DOI: 10.58168/MIST2025_341-344
УДК 004.9

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ДЛЯ ЭФФЕКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СЕТЕЙ

А.К. Назарова[1], Т.В. Скворцова[1], А.С. Кравченко[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В данной статье анализируется моделирование, используемое для защиты систем. Имитационное моделирование – это распространенный вид аналогового моделирования, реализуемый с использованием набора математических инструментов, специальных программ компьютерного моделирования и специальных ИТ-инструментов, позволяющих создавать аналоговые процессы в памяти компьютера, с помощью которых можно проводить целенаправленное изучение структуры и функций реальной системы в режиме ее "имитации", а также оптимизируйте некоторые из его параметров.

Ключевые слова: защита, система, имитационное моделирование.

USING SIMULATION MODELING TO EFFECTIVELY PROTECT SYSTEMS

A.K. Nazarova[1], T.V. Skvortsova[1], A.S. Kravchenko[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This paper analyzes the simulation used to protect systems. Simulation modeling is a common type of analog modeling implemented using a set of mathematical tools, special computer simulation programs, and special IT tools that allow creating analog processes in computer memory, with which you can conduct a targeted study of the structure and functions of a real system in its "imitation" mode, and optimize some of its parameters.

Keywords: protection, system, simulation modeling.

Имитационное моделирование представляется в виде математического моделирования в сочетания с компьютерными технологиями. Создаются такие модели для наглядного и точного описания характеристик конкретных объектов.

На основе подобных моделей, возможно помимо обычного объяснения, предсказать то, как поведет та или иная система на практике.

Имитационное моделирование обращаются в следующих случаях:

- Если затраты на проведение экспериментов на реальном объекте или системе слишком велики, или проведение таких экспериментов в принципе невозможно.
- Если имитационная модель имеет наличие многих случайных перемен которые нельзя математически просчитать.

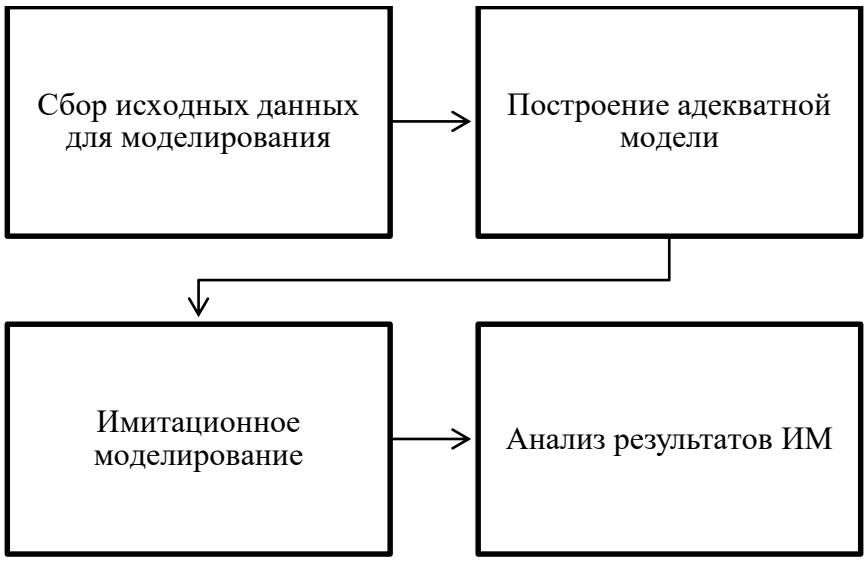

Рисунок 1 – Этапы построения имитационной модели

Информационная среда появилась с переходом нашего общества от постиндустриального периода к информационному периоду. В котором качество обмена информацией через информационные сети, такие как, скорость, надежность, и конфиденциальность, стали ключевыми факторами, как для обычного пользователя, так и для транснациональных компаний и государств. Информационная среда, состоит из набора сегментов, затрагивающих разные аспекты жизни человека: программные средства, информационные и медиа ресурсы. Создавая целые организм, как грибница, она так же подтверждена потенциальным угрозам, со стороны злоумышленников, так и со стороны пользователей и человеческого фактора.

Обычное разрозненное исследование угроз безопасности информационных сетей может не дать комплексного виденья сильных и слабых сторон защиты сети. Поэтому не редко к подобному анализу проектов, используют имитационное моделирование.

Блочный принцип имитационных моделей, позволяет разбить любую систему на визуально понятные и читаемые блоки, связанные между собой определенным числом связей. На основе результатов работы с имитационными моделями, достаточно просто заменять отдельные блоки, не нарушая основную структуру модели.

Так же имитационные модели позволяют просчитать риски и последствия различных нарушений работы сети, как из-за внешних атак, так и из-за халатности личного персонала. Что в свою очередь позволяет выстроить алгоритм действий при той, или иной ситуации, а также просчитать финансовые потери.

Благодаря функционалу имитационного моделирования, можно рассмотреть не только критические ситуации информационной сети, но так же спрогнозировать производительность сети или конкретных ее частей. Оптимальные пути ее развития, оптимизация затрачиваемых компьютерных или сетевых ресурсов.

Основным направлением развития имитационных моделей будет использование машинного обучения. В анализе информационных систем, ИИ может предсказывать поведение, как пользователей, так и хакеров, воссоздавая максимально точное поведение и тактику атак на сетевую инфраструктуру.

Из вышеперечисленного можно сделать вывод, что имитационное моделирование как никогда актуально, и имеет пути развития. Благодаря проведению достаточно точных экспериментов, не подвергая риску реальную инфраструктуру. Рассматривая сеть в полном ее исполнении или конкретную ее часть, заменяя ее отдельные модули, под определенные цели и задачи. Позволяет использовать данный метод, как на обычном пользовательском уровне, так и в стратегически важных отраслях, таких как медицина, производственные линии или оборонная промышленность.

Список литературы

1. Юрчишина, М. В. Алгоритмическая модель СППР «Оптимальный учебный план» / М. В. Юрчишина, К. И. Бушмелева // Моделирование систем и процессов. – 2024. – Т. 17, № 4. – С. 84-95. – DOI 10.12737/2219-0767-2024-17-4-84-95. – EDN OJFBGD.

2. Высоцкая, И. А. Обоснование информационно-интеллектуальной поддержки принципов действия технических систем / И. А. Высоцкая // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 19-26. – DOI 10.12737/2219-0767-2024-17-1-19-26. – EDN DCEATL.

3. Высоцкая, И. А. Обоснование методов поиска принципов действия сложных технических систем и объектов / И. А. Высоцкая // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 27-34. – DOI 10.12737/2219-0767-2024-17-1-27-34. – EDN GASZOW.

4. Карпов В.В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа. // Программные продукты и системы. – 2003. – №1. – С. 31

5. Девянин П.Н., Михальский О.О. и др. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.

References

1. Yurchishina, M. V. Algorithmic model of the DSS "Optimal curriculum" / M. V. Yurchishina, K. I. Bushmeleva // Modeling of systems and processes. – 2024. – Vol. 17, No. 4. – pp. 84-95. – DOI 10.12737/2219-0767-2024-17-4-84-95. – EDN OJFBGD.

2. Vysotskaya, I. A. Substantiation of information and intellectual support for the principles of operation of technical systems / I. A. Vysotskaya // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – pp. 19-26. – DOI 10.12737/2219-0767-2024-17-1-19-26. – EDN DCEATL.

3. Vysotskaya, I. A. Substantiation of methods of searching for principles of operation of complex technical systems and objects / I. A. Vysotskaya // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – PP. 27-34. – DOI 10.12737/2219-0767-2024-17-1-27-34. – EDN GASZOW.

4. Karpov V.V. Probabilistic model for assessing the security of computer equipment with a hardware and software package for protecting information from unauthorized access. // Software products and systems. – 2003. – No. 1. – p. 31

5. Devyanin P.N., Mikhalsky O.O. and others. Theoretical Foundations of computer security. Moscow: Radio and Communications, 2000.