В связи с вышеизложенным, учитывая особый статус КВОИ, наряду с такими объектами защиты, как объекты информатизации, предназначенные для обработки государственных секретов, для реализации единых подходов в обеспечении безопасности необходимо разработать и внедрить ряд документов, устанавливающих: базовую модель угроз безопасности КВОИ; базовый набор мер защиты информации; руководящие указания по выбору мер защиты информации.

УДК 519.876

Н.М. Бобович

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРИ ОЦЕНКЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Нормативные правовые акты, принятые на национальном уровне Республики Беларусь в последние годы, требуют осуществления таких мер обеспечения безопасности критически важных объектов информатизации (КВОИ), которые бы до минимума снижали как величину риска при воздействии на них дестабилизирующих воздействий, так и величину возможного ущерба [1, 2]. Одним из методов снижения риска до приемлемого уровня является управление риском (риск-менеджментом), по которым понимают процесс принятия и исполнения решений, направленных на снижение вероятности неблагоприятного результата и минимизацию возможных потерь. Начальным этапом такого управления является проведение экспертной оценки возможного риска, при которой вероятны ошибки или недостаточно полный учет отдельных факторов. Чтобы избежать ситуации, когда один и тот же эксперт осуществляет оценку и несет ответственность за принимаемые решения, оценка должна проводиться разными структурными подразделениями.

Устранение перечисленных недостатков возможно за счет оценки рисков путем проверки соответствия текущего состояния безопасности требованиям международных стандартов и национальных руководящих документов.

Однако на практике КВОИ функционируют в условиях различных случайных воздействий и возмущений, поэтому система защиты КВОИ может быть описана только стохастически, а воздействие дестабилизирующих воздействий можно описать только с некоторой вероятностью. Сами КВОИ являются достаточно сложными, и их исследование осуществляется с помощью системного подхода, который во многом базируется на моделировании реальных процессов, происходящих в системе.

Используются три основных вида моделей: эвристические, натурные и математические.

Эвристические модели представляют собой образы, которые возникают в сознании исследователя (например, при формировании требований к безопасности КВОИ на этапе проектирования).

Натурные модели – подобные реальные объекты в материальном смысле слова, отличаются по размерам, материалу элементов, внешних условий и т. д. (примером могут служить исследования электромагнитных излучений технических средств КВОИ в лабораторных условиях).

Математические модели представляют собой эквивалент объекта, отражающий в математической форме важнейшие его свойства – законы, которым он подчиняется, связи, присущие составляющим его частям, и т. д. [3].

Одним из частных случаев математического моделирования является имитационное моделирование, которое успешно используется в следующих случаях: отсутствует возможность построения аналитической модели; дорого или невозможно экспериментировать на реальном объекте; требуется сымитировать поведение системы во времени.

При имитационном моделировании различают две основные разновидности данного метода: метод имитационного моделирования (статистическое моделирование); метод Монте-Карло (статистическое испытание).

Наиболее распространенной программой имитационного моделирования является GPSS (General Purpose Simulation System – система моделирования общего назначения), которая появилась в 1961 г. [4]. Программа предназначена для моделирования систем массового обслуживания. Известными версиями являются – GPSS World (1993) и Micro-GPSS (2) (1996). Основным недостатком GPSS является плохая графическая интерпретация, что снижает наглядность создаваемой модели.

Другая известная программа MATLAB, по существу, представляет собой высокопроизводительный язык, используемый для технических расчетов, причем он используется для моделирования и в тех случаях, когда задачи выражаются в форме, близкой к математической. Приложение к MATLAB – пакет Simulink позволяет пользователю на экране монитора из библиотеки стандартных блоков и модулей создавать с помощью графических связей модель устройства или процесса, т. е. имитировать работу реального объекта. При этом пользователю достаточно общих знаний при работе на компьютере и знание той предметной области, к которой принадлежит моделируемый объект.

При разработке систем измерений, испытаний и управления достаточно эффективной является среда графического программирования LabView, которая программно совместима с MATLAB и Simulink и позволяет включать в имитационную модель различные датчики, созданные в среде LabView.

Язык программирования Visim предназначен для имитационного моделирования. Он сочетает в себе характерный для Windows интерфейс, позволяет создавать блочные диаграммы и мощное моделирующее ядро [5].

Перспективным методом имитационного моделирования является программный продукт AnyLogic, первая версия которого появилась в 2000 г. AnyLogic использует универсальный объектно-ориентированный подход (язык Java), а интерфейс разработан на визуальном подходе. Поэтому платформа поддерживает все способы моделирования систем: агентное моделирование, дискретно-событийное моделирование и системную динамику [6]. AnyLogic позволяет решать разнообразные задачи в области производства, образования, здравоохранения, финансов, управления рисками и т. п.

Имитационное моделирование КВОИ и его элементов может быть осуществлено с помощью системы имитационного моделирования Arena, которая включает следующие основные подсистемы: источники (Create); стоки (Dispose); процессы (Process); очереди (Quene). От источников в модель поступают данные (объекты) со скоростью, которая задается статистической функцией. Данные (объекты) после прохождения модели поступают в сток. В очереди данные (объекты) ожидают обработки перед тем, как попасть в некоторый процесс. Время обработки (производительность процесса) может быть разной и случайной. В итоге перед некоторыми процессами образуется очередь (из данных или объектов). Как правило, Arena используется для минимизации количества данных (объектов) в очереди, причем тип очереди может быть либо последовательным (первые пришедшие в очередь первыми идут в обработку), либо стековым (последние пришедшие в очередь первыми идут в обработку).

В имитационном моделировании для решения задач теории массового обслуживания эффективно используется метод Монте-Карло (ММК) [7], который основан на получении большого числа реализаций стохастического (случайного) процесса и формируется таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи. Прямое моделирование с помощью ММК какого-либо физического процесса подразумевает моделирование поведения отдельных частей исследуемой физической системы. Поэтому, например, ММК можно использовать для моделирования устойчивости функционирования элементов КВОИ за какой-то период.

При этом следует учитывать, что в таких случаях неизвестны (или известно приближенно) средние значения каких-то параметров моделируемого устройства, а также обычно неизвестны и законы распределения этих параметров. Поэтому при ММК делаются допущения, что закон распределения либо равномерен, либо нормален.

Проведенный выше анализ показывает, что универсального метода моделирования КВОИ для оценки текущего состояния их безопасности не существует. Поэтому целесообразно моделировать подсистемы КВОИ в отдельности, используя различные программные продукты по отдельности или в их комбинации.

1. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации [Электронный ресурс] : указ Президента Республики Беларусь от 25 окт. 2011 г. № 486 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2014.

2. О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации [Электронный ресурс] : постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2014.

3. Самарский А.А., Михайлов А.П. Математическое моделирование. Идеи. Методы. Примеры : 2-е изд., испр. М. : Физматлит, 2002.

4. Томашевский В.Н., Жданова Е.Г. Имитационное моделирование в среде GPSS. М. : Бестселлер, 2003.

5. Дьяконов В.П. Визуальное математическое программирование VisSim+ Mathcad+ MATLAB. М. : Солон-Пресс, 2009.

6. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic СПб. : БХВ-Петербург, 2009.

7. Ермаков С.М. Метод Монте-Карло в вычислительной математике (Вводный курс). СПб. : Невский Диалект ; М. : БИНОМ. Лаб. знаний, 2009.

УДК 004.056

А.С. Дубровин, С.Ю. Хабибулина

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К ПРОБЛЕМЕ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА ОСНОВЕ ИХ ЭТАЛОННОГО МОДЕЛИРОВАНИЯ

Современный подход к решению проблемы комплексного обеспечения безопасности объектов информатизации поддерживается в Российской Федерации группой стандартов ГОСТ Р ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безо-