УДК 004.56:681.3

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 3, pp. 268-272

КЛАССИФИКАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ДЛЯ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

А.Н. Орехов, В.А. Хорошко

Национальный авиационный университет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

В работе рассматривается системная классификация моделей информационного пространства систем управления воздушным движением по совокупности трех критериев, которые позволяют проводить моделирование их функционирования. Для выбора методов моделирования оценивается уровень возможности зависимостей между элементами системы.

Ключевые слова: математическая модель, система защиты информации, информационное пространство, система управления воздушным движением.

Введение

Системы управления воздушным движением (СУВД) относятся к категории систем с ограниченным доступом. Это связано с особенностями воздушного транспорта и задачами, которые определяются назначением СУВД. В настоящее время существуют ряд способов воздействия на информационное пространство (ИП) СУВД с целью противодействия их нормальному функционированию. Это приводит к необходимости ограничения доступа к ИП СУВД, а также обеспечения защиты ИП. Успешное решение этой задачи обеспечивает безопасность, регулярность и экономичность полётов, повышение надежности и доступности информационного обеспечения.

Для предотвращения возможности реализации угроз ИП СУВД необходима разработка и использование комплексной системы технической защиты информации (КСТЗИ). Требования к такой системе предусматривают централизованное управление средствами и механизмами защиты на основе политики информационной безопасности и реализующего ее плана технической защиты информации.

Использование методов моделирования в области обеспечения безопасности ИП СУВД привело к разработке большого количества формальных моделей безопасности [1]. Формальные модели используются достаточно широко, потому что только с их помощью можно доказать безопасность системы или объекта, опираясь при этом на объективные и неопровержимые постулаты математической теории. Основная цель создания политики безопасности информационного пространства и описание ее в виде формальной модели - это определение условий, которым должно подчиняться поведение ИП СУВД, выработка критерия безопасности и проведение формального доказательства соответствия его этому критерию.

Целью статьи является разработка системной идентификации моделей ИП СУВД по совокупности критериев для улучшения ее функционирования.

Основная часть

Системная классификация моделей может быть осуществлена по совокупности трех критериев следующего содержания:

1. Способ моделирования, то есть основной прием, который положен в основу построения модели;
2. Характер системы – показатель, который выявляет взаимосвязи между надлежащими определению на модели значениями характеристик системы, которая моделируется, параметрами системы и внешней средой;
3. Масштаб моделирования – показатель, который отображает уровень характеристик, которые определяются на модели.

Согласно первого критерия все модели могут быть разделены на аналитические, подаваемые в виде некоторой совокупности аналитических зависимостей, и статистические, когда моделируемая система представляется в виде некоторого аналога, отображающего для определенных характеристик зависимости реальной системы. Само определение значений этих характеристик осуществляется методом многоразовой имитации реализации зависимостей характеристик от знаковых параметров реальной системы, внешней среды и статистической обработкой полученных при этом результатов.

Сформулированных зависимостей получается очень много, но для выбора методов моделирования наибольшее значение имеет уровень возможностей указанных зависимостей. По этому признаку моделируемые системы разделяются на детерминированные и стохастические.

В соответствии с третьим критерием, модели можно разделить на общие и частные. Общие модели строятся с целью определения значений некоторых обобщенных характеристик моделируемых систем. Частные – с целью определения значений частичных, локальных характеристик [2].

Таким образом, задача заключается в построении модели КСТЗИ ИП СУВД, а также имитации на ней процессов функционирования реальной КСТЗИ ИП СУВД. Методы моделирования являются способами исследования системы с целью построения ее модели. В связи с этим классификация методов моделирования соответствует системной классификации моделей. Исходя из целей моделирования, методы можно разделить на две группы: методы построения моделей или методы описания структуры и процессов функционирования моделируемых систем; методы имитации процессов функционирования систем.

При аналитическом моделировании структура моделируемого ИП СУВД и процессы его функционирования подаются в виде некоторых выражений, которые отображают зависимость определяемых характеристик системы от ее параметров и параметров внешней среды. Имитация процессов функционирования систем является вырожденной, она сводится к расчету по выражениям [1] значений определяемых характеристик для заданных значений параметров системы и внешней среды. Другими словами, в анализируемых моделях структура моделируемых систем и процессы их функционирования подаются в неявном виде.

При статическом моделировании структуры СТЗИ, СУВД и ИП адекватно отображаются в модели. При этом степень адекватности модели реальной системе в процессе имитации определяются целями моделирования, т.е. характеристиками систем, которые могут быть получены в процессе моделирования. Значения характеристик, которые определяются в процессе моделирования, должны соответствовать значениям тех характеристик, которые будут или могут иметь место в процессе функционирования реальных систем.

Построение статистической модели содержится в описании структуры и процессов функционирования ИП СУВД, а имитация процессов функционирования в

проработке тем или иным способом изменений во времени состояний модели системы и принятии на каждом шаге имитации решений, которые обусловлены созданной ситуацией и правилами функционирования реальной системы.

Описание моделируемой системы должно содержать: перечень всех ее значимых элементов; взаимные связи между элементами; характер этих взаимосвязей.

Для описания процессов функционирования стохастических систем необходимы способы отображения случайных факторов. Такие способы содержатся в следующих: метод статистических испытаний или Монте-Карло, теории массового обслуживания, теории вероятных автоматов, неформальной теории систем, нестрогой математики.

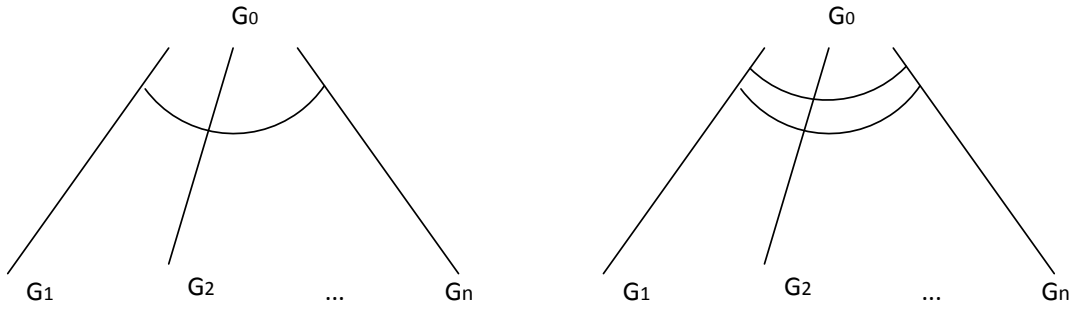
В соответствии с классификацией примеры моделей СТЗИ ИП СУВД как детерминированной системы приведены в [1-4], как стохастической системы - в [2,3,5].

Необходимо отметить, что среди моделей систем и процессов защиты информации не встречаются те, которые относятся к статистическим общим для стохастических систем. Это объясняется трудностями, связанными с отсутствием представлений о распределении вероятностей большого числа случайных событий.

Информационная система нуждается в анализе и использовании данных успешно реализованных угроз, накопленных в прошлом. Для реализации простейшего метода, в основе которого лежит библиотека шаблонов атак, необходимо осуществлять аудит работы ИП СУВД и подробно документировать ход атаки. Результатом хода документирования и анализа реализации угрозы является шаблон и дерево атаки. Затем из деревьев выделяются все возможные сценарии реализации угрозы. По мере накопления опыта формируется библиотека шаблонов реализации угроз. Практичность использования дерева атак на ИП СУВД состоит в повторном использовании предварительно разработанных моделей реализации угрозы.

Дерево атаки состоит из узлов [1], которые представляют собой цели или подцели атаки. При этом узел атаки может состоять из:

- набора подцелей атаки, каждая из которых должна быть достигнута для успешного осуществления атаки (И–декомпозиции) (рис.1(а)). Цель G_0 будет достигнута лишь в том случае, если будет достигнута каждая из подцелей $G_1, G_2, ..., G_n$;
- набора целей атаки, хотя бы одна из которых должна быть достигнута для успешного осуществления атаки (ИЛИ–декомпозиции) (рис.1(б)). Цель G_0 будет достигнута в случае, если будет достигнута хотя бы одна из подцелей $G_1, G_2, ..., G_n$.



а **б**

Рис. 1. Структурное представление декомпозиции**:** а – И–декомпозиции; б – ИЛИ–декомпозиции.

Дерево атаки может состоять из любого набора И– и ИЛИ–декомпозиций. Моделирование атак с помощью деревьев атак позволяет детализировать сценарий до уровня, выбранного разработчиком. Недостатком данного подхода является низкий уровень «эвристики», привязанность к известным типам атак, возможность обнаружения действий нарушителя только по известным сценариям.

Возможно улучшение способа моделирования угроз деревом атак. Для этого необходимо объединить ручное расширение дерева атак и применение библиотек атак [1]. На рис.2. приведена блок-схема процесса использования этого способа.

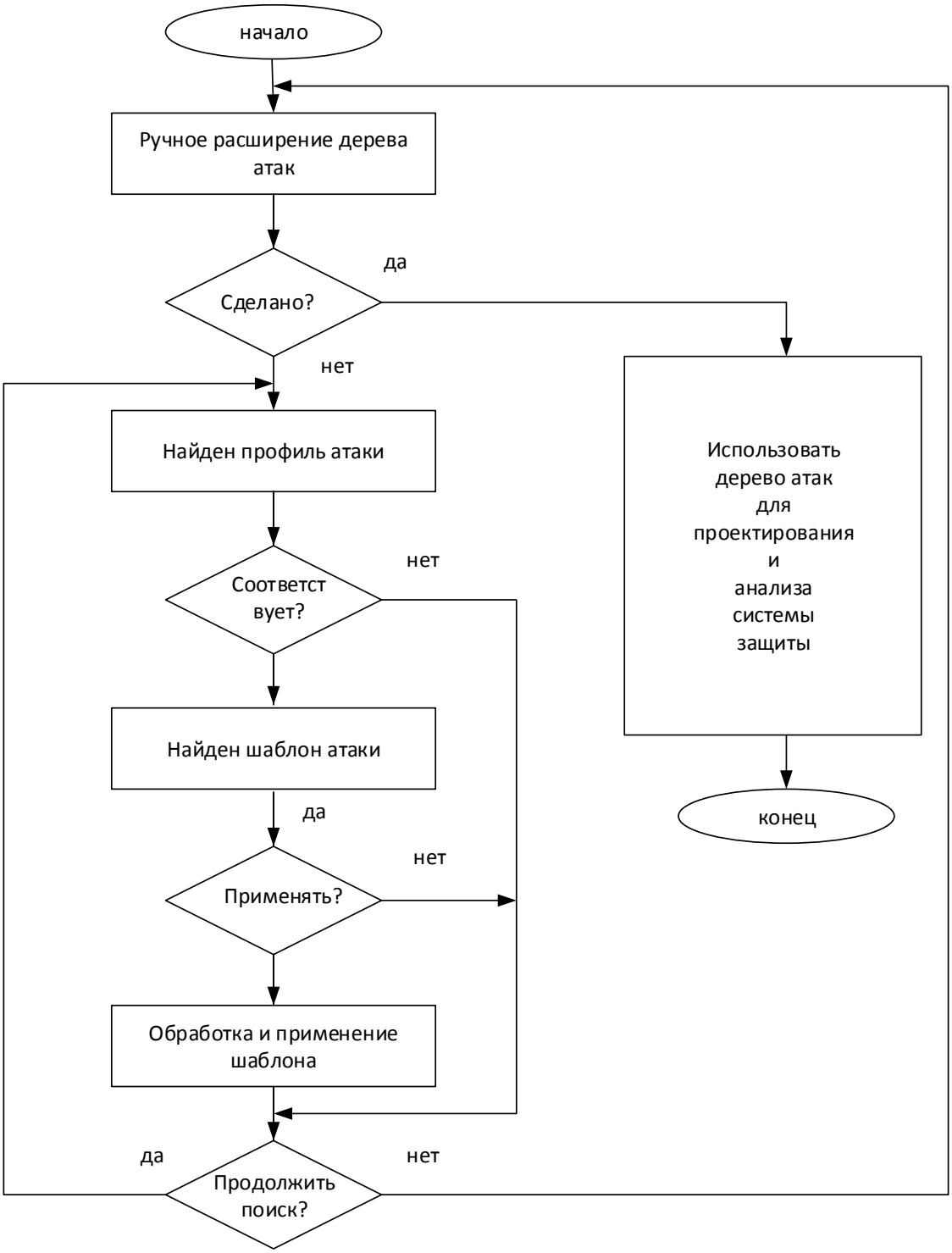


Рис. 2. Блок-схема процесса расширения библиотеки шаблонов атак

Введем понятия шаблона и профиля атаки. Определим шаблон атаки как родственное представление преднамеренной, злонамеренной атаки. Каждый шаблон атаки содержит: общую цель атаки, определяемую шаблоном; список предварительных условий для его использования; шаги для выполнения атаки; список постсостояний системы на случай успешного выполнения атаки. Предварительные условия включают в себя предположения о состояниях системы, при которых возможно реализовать

угрозы. Профили атак содержат: модель общих связей, взаимоотношений; список вариантов; глоссарий определенных терминов и фраз.

Модель связей представляет собой шаблон архитектуры с параметрами, которые могут включать специфичные варианты. Шаблоны атак также определены в терминах вариантов. Как показано на блок-схеме (рис.2) моделирование с помощью метода дерева атак может быть улучшено компромиссным решением – объединением ручного расширения библиотеки атак и использованием приложений для работы с шаблонами. Ручное расширение дерева атак в основном зависит от личного опыта разработчика атак. Использование приложений для работы с шаблонами также зависит от разработчика, но в меньшей степени.

Выводы

Предложена системная классификация моделей ИП СУВД по совокупности трех критериев, которые позволяют проводить моделирование. Для выбора методов моделирования наибольшее значение имеет уровень зависимостей между элементами системы.

Список литературы

1. Богданов, А.М. Моделирование безопасной обработки информации в компьютерных системах / А.М. Богданов, А.В. Корнейко. – К: Наукова думка, 2000. – 160 с.
2. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. В 2-х томах / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 293 с.
3. Девянин, П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский и др. – М.: Радио и связь, 2000. – 192 с.
4. Грушко, А.А. Теоретические основы защиты информации / А.А. Грушко, Е.Е. Тимонина. – М.: Изд-во «Яхтсмен», 1996. – 187 с.
5. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М: Горячая линия - Телеком, 2000. – 452 с.

КЛАСИФІКАЦІЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЛЯ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

А.Н. Орєхов, В.О. Хорошко

Національний авіаційний університет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

У роботі розглядається системна класифікація моделей інформаційного простору систем управління повітряним рухом за сукупністю трьох критеріїв, які дозволяють проводити моделювання її функціонування, але для вибору методів моделювання необхідно оцінити рівень можливості залежностей між елементами системи.

Ключові слова: математична модель, система захисту інформації, інформаційний простір, система управління повітряним рухом.

CLASSIFICATION OF MATHEMATICAL MODELS OF SYSTEMS OF PROTECTION OF INFORMATION SPACE FOR AIR TRAFFIC CONTROL

A.N. Orekhov, V.A. Khoroshko

National Aviation University,
pr. Komarova, 1, Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net

The paper deals with the classification system model information space systems, air traffic control for a set of three criteria that allow the simulation of its operation, but the choice of modeling methods necessary to assess the level of possible relationships between the elements of the system.

Keywords: mathematical model, the system of information protection, information space, air traffic control system.