МОДЕЛИРОВАНИЕ И ОЦЕНКА КАЧЕСТВА СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ НА ОСНОВЕ АГЕНТНОГО ПОДХОДА И АЛГОРИТМА СОБЫТИЙНО-УПРАВЛЯЕМЫХ ТРАЕКТОРИЙ

И.К. Шарков, Ю.Б. Сениченков (Санкт-Петербург), Ю.Б. Колесов (Москва)

Введение

Обеспечением безопасности на охраняемой территории занимаются системы физической защиты (СФЗ). СФЗ – кибер-физическая система, использующая физические технические и инженерные средства охраны, а также человеческие ресурсы службы безопасности. СФЗ размещается на реальном объекте и позволяет противостоять атакам нарушителя на охраняемый объект. Эффективность СФЗ определяется оценками качества. Основными оценками качества СФЗ в распространенной практике являются вероятности обнаружения $P_{Обн.}$ и нейтрализации $P_{Нейтр.}$ на пути проникновения вероятного нарушителя.

Для получения оценок качества СФЗ используются следующие методы: натурные испытания, экспертная оценка и вычислительный эксперимент. Натурные испытания длительны, дороги и осуществимы только для уже построенной системы. Экспертная оценка содержит в себе субъективную составляющую, которую необходимо подкреплять. Вычислительный эксперимент позволяет путем применения методик и инструментов математического моделирования для анализа СФЗ минимизировать субъективную составляющую экспертного мнения и подкрепить его с помощью математически обоснованных характеристик и оценок эффективности СФЗ.

Моделирование и оценка качества СФЗ – сложная комплексная задача, актуальная как с точки зрения практики, так и законодательства. Существуют множество различных подходов к моделированию и оценке качества таких систем. Предлагаемы агентный подход моделирования позволяет подробно описать структуру СФЗ на уровне её локальных элементов (агентов) и законов их взаимодействия, а алгоритм событийно-управляемых траекторий дает возможность осуществлять имитационные эксперименты без заранее подготовленных сценариев или графов. Такая модель будет максимально приближена по своим свойствам и характеристикам к реальной СФЗ, противостоящей нарушителю, а оценка её эффективности будет основана на статистических испытаниях с проникновением с разных направлений атак.

1. Краткий обзор существующих подходов моделирования систем физической защиты

Первый работы по моделированию СФЗ связанны с анализом уязвимостей объектов атомной энергетики [1-3] и программными комплексами EASI и ASSES («Сандийские национальные лаборатории», США). В обзорах часто упоминаются отечественные программные комплексы СПРУТ (НПП «ИСТА-Системс), ВЕГА-2 (СНПО «Элерон»), Итерация (АО «Итерация»), САПР СИТЗО «Амулет» (АО Производственно-внедренческое предприятие «Амулет»). Часто структура системы упрощается (СФЗ описывается точками контроля и их параметрами), проникновение нарушителя происходит по заранее заданным сценариям (используются графы атак [4, 5]), и оцениваются вероятностно-временные характеристики эффективности СФЗ. Применение подхода имитационного моделирования ограничивается поиском пути на графе с помощью эвристических алгоритмов и логико-вероятностных характеристик (поиск самого уязвимого пути на графе) [6], а также методом точечных статистических испытаний [7]. В отдельных случаях проводится игровое моделирование с боестолкновением нарушителей и охранников [8].

Существуют различные способы расчета $P_{Обн}$ – вероятности обнаружения нарушителя и $P_{Нейтр.}$., вероятности того, что нарушитель будет своевременно

нейтрализован силами службы безопасности объекта до момента достижения цели проникновения. Для нейтрализации время реакции и выдвижения охранников на перехват с момента обнаружения проникновения должно быть меньше, чем оставшееся время движения нарушителя до цели.

Для оценки качества СФЗ разрабатываются сценарии проникновения нарушителя через череду препятствий. Сценарии можно представить виде графа путей [9], у которого вершины связаны с препятствиями, а ребра – с движением нарушителя по выбранному пути (рис. 1). Реализация сценария сводится к построению конкретного пути, в зависимости от реализовавшихся событий, и позволяет определить искомые вероятности $P_{Обн.}$ и $P_{Нейтр.}$ с помощью аналитических расчетов или статистического эксперимента.

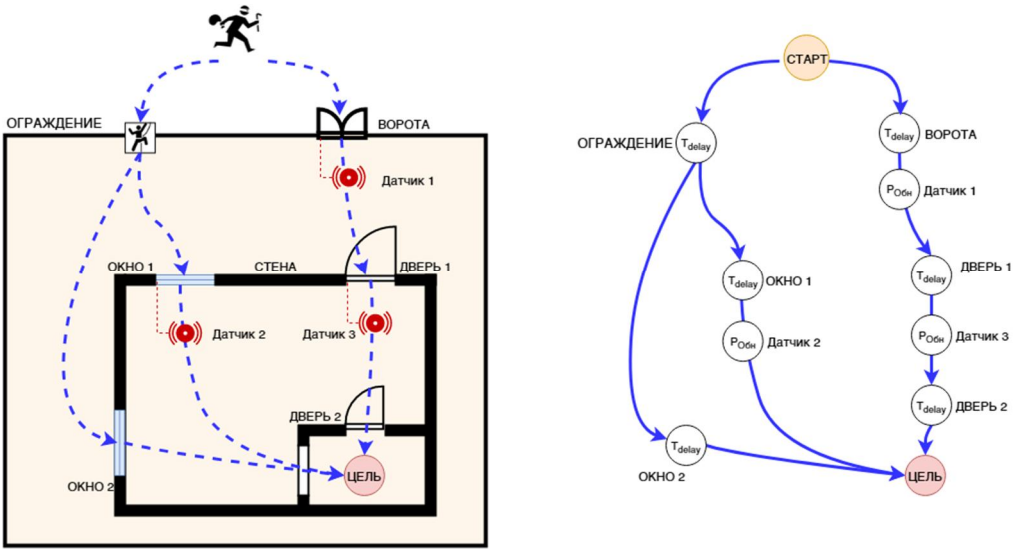

Рис. 1. Представление сценариев проникновения нарушителя в виде графа

Использование графа атак типично для моделирования СФЗ. Большинство существующих подходы моделирования СФЗ можно объединить в четыре группы [9] по способу получения оценки:

1. оценки вероятности обнаружения в случайной точке на территории объекта и перехвата нарушителя на пути до цели (например, «САПР СИТЗО» Амулет);
2. оценка эффективности СФЗ на заданном пути при заданных условиях и состоянии системы;
3. оценка эффективности СФЗ на основе анализа графов путей нарушителя по территории объекта (например, «ВЕГА-2» СНПО Элерон);
4. игровые и имитационные модели для оценки эффективности СФЗ (например, «ПОЛИГОН» СНПО Элерон, «Итерация-СФЗ» Итерация).

2. Выбор программного средства для разработки моделей и алгоритмов

Существуют различные среды моделирования, основанные на математическом моделировании: MATLAB, Dymola, AnyDynamics, AnyLogic, LabView или другие. Среди этих инструментов необходимо было выбрать такой, который позволил бы создавать интегрируемые модели для их дальнейшего использования в других программах. Создаваемые модели должны быть легко читаемыми и понятными сторонним экспертам, легко модифицируемыми. Это крайне важно, когда речь идет о новых требованиях к охране объектов, появлении новых элементов системы защиты (видеокамер, извещателей), о появлении угроз, которые ранее не принимались в расчет или не были до конца изучены (например, БПЛА-нарушители).

Для разработки агентной модели СФЗ был выбран отечественный продукт имитационного моделирования – AnyDynamics (существенно модифицированный вариант среды Rand Model Designer), использующий объектно-ориентированный язык моделирования (ООМ) высокого уровня, основанный на объектной парадигме UML, позволяющий создавать модели крупномасштабных систем [10, 11]. AnyDynamics позволил создать все необходимые модели: человека-охранника, датчиков, погодных условий, имитировать ложные тревоги, и экспортировать построенную модель в виде динамической библиотеки Windows (DLL).

3. Агентный подход моделирования СФЗ

Для моделирования и анализа качества СФЗ используется кортеж:

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

где: «Объект» содержит в себе все моделируемые элементы СФЗ, топологию объекта и инфраструктурные особенности; «Проникновение» – описывает Акт Незаконного Вмешательства (событие), движение нарушителя через охраняемую зону «Объекта» по выбранном пути к цели проникновения, используя конкретную 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.

Всю структуру СФЗ можно описать с помощью её базовых элементов: инженерных и технических средств охраны (ИСО и ТСО), а также сил службы безопасности (СБ) – каждая сущность, будь то извещатель или охранник, будет представлена своей собственной математической моделью - агентом. Особенность агентного подхода заключается в том, что каждый элемент может функционировать независимо от остальных, а взаимодействие с другими осуществляется с помощью внешних связей, глобальных параметров и описанных локальных законов. Вместе они формируют единую взаимосвязанную систему охраны.

В соответствии с формулой (1) была разработана модель со следующей структурой:

- **Модель > Объект > СФЗ > ИСО:**
  - **Барьер** – протяженный элемент ИСО (например, ограждение), сдерживающий проникновение по времени при его сквозном поперечном пересечении;
  - **Препятствие** – элемент ИСО, представленный пространством, замедляющим скорость проникновения;
- **Модель > Объект > СФЗ > ТСО:**
  - **Извещатель** – устройство обнаружения проникновения, подающее сигнал тревоги с собственной вероятностью $P_{Обн}$;
  - **Видеокамера** – устройство визуального обнаружения;
- **Модель > Объект > СФЗ > Служба Безопасности:**
  - **Оператор** – сотрудник СБ, выполняющий мониторинг сигналов тревоги, принимающий решения и осуществляющий контроль и командование охраной при обнаружении нарушителя;
  - **Группа реагирования** (охранник/патруль) – сотрудники СБ, выполняющие перехват нарушителя и пассивный мониторинг объекта в своей локально зоне видимости или выполняющий цикличный обход объекта;

- **Система видеоаналитики** – система, занимающаяся сбором и анализом информации с видеокамер;

· **Модель > Проникновение**
- **Периметр возникновения нарушителя** – заданный периметр, на котором с равномерным законом распределения по всей длине возникает нарушитель;
- **Нарушитель** – злоумышленник, проникающий на территорию объекта к выбранной цели, обладающий набором заданных параметров и психофизических характеристик;
- **Траектория движения** – траектория проникновения к цели;

· **Модель > Внешние условия**
- **Погода** – совокупность внешних факторов среды, влияющих на дистанцию обзора, вероятность срабатывания тех или иных устройств, частоту ложных тревог и т.д.
- **Наработка на ложную тревогу** – модель, описывающая вероятность и устройство возникновения сигнала ложной тревоги в СФЗ;

· **Модель > Исход > Цель проникновения** – точка или область, в которую стремится попасть нарушитель для осуществления преступных действий.

Каждый агент имеет свои параметрами. Так, например, элементы технических средств охраны могут быть описаны параметрами, соответствующими их паспортным характеристикам: геометрией зоны обнаружения, вероятностью обнаружения, временем обработки и передачи сигнала и т.п. Это относится так же и к инженерным средствам охраны.

Параметры, описывающие человеческие характеристики и взаимодействие элементов с человеком (например, преодоление ограждения), для повышения их объективности должны быть описаны с помощью вероятностных характеристик или случайных параметров в заданных интервалах с указанным законом распределения.

4. Создание сценария проникновения

Для создания сценария применяется алгоритм, использующий карты поведения среды AnyDynamics, в основе которого лежит динамически формируемая траектории движения, разбиваемая событиями на отдельные фрагменты. Сценарий - это последовательность событий, координат точек, где эти события произошли, и фрагментов траекторий между ними. События формируются динамически, как результат взаимодействия агентов. Это укладывается в парадигму уже существующих методик моделирования и оценки качества СФЗ, но при этом нет необходимости использовать заранее заготовленные сценарии или графы атак. В предлагаемом подходе сценарий движения нарушителя может быть скорректирован прямо по ходу эксперимента, если траектория из места положения нарушителя была изменена под действием логико-вероятностных характеристик модели.

Точками событий, разделяющими путь нарушителя на фрагменты траектории, могут являться:

· точка принятия решения о смене направления движения (переход на новую траекторию);

· точка принятия решения о смене скорости движения;

· точка начала и точка окончания преодоления препятствия;

· точка входа в зону обнаружения и точка выхода из неё;

· и т.д.

Аналогичный подход применяется и для формирования сценария движения охранников. Фактически, каждое значимое для мобильного агента событие может повлиять на формирование сценария его движения через структуру СФЗ.

Пример разбитого на фрагменты пути движения нарушителя можно увидеть на рис. 2:

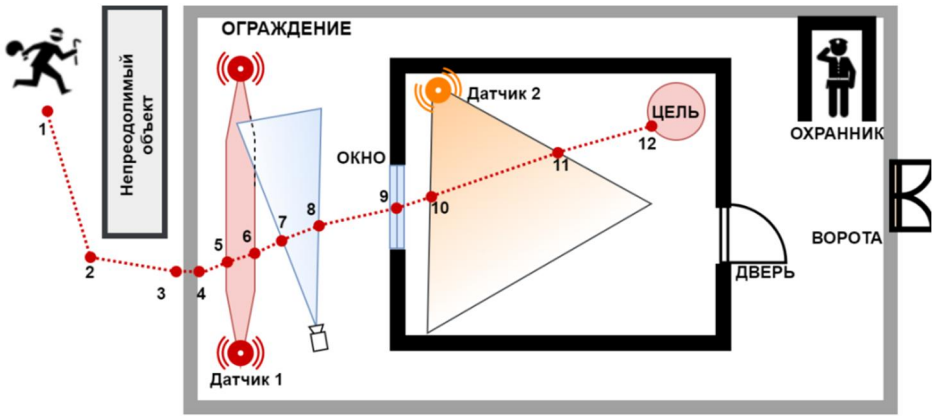

Рис. 2. Траектория проникновения нарушителя, разбитая на множество фрагментов событиями (особые точки) от старта (1) до финиша (12)

На рис. 2 видно, что путь нарушителя разделен на фрагменты событиями: 1 – начало движения, 2 – смена направления (обходит препятствие), 3-4 – преодоление ограждения, 5-6 – пересечение зоны обнаружения первого датчика, 7-8 – пересечение зоны обзора видеокамеры, 9 – задержка при преодолении окна, 10-11 – пересечение зоны датчика в помещении, 12 – достижение цели проникновения.

Для формирования событийно-управляемых траекторий используется прокладчик пути «Polaris» [12]. «Polaris» формирует траекторию между текущим положением нарушителя и целью его движения в пространстве со сложной геометрией различных препятствий для больших охраняемых объектов. Проложенный путь разделяется на фрагменты событиями, привязанными к координатной сетке, на которой взаимодействуют различные агенты СФЗ. Событийно-управляемые траектории описывают условия «свободного перемещения» и «преодоления препятствия». В практической реализации предлагаемой методики фрагменты событийно-управляемой траектории описаны абстрактным классом «ФрагментТраектори» (рис. 3), дочерними классами «ФрагментПеремещение» (свободное движение), «ФрагментБарьер» (замедление перемещения по времени, например на ограждении) и пара «ФрагмВходПреп» и «ФрагмВыходПреп» (пересечение сложного препятствия, например охранный ров).

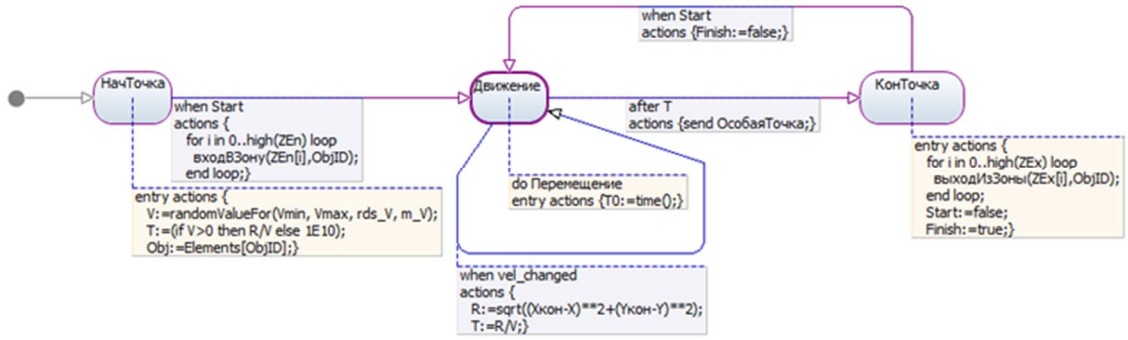

Рис. 3. Класс «ФрагментПеремещение» на основе абстрактного класса «ФрагментТраектории»

Состояния начальной и конечной точки – это границы, между которыми осуществляется движение. В течение интервала времени T пока состояние «Движение» с непрерывной локальной деятельностью «Перемещение» является текущим, координаты X и Y объекта непрерывно изменяются в соответствии с уравнениями:

$$
\begin{gathered}
d(X)/dt = Vx \\
d(Y)/dt = Vy \\
Vx = V*cosA*D \\
Vy = V*sinA*D \\
\text{unknown } X, Y, Vx, Vy
\end{gathered} \qquad (2)
$$

Перемещению по различным участкам местности (свободный участок, водоем, препятствие и т.п.) соответствуют различные значения параметров Vmin и Vmax.

Классы «ФрагмВходПреп» и «ФрагмВыходПреп», как и «ФрагментБарьер» тоже являются потомками класса «ФрагментТраектории». В них заданы дополнительные параметры Tmin и Tmax, описывающее затраченное время на границах препятствия или при преодолении барьера, добавлены некоторые внутренние переменные и переопределена карта поведения. Внешний вид общей UML-схемы для этих классов сохраняется, а для «ФрагментБарьер» добавляется локальная деятельность для состояния «Движение», описывающее перемещение нарушителя через любой вид барьеров СФЗ (ограждения, заграждения и т.п.) с формулами непрерывной в деятельности, аналогичными (2):

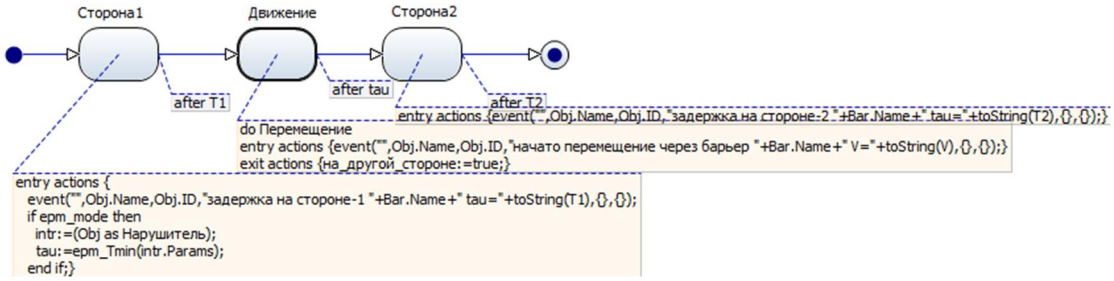

Рис. 4. Локальная деятельность в состоянии «Движение» класса «ФрагментБарьер»

Количество классов, описывающих процесс движения нарушителя на фрагментах в тех или иных условиях, может быть увеличено при необходимости, если такое требуется в задачах моделирования СФЗ. Движение через зоны обнаружения и обзора ничем не отличается от стандартного перемещения по какому-либо участку местности и может соответствовать нахождению нарушителя, как на открытом пространстве, так и на ИСО.

Пример простого сценария движения можно увидеть на рис. 5, где нарушитель во время движения (S1,S3) преодолевает пространство с барьером (S2) и препятствием (S4,S6), где нужно войти, двигаться внутри (S5) и выйти с другой стороны:

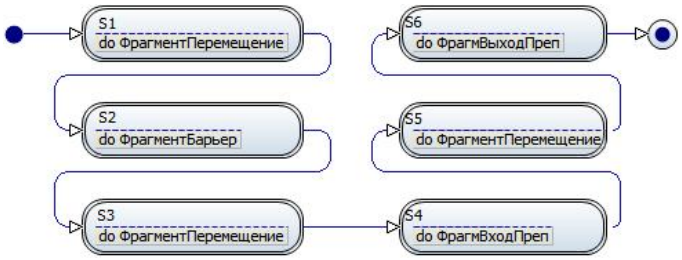

Рис. 5. Фрагменты траектории в простом сценарии движения нарушителя через барьер и препятствие

5. Оценка качества СФЗ с помощью предлагаемого подхода

Так как построение аналитических зависимостей для определения вероятностей $P_{Обн.}$ и $P_{Нейтр.}$ затруднительно из-за высокой сложности агентной модели, можно использовать метод статистических испытаний (метод Монте-Карло) [13, 14]. Предлагаемый подход моделирования и оценки СФЗ с помощью агентного подхода и событийно-управляемых траекторий позволяет проводить статистический эксперимент

с проникновением нарушителя. Для каждого агента исследуемой системы и события в ней предлагается «розыгрыш» случайных параметров в описанных диапазонах и получение с помощью вычислительного эксперимента множества «реализаций» фазовой траектории этой системы (испытаний). Результаты записывается в локальную базу данных и обрабатываются обычными методами математической статистики.

С помощью доверительного интервала можно определить достаточное количество экспериментов, необходимое для получения оценок $P_{Обн.}$ и $P_{Нейтр.}$ с заданной надежностью. Искомая вероятность p определяется как частота $\overline{P}$:

$$p_{\text{Нейтр}} \approx \overline{P_{\text{Нейтр}}} = {}^{M}/_{N} \quad (3)$$

где N – общее число всех экспериментов с проникновением нарушителя, а M – число испытаний, в которых нарушитель был пойман

Вероятность того, что искомая вероятность p и частота $\overline{P}$ будут отличаться не более чем на величину ε, определяется по формуле:

$$P(|P = p| < \varepsilon) = 2\Phi\left(\frac{\varepsilon\sqrt{N}}{\sqrt{p(1-p)}}\right) \quad (4)$$

где Ф – функция Лапласа.

Выводы

В данной статье предложен новый метод моделирования и оценки качества СФЗ на основе агентного подхода с использованием алгоритма формирования событийно-управляемых траекторий.

Данный подход позволяет описать модель СФЗ с высокой точностью, недоступной для других существующих подходов, исключает необходимость в заранее заготовленных сценариях и графе путей проникновения, а также полностью автоматизирует процесс постановки сценариев проникновения, что отводит роль эксперта на этап оценки результатов моделирования.

Построена имитационная модель СФЗ, сотрудников служб безопасности объекта и нарушителя с помощью агентного подхода и алгоритм формирования событийно-управляемых траекторий для создания сценариев проникновения нарушителя и движения охранников.

Для разработки моделей использовалась среда моделирования AnyDynamics, алгоритм поиска пути «Polaris» и среда графического проектирования моделей СФЗ в виде плана «АКИМ» (ООО «ПЕНТАКОН»).

Литература

1. **D.L. Siazon Jr.** The convention on the physical protection of nuclear material, IAEA BULLETIN, vol. 22, nos. 3, pp. 57-62, 1980.
2. **J.C. Matter,** SAVI: A PC-Based Vulnerability Assessment Program, SAND88-1279. Albuquerque, NM: Sandia National Laboratory, 1988.
3. **Sasser D.W.** Users guide for EASI graphics - Sandia Labs., 1978 Albuquerque, N.Mex. (USA). С. 37-39.
4. **Тарасов А.Д.** Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: дис. на соиск. учен. степ. канд. тех. наук: 05.13.19: защищена 15.12.17 / Тарасов Андрей Дмитриевич. Уфа, 2017. 144 с.
5. **Степанов Б.П., Годовых А.В.** Основы проектирования систем физической защиты ядерных объектов: учебное пособие / Томский политехнический университет. Томск: Изд-воТомского политехнического университета, 2009. 118 с.
6. **Олейник А.С.** Методика использования имитационной модели для совершенствования системы физической защиты ядерно опасных объектов // Труды

Академии управления МВД России. 2011. № 4(20). С. 114-117.
7. **Мосолов А.С.** Оценка эффективности системы безопасности на основе метода Монте-Карло // Системы безопасности. 2014. No 1. С. 74-77.
8. **Измайлов А.В., Журин С.И.** Защита критически важных объектов. Система оценки состояния СФЗ // Системы безопасности. 2012. №6.
9. **Шанаев Г.Ф.** Системы защиты периметра / Г.Ф. Шанаев, А.В. Леус. М.: Security Focus,. 2011. 280 с.
10. **Ю.Б. Колесов Ю.Б. Сениченков.** Математическое моделирование гибридных динамических систем. СПб.: Изд-во СПбГПУ, 2014. 236 с.
11. **Ю.Б. Колесов, Ю.Б. Сениченков.** Объектно-ориентированное моделирование в среде Rand Model Designer 7: Изд. Проспект, 2016. 256 с.
12. **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.
13. **Вентцель Е.С.** Исследование операций. М.: «Советское радио», 1972. 552 с.
14. **И.М. Соболь.** Метод Монте-Карло. – М.: Наука, 1978. 64 с.