УДК 004.413:004.056
DOI: 10.36979/1694-500X-2023-23-4-59-66

МЕТОДЫ ФОРМАЛИЗАЦИИ РЕШЕНИЙ АКТУАЛЬНЫХ ПРОБЛЕМ АППАРАТНО-ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

С.В. Корякин

Аннотация. Рассматриваются вопросы решения проблем защиты информации в автоматизированных системах (АС). Предлагается метод формализации решений актуальных проблем аппаратно-программного обеспечения информационной безопасности в АС. Предложена методология, согласно которой происходит обработка информации о возникающих проблемах и угрозах, приводящих к нарушению безопасности АС. При этом данная предложенная методология предполагает использование существующих методов и способов защиты информации, включая средства программно-аппаратных компонентов, которые, в свою очередь, являются специализированными экспертными системами. Это позволяет структурировать набор наиболее эффективных решений, формировать и расширять функционал подсистем защиты информации АС. Обоснована необходимость решения задач и актуальных проблем аппаратно-программного обеспечения информационной безопасности в АС, работающих в режиме реального времени.

Ключевые слова: модель; этапы проектирования; системы реального времени; автоматизированная система защищенного исполнения; информационная безопасность; защита данных; программно-аппаратное ядро; технологии проектирования.

АВТОМАТТАШТЫРЫЛГАН СИСТЕМАЛАРДА МААЛЫМАТТЫК КООПСУЗДУКТУН АППАРАТТЫК-ПРОГРАММАЛЫК КАМСЫЗДООСУНУН АКТУАЛДУУ МАСЕЛЕЛЕРИН ЧЕЧҮҮНҮН ЖОЛДОРУН ФОРМАЛДАШТЫРУУ ЫКМАЛАРЫ

С.В. Корякин

Аннотация. Макалада автоматташтырылган системалардагы (АС) маалыматты коргоо көйгөйлөрүн чечүү маселеси каралат. АСта маалыматтык коопсуздукту аппараттык- программалык камсыздоонун актуалдуу маселелерин чечүүнүн жолдорун формалдаштыруу ыкмасы сунушталат. АСнын коопсуздугунун бузулушуна алып келген пайда болгон көйгөйлөр жана коркунучтар жөнүндө маалымат иштелип чыккан методология сунушталды. Ошол эле учурда бул сунуш кылынган методология маалыматты коргоонун колдонулуп жаткан ыкмаларын жана жолдорун, анын ичинде программалык-аппараттык компоненттердин каражаттарын колдонууну болжолдойт, алар өз кезегинде адистештирилген эксперттик системалар болуп саналат. Бул эң натыйжалуу чечимдердин комплексин түзүүгө, АСнын маалыматын коргоонун чакан системаларынын функционалдуулугун калыптандырууга жана кеңейтүүгө мүмкүндүк берет. Реалдуу убакыт режиминде иштеген АСда маалыматтык коопсуздукту аппараттык-программалык камсыздоонун маселелерин жана актуалдуу көйгөйлөрүн чечүү зарылдыгы негизделген.

Түйүндүү сөздөр: модель; долбоорлоо этаптары; реалдуу убакыт системалары; корголгон аткаруунун автоматташтырылган системасы; маалыматтык коопсуздук; маалыматтарды коргоо; программалык-аппараттык өзөк; долбоорлоо технологиялары.

METHODS FOR FORMALIZING SOLUTIONS TO ACTUAL PROBLEMS OF HARDWARE AND SOFTWARE INFORMATION SECURITY IN AUTOMATED SYSTEMS

S.V. Koryakin

Abstract. The article is about the issues of solving the problems of information security in automated systems (AS). Also, in this article proposes a method for formalizing solutions of actual problems of hardware and software information security in the AS. A methodology is proposed according to which information is processed about emerging problems and threats that lead to a violation of the security of the automated systems. At the same time, this proposed methodology assumes the use of existing methods and methods of information protection, including hardware and software components, which, in turn, are specialized expert systems. This allows you to structure a set of the most effective solutions, form and expand the functionality of the information security subsystems of the automated systems. The necessity of solving problems and actual problems of hardware and software information security in real-time operating systems (RT) is substantiated.

Keywords: model; design stages; real-time systems; automated system of protected execution; information security; data protection; hardware and software core; design technologies.

Считается, что мониторинг параметров подсистем защиты автоматизированных информационных систем (АИС) «представляет собой область интересных и своеобразных задач профессиональной выработки решений в сложных ситуациях или ситуациях с неполной информацией. Особенность работы специалиста по информационной безопасности (ИБ) состоит в том, что объект АИС чрезвычайно сложен, а решение должно быть принято обязательно. Значительная часть информации о угрозах информационной безопасности АИС имеет невербальный характер. Формализация и структуризация хотя бы части используемой специалистом по ИБ информации, могут быть полезны для самого специалиста по ИБ, т. е. часть вопросов упростится и может быть решена формально, что, в свою очередь, создает предпосылки для решения более сложных профессиональных проблем» [1].

«В реально возникающих физических и технических задачах оптимизации многомерных функций существует так называемая локальная организация данных. При этом большая часть переменных оказываются несущественными, то есть минимум оценочной функции по ним достигается за сравнительно небольшое число шагов, а несколько (1–3) переменных оказываются существенными, то есть минимизация по ним требует заметно большего числа существенно более крупных (нелокальных) шагов, что дает заметно меньшие значения оценочной функции. Данная закономерность связана с особой структурой данных («хорошо организованная задача»), аналоги которой проявляются, например, при анализе построения произвольных движений млекопитающих» [1].

В обобщенном виде локальную организацию данных при решении физических и технических задач оптимизации многомерных функций в информационных системах можно сравнить с кровеносной системой человека, где в качестве систем передачи информации выступают большой и малый круг кровообращения, роль каналов передачи информации выполняют кровеносные сосуды, а в качестве потока данных выступает артериальный и венозный кровеносные потоки, соответствующие передаваемому TX и принятому RX потокам передаваемых данных в информационных системах. Внутренние органы, мягкие и твердые ткани организма человека выступают в роли элементов (датчики, сенсоры, устройства ввода вывода информации) и устройств (сетевые коммутаторы, маршрутизаторы и другие устройства, входящие в состав эталонной модели сетевого взаимодействия OSI), отвечающих за прием и передачу информации из глобальной и локальной среды [2].

В качестве локальной среды будем понимать внутренние процессы, происходящие в организме человека. В дальнейшем будем называть их внутренней локальной сетью – «LAN», соответственно, в качестве внешней среды будем понимать процессы взаимодействия человека с окружающим миром и будем называть их процессами взаимодействия в глобальной сети «WAN». На рисунке 1 в упрощённом виде представлена кровеносная система человека [3].

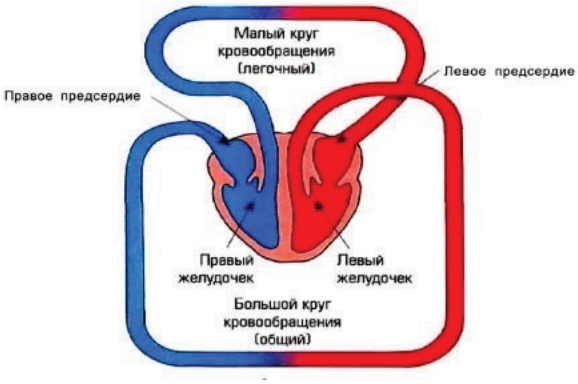

Рисунок 1 – Схема модели кровеносной системы человека

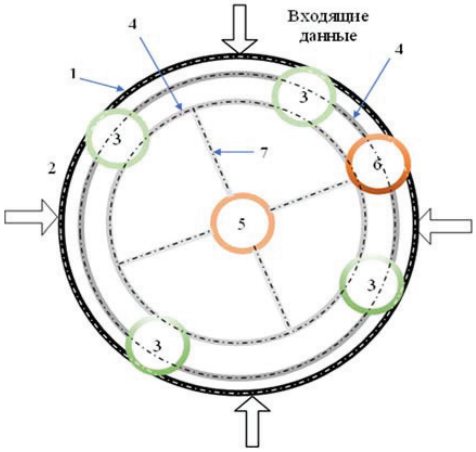

Рисунок 2 – Модель формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки

Исходя из приведенных выше сравнительных аналогий модели кровеносной системы человека с моделью сетевого взаимодействия OSI, предложим модель формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки, которая будет функционировать на основе принципов функционирования прототипа – модели кровеносной системы человека.

Схему модели формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки, далее «модель формализации» представим на рисунке 2.

Введем элементы, входящие в состав модели, и приведем их аналоги в модели кровеносной системы человека в соответствии с уровнями модели OSI:

1. Элементы приема и передачи информации (сенсоры, датчики, устройства ввода и вывода и т. д.) – точки соединения кровеносных сосудов с органами, твердыми и мягкими тканями человека.
2. Каналы передачи информации – кровеносные сосуды.
3. Программно-аппаратные устройства АИС – внутренние органы человека.
4. Система маршрутизации и сетевого взаимодействия (LAN/WAN) – большой и малый круги кровообращения.
5. Нейросетевой модуль взаимодействия между нейронной сетью и программно-аппаратными компонентами АИС – сердце.
6. Нейронная сеть – головной мозг человека.
7. Данные – кровь человека.

Рассмотрим принцип функционирования модели формализации. В качестве центрального элемента, отвечающего за функционирование модели, выступает нейронная сеть, которая отвечает за управление всеми элементами, входящими в состав модели функционирования, обработку и анализ данных, формирование правил и алгоритмов функционирования и взаимодействия всех элементов, входящих в состав модели [4].

Нейронная сеть через нейросетевой модуль взаимодействия управляет всеми элементами, входящими в состав информационной системы (программно-аппаратными устройствами и элементами

приема/передачи информации), взаимодействующими между собой по каналам передачи информации при помощи системы маршрутизации и сетевого взаимодействия (WAN/LAN). Следовательно, при помощи модели функционирования становится возможным формализовать наиболее важные проблемы аппаратно-программного обеспечения информационной безопасности в автоматизированных системах при помощи различных методов, предсказывающих состояние системы на основе известной истории поведения объекта (фактически, анализа данных наблюдений, временных рядов) [5].

«В современной теории нелинейных динамических систем существует метод «русел и джокеров», использующий близкие идеи о структуре переменных системы. Аналоги такого же представления можно обнаружить в классической гештальтпсихологии, которая трактует восприятие некоторой ситуации каждым из ее участников в виде единого образа, организованного вокруг своего «центра интереса». Возможно, что в ходе эволюции механизмы работы нервной системы человека восприняли этот принцип организации информации, следствием этого стал известный феномен «семь плюс или минус два», обнаруженный при исследованиях объема внимания. Во всяком случае, важной частью структуризации и формализации данных, используемых в процессе обеспечения защиты АИС от угроз информационной безопасности, будем считать поиск небольшого количества существенных переменных в каждой проблемной ситуации принятия специалистом решения в его профессиональной области. В отличие от случая функции, заданной численно или формулой, поиск таких переменных в задаче обеспечения безопасности АИС требует специфических методов» [6].

Исторически определились два типа возможных носителей полученного знания: текст и программа для компьютера. Выбор одного из них диктовал в значительной мере характер и способ использования результатов. Если мы выбираем текст в качестве носителя нового знания, то нам, естественно, необходимо стремиться к максимально подробной вербализации знания, а методы исследования должны способствовать наилучшему словесному контакту со специалистом, занимающимся исследованием выделенной проблемной области. Одним из сильнейших достижений на этом пути является методика структуризации знания, использующая метод экспертной диагностики.

При выборе программы в качестве носителя знаний мы вынуждены ориентироваться на методы моделирования и распознавания, и неизбежно приходим к установке на создание программы, принимающей профессиональное решение за специалиста, без его участия.

В этом случае подробности рассуждений специалиста по ИБ неинтересны, важно лишь совпадение выбора, осуществленного программой, с действием специалиста по ИБ. «Такова логика классического подхода «черного ящика»: если действия двух решателей одной проблемы (человека и компьютера) при одинаковых входных сигналах совпадают, моделирование считается успешным. Этот путь избрали создатели многих диагностических программ и впоследствии экспертных систем. Подчеркнем, что трудности подхода велики и «человекообразные рассуждения» часто оказываются в числе первых жертв чисто машинного решения проблемы» [6].

Методы получения готового знания от специалиста обычно ориентированы на передачу знания компьютерной программе в виде экспертного высказывания. При этом специалист, выступающий в качестве эксперта, должен дать определенный ответ на все возможные варианты вопросов, при помощи которых максимально описывается угроза информационной безопасности и содержащие список указаний к действию по ее ликвидации. В практической работе специалиста обслуживающего АИС такой случай крайне редок. Не интересующие его сочетания признаков и варианты заключений могут быть даже осмысленными, но поскольку они не относятся к его области интересов, это может привести к ответу случайному или даже невнятному. Другой вариант – знание вырабатывает программа на основании отобранного экспертом по ИБ материала по ее собственным правилам неформализованного умения угадать ответ. Существует опасность получить в результате информационную систему, «адаптированную» на фиксированное количество угроз ИБ, но беспомощную за пределами границ материала, отобранного экспертом.

Описанные два крайних подхода не охватывают всю проблему структуризации знания по обеспечению информационной безопасности АИС. С одной стороны, метод экспертной диагностики позволяет обнаружить состав и организационную структуру тех данных, которые имеют название, классифицированы и введены в базу знаний для исследований специалистами. Они позволяют также уточнять определения уже известных разновидностей данных. С другой стороны, логические конструкции, используемые в экспертных системах, пригодны для оперирования только полностью формализованными элементами. Остаются как минимум два пробела. Данные, используемые специалистом по ИБ на интуитивном уровне, нужно обнаружить и описать. В рамках метода экспертной диагностики такая задача требует несоразмерных усилий и изощренной квалификации группы экспертов по ИБ, исследующих выделенную проблемную область. Кроме того, экспертная информация об одном и том же процессе может существовать одновременно в нескольких формах, использующих разные наборы переменных, отражающих различные стороны процесса обеспечения безопасности АИС. Разные правила принятия одного и того же решения могут использовать различные наборы сведений. Тем самым формализация первичных наблюдений оказывается тесно связанной с построением правил диагностики и анализа защищенности АИС, использующих каждый раз наиболее подходящий для данной ситуации набор сведений. Можно кратко выразить цель формализации знания эксперта по ИБ в данной работе: «Вместе с экспертом по ИБ выработать новое формализованное знание, которым специалист по ИБ может пользоваться, как еще одним источником информации в своей профессиональной деятельности».

«При этом следует использовать метод экспертной диагностики для анализа его подхода к проблеме, структуризации информации и изучения методов рассуждения. Также естественно решать вместе с ним частные проблемы АИС, порожденные количественным характером некоторых типов данных и сложными логическими конструкциями, возникающими при анализе достаточно редких и разнообразных случаев несанкционированного доступа к АИС» [7].

«В случаях совместной работы программы и специалиста по ИБ необходимо, чтобы специалист по ИБ имел возможность контролировать используемые данные, их преобразования и ход рассуждений, сохраняя свою самостоятельность и независимость как исследователь» [7]. Это приводит к потребности иметь достаточно лаконичный язык манипулирования элементами рассуждений и заключений, при этом специалист по ИБ должен обладать возможностью легко отслеживать связь логических конструкций с первоначальной информацией, а программа обеспечивает упрощение и оптимизацию специалиста по ИБ.

Проводя анализ современного состояния задачи обеспечения комплексной защиты АИС от угроз ИБ и НСД, были выявлены наиболее опасные источники угроз ИБ, возникающих в процессе эксплуатации АИС – вирусы, вредоносное ПО, атаки хакеров, приводящие к утечке данных хранящихся в базах данных АИС. Данные источники представляют реальную угрозу для стабильной работы АИС и могут вызвать, в основном, временные нарушения функционирования [8].

«Современный уровень науки в вопросах обеспечения информационной безопасности АИС пока не всегда позволяет расчетным путем находить совершенные решения по обеспечению защиты ресурсов АИС, в том числе элементов и устройств. Обычный путь решения данной задачи – это опытное конструирование подсистем защиты информации ИАС и их устройств на основе имеющегося опыта в области ИБ, с учетом результатов экспериментальных исследований и моделирования, с последующей опытной доработкой» [9].

«Попытки решить задачу защиты АИС от угроз ИБ на основе моделирования численными методами, приводит к трудностям с вычислениями в больших областях, где, как правило, присутствуют большое количество объектов меньших размерностей. С другой стороны, применение конечных аналитических моделей также практически невозможно из-за сложности всей конструкции как подсистем защиты, так и самих АИС, в которой необходимо учесть большое количество входных параметров, в том числе и заранее неизвестных, описывающих данные конструкции» [9].

Поэтому, «методика анализа и повышения защищенности АИС должна включать экспериментальные исследования, направленные на выявление механизмов проникновения и параметров угроз безопасности, разработку математических моделей и прогнозирования защищенности АИС от угроз ИБ. Разработка методики и математических моделей для анализа угроз и прогнозирования защищенности АИС является одной из научных задач данной работы. Одной из практических задач данной работы является повышение защищенности АИС от угроз путем использования предложенных практических рекомендаций» [9].

Таким образом, в рамках данной работы, на основе модели формализации (рисунок 3), разработана методика формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки [10].

«Она содержит несколько основных частей: выявление наиболее вероятных типов и параметров источников угроз ИБ, а также наиболее опасных механизмов воздействия на АИС в области ее эксплуатации; количественные экспериментальные исследования угроз и качественные оценки защищенности АИС при воздействии угроз ИБ. Данные экспериментальные исследования позволяют понять пути проникновения вредоносного программного обеспечения и механизмы влияния на элементы АИС: через информационную подсистему или подсистему электропитания; разработку моделей и моделирование механизмов защиты в АИС при воздействии угроз ИБ, основываясь на результатах экспериментальных исследований.

Данный этап также включает оценку адекватности и точности предложенных моделей, а также корректировку при необходимости; прогнозирование защищенности АИС при воздействии различного рода угроз ИБ на основе предложенного метода в соответствии с установленными критериями качества функционирования. Если установленные разработчиком требования по защищенности АИС при воздействии угроз ИБ не выполняются, то необходимо использовать известные или новые методы и рекомендации для снижения последствий от угроз ИБ» [11].

Рассмотрим алгоритм применения метода формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки (см. рисунок 3).

1. «Выявление наиболее вероятных типов и параметров источников информационной безопасности в области эксплуатации АИС.

1.1. Анализ всех типов источников угроз ИБ и выявление наиболее вероятного типа в области эксплуатации АИС.

1.2. Анализ требований нормативных документов в области защищенности при воздействии угроз ИБ для всех программно-аппаратных компонентов АИС. Обоснованный выбор уровня жесткости испытаний осуществляется на основании нормативных документов в области ИБ или определяется техническим заданием.

1.3. Анализ и выбор параметров источников угроз ИБ в области эксплуатации АИС в зависимости от внешних условий: параметров окружающей среды, характеристик используемых материалов для элементов и устройств и каналов передачи информации» [9].

2. «Выявление наиболее опасных механизмов и путей воздействия угроз ИБ на АИС.

a) анализ структуры, функционала, конструкции, технологий передачи данных и электропитания современных АИС;

b) выявление и анализ механизмов воздействия угроз ИБ в области эксплуатации АИС;

c) выявление и анализ путей воздействия угроз ИБ в области эксплуатации АИС;

d) выбор наиболее опасного механизма воздействия угроз ИБ в области эксплуатации АИС;

e) выбор наиболее опасного пути воздействия угроз ИБ в области эксплуатации АИС» [9].

3. «Экспериментальные исследования защищенности АИС при воздействии на них угроз ИБ.

3.1. Анализ и выявление наиболее опасных путей проникновения угроз ИБ и механизмов влияния на элементы АИС через информационную подсистему или подсистему электропитания» [9].

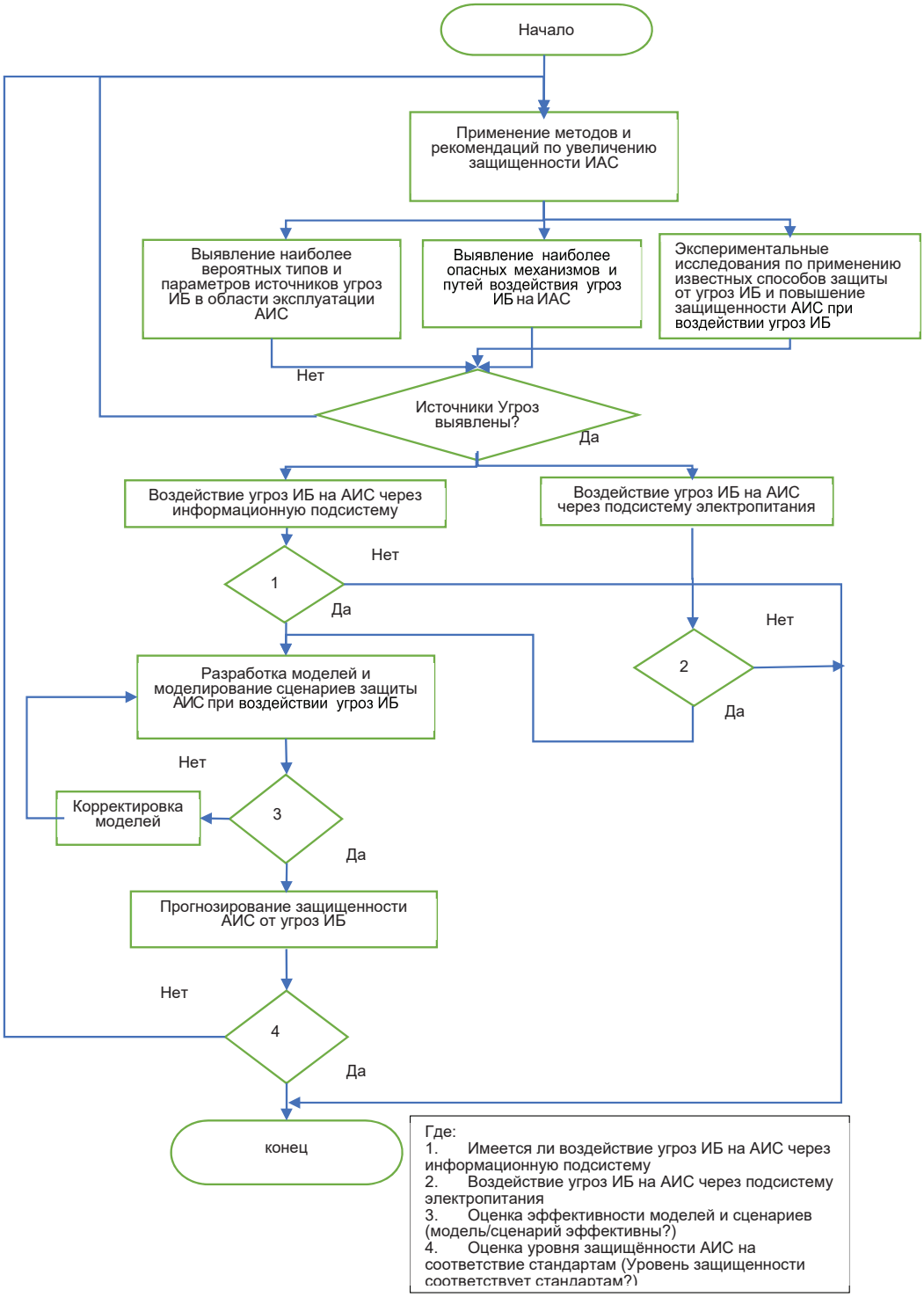

Рисунок 3 – Алгоритм применения метода формализации актуальных проблем аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки

4. Разработка моделей противодействия угрозам ИБ и моделирование архитектурных схем АИС при воздействии угроз ИБ.

5. Прогнозирование защищенности АИС.

6. Применение методов и рекомендаций по снижению угроз ИБ.

Таким образом, предложенный метод реализован в виде итерационного процесса с целью обеспечения заданных требований защищенности АИС от воздействия угроз ИБ. Применение данного метода позволяет формализовать актуальные проблемы аппаратно-программного обеспечения информационной безопасности в автоматизированных системах защищенного исполнения на этапе разработки. Необходимо учесть возможные последствия воздействия угроз ИБ, предпринять заранее необходимые меры и создавать устройства с улучшенными техническими и эксплуатационными характеристиками с точки зрения защищенности от угроз ИБ. Применение данной методики на этапе разработки АИС также позволяет снизить затраты на обеспечение информационной безопасности.

Поступила: 26.12.22; рецензирована: 11.01.23; принята: 13.01.23.

Литература

1. *Островский О.В.* Качественные и количественные аспекты клинической диагностики в медицинской практике, основанной на доказательствах / О.В. Островский, Е.В. Веровский, Т.С. Дьяченко // Вестник Волгоградского госуд. мед. ун-та. 2006. № 4(20). С. 11–15. URL: https://elibrary.ru/item.asp?id=12945696 (дата обращения: 02.01.2023).
2. *Брякин И.В.* Информационная безопасность в системах реального времени / И.В. Брякин, С.В. Корякин // Проблемы автоматики и управления. 2017. № 2 (33). С. 115–121.
3. Кровеносная система человека. URL: https://www.gdp1podolsk.ru/blog/kratko-i-ponjatno-o-krugah krovoobrashhenija/ (дата обращения: 10.09.2022).
4. *Корякин С.В.* Разработка концепции построения программно-аппаратного ядра универсальной среды проектирования автоматизированных систем защищенного исполнения / С.В. Корякин // Проблемы автоматики и управления. 2020. № 1 (38). С. 60–69.
5. *Корякин С.В.* Универсальная телекоммуникационная система для мониторинга эпидемиологической обстановки КР / С.В. Корякин // Вестник КРСУ. 2020. № 12. Т. 20. С. 152–158.
6. *Жидкова Е.А.* Развитие учетно-аналитической концепции контроллинга / Е.А. Жидкова. URL: https:// marketing.wikireading.ru/hk2XoNR56O. (дата обращения: 22.09.2022).
7. *Паринов А.В.* Методы формализации профессиональных знаний врача на основе интеллектуальных технологий идентификации состояния здоровья пациента и выбора тактики лечения: дис. … канд. техн. наук / А.В. Паринов. URL: http://dlib.rsl.ru/rsl01003000000/rsl01003307000/rsl01003307957/ rsl01003307957.pdf (дата обращения: 02.01.2023).
8. *Корякин С.В.* Разработка универсальной среды проектирования автоматизированных систем защищенного исполнения / С.В. Корякин // Проблемы автоматики и управления. 2021. № 2. С. 40–55.
9. *Шкиндеров М.С.* Помехоустойчивость систем контроля и управления доступом в здания при воздействии импульсных электромагнитных помех / М.С. Шкиндеров. URL: http://dlib.rsl.ru/rsl01010000000/ rsl01010625000/rsl01010625081/rsl01010625081.pdf. (дата обращения: 02.01.2023).
10. *Корякин С.В.* О построении модульных платформ комплексной защиты информации под управлением экспертных систем / С.В. Корякин // Вестник КРСУ. 2022. Т. 22. № 4. С. 68–73.
11. *Сафина Р.М.* Помехоустойчивость систем контроля и управления доступом в здания при воздействии электромагнитных помех по сети электропитания / Р.М. Сафина, М.С. Шкиндеров, Р.Р. Мубараков // Журнал радиоэлектроники. 2021. № 6. URL: https://doi.org/10.30898/1684-1719.2021.6.9. (дата обращения: 02.01.2023).