрагментов, которые бывают двух типов: фрагменты, где осуществляется передвижение, и фрагменты, где осуществляется пересечение препятствий или различных зон.

При движении по фрагменту траектории, который предполагает только перемещение, осуществляется движение нарушителя с постоянной скоростью. Скорость определяется случайным выбором в диапазоне от минимальной до максимальной скорости, допустимой для данного участка передвижения. Скорость перемещения ограничивается параметром максимальной допустимой скорости для нарушителя. Конкретное значение скорости разыгрывается в начальной точке фрагмента по методу PERT (определение длительности работ по минимальной и максимальной экспертной оценке). Этот метод предполагает использование бета-распределения с относительной модой 0,4.

Фрагменту траектории "вообще" устанавливают абстрактный гибридный класс "ФрагментТраектории" (фиг. 2).

Выходы X и Y содержат значения текущих координат объекта, начальные и конечные значения которых задают соответствующими параметрами. В карте поведения заданы три состояния, соответствующие начальной особой точке, отрезку и конечной особой точке фрагмента траектории.

Затем определяют класс "ФрагментПеремещение" - потомок класса "ФрагментТраектории" (фиг. 3). В этом классе заданы дополнительные параметры Vmin и Vmax - минимальная и максимальная скорость перемещения, добавлены некоторые внутренние переменные и переопределена карта поведения. Во входных действиях состояния "НачТочка" разыгрывается случайное значение скорости перемещения V и вычисляется время перемещения T. Состоянию "Движение" приписывают непрерывную деятельность, задаваемую локальным классом "Перемещение" (фиг. 4). Таким образом, в течение интервала времени T, пока состояние "Движение" является текущим, координаты X и Y объекта непрерывно изменяются в соответствии с уравнениями, показанными на фиг. 4.

Перемещению по различным участкам местности соответствуют различные значения параметров Vmin и Vmax.

Определяют класс "ФрагментПрепятствие" - потомок класса "ФрагментТраектории" (фиг. 5). В этом классе заданы дополнительные параметры Tmin и Tmax - минимальное и максимальное время преодоления препятствия, добавлены некоторые внутренние переменные и переопределена карта поведения. Во входных действиях состояния "НачТочка" разыгрывается случайное значение времени преодоления препятствия T. Предполагается, что преодоление препятствия - это неделимый акт, и по истечении времени T текущие координаты X и Y скачком изменяются во входных действиях состояния "КонТочка" - принимают конечные значения.

Различным видам препятствий (ограждение, ров и т.д.) соответствуют различные значения параметров Tmin и Tmax.

Таким образом, траектория движения в целом может моделироваться как последовательность вы-

полнения моделей фрагментов траектории. Наиболее простым решением является представление фрагментов траектории отдельными состояниями карты поведения, которым в качестве локальной деятельности приписаны экземпляры соответствующих классов (фиг. 6).

Однако в этом случае для каждой конкретной траектории потребуется генерация новой конкретной выполняемой модели, что приведет к значительной сложности модуля моделирования и снижению производительности. Более эффективным решением является динамическое создание объектов и связей, необходимых для моделирования конкретной траектории.

На фиг. 7 показан класс "Нарушитель". В динамическом массиве TR находятся ссылки на объекты - потомки класса "ФрагментТраектории". Эти объекты - экземпляры классов "ФрагментПеремещение" или "ФрагментПрепятствие" - добавляют в массив с помощью видимых извне процедур в начальной точке прогона модели.

Движение по траектории моделируют следующим образом. Из массива TR выбирают в рабочий указатель TF текущий фрагмент траектории и на него посылают сигнал "Start", который запускают функционирование соответствующего объекта (фиг. 2). Переход к следующему фрагменту происходит по завершении работы текущего - карта поведения объекта TF достигает конечного состояния.

Непрерывная локальная деятельность "Динамика_i" обеспечивает постоянное вычисление текущих координат X и Y (фиг. 8). Движение по траектории может быть прервано в случае нейтрализации нарушителя. Это событие вырабатывается в карте поведения модели в целом.

Модель действий группы реагирования.

Под группой реагирования подразумевается мобильная группа охранников, которая выдвигается по сигналу тревоги для нейтрализации причины её возникновения, в данном случае, нарушителя. В первом приближении тактика действий группы реагирования сводится к выдвижению по заданной траектории к желаемой цели проникновения нарушителя.

Получив сигнал тревоги от диспетчера (оператор службы безопасности на объекте), группа реагирования с определенной задержкой, задаваемой минимальным и максимальным значениями, начинает движение по контрольной траектории. Движение по траектории моделируют аналогично движению нарушителя (фиг. 9). При сближении группы реагирования и нарушителя на расстояние прямой видимости группа реагирования прекращает движение по программной траектории и начинает осуществлять перехват нарушителя по методу, когда вектор скорости перехватчика всегда направлен на нарушителя.

Модель действий оператора.

Под оператором подразумевается диспетчер службы безопасности на объекте, который следит за датчиками СФЗ на пульте управления. Также он может осуществлять осмотр территории через видеокамеры и отслеживать перемещение нарушителя.

В данном случае моделью описана упрощенная последовательность действий. Получив сигнал тревоги от какого-либо извещателя (на фиг. 1 это сигнал от линейного извещателя при движении нарушителя между точками 1 и 2), диспетчер выполняет следующие действия: определяет нужный участок периметра и переключает на монитор изображение с нужной телекамеры; с помощью телекамеры осматривает участок (для поворотных камер осуществляется поворот); производит оценку угрозы; в случае определения угрозы подает сигнал тревоги группе реагирования.

Все действия диспетчера занимают некоторое время, задаваемое минимальным и максимальным значениями. Для оценки угрозы задают вероятность P принятия верного решения (фиг. 10).

Модель монитора.

Монитор - это специальный оператор, который циклически просматривает изображения, поступающие со всех камер, и при обнаружении нарушителя в зоне камеры выдает сигнал извещения, аналогичный сигналу извещателей (фиг. 11). Распознавание нарушителя происходит с некоторой вероятностью.

Модель извещателя.

Под извещателем подразумеваются элементы технических средств охраны, которые способны обнаруживать нарушение их зоны чувствительности нарушителем. Извещатели бывают различных видов и типов, однако общая концепция их действия следующая: при возникновении значительных возмущений в зоне чувствительности извещателя (вибрация для виброчувствительных, изменения электромагнитного поля для емкостных, физическое препятствие для оптического света для оптических и т.д.) устройство генерирует сигнал тревоги, который передается на пульт охраны или в систему анализа и обработки сигналов тревоги.

В модели это реализовано следующим способом: при появлении объекта в зоне чувствительности после некоторой задержки τ вырабатывается с вероятностью P потенциальный сигнал извещения. Задержка τ распределена по треугольному закону. Сигнал снимают после выхода объекта из зоны чувствительности (фиг. 12), однако факт возникновения тревоги фиксируют в общей модели системы.

Модель в целом.

Модель в целом (класс "Модель") содержит как минимум три статических объекта: экземпляры классов "Нарушитель", "Диспетчер" и "ГруппаРеагирования" и необходимые объекты: модели извещате-

лей, камер наблюдения и т.д. (фиг. 13). Карта поведения класса "Модель" отслеживает варианты завершения прогона модели (фиг. 14). Задание функции "нейтрализация" показаны на фиг. 15.

Для реализации имитационного моделирования формируют требуемую программную оболочку, в которой задают условия расположения элементов СФЗ, выставляют параметры для элементов СФЗ, обозначают траектории движения для моделей нарушителя и группы реагирования, а также выставляют необходимые параметры для моделей оператора и монитора.

Модель СФЗ разрабатывают вручную с помощью RMD 7 Professional и помещают в программную оболочку как встраиваемая модель - model.dll.

Модель СФЗ включает в себя определения стандартных классов и экземпляры объектов, имитирующих нарушителя, диспетчера, группу реагирования. В состав оболочки входит модуль моделирования: объект класса "p_Model" - потомок имеющегося класса "vm_Model", скрывающий низкоуровневый интерфейс работы со встраиваемой моделью на уровне API.

Предварительно оболочка передает в модуль моделирования информацию о траекториях движения нарушителя и группы реагирования. На основе этой информации модуль моделирования путем вызова соответствующих "public"-методов существующих объектов создает во встраиваемой модели необходимые дополнительные динамические объекты и связи.

В режиме визуального моделирования модуль моделирования продвигает модельное время на заданный шаг или до ближайшего дискретного события и возвращает значения текущих координат нарушителя и группы реагирования, а также информацию о дискретных событиях.

В режиме расчета стохастических показателей модуль моделирования самостоятельно проводит стохастический вычислительный эксперимент и возвращает готовые результаты.

На фиг. 16 изображено окно создания нового проекта, где можно загрузить чертеж в общеизвестных форматах, например DXF.

На фиг. 17 показано окно настройки параметров модели, где указывают глобальные настройки моделей, например, временные интервалы и вероятности. Непосредственно при самой подготовке модели можно ввести больше параметров и конкретизаций. Вкладка журнал - фактическая запись хода экспериментов в виде "журнала событий". У этого режима есть анимация экспериментов и фильтры выводимой информации, которые позволяют отсеять все ложные тревоги или удачные перехваты нарушителя.

Создают объект с инфраструктурой, преследуемыми на нем целями и выполняемыми задачами согласно плану (фиг. 19). Для этого создают новый проект, формируют чертеж из инженерных средств охраны: ограждения, здания, ворота и т.д. (фиг. 20). При создании каждого элемента выставляют особые настройки, подключают интересующую модель, например параметры ограждения, извещателей, камеры и т.д. (фиг. 21). Затем усложняют инфраструктуру, ИСО и ТСО объекта, выставляют цель проникновения (фиг. 22), устанавливают препятствия (шлагбаум) (фиг. 23), расставляют и настраивают извещатели, в данном случае оптико-электронный датчик) (фиг. 24-25). Зоны обнаружения датчиков пересекают крестнакрест, чтобы исключить слепую зону - зону сниженной чувствительности возле приемников и передатчиков. Зона обнаружения датчиков получается объемная, т.е. если приблизить план, то будет видно полосу чувствительности. Готовят проект к моделированию, для чего создают экспертную траекторию проникновения нарушителя (фиг. 26), т.е. ту траекторию, которую "рисует проектировщик", основываясь на своем опыте и догадках, и проводят её исследование с участием группы реагирования. Выбирают модель нарушителя (фиг. 27). Осуществляют процесс моделирования проникновения нарушителя по экспертной траектории (фиг. 28). Результат серии экспериментов над траекторией по вероятности проникновения, т.е. достижение вероятности, попадающей в интервал доверительной, показан на фиг. 29. Графический интерфейс пользователя предлагает возможность продолжить экспериментирование или остановить. Результат исследования экспертной траектории показал вероятность перехвата почти 0,7, что достаточно мало (фиг. 30). Результат представляют в виде отчёта (фиг. 31). Исследуют ту же траекторию, но теперь добавляют виброчувствительный извещатель на ограждение в левый нижний угол (фиг. 32) и отображают результат этого исследования (фиг. 33). Результат превышает 0,9 вероятности перехвата, что намного лучше предыдущего исследования с меньшим количеством датчиков. Исследуют этот же участок, но только со случайными траекториями из этой области (фиг. 34). Для этого формируют два участка - периметр проникновения, где создают нарушителей случайным образом. С этого периметра они начинают свое движение по направлению к цели с преодолением препятствий и обходом зданий. В целом со всего участка при 1000 испытаний вероятность перехвата составляет 0,88, что несколько ниже предыдущего результата. Очевидно, что данный результат связан со слабой защитой извещателями области у внешних ворот и при преодолении внутренних ворот, так как большая часть "красных" траекторий идут через этот участок. Красные траектории отображают неудачное задержание, нарушитель прошел к цели. Строят большой периметр проникновения с множеством секторов вокруг объекта (фиг. 35). Исследуют большой периметр по секторам (фиг. 36) и осуществляют моделирование (фиг. 37). На фиг. 38 показан результат более 2 тысяч испытаний. Сектора 12-23 и 26-42 не защищены абсолютно, так как нарушителей не удается обнаружить или вовремя перехватить. На фиг. 39 показан результат более 5 тысяч испытаний. Таким образом, начинает строиться гистограмма успешных перехватов. Нарушители, которые идут через пост охраны, часто перехватываются, так как выставлена настройка перехвата нарушителей в

радиусе 50 м от сотрудников поста охраны. В данном случае между ними и нарушителем находится стена здания с коэффициентом прозрачности 0,7 (наличие окон и звуковой проницаемости), в связи с чем они видят или слышат нарушителя. На фиг. 40 показаны траектории проникновения.

Программное обеспечение позволяет генерировать файл отчета.

Так как такой объект не удовлетворителен по количеству "дыр" в системе охраны, необходимо его доработать. Для этого используют различные виды камер и систем обнаружения, оповещения, разные извещатели с разными способами обнаружения, зонами обнаружения и т.д. (фиг. 41). Результат исследования такого объекта - более 13 тысяч испытаний показан на фиг. 42, а результат свыше 14 тысяч испытаний - на фиг. 43, т.е. чем выше число испытаний, тем точнее результат. Рано или поздно значения вероятностей будут меняться уже в десятитысячных долях и т.д.

Расчет производился чуть менее 2 ч на персональном компьютере пользователя. Из него видно, что хуже всего защищены участки 41 и 42. На основе этого можно принять меры к корректировке проекта. Идеальный результат - более ровная гистограмма с наибольшим числом успешных перехватов на участке 25. Однако абсолютный максимум по всему периметру недостижим с усложнением модели и приближением её к реалистичности, потому желательные результаты - более 98-99%.

Модели извещателей, камер, ограждений, нарушителей, специфических областей и т.д. можно осуществлять в отдельном редакторе. Формирование плана охраняемого объекта можно осуществлять поверх загруженных чертежей. При этом существует возможность привязки линий, узлов и координат к элементам на самом чертеже, что облегчает работу при подготовке чертежа на экспорт. Впоследствии на основе этого чертежа уже будет доведена основная конструкторская документация по объекту. Также среда моделирования способна выдавать списки для спецификации.

Таким образом, заявляемый способ реализован в программном продукте, который является САПР с применением технологии проведения вычислительных экспериментов для оценивания проектируемой СФЗ охраняемых объектов и анализа уязвимости. В отличие от существующих в настоящий момент других программных решений, данный программный комплекс позволяет формировать не только оценку защищенности объекта по критерию фактического перехвата злоумышленника, но и обладает следующими преимуществами. Позволяет оценивать работу построенной СФЗ на предмет задерживающей (противодействие проникновению) способности со стороны инженерных средств охраны, на предмет обнаруживающей (достоверное и своевременное обнаружение) способности технических средств охраны. Позволяет производить наглядное проектирование СФЗ на карте объекта, формировать материалы для включения их в проектную документацию, изменять и настраивать структуру СФЗ для поиска наиболее оптимальной комбинации в отношении стоимости системы и её эффективности. Позволяет формировать свои собственные библиотеки элементов СФЗ, моделей нарушителей и группы реагирования (службы безопасности), а также сформировать обучающий программно-аппаратный тренажерный комплекс для обучения специалистов в сфере комплексных систем безопасности, обучения работников службы безопасности на конкретных объектах. Таким образом, осуществляется расширение функциональных возможностей программно-аппаратного комплекса.

В случае, если существует возможность, вместо моделей элементов технического средства охраны, инженерного средства охраны, нарушителя и службы безопасности могут использоваться конкретные реально функционирующие элементы технических средств охраны, инженерных средств охраны, а также реальные действия нарушителя и службы безопасности.

Приведённые примеры являются частными случаями и не исчерпывают всех возможных реализаций заявляемого изобретения.

Заявляемое изобретение может быть реализовано с помощью известных устройств и программных продуктов, реализованных, например, с помощью API. Все данные, передаваемые между пользовательскими компьютерными устройствами, сервером и базой данных, могут быть реализованы с помощью известных сетей связи на базе протоколов, известных специалисту в данной области техники.

Специалисту в данной области техники должно быть понятно, что различные вариации заявляемой системы не изменяют сущность изобретения, а лишь определяют его конкретные воплощения и применения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ автоматизированного проектирования и анализа систем физической защиты (СФЗ) и систем безопасности в целом, характеризующийся тем, что формируют библиотеки динамических математических моделей технических средств охраны, инженерных средств охраны, нарушителей и службы безопасности, формируют базу данных часто используемых элементов СФЗ с уникальными наборами параметров, формируют модель территории охраняемого объекта, на территории охраняемого объекта формируют элементы технических средств охраны и инженерных средств охраны, формируют и настраивают динамические математические модели структур службы безопасности охраняемого объекта, формируют динамическую математическую модель угроз, в рамках которой настраивают динамические математические модели нарушителей, экспертных траекторий проникновения, областей и зон внешнего

проникновения, областей и зон внутреннего проникновения и создают цели интереса и проникновения, осуществляют моделирование, причем на этапе имитационного моделирования осуществляют по меньшей мере динамическое моделирование различных моделей движения различных моделей нарушителей по экспертным или случайным траекториям проникновения, исследование работы системы обнаружения, исследование задерживающей способности средств защиты периметра, исследование вероятности успешного задержания нарушителя до его достижения цели с помощью использования различных комбинаций элементов СФЗ с уникальными наборами параметров и моделирования уникальной структуры объекта с помощью указанных элементов СФЗ, и имитационная модель включает в себя по меньшей мере четыре параллельных процесса, независимо развивающихся в модельном времени: модель действий нарушителя, модель действий оператора, модель действий монитора, модель действий группы реагирования, и динамически моделируют взаимодействие указанных четырех процессов между собой путем создания в имитационной модели динамических объектов и связей; после этапа имитационного моделирования, на основании смоделированных экспериментов, формируют статистические данные, осуществляют автоматизированное формирование и анализ оценки уязвимости объекта и формируют оценку уязвимости объекта по различным критериям на основе полученных статических данных, в случае неудовлетворительной оценки уязвимости объекта осуществляют доработку и повторную оценку систем физической защиты и систем безопасности охраняемого объекта необходимое количество раз до момента создания удовлетворяющей всем требованиям системы физической защиты и системы безопасности охраняемого объекта в целом.

2. Способ по п.1, характеризующийся тем, что после формирования оценки уязвимости объекта осуществляют доработку динамических математических моделей технических средств охраны, инженерных средств охраны и службы безопасности.

3. Способ по п.1, характеризующийся тем, что осуществляют экспорт проекта плана объекта в элементы проектной документации.

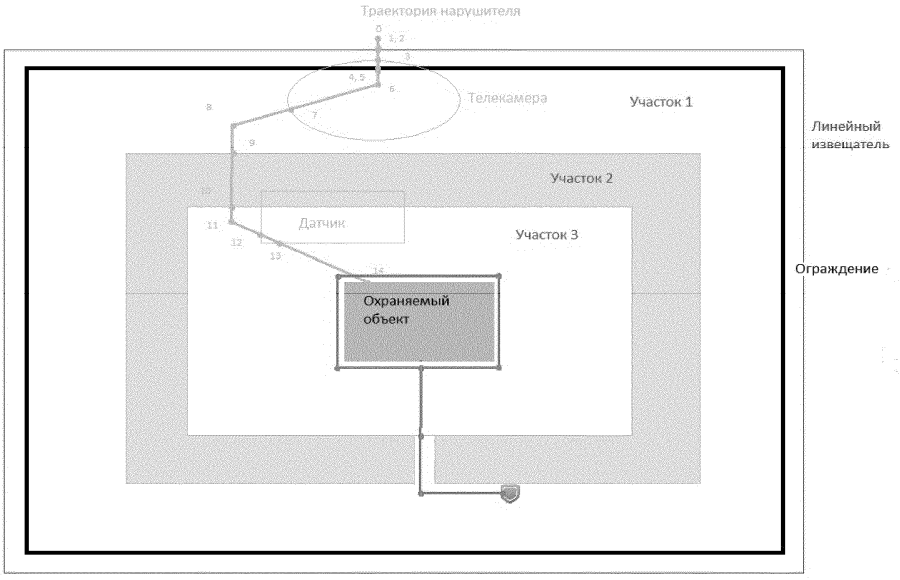
4. Способ по п.1, характеризующийся тем, что дополнительно формируют математические модели специфических областей и инфраструктуры.

5. Способ по п.1, характеризующийся тем, что учитывают экспертную траекторию движения нарушителя.

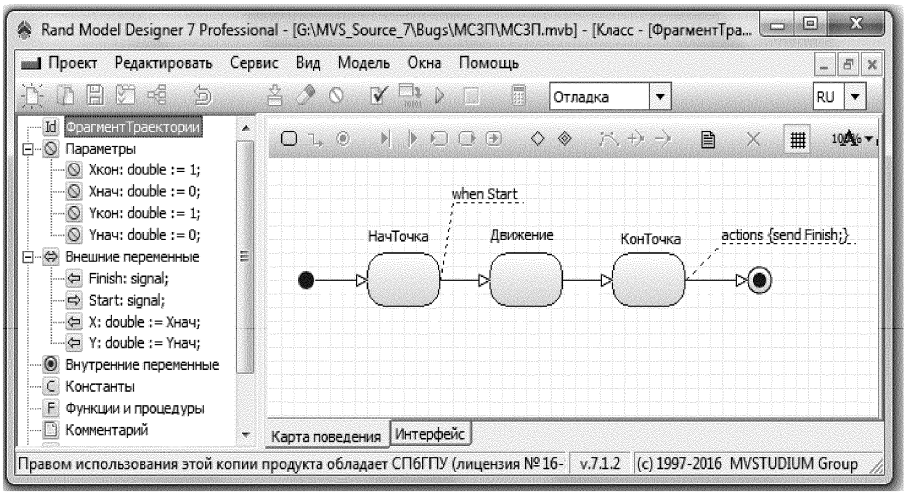
6. Способ по п.1, характеризующийся тем, что учитывают экспертную траекторию движения службы охраны.

7. Способ по п.1, характеризующийся тем, что учитывают случайную траекторию движения нарушителя.

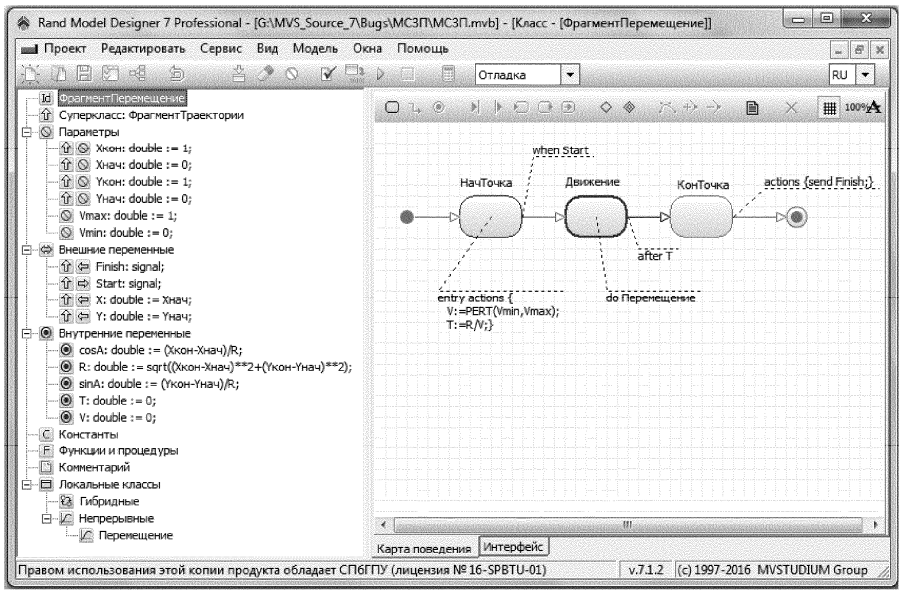
8. Способ по п.1, характеризующийся тем, что в качестве динамической математической модели технического средства охраны, инженерного средства охраны, нарушителя и службы безопасности используют реально функционирующий элемент технического средства охраны, инженерного средства охраны, нарушителя и службы безопасности.



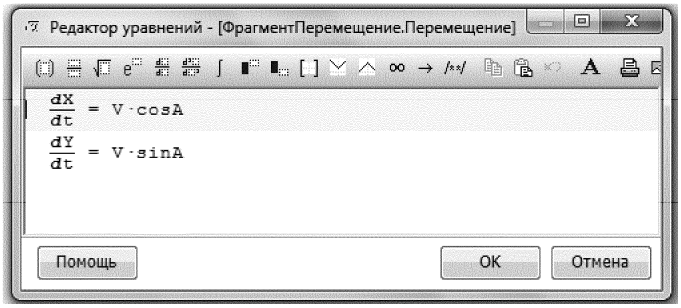
Фиг. 1



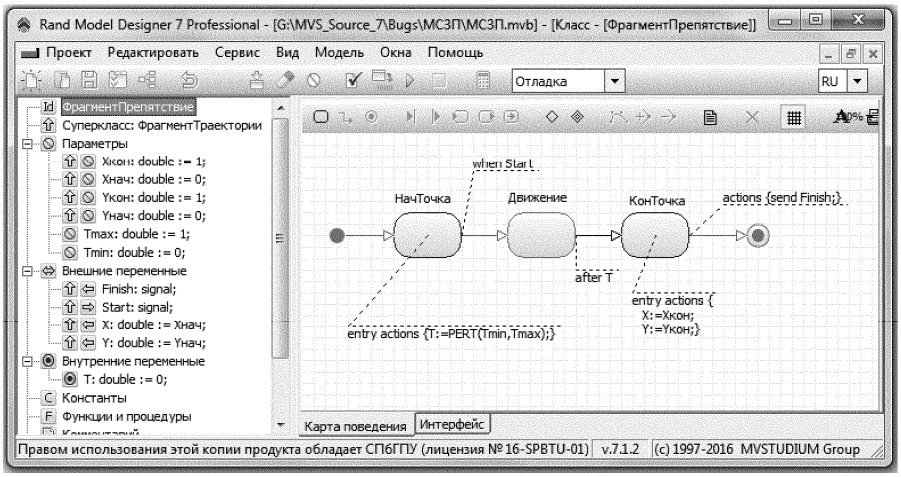
Фиг. 2



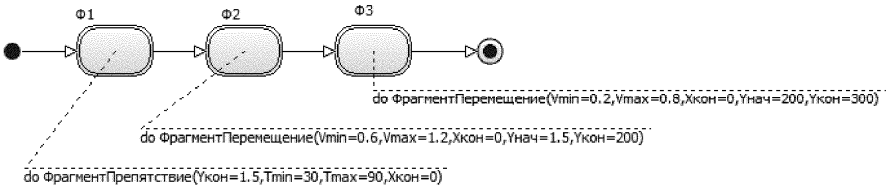
Фиг. 3



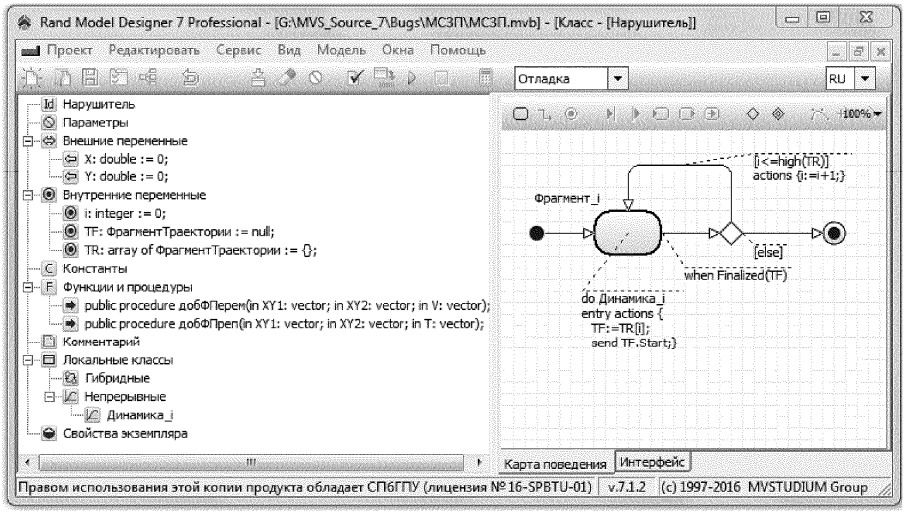
Фиг. 4



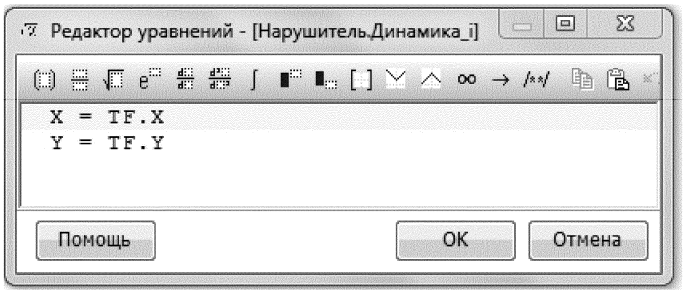
Фиг. 5



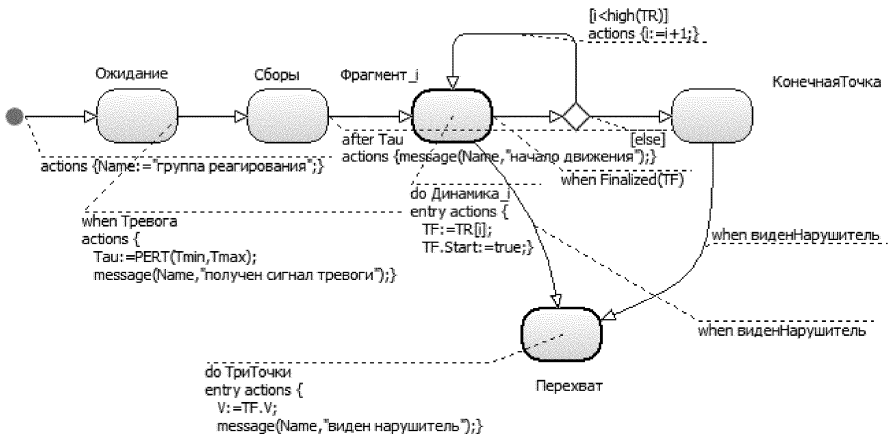
Фиг. 6



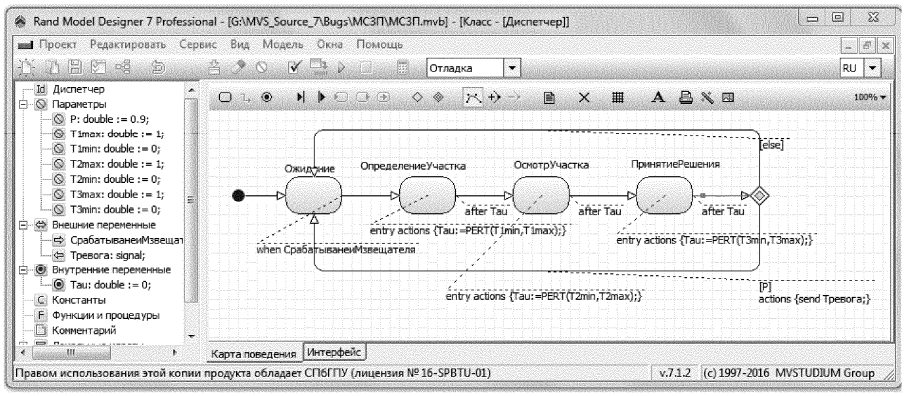
Фиг. 7



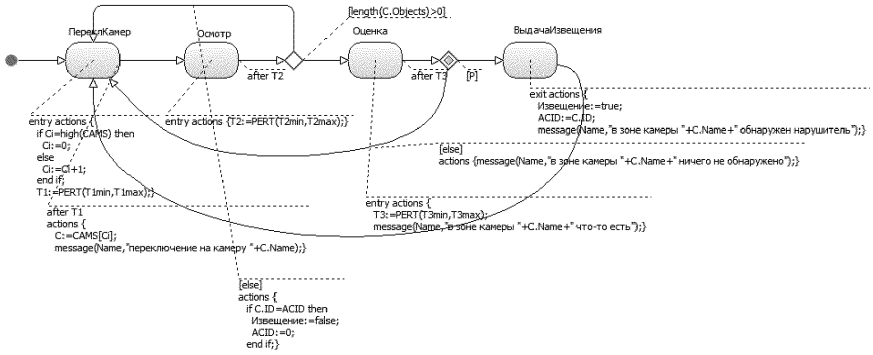
Фиг. 8



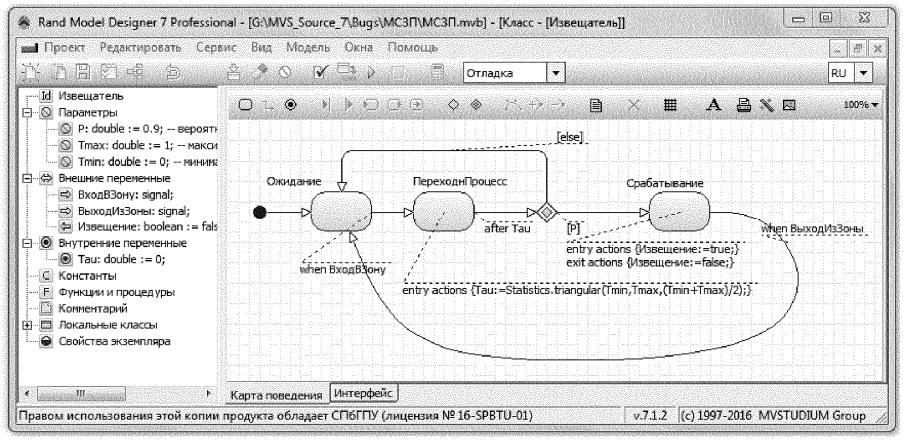
Фиг. 9



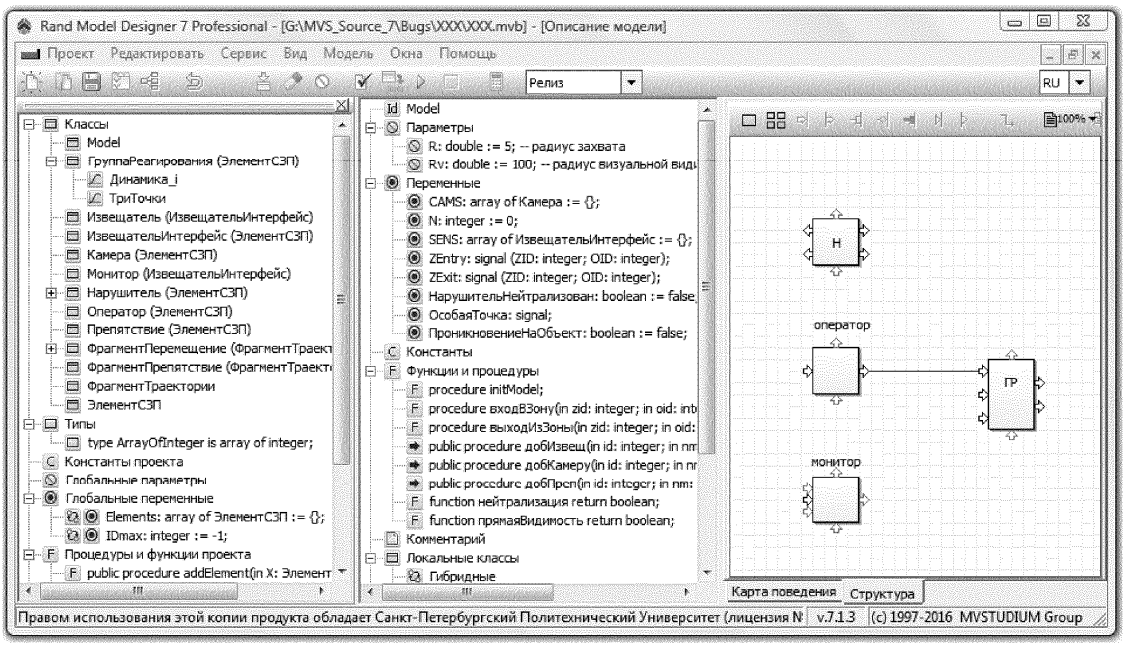
Фиг. 10



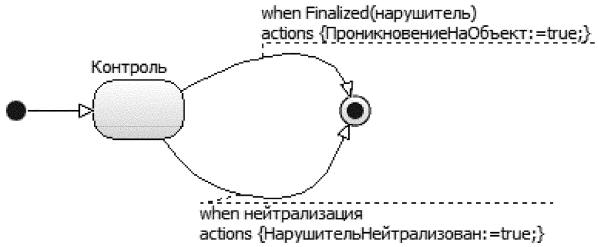
Фиг. 11



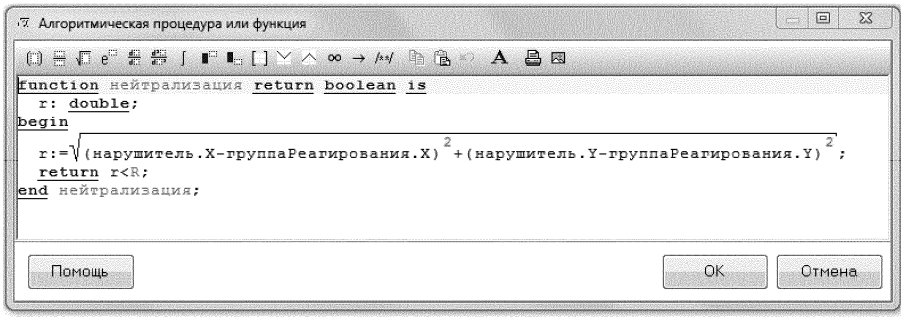
Фиг. 12



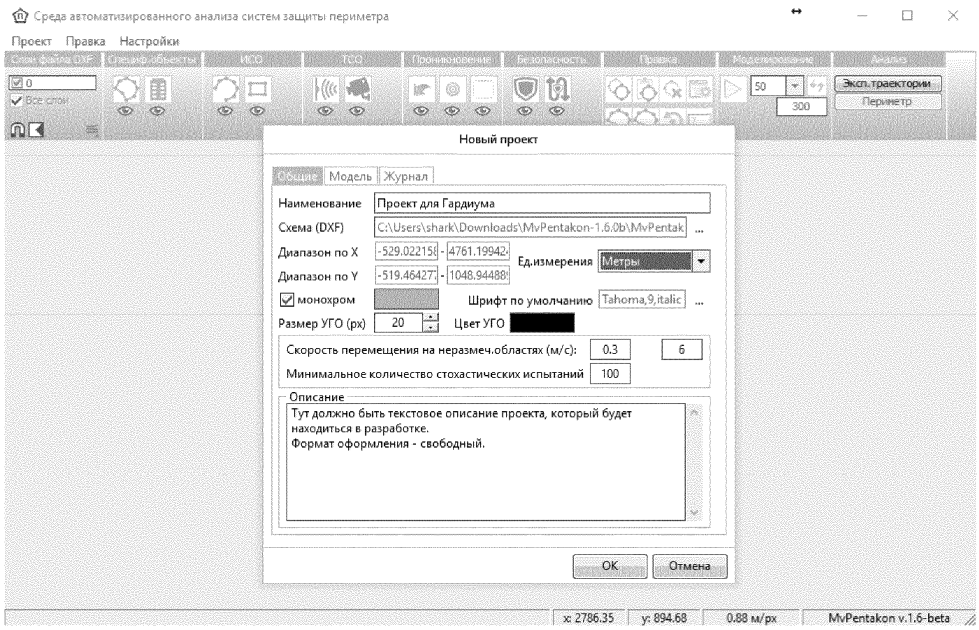
Фиг. 13



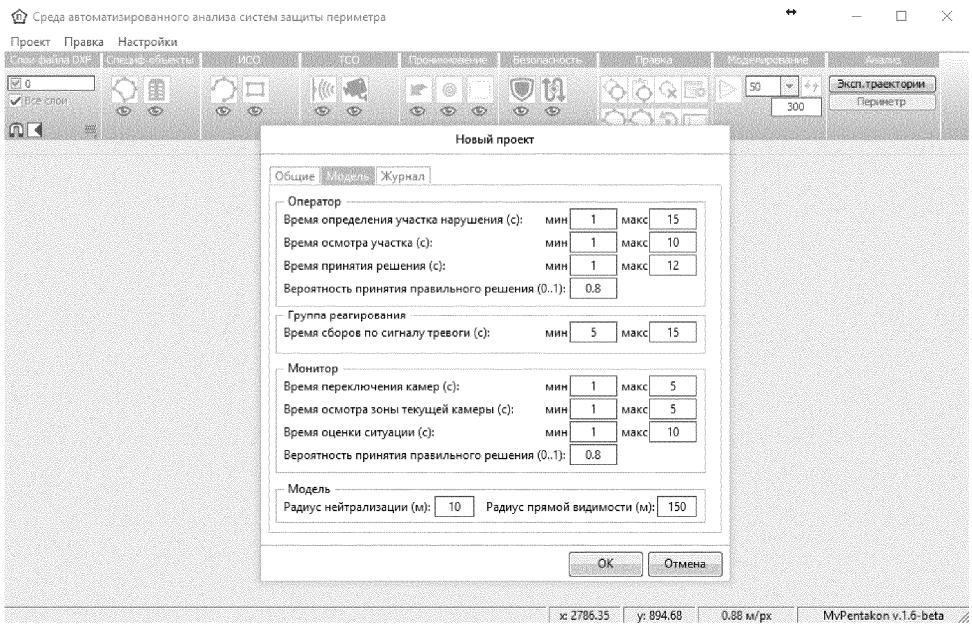
Фиг. 14



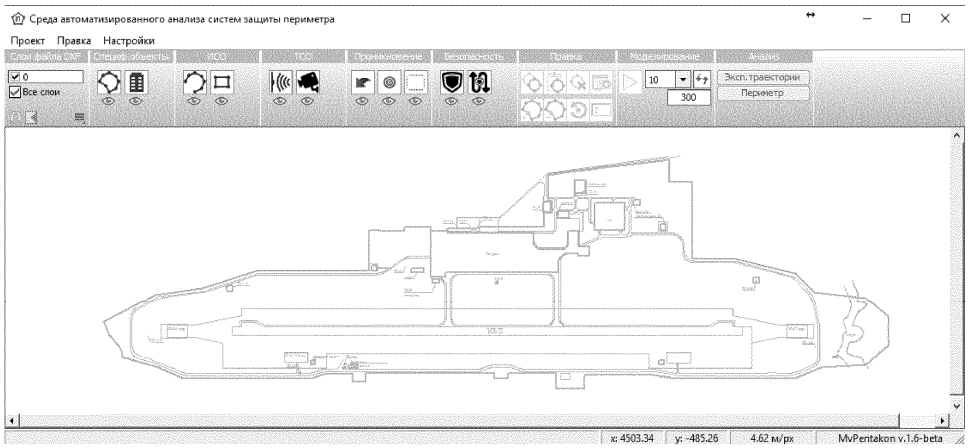
Фиг. 15



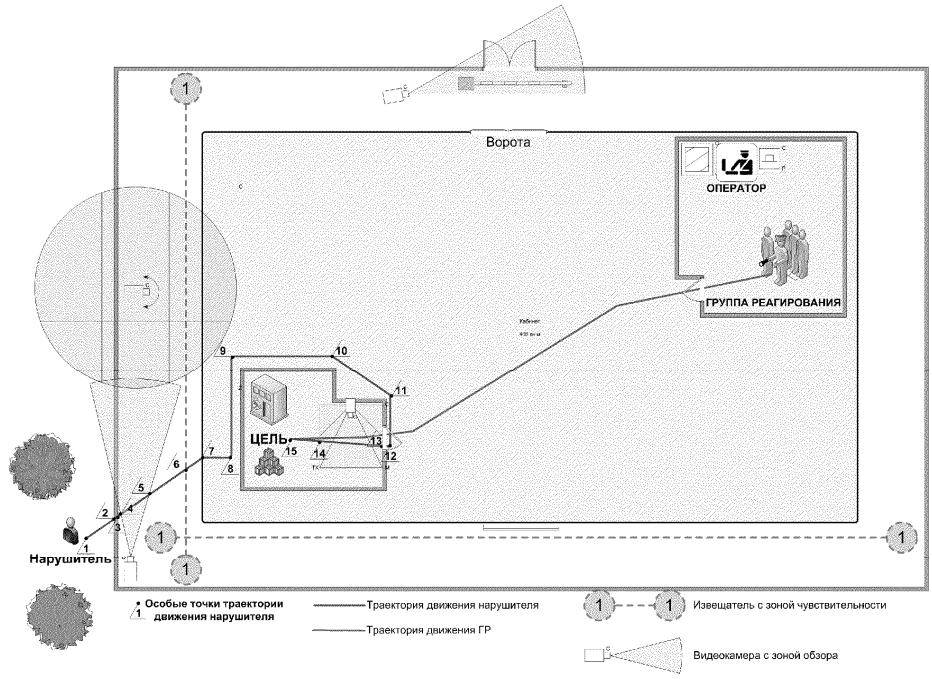
Фиг. 16



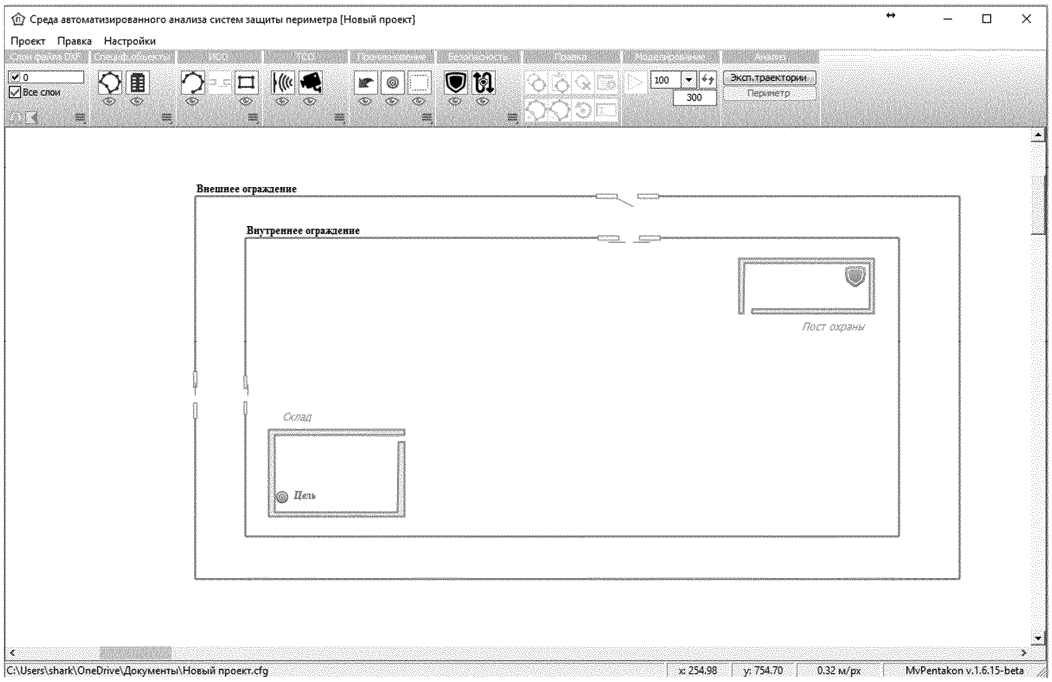
Фиг. 17



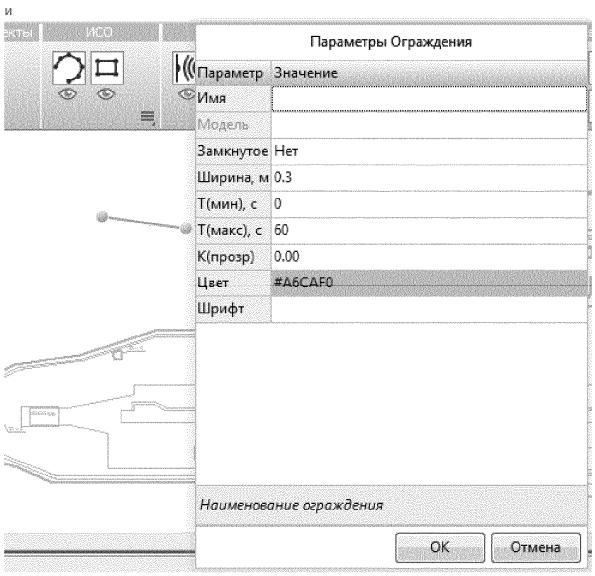
Фиг. 18


Ворота
ОПЕРАТОР
ГРУППА РЕАГИРОВАНИЯ
ЦЕЛЬ
Нарушитель
Особые точки траектории движения нарушителя
Траектория движения нарушителя
Траектория движения ГР
Извещатель с зоной чувствительности
Видеокамера с зоной обзора

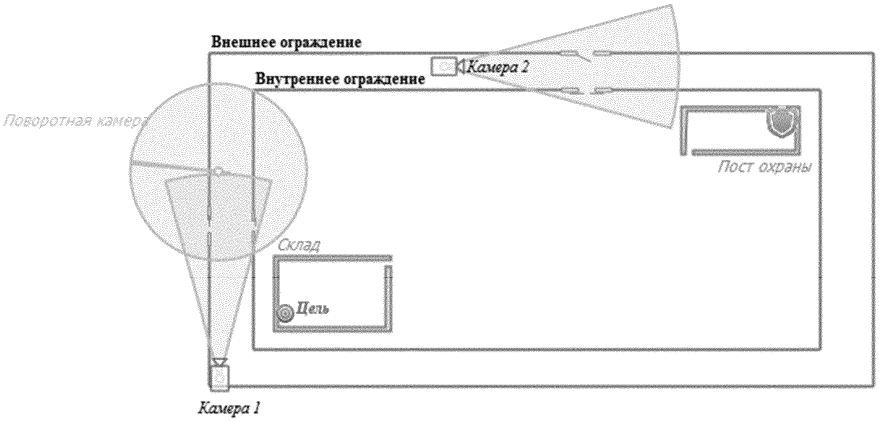
Фиг. 19


Среда автоматизированного анализа систем защиты периметра [Новый проект]
Проект
Правка
Настройки
Все слои
Эксп. траектории
Периметр
Внешнее ограждение
Внутреннее ограждение
Пост охраны
Склад
Цель
C:\Users\shark\OneDrive\Документы\Новый проект.cfg
x: 254.98
y: 754.70
0.32 м/px
MvPentakon v.1.6.15-beta

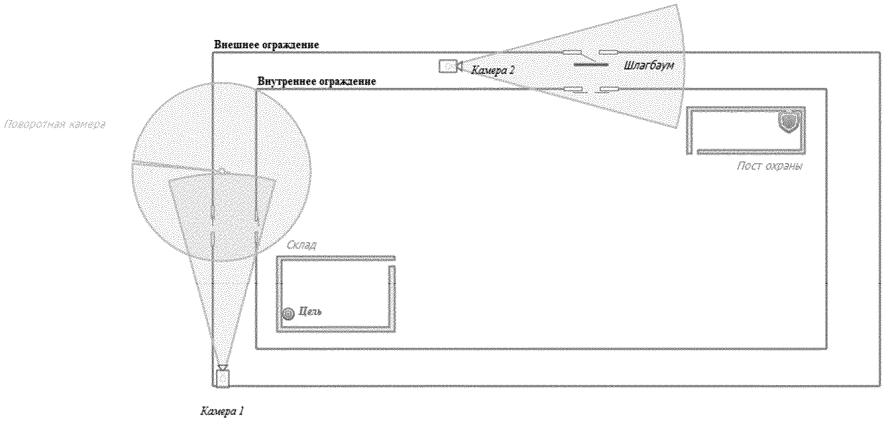
Фиг. 20



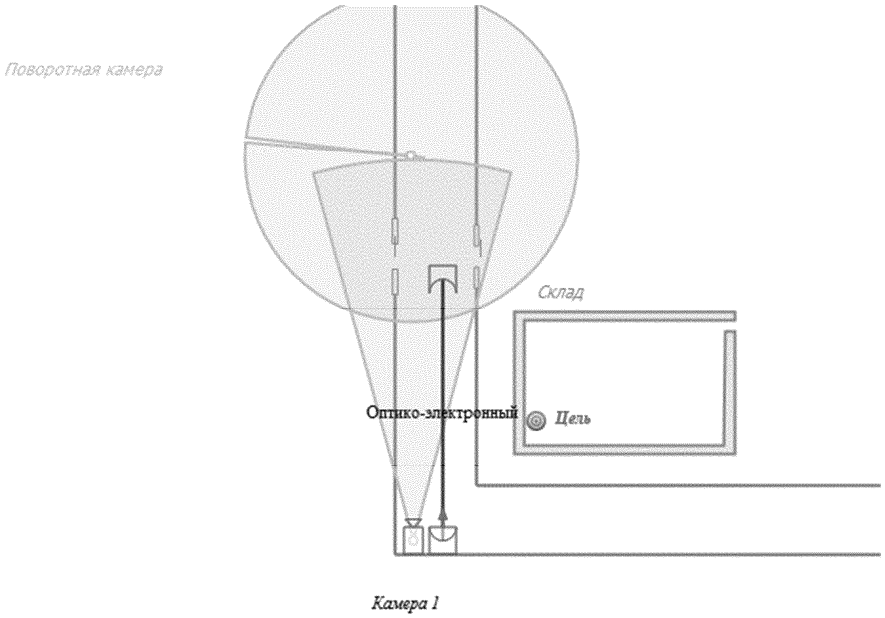
Фиг. 21



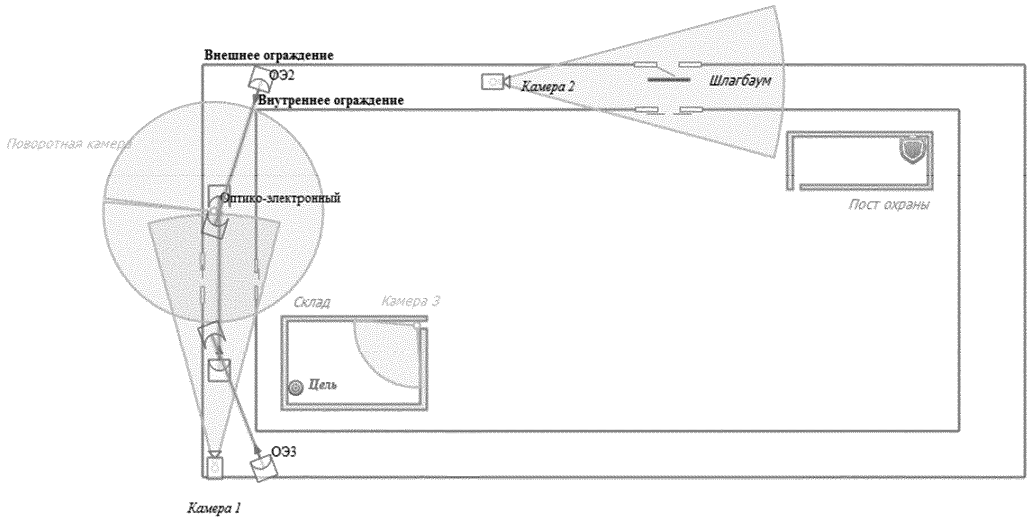
Фиг. 22



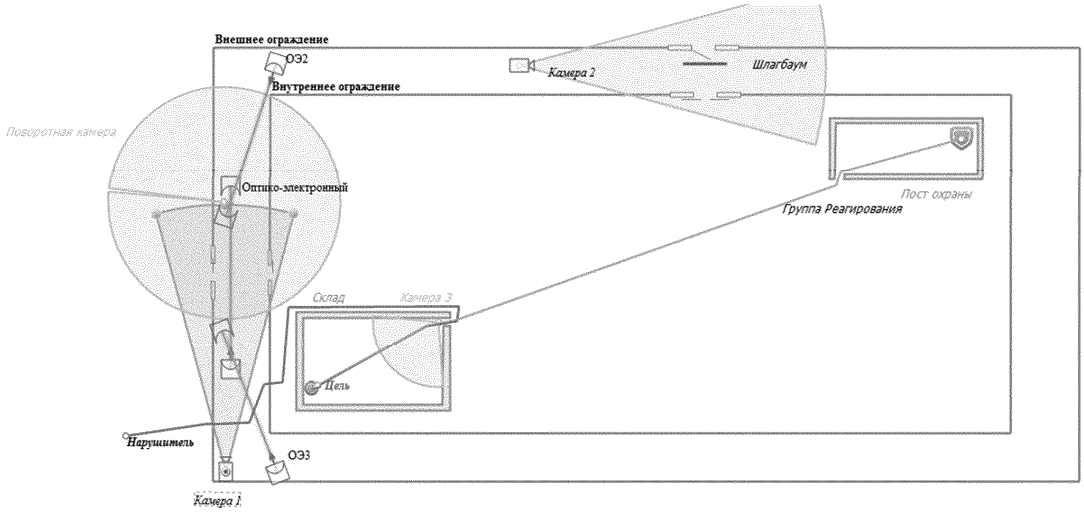
Фиг. 23



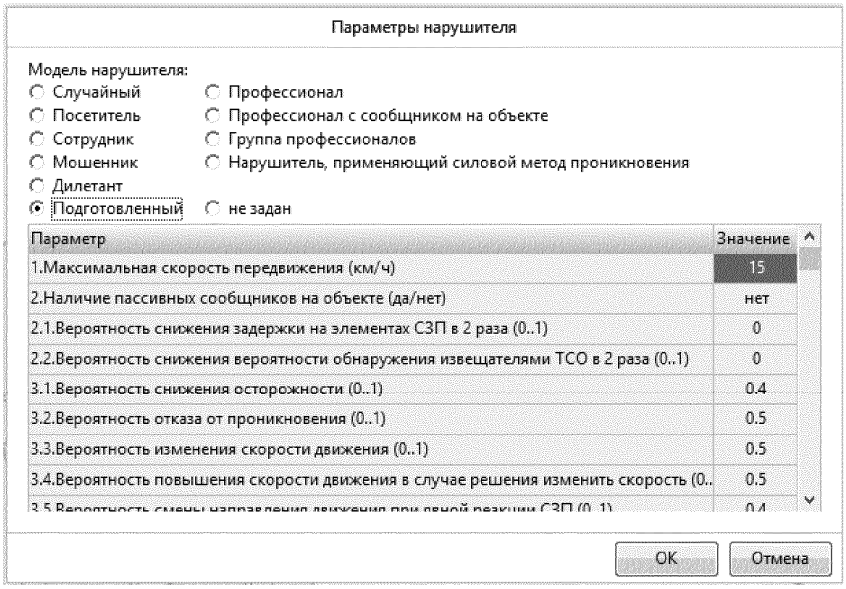
Фиг. 24



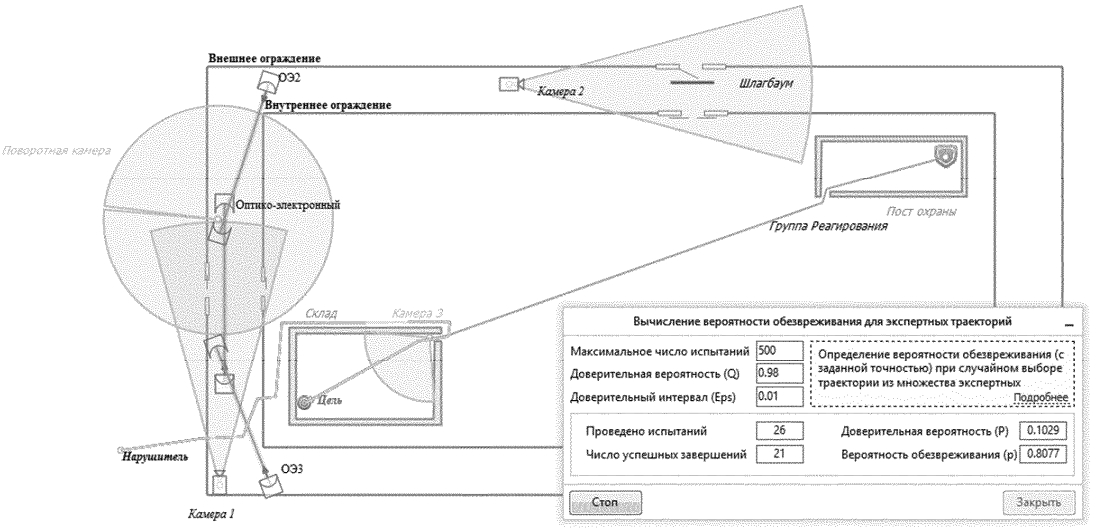
Фиг. 25



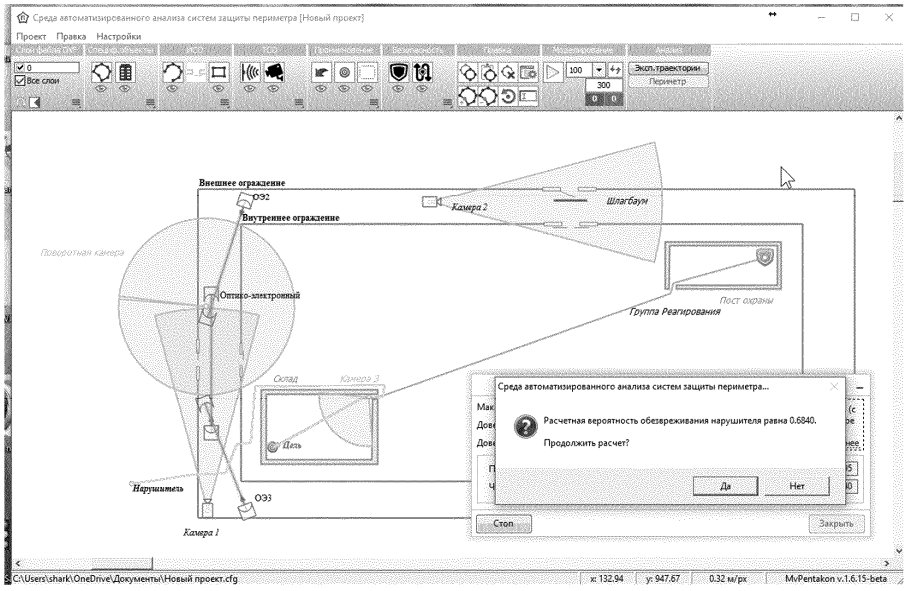
Фиг. 26



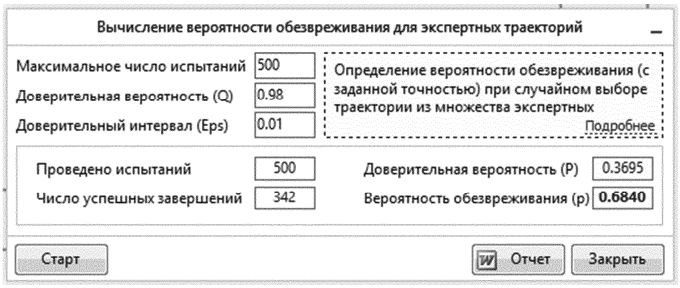
Фиг. 27



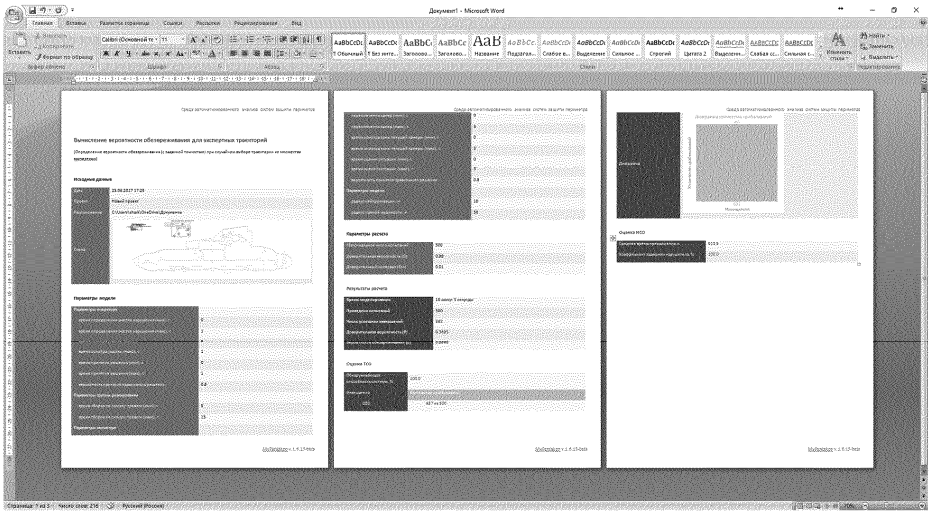
Фиг. 28



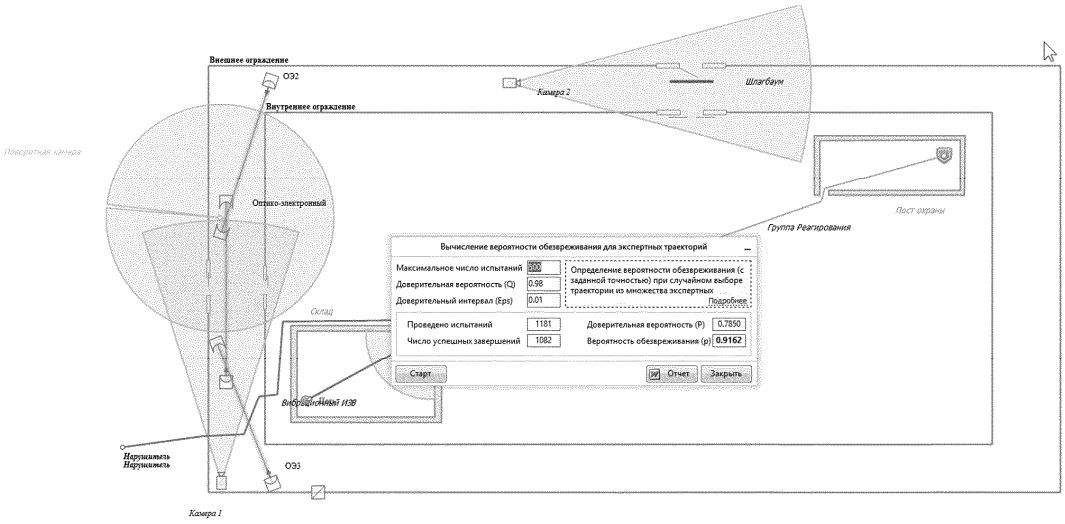
Фиг. 29



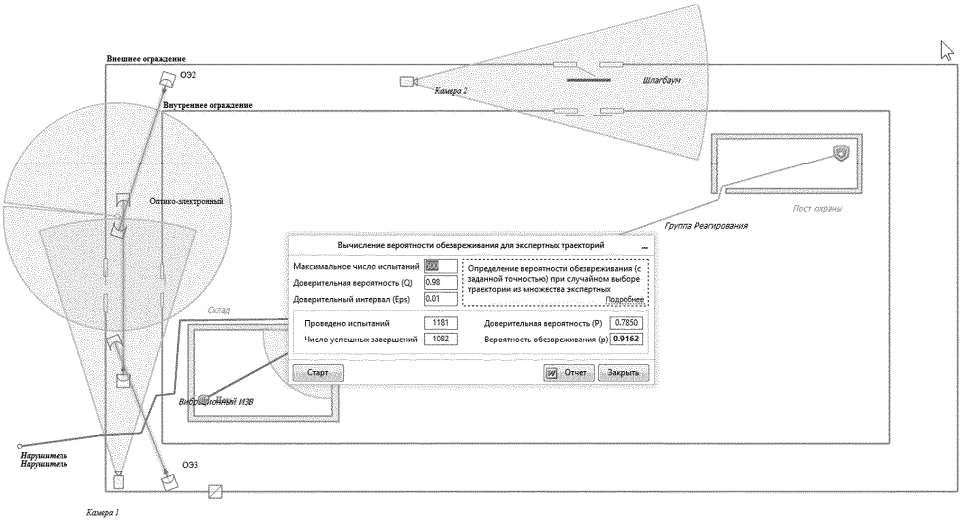
Фиг. 30



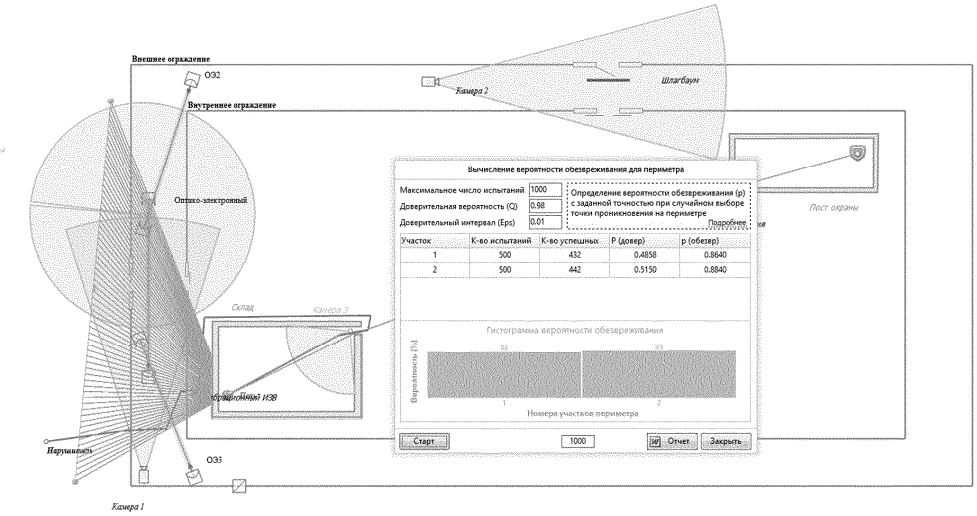
Фиг. 31



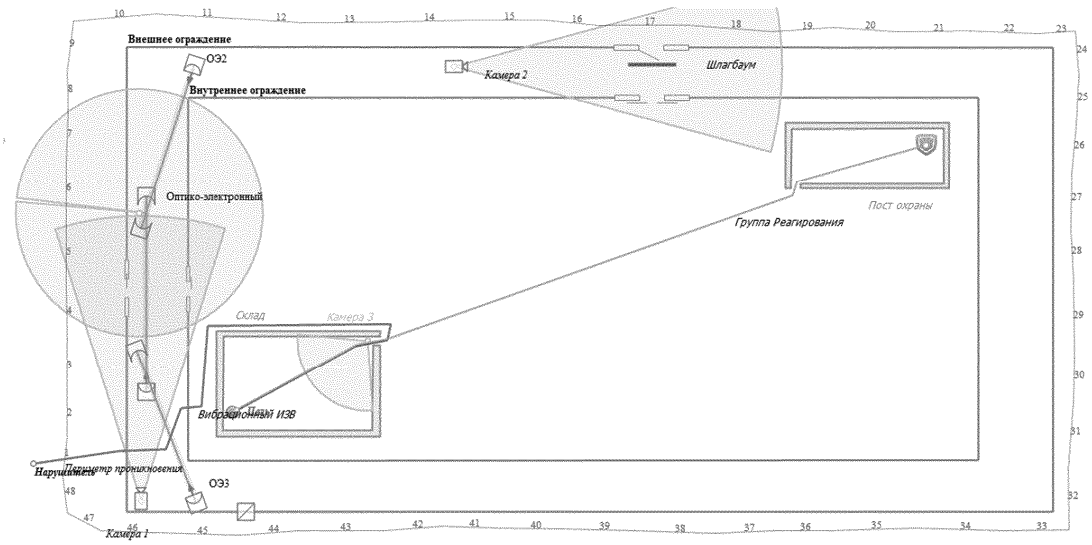
Фиг. 32



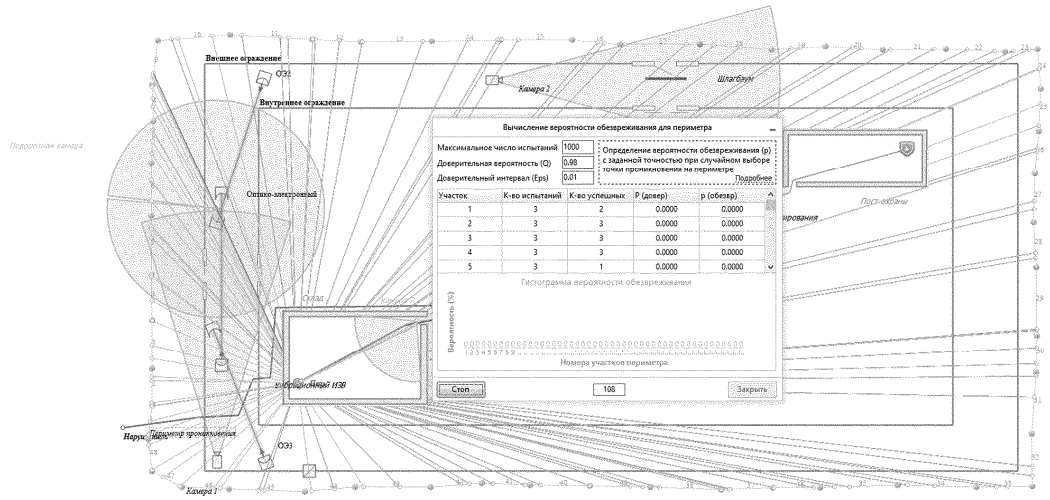
Фиг. 33



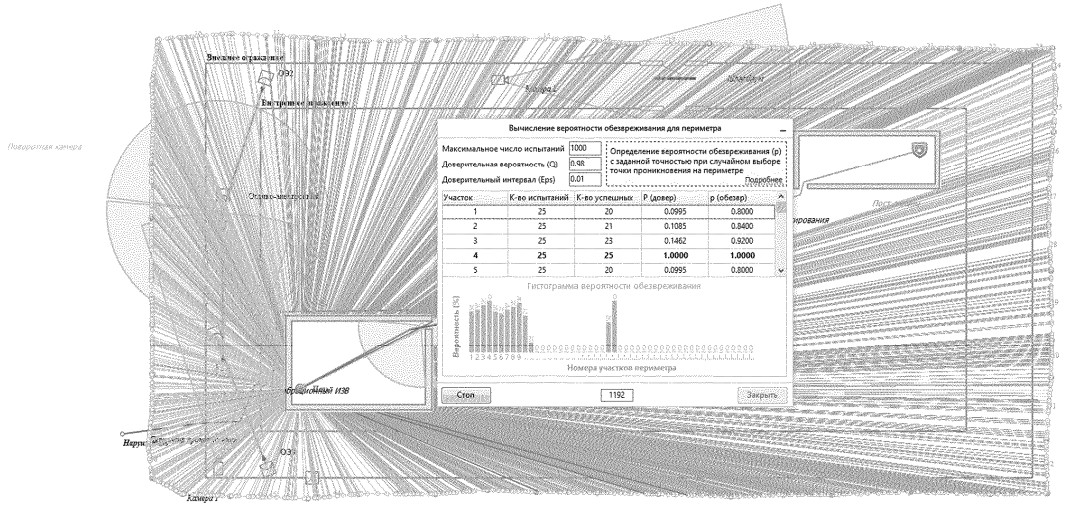
Фиг. 34



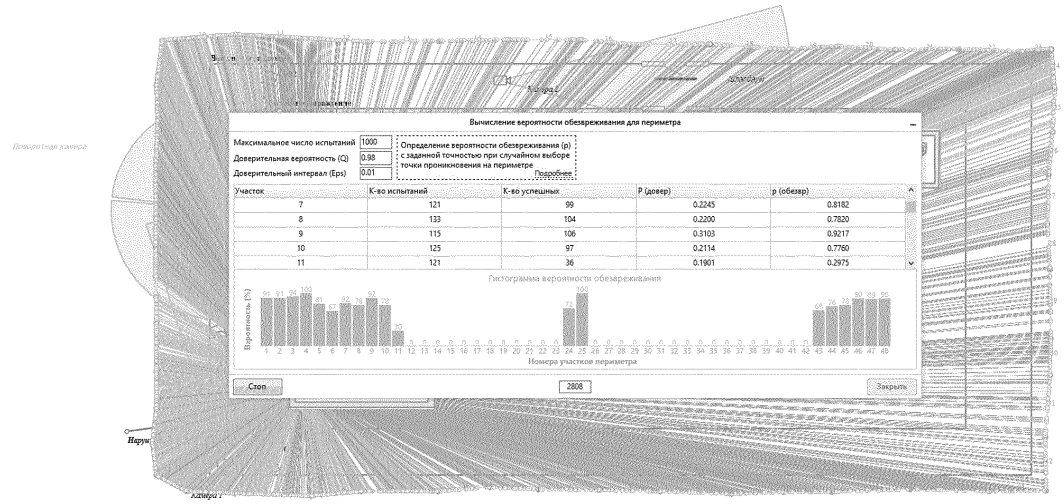
Фиг. 35



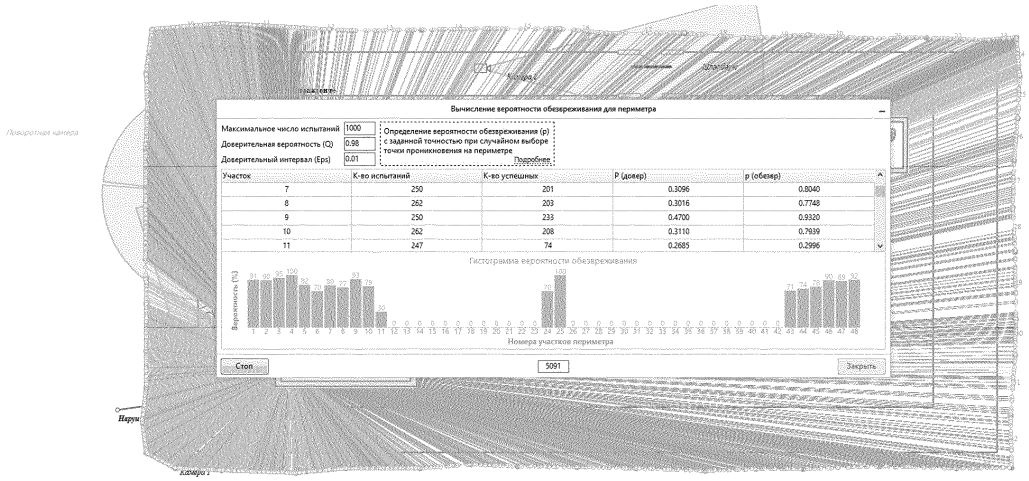
Фиг. 36



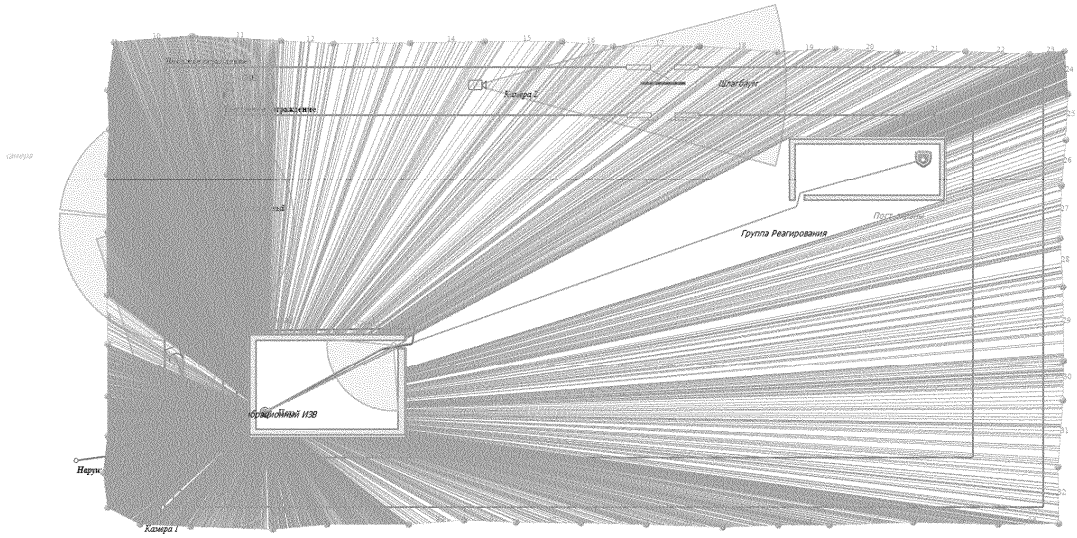
Фиг. 37



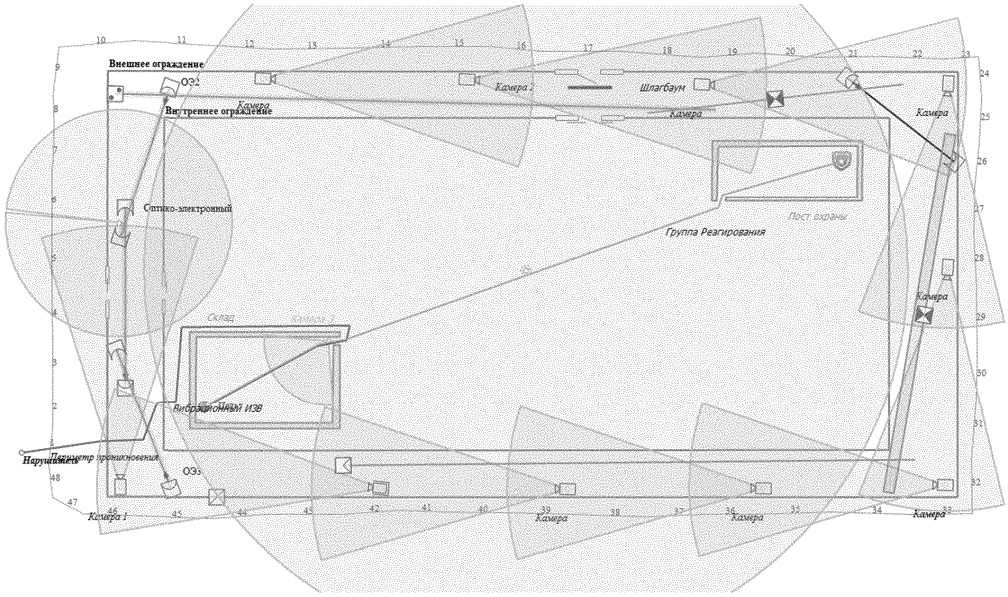
Фиг. 38



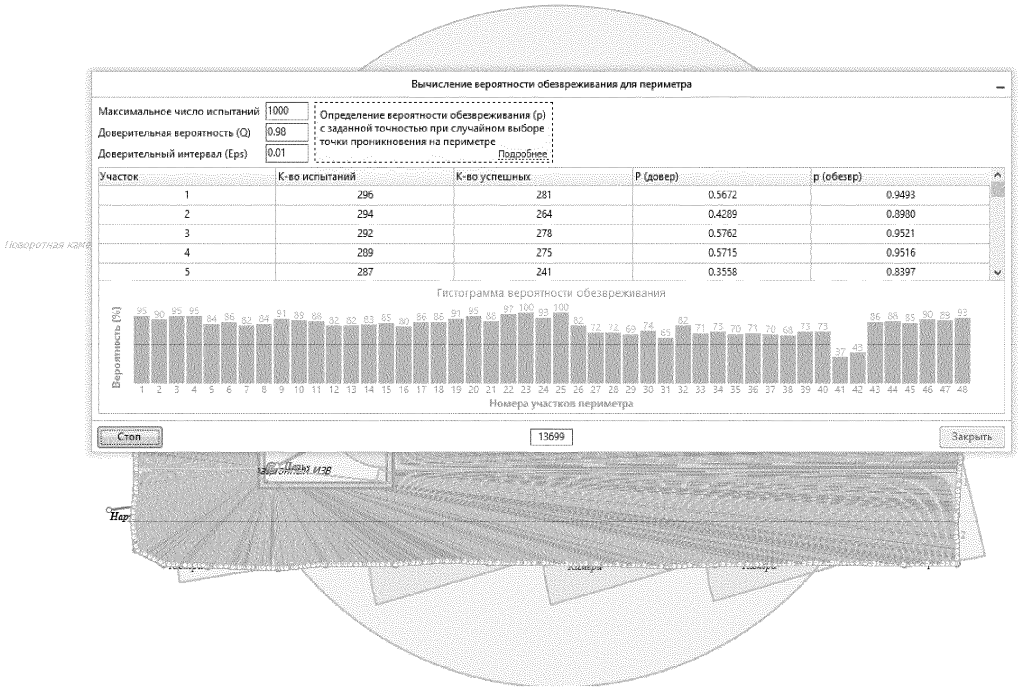
Фиг. 39



Фиг. 40



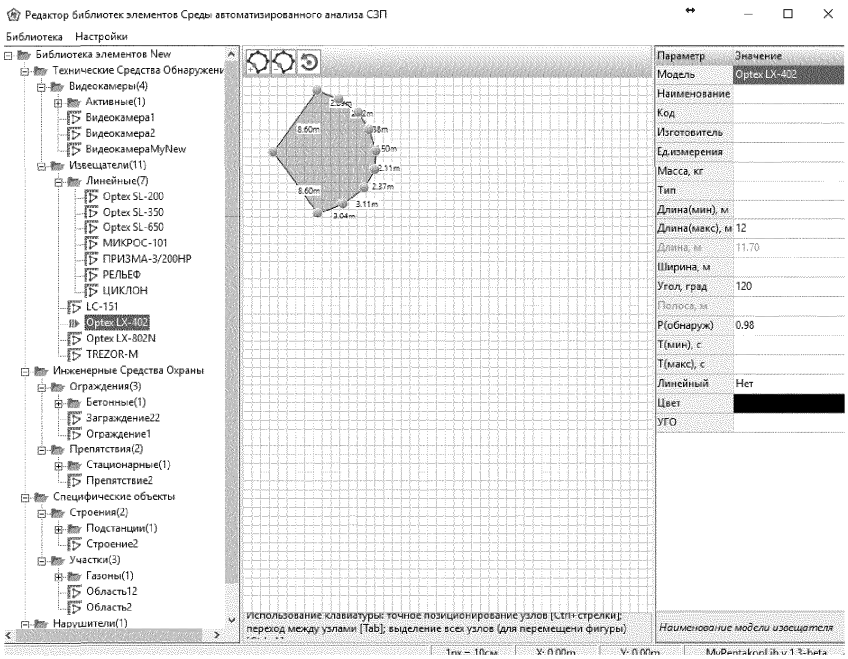
Фиг. 41


Вычисление вероятности обезвреживания для периметра
Максимальное число испытаний 1000
Доверительная вероятность (Q) 0.98
Доверительный интервал (Eps) 0.01
Определение вероятности обезвреживания (p) с заданной точностью при случайном выборе точки проникновения на периметре
Подробнее
Участок | К-во испытаний | К-во успешных | P (довер) | p (обезвр)
1 | 296 | 281 | 0.5672 | 0.9493
2 | 294 | 264 | 0.4289 | 0.8980
3 | 292 | 278 | 0.5762 | 0.9521
4 | 289 | 275 | 0.5715 | 0.9516
5 | 287 | 241 | 0.3558 | 0.8397
Гистограмма вероятности обезвреживания
Вероятность (%)
Номера участков периметра
Стоп
13699
Закрыть

Фиг. 42


Вычисление вероятности обезвреживания для периметра
Максимальное число испытаний 1000
Доверительная вероятность (Q) 0.98
Доверительный интервал (Eps) 0.01
Определение вероятности обезвреживания (p) с заданной точностью при случайном выборе точки проникновения на периметре
Подробнее
Участок | К-во испытаний | К-во успешных | P (довер) | p (обезвр)
1 | 315 | 297 | 0.5555 | 0.9429
2 | 314 | 284 | 0.4534 | 0.9045
3 | 311 | 296 | 0.5895 | 0.9518
4 | 308 | 294 | 0.6005 | 0.9545
5 | 307 | 260 | 0.3735 | 0.8469
Гистограмма вероятности обезвреживания
Вероятность (%)
Номера участков периметра
Старт
14615
Отчет
Закрыть

Фиг. 43


Редактор библиотек элементов Среды автоматизированного анализа СЗП
Библиотека
Настройки
Библиотека элементов New
Технические Средства Обнаружени
Видеокамеры(4)
Активные(1)
Видеокамера1
Видеокамера2
ВидеокамераMyNew
Извещатели(11)
Линейные(7)
Optex SL-200
Optex SL-350
Optex SL-650
МИКРОС-101
ПРИЗМА-3/200НР
РЕЛЬЕФ
ЦИКЛОН
LC-151
Optex LX-402
Optex LX-802N
TREZOR-M
Инженерные Средства Охраны
Ограждения(3)
Бетонные(1)
Заграждение22
Ограждение1
Препятствия(2)
Стационарные(1)
Препятствие2
Специфические объекты
Строения(2)
Подстанции(1)
Строение2
Участки(3)
Газоны(1)
Область12
Область2
Нарушители(1)
Параметр
Значение
Модель
Optex LX-402
Наименование
Код
Изготовитель
Ед.измерения
Масса, кг
Тип
Длина(мин), м
Длина(макс), м
12
Длина, м
11.70
Ширина, м
Угол, град
120
Полоса, м
P(обнаруж)
0.98
T(мин), с
T(макс), с
Линейный
Нет
Цвет
УГО
Использование клавиатуры: точное позиционирование узлов [Ctrl+стрелки]; переход между узлами [Tab]; выделение всех узлов (для перемещени фигуры)
Наименование модели извещателя

Фиг. 44