УДК 004.051

АНАЛИЗ ТЕХНОЛОГИИ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ ВИЗУАЛИЗАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Ф.М. Пыршев
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail pyrshev.f.m@edu.mirea.ru

П.И. Карасев
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail karasev@mirea.ru

Almali Ahmed Adnan Lateef
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: AlmaliAhmedAdnan@mail.ru

Al-Ameedee Mustafa Abdulkadhim Dhahir
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: AmeedeeMustafa@mail.ru

Ключевые слова: имитационное моделирование, технические средства защиты информации, визуализация, модели угроз, анализ реакции системы, тестирование стратегий безопасности, процессы защиты, технология, инструмент, информационная безопасность.

Аннотация: В статье рассматривается технология имитационного моделирования как инструмент для визуализации технических средств защиты информации. Описываются основные особенности технологии, такие как создание моделей угроз, анализ реакции системы, тестирование стратегий безопасности и визуализация процессов защиты.

1. Введение

В современных условиях защита информации является одной из важнейших задач для организаций любого масштаба. Для обеспечения эффективной защиты необходимо учитывать множество факторов, таких как тип информации, используемая инфраструктура, потенциальные угрозы и способы их реализации. Для эффективной защиты в современных реалиях необходимо использовать моделирование. Применительно к естественным и техническим наукам принято различать следующие виды моделирования:

- концептуальное моделирование — это метод, который позволяет воссоздать исследуемый объект или систему на основе уже известных фактов и представлений. В этом случае используются специальные знаки, символы, операции или язык;

- физическое моделирование, в свою очередь, предполагает создание модели и моделируемого объекта. Здесь модель и объект – это реальные объекты или процессы, которые могут иметь одну или различную физическую природу. При этом в модели и в объекте-оригинале выполняются схожие процессы;
- структурно-функциональное моделирование является методом представления исследуемого объекта в виде схемы, графика, чертежа, диаграммы, таблицы, рисунка или любой другой комбинации этих элементов, дополненные специальными правилами их объединения и преобразования;
- Математические модели могут быть представлены в виде уравнений, неравенств, функций и других математических выражений, а логические модели - в виде логических правил и отношений. Математическое моделирование позволяет количественно анализировать поведение объекта и делать прогнозы;
- имитационное (программное) моделирование, при котором логико-математическая модель исследуемого объекта представляет собой алгоритм функционирования объекта, реализованный в виде программного комплекса для компьютера.

Но возникает проблема того, что ни каждый вид моделирования подходит для решения специфических задач защиты информации:

- концептуальное моделирование недостаточно для решения некоторых проблем в рамках системы;
- физическое моделирование чаще всего избыточно, так как симуляция физических процессов не так важно для визуализации технических средств защиты информации;
- структурно-функциональное моделирование больше подходит для этой цели, но всё ещё недостаточно;
- математическое моделирование подходит для этих целей, но оно неудобно в обращении и требует высоких трудозатрат;
- имитационное моделирование же идеально подходит для той цели, сохраняя наглядность модели, позволяя решать логические проблемы и не пере усложняя модель.

Из этого следует, что имитационное моделирование является наиболее подходящим и мощным инструментом, который может помочь специалистам в решении задач защиты информации. Оно позволяет создавать виртуальные модели информационных систем и угроз, а также оценивать эффективность различных методов защиты [1].

2. Исторические примеры применения имитационного моделирования

Исторические примеры его использования в сфере безопасности информации представлены в контексте более широких областей.

Военная и военно-промышленная области (Симуляция боевых операций (20-й век)). Военные силы многих стран использовали имитационное моделирование для симуляции боевых операций и тактик. Например, во время холодной войны, моделирование ядерных взрывов и последствий ядерной войны было проведено для понимания возможных последствий и разработки стратегий противостояния [2].

Аэрокосмическая и авиационная отрасли (Моделирование полетов и тестирование безопасности (20-21 век)). В отраслях авиации и космоса использовалось имитационное моделирование для тестирования безопасности полетов. Например, создание виртуальных моделей полетов позволяло анализировать влияние различных факторов на безопасность и эффективность полетов.

Информационные технологии (Моделирование кибератак (с конца 20-го века)). С развитием компьютерных технологий и интернета имитационное моделирование начало применяться для моделирования кибератак. В истории были случаи, когда специалисты по безопасности создавали виртуальные среды для анализа и тестирования различных видов хакерских атак и вирусов [3].

3. Примеры применения имитационного моделирования для визуализации технических средств защиты информации

Имитационное моделирование может использоваться для визуализации технических средств защиты информации в следующих аспектах:

Создание моделей угроз. Имитационное моделирование позволяет создавать виртуальные модели потенциальных угроз и атак на информационные системы. Это может включать моделирование вирусов, хакерских атак, фишинговых попыток и других угроз без фактического воздействия на реальные системы. Такие модели могут использоваться для обучения персонала, тестирования систем защиты и разработки новых методов защиты.

Анализ реакции системы. С помощью имитационного моделирования можно оценить, как технические средства защиты информации реагируют на различные сценарии угроз. Моделирование позволяет определить уязвимые места в системе и эффективность существующих методов защиты. Такие результаты могут использоваться для принятия решений о модернизации системы защиты или разработке новых методов защиты.

Тестирование стратегий безопасности. Имитационное моделирование позволяет тестировать различные стратегии защиты информации. Это включает в себя изменение параметров системы без риска нанесения реального ущерба. Такие испытания могут помочь специалистам определить наиболее эффективную стратегию защиты для конкретной информационной системы [4-5].

Визуализация процессов защиты. Технология позволяет визуализировать сложные процессы защиты информации, что помогает специалистам лучше понимать систему и принимать обоснованные решения при выборе средств защиты и разработке стратегий безопасности. Такие визуализации могут использоваться для обучения персонала, демонстрации эффективности системы защиты и повышения осведомленности о вопросах информационной безопасности.

3. Заключение

Имитационное моделирование является мощным инструментом, который может быть использован для визуализации технических средств защиты информации. Оно позволяет решать широкий спектр задач, таких как создание моделей угроз, анализ реакции системы, тестирование стратегий безопасности и визуализация процессов защиты. Использование имитационного моделирования может помочь специалистам повысить эффективность защиты информации и снизить риски возникновения инцидентов информационной безопасности.

Список литературы

1. Бокова А.В., Гусев А.А. Использование имитационного моделирования в истории информационной безопасности.

2. Бокова А.В., Гусев А.А. Имитационное моделирование систем.
3. Титов В.А. Методы и технологии моделирования.
4. Гусев А.А., Карпов А.В., Карпов В.В. Информационная безопасность.
5. Шаталов А.П. Информационная безопасность.