УДК 681.5


Е.Н. Давыдова, А.А. Коппалина
Вологодский государственный университет

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ БЕЗОПАСНОСТИ ДЛЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

В статье рассматривается построение модели системы безопасности автоматизированной системы управления предприятием (АСУП). Для этого проведен сравнительный анализ уже существующих моделей, разработана методика построения модели и приведен ее алгоритм. Описывается архитектура мультиагентных систем защиты информации и их применение в разрабатываемой модели.

Модель системы безопасности, многоагентные системы, автоматизированные системы, информационная безопасность, распределенные системы, вычислительные системы.

Информатизация – неотъемлемая часть современного общества. Через компьютеры проходит обслуживание банков, ведется документооборот организации, осуществляется автоматизация предприятия. Компьютеры – основа АСУП, осуществляющих базовые процессы: разработку, внедрение и сопровождение информационных систем.

АСУП – это система управления, построенная на базе средств вычислительной техники, математических и экономических методов и информационных технологий. Аппаратное обеспечение АСУП имеет в большинстве случаев распределенную архитектуру клиент – сервер и состоит из серверов и рабочих пользовательских компьютеров, объединенных общей сетью обработки информации. Такая система подвержена угрозам безопасности и утечке информации. Чтобы этого избежать, необходимо обеспечить систему защиты АСУП и свести к минимуму потенциальные внешние угрозы [1]. Угрозой является действие, которое вызывает нарушение защищенности информации, которая обрабатывается информационной системой [2].

Таким образом, поставим задачу усовершенствовать систему защиты АСУП путем создания модели обработки информации в системах безопасности. Но перед тем как разработать модель, необходимо обозначить методику исследования модели системы безопасности АСУП. В данном случае разработаем следующую методику, состоящую из нескольких этапов:

1. Определение исходных данных и их анализ. Исходные данные: характеристики сети/подсети, типы данных, аппаратное и программное обеспечение, типы угрозы безопасности, наборы правил фильтрации и т.д.
2. Определение методов построения, вид модели, условия ее выполнения.
3. Анализ моделей систем безопасности. Определение требований.
4. Построение общей модели системы безопасности.
5. Определение вариантов модели системы безопасности [3]. Определение наборов правил фильтрации, направленных на противодействие выявленным угрозам безопасности.
6. Формирование набора правил фильтрации.
7. Построение модели системы безопасности.
8. Определение критериев работы разработанной модели.
9. Переход от модели к имитационному моделированию.
10. Оценка полученных результатов.

Таблица 1

Результаты оценки моделей системы безопасности сетей

Критерии	Обобщенная модель системы безопасности данных	Базовая модель безопасности Клеменса	Общая статистическая модель анализа	Мандатная модель	Модель Биба	Матричная модель	Модель Белла-Лападула	Модель на сетях Петри
Количественная оценка уровня безопасности	+	+	+	–	–	–	–	–
Количественная оценка экономической эффективности	–	+	+	–	–	–	–	+
Отсутствие дополнительных функциональных зависимостей	–	+	–	+	+	+	+	+
Учет особенностей организационного построения системы	–	–	–	–	–	–	–	+
Анализ требований с учетом различных источников угроз	–	–	–	–	–	–	–	+
Параллелизм информационных процессов	–	–	–	–	–	–	–	+
Абстрактность	–	–	–	+	+	+	+	+
Графическое построение	–	–	–	–	–	–	–	+

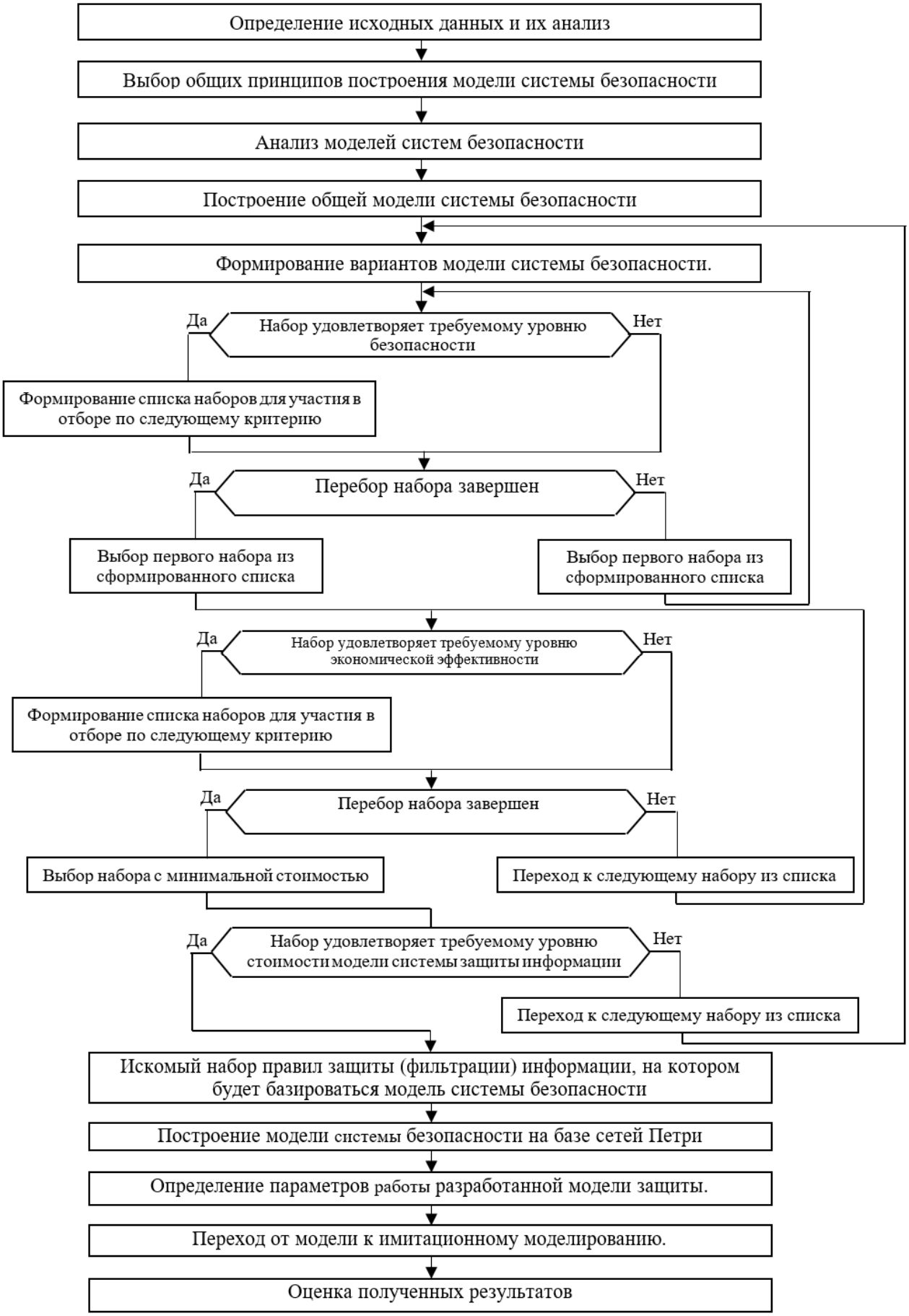

Рис. 1. Алгоритм методики исследования модели системы безопасности

Исходя из вышеперечисленного, можно изобразить методику исследования в виде алгоритма, представленного на рисунке 1.

За основу построения возьмем модель системы безопасности АСУП на базе применения межсетевых экранов, ограничивающих доступ извне.

Анализ возможных моделей системы безопасности АСУП представлен в таблице 1. В ней приведена оценка наиболее известных моделей по ряду выбранных нами критериев.

Модель на сетях Петри выигрывает по количеству реализованных требований, предъявляемых к разрабатываемой модели. Исходя из этого, выбираем ее в качестве базы, которую будем модифицировать для создания собственной модели безопасности.

Как говорилось выше, разрабатываемая система безопасности является распределенной, потому что:

1) представляет собой совокупность межсетевых экранов, находящихся отдельно друг от друга;

2) задачи системы распределены между отдельными ее модулями:

− база данных защиты (хранение информации о правах доступа);

− сервер аутентификации и идентификации (LDAP-сервер);

− модуль управления межсетевыми экранами;

− модуль диспетчера доступа (проверка права пользователя на совершение действия к данному объекту на основе правил разграничения доступа);

− модуль фильтрации (анализ поступающих пакетов данных: блокировка или преобразование пакета);

− модуль регистрации событий.

В качестве архитектуры модели была взята архитектура многоагентной системы безопасности. Многоагентная система – система, в которой взаимодействуют два и более интеллектуальных агента. Агент – самостоятельная интеллектуальная система, обладающая некоторой совокупностью знаний о себе и окружающем мире.

В нашей системе будут функционировать следующие агенты:

1) агент разграничения доступа, ограничивающий доступ к данным в соответствии с политикой предоставления прав пользователям;

2) агент аутентификации и идентификации;

3) агент фильтрации;

4) агент регистрации событий;

5) мета-агенты, ответственные за согласование работы системы безопасности.

В данной структуре взаимодействия агентов зачастую реализуется синхронный режим обмена сообщениями: такие агенты, как агент фильтрации, аутентификации и идентификации, диспетчера доступа, останавливают свою работу до получения ответа от мета-агента, который, в свою очередь, выдает ответ на сообщения в соответствии с модулем базы данных защиты. Из минусов: временные затраты.

Модернизированная структура взаимодействия агентов, в которой выявленный недостаток исправлен путем смены режима на асинхронный, представлена на рисунке 2.

Рис. 2. Структура взаимодействия агентов (частный случай)

Каждый агент имеет свою собственную базу данных защиты. В таком случае значительно сокращается время на обработку входящего пакета. Поступающий на вход системы пакет данных вначале передается агенту аутентификации и идентификации. Он на основе записей базы данных защиты решает: уничтожить или передать пакет дальше. Отправляет соответствующее сообщение агенту регистрации событий и мета-агенту. Если пакет идет на дальнейшую проверку, то он перенаправляется агенту фильтрации. Там его проверяют в соответствии с базой данных фильтрации. Следующий в очереди агент – агент разграничения доступа. Его основа – база полномочий и характеристик доступа. Если пакет не удовлетворяет хотя бы одной записи базы данных фильтрации, то пакет подлежит уничтожению. Если проверка пройдена агентом фильтрации, то пакет передается на выход, а агенту регистрации посылается соответствующее сообщение. Мета-агент выступает в роли менеджера по управлению работой агентов: ему агенты отправляют сообщения о проделанных действиях.

Дальнейшие этапы создания модели находятся в разработке. Необходимо осуществить переход от общей модели системы безопасности к формальной и осуществить переход от созданной модели к имитационному моделированию.

Подводя итоги, можно сказать, что архитектура модели системы защиты будет базироваться на мультиагентах, т.е. компоненты системы будут выражены через агентов – интеллектуальные автономные аппаратно-программные единицы. Каждый агент знает свои задачи, которые ему необходимо выполнить, знает, кому адресовать сообщение о выполненной работе и кому направить запрос, если действие вне его полномочий. Сообщения агентов представлены в форме, понятной другим агентам.

Литература

1. Давыдова, Е. Н. Методика оценки достаточности системы защиты компьютерной информации / Е. Н. Давыдова, Д. Ю. Крюкова, О. А. Панфилова / Вестник Воронежского института ФСИН России. – 2020. – № 1. – С. 68–76.

2. Коппалина, А. А. Защита информационных систем от комплексных внешних воздействий / А. А. Коппалина // XIV Ежегодная научная сессия аспирантов и молодых ученых : материалы Всероссийской научной конференции Вологда, 2020. – Т. 1. – С. 75–78.

3. Арьков, П. А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени кандидата технических наук / Павел Алексеевич Арьков. – Волгоград, 2009. – 185 с.

E.N. Davydova, A.A. Koppalina
Vologda State University

DEVELOPMENT OF A SECURITY MODEL FOR AUTOMATED ENTERPRISE MANAGEMENT SYSTEM

The article discusses the construction of the security system model of the automated control system. For this, a comparative analysis of already existing models was carried out, a methodology for constructing a model was developed and its algorithm was presented. the architecture of multi-agent information security systems and their application in the developed model are described.

Security system model, multi-agent systems, automated systems, information security, information protection, distributed systems, computing systems.