ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

ШАРКОВ Илья Кириллович

Презентация к научно-квалификационной работе аспиранта (научному докладу):

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ И ОЦЕНКА КАЧЕСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОХРАНЯЕМЫХ ОБЪЕКТОВ

Направление подготовки

- 09.06.01 «Информатика и вычислительная техника»

Направленность

- 05.13.01 «Системный анализ, управление и обработка информации (по отраслям)»

Санкт-Петербург 2021

Область тематики работы:

Системы Физической Защиты на охраняемых объектах

Для защиты охраняемых объектов от посягательств нарушителя создают целые комплексы мер по обеспечению их безопасности. Охрана реального объекта представляется в виде **системы физической защиты** (СФЗ).

- СФЗ – **кибер-физическая система**, использующая физические технические и инженерные средства охраны, а так же человеческие ресурсы службы безопасности. Всё это размещается на реальном объекте и позволяет противостоять атакам нарушителя на охраняемый объект.

- **Моделирование и оценка СФЗ** – сложная комплексная задача, которая актуальна как с точки зрения практики, так и законодательства (см. требования по оценке качества СФЗ в постановлениях правительства по транспортной безопасности, ТЭК и т.п.).

Актуальность работы

Работа «Имитационное моделирование и оценка качества физической защиты охраняемых объектов» выполнена по направлению 09.06.01 «Информатика и вычислительная техника», направленность - 05.13.01 «Системный анализ, управление и обработка информации (по отраслям).

В виду увеличивающегося количества и разнообразия террористических угроз, видов мошенничества и нарушения условий безопасности и территориальной целостности различных объектов, требуются современные методы проектирования и достоверной оценки качества СФЗ.

Актуальные задачи и инструменты:

- **Количественная оценка качества** СФЗ **необходима** для определения уязвимости систем к атакам тех или иных видов нарушителя. Такую оценку важно знать как на этапе эскизного проектирования, так и на этапе анализа уже построенных систем.
- **Имитационное моделирование** является современным и эффективным способом анализа и оценки сложных крупномасштабных структур СФЗ.
- Существует **потребность в повышении объективности оценок** путем применения **методик и инструментов математического моделирования для анализа** СФЗ позволяет минимизировать субъективную составляющую экспертного мнения и заменить её с помощью математически обоснованных характеристик и оценок эффективности СФЗ.

Цель и задачи исследования

Целью является **исследование возможностей и полезности применения имитационного моделирования** для анализа Систем Физической Защиты (СФЗ).

Задачи исследования:

- **Разработка имитационных моделей** СФЗ, сотрудников служб безопасности объекта и нарушителя для анализа и оценки защищенности кибер-физической системы охраны объекта с помощью агентного подхода.
- **Разработка алгоритма событийно-управляемых траекторий** для формирования сценариев проникновения нарушителя и движения охранников, применяемого совместно с эвристическим алгоритмом поиска оптимального пути «Polaris» без заранее созданного графа.

Научная новизна работы

Научная новизна работы заключается в предлагаемом подходе моделирования и оценки СФЗ, ранее не применявшемся в распространённой практике. Основные отличительные признаки подхода и их новизна:

- **Объектно-ориентированный подход** к разработке математических моделей (ООМ), выраженный в парадигме UML (использован инструмент AnyDynamics).
- **Агентное моделирование** системы, где каждый компонент СФЗ, операторы, охранники и нарушители представлены своей независимой моделью. **В виде классов** представлены все необходимые сущности.
- Алгоритм **событийно-управляемых траекторий** и алгоритм поиска оптимального пути между точками, которые позволяют:
  - Применять **гибридные автоматы** для формирования сценариев взаимодействия человека и СФЗ, а так же логико-вероятностные характеристики поведения этого человека;
  - Создавать пути без использования заранее заготовленного графа.

Компьютерное моделирование СФЗ:

Общее представление СФЗ как модели

В самом общем представлении модель СФЗ – это кортеж, который можно рассматривать в виде минимального набора:

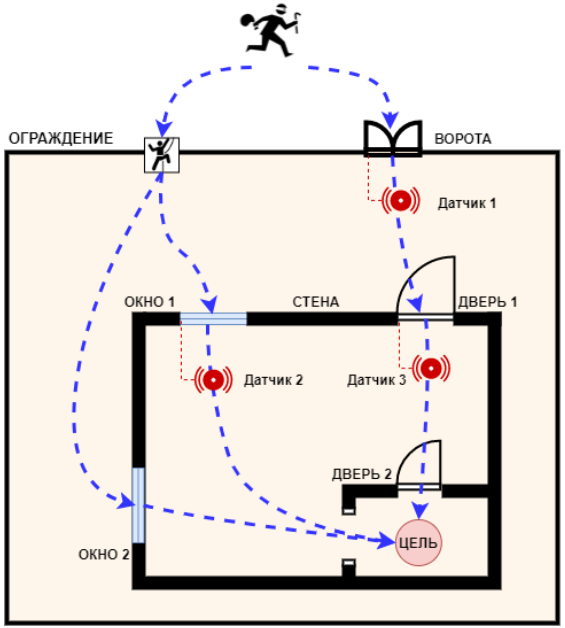
$$\sum \textbf{Модель} = \{\textbf{Объект, Проникновение, Внешние условия, Исход}\}, \text{ где:}$$

- «**Объект**» содержит в себе все моделируемые элементы СФЗ, топологию объекта и инфраструктурные особенности.
- «**Проникновение**» - моделируемый сценарий движения нарушителя через охраняемую зону объекта, включающее в себя путь движения до цели проникновения. В наиболее продвинутых моделях, рассматривается так же и модель нарушителя.
- «**Внешние условия**» - условия, влияющие как на работу СФЗ «Объекта», так и на «Проникновение»: ограничение видимости, ложные тревоги и т.д.
- «**Исход**» - рассматриваемые моделью возможные результаты проникновения нарушителя и противодействия ему со стороны СФЗ, обычно это обнаружение и нейтрализация.

Компьютерное моделирование СФЗ:

Понятие о сценарии проникновения нарушителя

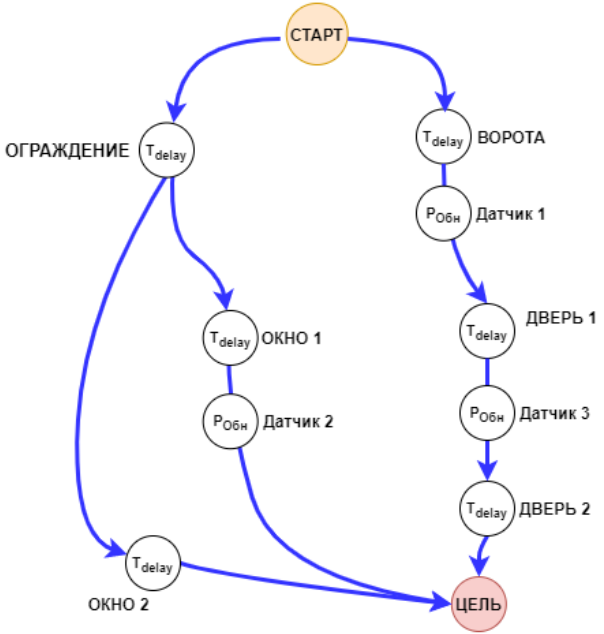
Сценарии проникновения нарушителя (его путь движения) можно представить как траектории через СФЗ объекта, которые складываются в граф множества путей:



- Вершины = препятствия;
- Ребра = движение;

Функциями СФЗ является:

- Обнаружение;
- Сдерживание;
- Противодействие;



Существующие решения:
Группы подходов моделирования и оценки СФЗ

Можно выделить 4 группы подходов моделирования и оценки СФЗ:

1. **на заданном пути** при заданных условиях и состоянии системы («EASI», «ASSES» США);
2. **в случайной точке** на территории объекта («САПР СИЗТО» Амулет);
3. **на основе анализа графов** путей нарушителя по территории объекта («Вега-2» Элерон, «SAVI» США);
4. **с помощью имитационного моделирования** и **игровых моделей** боестолкновений («ПОЛИГОН» Элерон, «Итерация-СФЗ» Итерация, «АКИМ» ПЕНТАКОН);

В каждой группе существуют свои особенности и недостатки подходов.

Эти практики были учтены при формировании нового метода моделирования и оценки СФЗ.

Предлагаемый подход:
Имитационное моделирование и оценки СФЗ

Был разработан подход с применением агентного моделирования и алгоритмами событийно-управляемых траекторий для проведения имитационных экспериментов с проникновением нарушителя. Перед реализацией подхода были поставлены задачи преодолеть описанные ранее недостатки.

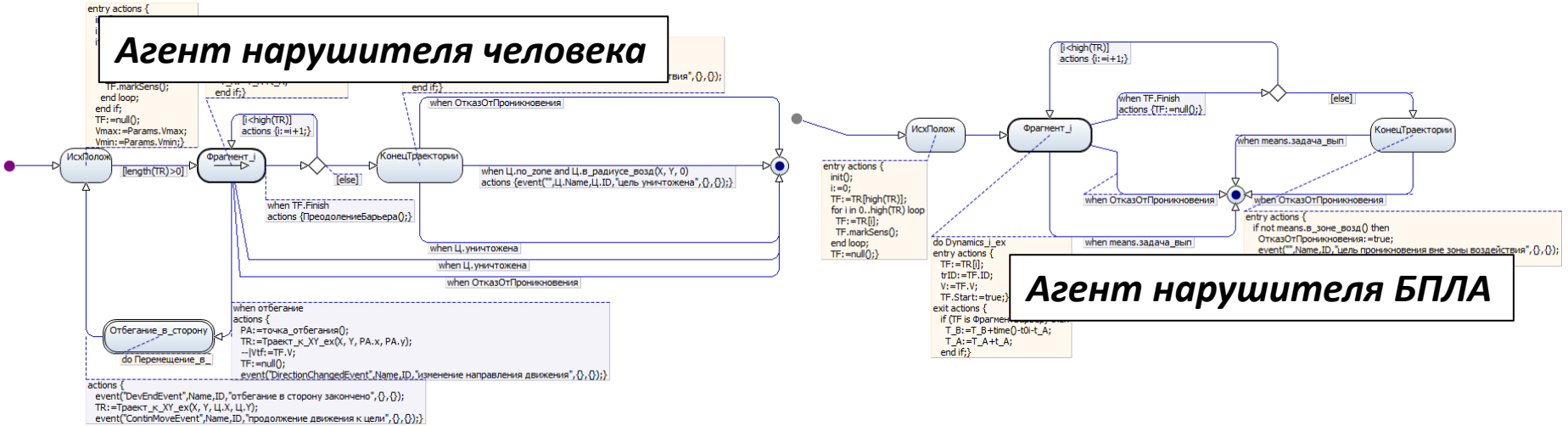
Основные решения подхода:

- **Агентное моделирование** в задачах моделирования СФЗ;
- **Событийно-управляемые траектории** проникновения в задачах формирования сценариев проникновения;
- Применение **эвристического алгоритма поиска пути** «Polaris» в задачах поиска пути;
- Сбор результатов имитационных экспериментов над СФЗ и **формирование оценок с помощью доверительных интервалов**;
- **Графический язык моделирования** (конструктор модели СФЗ).

Предлагаемый подход:

Агентное моделирование

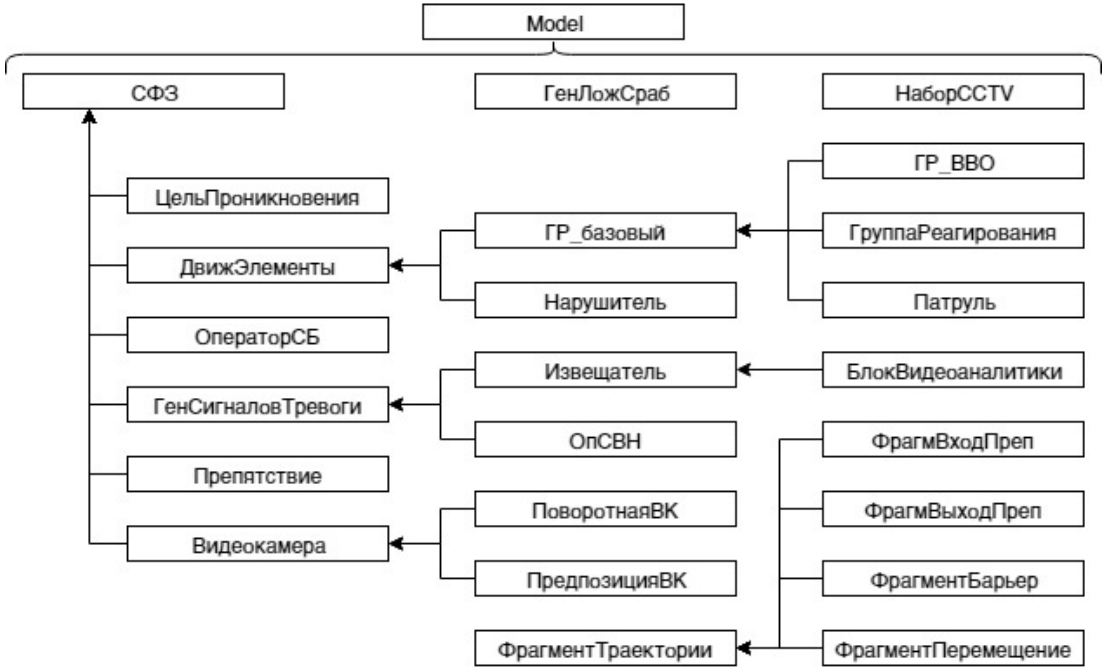
Все элементы СФЗ, охранники, операторы и нарушитель **описываются агентными моделями** с уникальными параметрами, свойственные им. Параметры и логики опираются на документацию устройств (ИТСО), вероятности, должностные инструкции и задаются интервалами с выбранным законом распределения. Каждый агент опирается на **локальные законы поведения** и взаимодействия с другими элементами, приближенные к реальности, что **повышает уровень автоматизации** описания модели цифрового двойника.



Предлагаемый подход:

Классы сущностей в представлении модели

Была построена система классов:



Модель

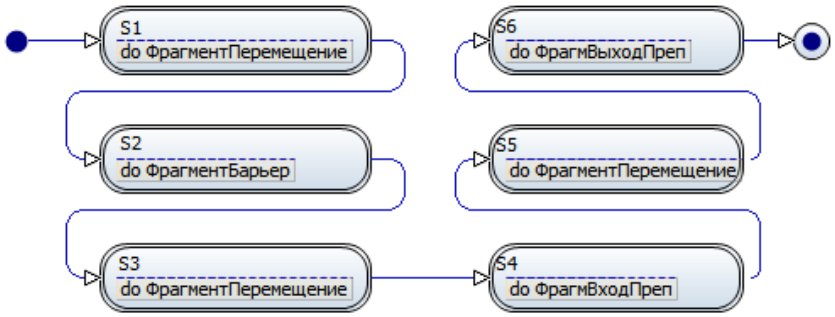
- Объект
  - СФЗ
    - ИСО
      - Барьер ;
      - Препятствие;
    - ТСО
      - Извещатели;
      - Видеокамеры;
  - СБ
    - Оператор;
    - Группа реагирования (охрана);
    - Патруль;
    - Система видеоаналитики;
- Проникновение: нарушитель, траектория;
- Внешние условия: погода, ложные тревоги;
- Исход: цель проникновения.

Предлагаемый подход:

Алгоритм событийно-управляемых траекторий

Алгоритм **построен на гибридных автоматах**. Он формирует фрагменты траектории, на которых происходят события эксперимента, складывающиеся в сценарий. При использовании алгоритма поиска путей («Polaris» или иной альтернативы) полностью **автоматизируется процесс постановки сценариев**, что отводит **роль эксперта на этап оценки результатов моделирования**.

Кроме того, возможно моделирование **динамических сценариев**, которые изменяются прямо по ходу эксперимента под действием логико-вероятностных алгоритмов.



С.-у. тр. можно представить тремя и более классами по характеру их взаимодействия:
1)Абстрактный класс «***ФрагментТраектории***»,
2)Дочернего класса «***ФрагментПеремещение***»,
3)Дочернего класса «***ФрагментПрепятствие***»,
4) и т.д.

Статистический эксперимент:

Основной подход и оценки

Используется метод доверительных интервалов для определения достаточного числа экспериментов, чтобы получить достоверную оценку:

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

где p – вероятность,
$\overline{P}$ - частота,
Ф – функция Лапласа,
ε – доверительный интервал

Основные:

- Вероятность обнаружения с помощью ТСО ($\mathbf{P_{обн}}$);
- Вероятность нейтрализации нарушителя ($\mathbf{P_{нейтр}}$);
- Наиболее уязвимые траектории (пути и координаты);
- Время задержки нарушителя на ИСО (t);
- Эффективность задержки движения нарушителя (коэффициент);
- Частота срабатываний тех или иных ТСО в экспериментах (ν) и т.д.

Практическая реализация:

Программный комплекс «АКИМ»

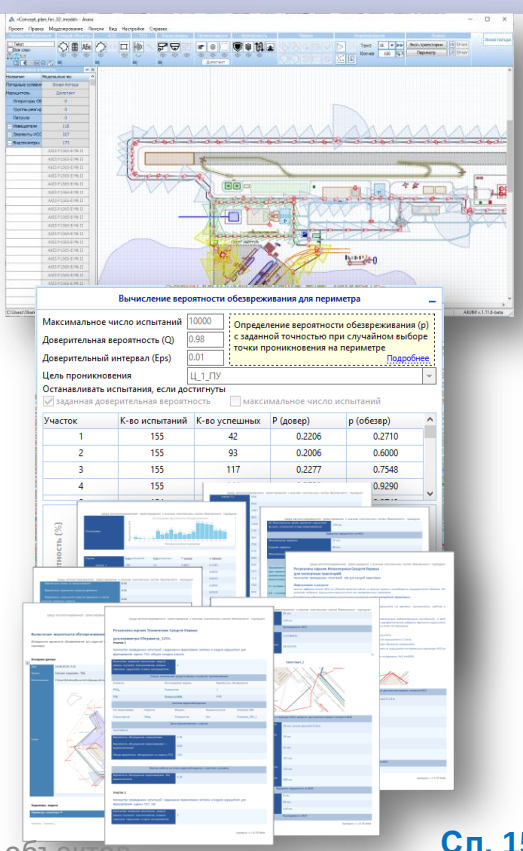
Модели, создаваемые AnyDynamics, можно компилировать в динамические подключаемые библиотеки (DLL) – это дает возможность использования описанного интерфейса взаимодействия с разработанными динамическими моделями математических моделей в различных программных обертках.

Специально для задач создания и моделирования цифровых двойников охраняемых объектов были созданы программные обертки «АКИМ» (Delphi) и «AKIM+» (.Net).

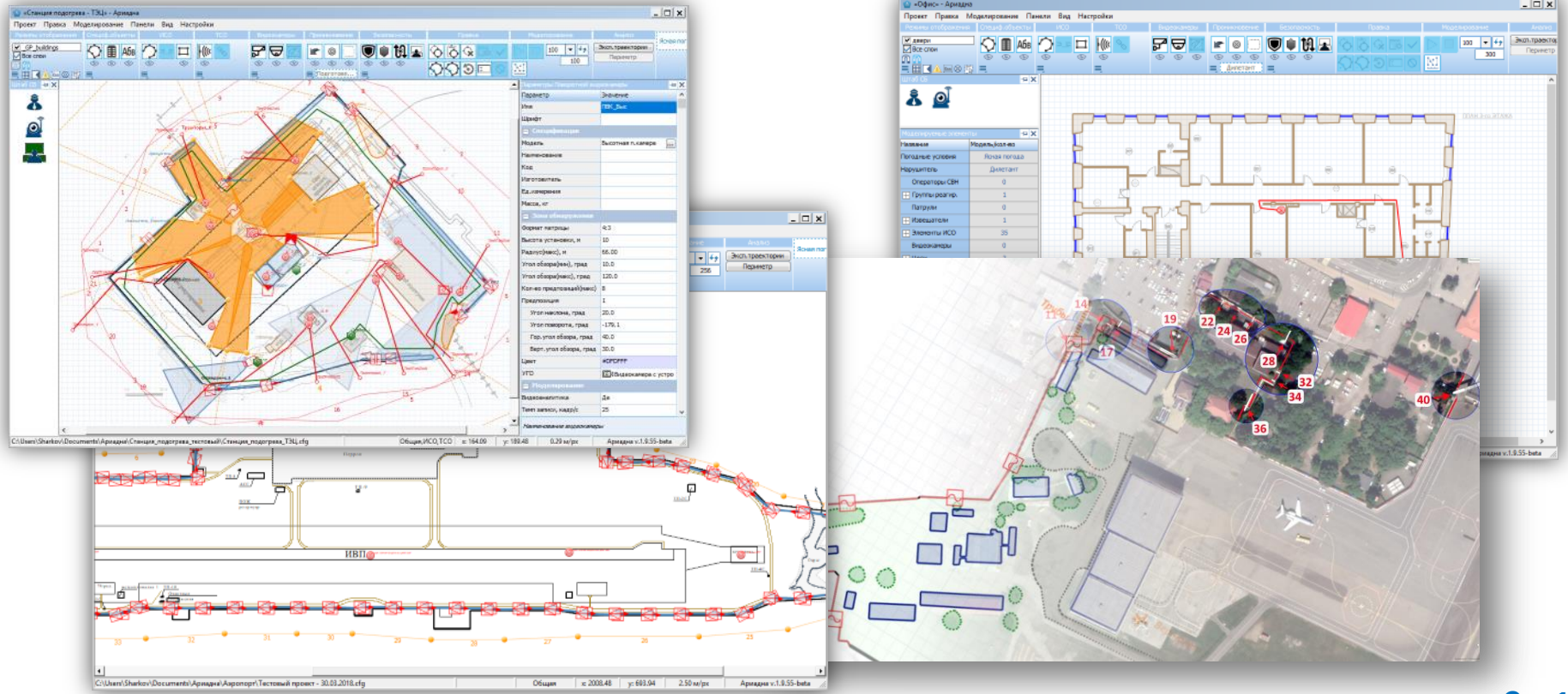
Практическая ценность предложенного метода в составе «АКИМ»:

Эксперт получает следующие возможности:

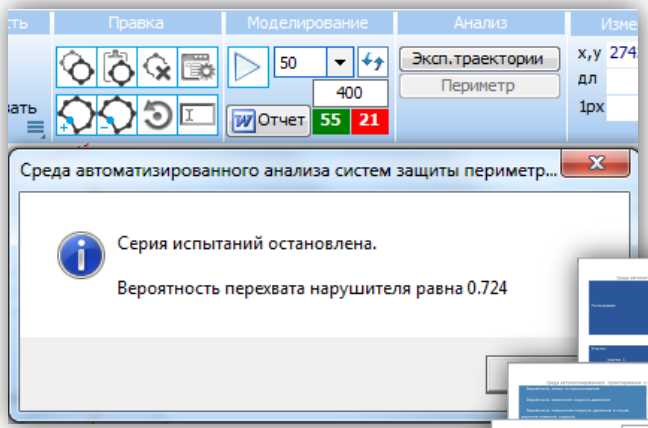
- **Автоматизация проектирования** сложных СФЗ в **графическом представлении** – в виде чертежа или 3D-представления;
- **Создание планов** наличия и расположения **сил служб безопасности** на объектах: посты охраны, траектории патрулирования, наличие операторов СБ;
- **Автоматизированный анализ** и **формирование оценок** качества созданного цифрового двойника СФЗ по разным условиям и направлениям проникновения;
- **Определение мер противодействия** угрозам со стороны нарушителей с последующим сравнением результатов;
- И т. д.



Примеры графического описания моделей СФЗ в «АКИМ»

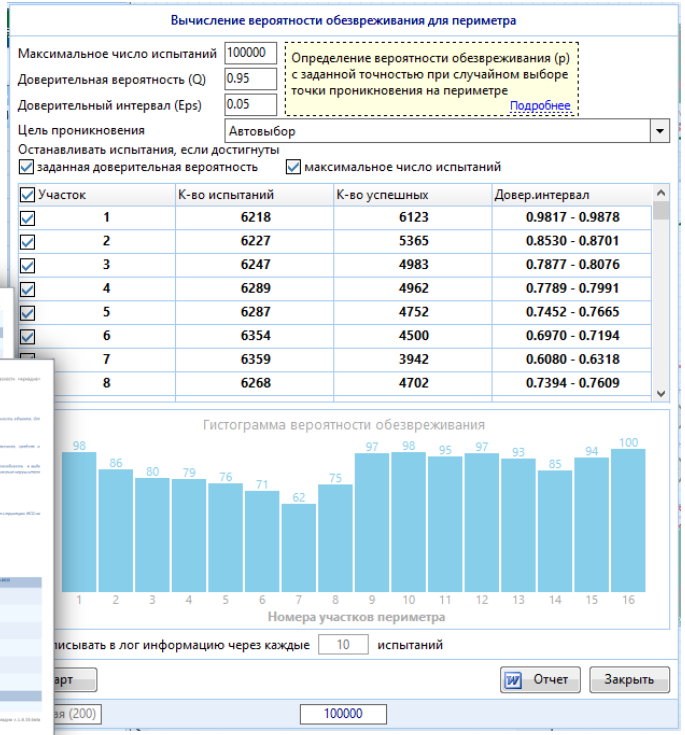


ПРИМЕРЫ ВЫВОДА РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ



Демонстрационный режим

Программные отчеты



В процессе моделирования

Личный вклад аспиранта

Аспирант выполнял научную работу в течение обучения в Политехническом университете Петра Великого и практическую реализацию в ООО«ПЕНТАКОН»:

- Участие в разработке агентных моделей СФЗ, охраны и нарушителя
- Разработка эвристического алгоритма «Polaris»
- Участие в разработке графического языка создания моделей в «АКИМ»
- Анализ и формулировка количественных оценок СФЗ
- Формулировка критериев оценки качества СФЗ
- Написание научных и публицистических статей, участие в выставках и конференциях

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

СПАСИБО ЗА ВНИМАНИЕ!

Имитационное моделирование и оценка качества физической защиты охраняемых объектов

Слайды
21-32

ДОПОЛНИТЕЛЬНЫЕ СЛАЙДЫ ПРЕЗЕНТАЦИИ

SLIDE: 20

Для ответов на вопросы по теме НКР аспиранта «Имитационное моделирование и оценка качества физической защиты охраняемых объектов»

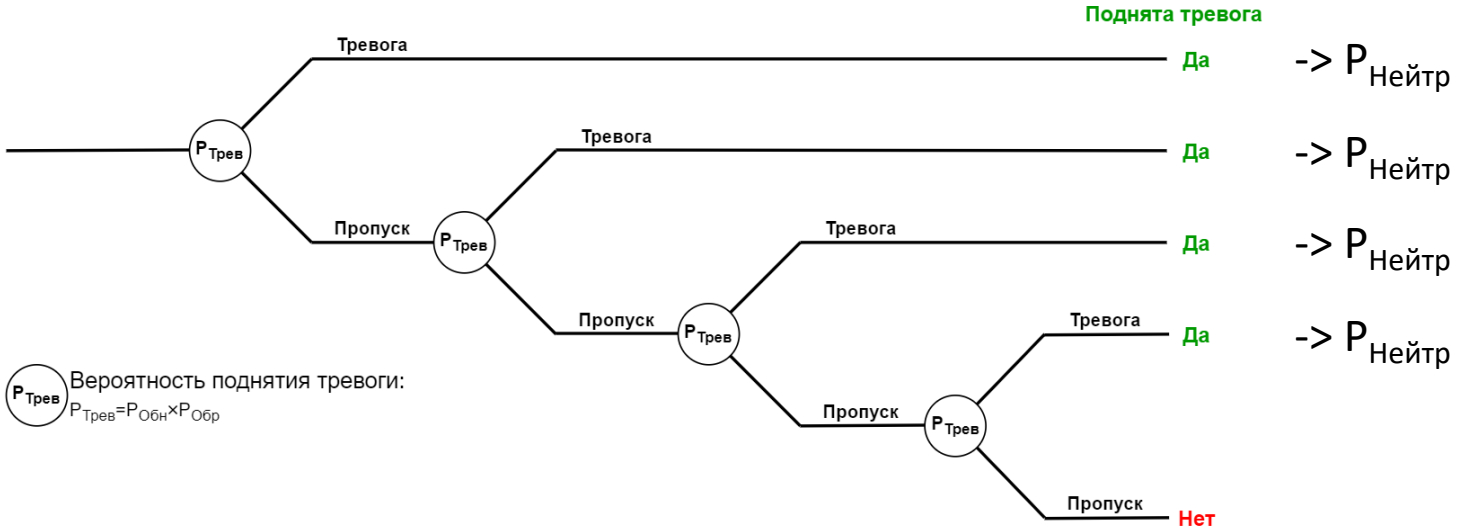
Существующие решения:

1. Заданная траектория проникновения

На заданном пути при заданных условиях и состоянии системы:

$$P_{Нейтр} = P_{Обн} \cdot P_{Обр} \cdot \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx,$$

где μx – математического ожидание нормального распределения для интервала времени между сигналом тревоги и перехватом,
а σx2 – СКО.



Существующие решения:

2. Испытания в случайных координатах охр. зоны

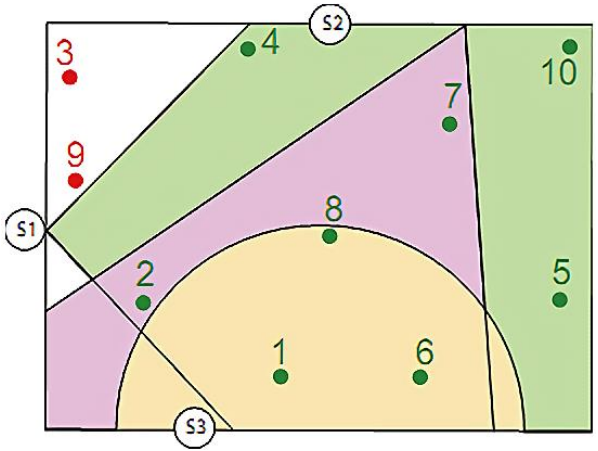
Генерируются тестовые воздействия в случайной точке на территории объекта:

- $P_{\text{Обн}} = \int_{x_0}^{x_{max}} p(x_{\text{Обн}})\, dx_{\text{Обн}}$

Интеграл от плотности распределения вероятности расстояния обнаружения с началом зоны от x_0 до x_{max}

- $P_{\text{Нейтр}} = P_{\text{Обн}} \cdot F \cdot \left(\frac{\xi \cdot T_i^{\text{Н}} - T_i^{\text{О}}}{\sqrt{\xi \cdot D_i^{\text{Н}} - D_i^{\text{О}}}} \right)$

где, ξ – коэффициент учета расположения технических средств обнаружения относительно физического барьера, T_i – математическое ожидание времени задержки нарушителя (Н) и реакции охраны (О), D_i – дисперсия времени задержки нарушителя и охранника.



Существующие решения:

3. Использование заготовленных графов путей

Анализ СФЗ на основе графа путей проникновений, который и является моделью СФЗ:

- Строится и описывается граф (экспертом или алгоритмом) подходящий выбранному методу исследования
- Выбирается путь тем или иным алгоритмом поиска, подходящим для выбранного графа
- Осуществляется расчет как в группах 1 и 2 или по собственной методике (существует много разных вариаций)

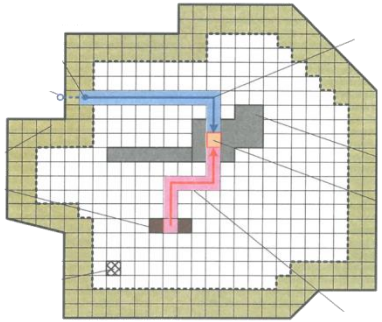
Существуют методики, применяющие особые подходы моделирования и анализа:

- Применение нечетких множеств для описания исходных данных
- Применение генетических алгоритмов, для обработки НМ и поиска пути
- И т. д.

Существующие решения:

4. Имитационное и игровое моделирование

- Описание модели основывается на тех же данных, что и во 3-ей группе подходов
- Поиск пути осуществляется с учетом логико-вероятностных характеристик нарушителя, перемещающегося по графу, и алгоритма поиска пути на графе
- Рассматриваются боестолкновения между силами нарушителей и охраны (напр., расчет исхода столкновения по формуле Ланчестера)



05.13.01 «Системный анализ, управление и обработка информации»

- **«Системный анализ, управление и обработка информации (по отраслям)»** — специальность, занимающаяся проблемами разработки и применения методов системного анализа сложных прикладных объектов исследования, обработки информации, **целенаправленного воздействия человека на объекты исследования, включая вопросы анализа, моделирования, оптимизации, совершенствования управления и принятия решений, с целью повышения эффективности функционирования объектов исследования**
- Значение решения научных и технических проблем данной специальности для народного хозяйства состоит в **разработке новых и совершенствовании существующих методов и средств анализа обработки информации и управления сложными системами, повышения эффективности надежности и качества технических, экономических, биологических, медицинских и социальных систем**

05.13.01 «Системный анализ, управление и обработка информации»

Представленная работа удовлетворяет следующим пунктам паспорта специальности 05.13.01 – «Системный анализ, управление и обработка информации (по отраслям)»:

п2. **Формализация** и **постановка задач системного анализа**, **оптимизации**, управления, **принятия решений** и **обработки информации**.

п3. **Разработка** критериев и **моделей** описания и **оценки эффективности решения** задач системного анализа, оптимизации, управления, принятия решений и обработки информации.

п**4.** **Разработка методов** и **алгоритмов** решения задач системного анализа, оптимизации, управления, принятия решений и обработки информации.

п5. **Разработка** специального **математического** и **алгоритмического обеспечения** систем анализа, оптимизации, управления, принятия решений и обработки информации.

п11. **Методы** и **алгоритмы прогнозирования** и **оценки эффективности**, **качества** и надежности сложных систем.

п12. **Визуализация**, трансформация и **анализ информации на основе компьютерных методов обработки информации**.

п13. Методы получения, анализа и обработки экспертной информации.

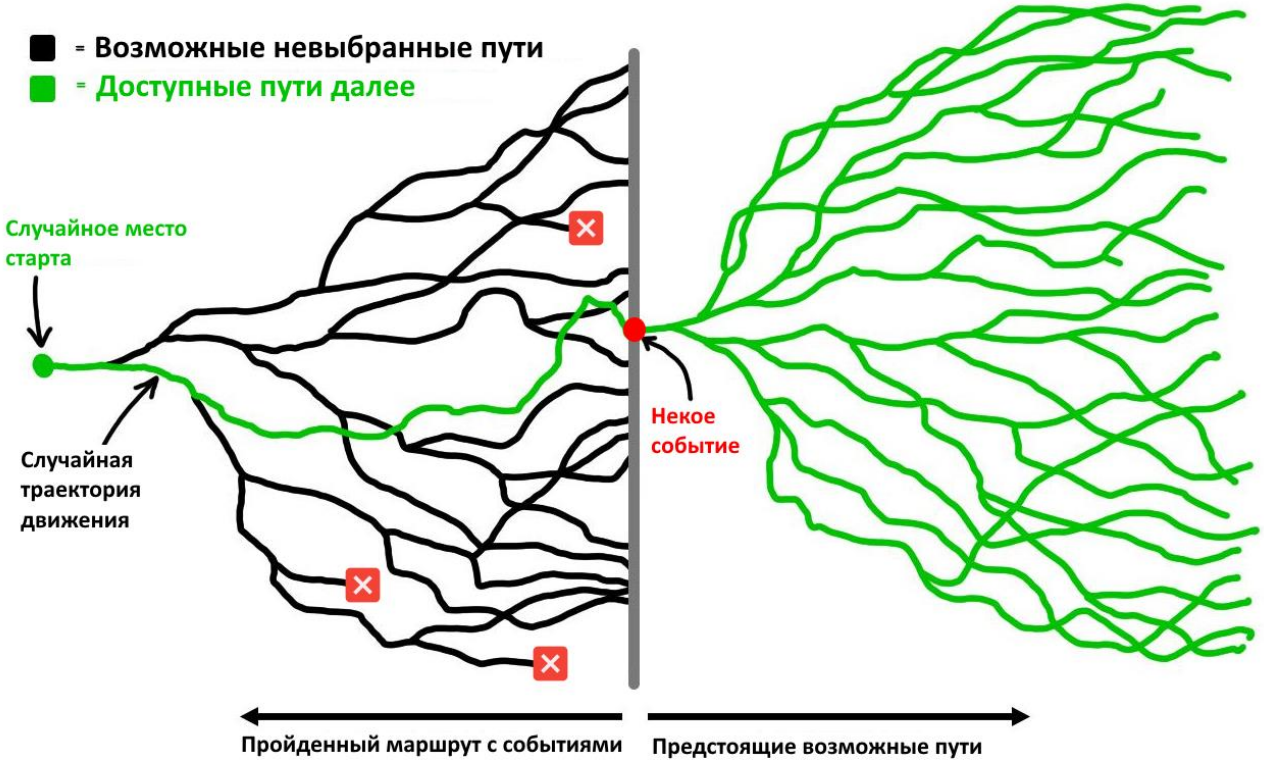
Основные недостатки существующих подходов

У всех групп и методик в них можно выделить следующие недостатки:

- Моделируются **только** **существующие** (готовые) **СФЗ** или их абстракции
- **Невозможно** **учесть все** возможные **сценарии** моделирования проникновения по графам
- **Затруднительно** **моделировать** подробную структуру СФЗ на большой площади
- Используются **субъективные** экспертные параметры
- **Затрудняется** **чтение** исходных данных о системе при использовании нечетких множеств

Случайный сценарий в ходе статист. испытаний:

Непредсказуемый ход развития событий

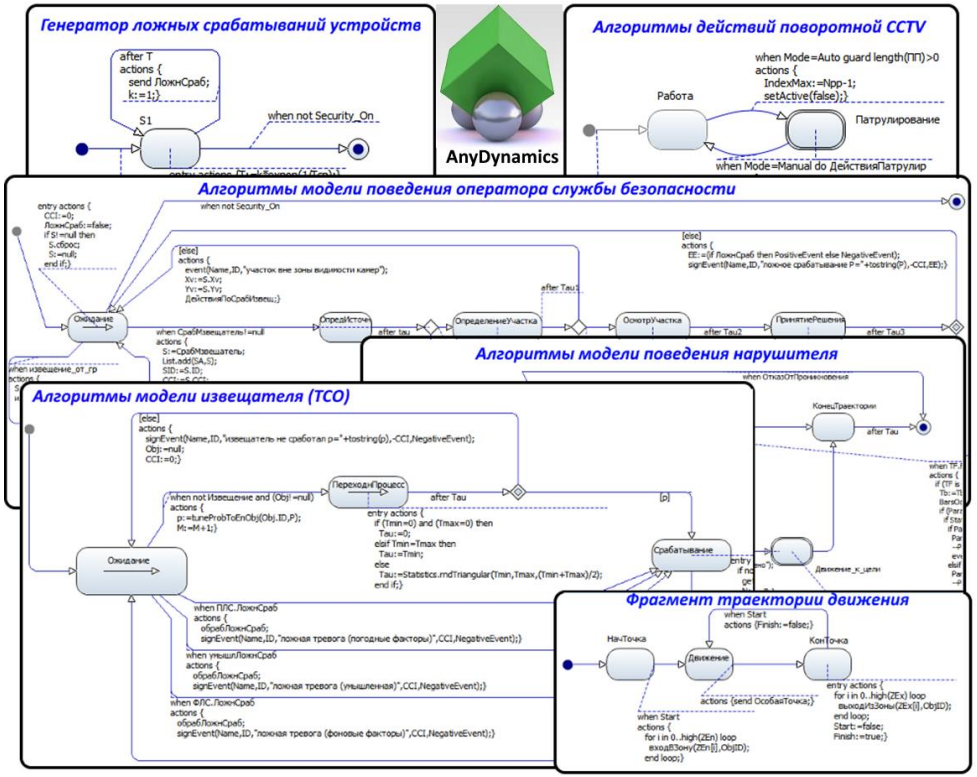


Реализация предлагаемого подхода:

Создание имитационной модели в **AnyDynamics**

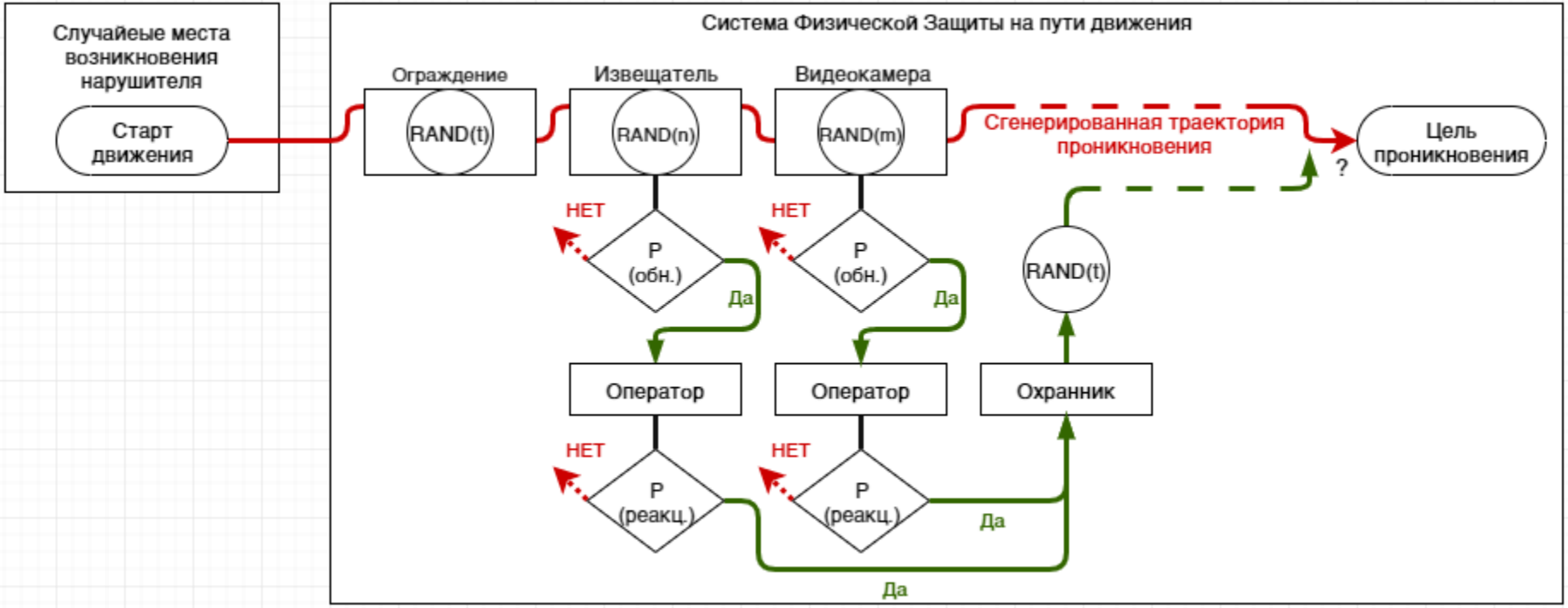
AnyDynamics подходит для задач моделирования жизнедеятельности крупномасштабных систем (систем физической защиты):

- Динамическое моделирование всех элементов системы
- Создание гибких логических моделей с применением вероятностей
- Возможность подробного пошагового моделирования всех процессов отработки систем безопасности и их реакции на каждое действие со стороны моделируемой проникающей угрозы
- Возможность интеграции моделей в различные программные обертки



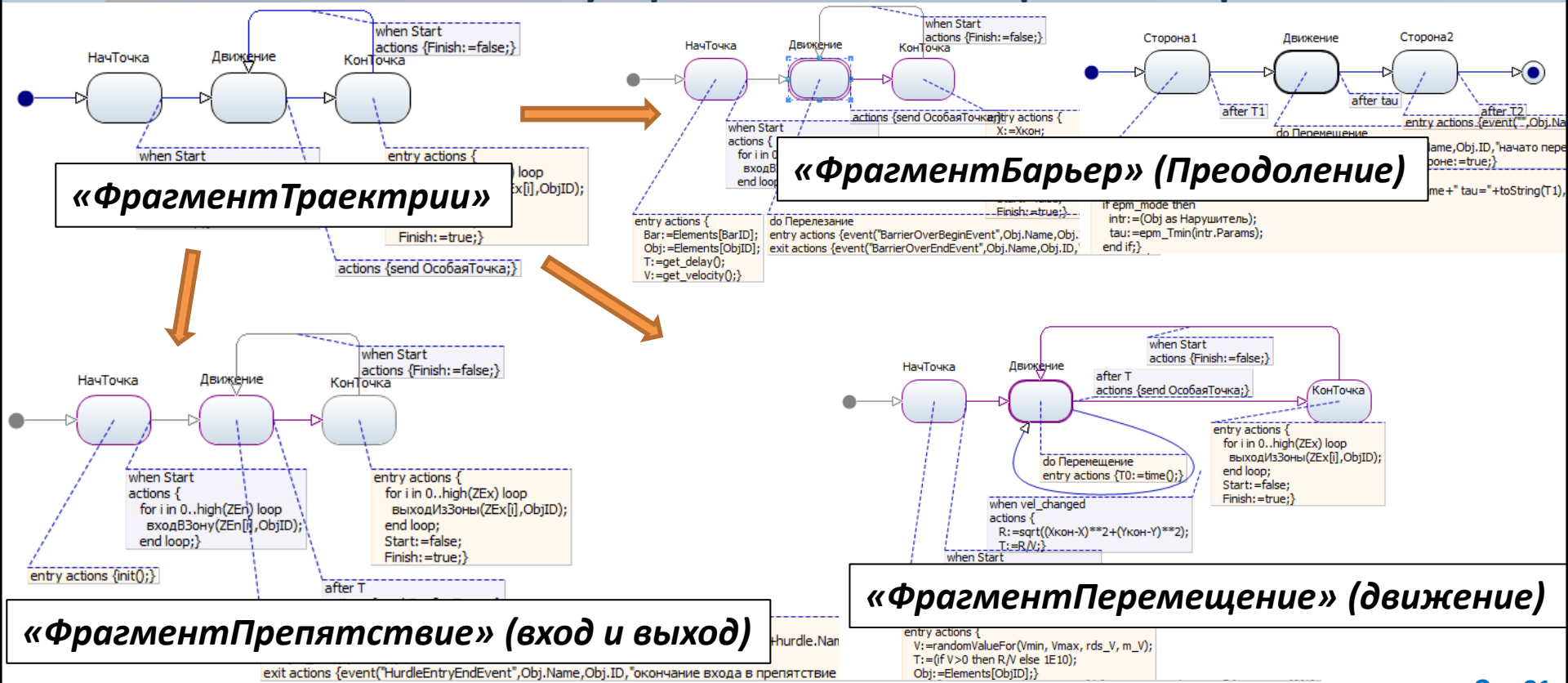
Предлагаемый подход:

Локальные правила взаимодействия агентов



Предлагаемый подход:

Состав событийно-управляемой траектории

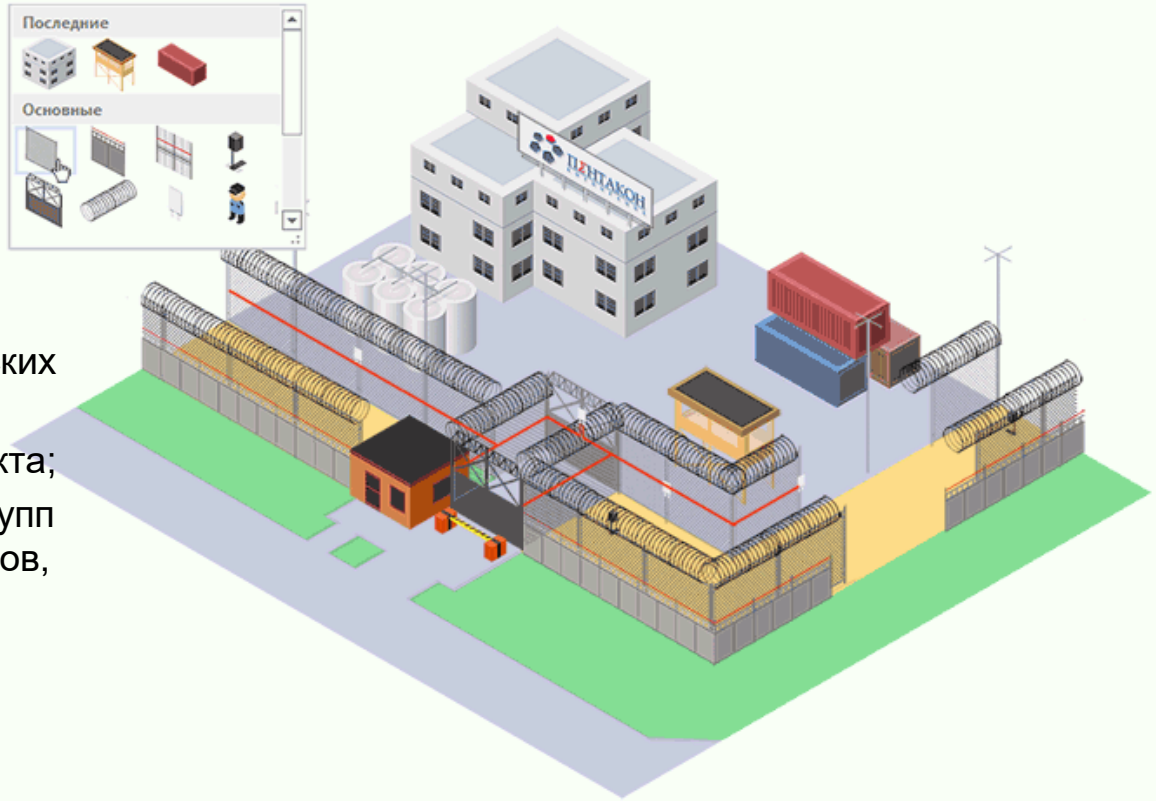


Графический редактор модели:

Цифровой двойник охраняемого объекта

Цифровой двойник СФЗ объекта состоит из территории, ИТСО и СБ:

1. Представление инфраструктуры и топологии территории объекта
2. Указание мест охраняемых зон и зон особого доступа
3. Элементы инженерных и технических средств охраны
4. Силы Службы Безопасности объекта;
5. Правила и логики действий для групп реагирования, патрулей, операторов, технических систем и их взаимодействия
6. И т. д.



Графический редактор модели:

Внешние условия и акт незаконного вмешательства (проникновение)

Добавление элементов условий проникновения и мест возникновения нарушителя:

1. Выбор внешних условий: погода, наличие саботажа и т.п.
2. Определение и выбор вероятных целей проникновения
3. Выбор и настройка моделей нарушителя
4. Выбор места возникновения
5. Проведение множества экспериментов с проникновением нарушителя на территорию цифрового двойника объекта