УДК 004.67 DOI: 10.26102/2310-6018/2020.30.3.005

Обеспечение функциональной безопасности аппаратно-программных комплексов в условиях неопределенности среды использования

В.Е. Гвоздев, М.Б. Гузаиров, О.Я. Бежаева, А.С. Давлиева, Р.Р. Галимов
Уфимский государственный авиационный технический университет
Уфа, Российская Федерация

Резюме: Перспективным направлением обеспечения функциональной безопасности субъектоцентрических систем, к числу которых относятся информационно-вычислительные системы, представляющие собою аппаратно-программные комплексы, является так называемое «барьерное мышление» (англ. – barrier thinking). Появление этого научного направления датируется концом 80-х годов и связывается с именем J. Reason. Исходной посылкой научного направления является признание неизбежности наличия латентных дефектов в системах управления сложной системой. Фокусом философии является разработка многослойных, эшелонированных систем защиты от внешних агрессивных воздействий, а также проявлений латентных дефектов в системах управления. Практическая реализация методов, основанных на «барьерном мышлении» сводится к исключению возможности возникновения такого сочетания латентных дефектов на разных уровнях управления объектом (организационном, тактическом, операционном), при которых опасности трансформируются в нежелательные последствия. Одним из перспективных подходов к формированию систематической процедуры создания барьеров является подход, в зарубежной литературе известный как Anticipatory Failure Determination (AFD), а в отечественной – как «диверсионный анализ». Подход, именуемый «диверсионным анализом» включает в себя реактивный и проактивный подходы к обеспечению функциональной безопасности субъектоцентрических систем. В статье анализируется концептуальная основа AFD, результатом чего является заключение о том, что методологической основой AFD является системный анализ. Это обосновывает возможность адаптации моделей и методов системного анализа к задачам качественного и количественного исследования систем в рамках AFD. Приводится описание типовой схемы анализа событий в рамках AFD-1. Приводится пример использования этой схемы в случае анализа отказов программного продукта. В заключении определяются ограничения на область применимости AFD как методической основы обеспечение функциональной безопасности аппаратно-программных комплексов в условиях неопределенности среды использования.

Ключевые слова: цифровая экосреда, функциональная безопасность, аппаратно-программный комплекс, «барьерное мышление», диверсионный анализ.

Для цитирования: Гвоздев В.Е., Гузаиров М.Б., Бежаева О.Я., Давлиева А.С., Галимов Р.Р. Обеспечение функциональной безопасности аппаратно-программных комплексов в условиях неопределенности среды использования. *Моделирование, оптимизация и информационные технологии*. 2020;8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/GvozdevSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.005

Ensuring the functional safety of hardware and software systems in an uncertain environment of use

V.E. Gvozdev, M.B. Guzairov, O.Ya. Bezhaeva, A.S. Davlieva, R.R. Galimov
Ufa State Aviation Technical University
Ufa, Russian Federation

Abstract: A promising direction in ensuring the functional safety of subject-centric systems, which include information and computing systems, which are hardware and software systems, is the so-called "barrier thinking" (English - barrier thinking). The emergence of this scientific trend dates back to the late 80s and is associated with the name J. Reason. The starting point of the scientific direction is the recognition of the inevitability of latent defects in the control systems of a complex system. The focus of philosophy is the development of multilayer, layered systems of protection against external aggressive influences, as well as manifestations of latent defects in control systems. The practical implementation techniques based on "barrier thinking" is reduced to eliminating the possibility of such a combination of latent defects at various levels of the control object (organizational, tactical, operational), at which the hazards are transformed into unwanted effects. One of the promising approaches to the formation of a systematic procedure for creating barriers is the approach known in foreign literature as the Anticipatory Failure Determination (AFD), and in the domestic one as "diversion analysis". The approach called "diversion analysis" includes reactive and proactive approaches to ensuring the functional safety of subject-centric systems. This article analyzes the conceptual framework of AFD, the result of which is the conclusion that the methodological basis of AFD is system analysis. This justifies the possibility of adapting models and methods of system analysis to the problems of qualitative and quantitative research of systems within the framework of AFD. A description of a typical event analysis framework for AFD-1 is provided. An example of the use of this circuit in the failure analysis case of a software product is given. In conclusion, the restrictions on the scope of applicability of AFD as a methodological basis for ensuring the functional safety of hardware and software systems in the conditions of uncertainty in the environment of use are determined.

Keywords: digital environment, functional safety, hardware-software complex, "barrier thinking", diversion analysis.

For citation: Gvozdev V.E., Guzairov M.B., Bezhaeva O.Ya., Davlieva A.S., Galimov R.R. Ensuring the functional safety of hardware and software systems in an uncertain environment of use. *Modeling, optimization and information technology.* 2020;8(3). Available from: https://moit.vivt.ru/wp-content/uploads/2020/08/GvozdevSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.005 (In Russ).

Введение

Функциональная безопасность сетецентрических информационно-управляющих систем (СИУС) является критическим фактором эффективного сетецентрического управления [1,2]. Функциональная безопасность СИУС в равной мере определяется как свойствами узлов (информационно-вычислительных систем), так и каналов связи (коммуникационных систем). В [3] подчеркивается, что объединяющим узлы и каналы свойством является то, что они представляют собою аппаратно-программные комплексы (АПК).

В литературных источниках подчеркивается необходимость рассмотрения как неделимого целого аппаратную и программную составляющие АПК. В связи с этим можно утверждать, что совершенствование подходов к обеспечению функциональной безопасности программной составляющей АПК является фактором повышения функциональной безопасности СИУС.

СИУС относится к классу открытых систем. Одним из требований к СИУС является способность обеспечивать информационные потребности пользователей при динамически изменяющихся свойствах сети [1], т.е. при изменениях среды использования АПК (неопределенности свойств информации и данных, поступающих на входы узлов сети). Эта особенность ограничивает применимость ранее созданных методических основ обеспечения функциональной безопасности АПК, предполагающих априорное определение на предпроектной стадии границ среды использования АПК.

В настоящей работе в качестве перспективного направления обеспечения функциональной безопасности АПК в условиях неопределенности среды использования обсуждается подход AFD-1, известный в отечественной литературе как «диверсионный анализ».

Предпосылки использования AFD

Ограниченность подходов к обеспечению функциональной безопасности автоматизированных информационных систем, рассматривающих их как замкнутые системы, в условиях, когда они фактически становились открытыми, проявляется, например, в трансформации философии тестирования. Произошел переход от методов «белого» и «черного» ящиков к ad-hoc; исследовательскому и иным слабо формализованным подходам к испытаниям информационных систем.

Перспективным направлением обеспечения функциональной безопасности субъектоцентрических систем, появление которого датируется концом 80-х годов и связывается с именем J. Reason, является так называемое «барьерное мышление» (англ. – barrier thinking). Существо этого направления определяется метафорой «модель швейцарского сыра» – Swiss Cheese Model [3,4]. Исходной посылкой является признание неизбежности наличия источников опасности для объекта управления, а также латентных дефектов в самом объекте управления. Фокусом барьерного мышления является исключение условий (создание барьеров) возникновению такого сочетания латентных дефектов на разных уровнях управления объектом (организационном, тактическом, операционном), при которых опасности трансформируются в нежелательные события.

С нашей точки зрения одним из перспективных подходов к формированию систематической процедуры создания барьеров является подход, в зарубежной литературе известный как Anticipatory Failure Determination (AFD), а в отечественной – как «диверсионный анализ» [5-9].

Целью AFD является выявление условий, создающих предпосылки для преобразования опасностей в нежелательные события.

Содержанием AFD является решение задач трех классов:

1) Выявление потенциальных опасностей (различного рода организационных и проектных ошибок; опасных действий людей; отказов оборудования; климатических воздействий и т.д.).

2) Выявление возможных каузальных цепочек, описывающих причинно-следственные связи событий, связанных с преобразованием опасностей в инциденты, а также выделение условий, при которых возможна реализация событий.

3) Разработка реалистичных и эффективных мер (барьеров), препятствующих реализации каузальных цепочек.

В [5] приводятся сведения о том, что AFD является обобщением известных в теории управления рисками методов сценарного анализа: FMEA; HAZOP; PHA; Threat Analysis; Vulnerability Analysis; Fault Trees; Event Trees; Event Sequence Diagrams.

В рамках AFD различают два подхода: AFD-1 и AFD-2. Первый ориентирован на анализ нежелательных событий, которые уже имели место. Второй ориентирован на прогнозирование еще не реализовавшихся, но возможных событий. Концептуальные отличия AFD-1 от иных методов сценарного анализа состоит в смещении акцентов от вопроса «Почему произошло нежелательное событие?» к вопросу «Какими способами можно обеспечить реализацию наблюдавшегося события?». Концептуальную основу AFD-2 составляет смещение акцентов от вопроса «Что в системе может пойти неправильно?» к вопросу «Если необходимо нанести ущерб требуемого масштаба, какой

способ явится наиболее эффективным?». Из содержания AFD-1 и AFD-2 можно сделать заключение, что диверсионный анализ включает в себя реактивный и проактивный подходы к обеспечению функциональной безопасности.

Концептуальная основа AFD

Основополагающими принципами AFD являются:

1) Принцип успешного сценария (в оригинале – The Principle of S_0). Согласно этому принципу основу построения возможных сценариев инцидентов составляет четкое разграничение между желаемой траекторией изменения состояния системы (S_0) и траекториями, возникающими вследствие различного рода событий как во внешней среде, так и в самой системе.

2) Принцип наличия инициирующего события (в оригинале – The Principle of Initiation). Суть этого принципа состоит в том, что невозможно беспричинное отклонение от желаемой траектории изменения состояния сложной системы.

3) Принцип множественности последствий инициирующих событий (в оригинале – The Principle of Emanation). Согласно этому принципу одно и то же инициирующее событие может иметь разные последствия, причем последствия могут быть как позитивные, так и негативные.

4) Принцип бесконечности формирования цепочек причинно-следственных связей (в оригинале – The Principle of Unending Cause-Effect). Содержание этого принципа сводится к признанию условностей понятий «инициирующее событие» и «конечное состояние». Инициирующее событие может быть конечным событием ранее реализовавшейся каузальной цепочки. С другой стороны, в рамках рассматриваемой задачи конечное состояние может рассматриваться как инициирующее событие в рамках другой задачи, рассматривающей изучаемую систему на ином уровне абстракции.

5) Принцип детализации (в оригинале – The Principle of Subdivision). Согласно этому принципу каждый компонент сценария может быть в свою очередь представлен сценарием из более детальных компонентов.

6) Принцип эквивалентных траекторий (в оригинале – Pinch Point Principle). Согласно этому принципу к одному и тому же состоянию системы могут привести различные каузальные цепочки.

7) Принцип равной важности знаний о причинах и последствиях событий (в оригинале – Fault and Event Trees). Содержание этого принципа состоит в том, что при выработке мер по предотвращению нежелательных событий в равной степени важны вопросы: «Что послужило причиной (инициирующим событием) возникновения каузальной цепочки» и «К каким последствиям может привести возможное инициирующее событие». Иными словами, для предотвращения нежелательных событий в равной мере важны как эмпирический опыт и знания лиц, устанавливающих защитные барьеры, так и способность предвидеть возможность возникновения нежелательных событий.

8) Принцип достаточности ресурсов (в оригинале – The Principle of Resources). Согласно этому принципу для того, чтобы произошло какое-либо событие, в одном месте и в одно время должны присутствовать все необходимые ресурсы. Отсутствие хотя бы одного ресурса делает невозможным развитие каузальной цепочки. При этом важно то, что ресурсы не обязательно должны присутствовать в готовом к применению виде. Они могут синтезироваться из вторичных ресурсов, присутствующих в самой системе либо окружающей среде. Например, причиной потери работоспособности АПК вследствие отсутствия электропитания (отсутствие необходимого для нормальной работы ресурса) может оказаться обрыв силового кабеля

вследствие ремонтных работ. В качестве вторичных ресурсов в этом случае выступают: проведение ремонтных работ; внесение ошибок в схему прокладки кабелей; наличие инструмента, посредством которого можно нарушить кабель; наличие персонала, выполняющего ремонтные работы.

Из содержания основополагающих принципов AFD можно сделать вывод о сходстве этого подхода с другими известными в рамках системного анализа подходами. Так, например:

- содержание принципа успешного сценария по смыслу коррелирует с базовым положением теории надежности, согласно которому основу исследования свойств технических систем по критериям надежности составляет формальное определение понятия «отказ»;
- содержание принципа наличия инициирующего события коррелирует с содержание подхода Root Cause Analysis [10];
- содержание принципа множественности последствий инициирующих событий коррелирует с положениями SWOT-анализа;
- содержание принципа бесконечности в возникновении причинно-следственных связей по сути основан на известном в системном анализе понятии «уровень абстракции»;
- содержание принципа детализации по сути представляет собою нисходящий подход к исследованию систем;
- содержание принципа эквивалентных траекторий по сути означает то же самое, что и «принцип эквивалентных путей достижения цели»;
- содержание принципа равной важности знаний о причинах и следствиях событий по сути совпадает с признанием равнозначности нисходящего и восходящего подходов к исследованию систем;
- содержание принципа достаточности ресурсов практически дословно совпадает с формулировкой ресурсного подхода в системном анализе.

Отмеченные обстоятельства позволяют утверждать, что методологической основой AFD является системный анализ. Это обосновывает возможность адаптации моделей и методов системного анализа к задачам качественного и количественного исследования систем в рамках AFD.

Схема анализа событий в рамках AFD-1

Выполнение анализа событий в общем случае сводится к реализации следующей последовательности шагов:

Шаг 1. Формулировка проблемы.

Назначение этого шага – характеристика исследуемой системы, описание симптомов и непосредственных причин («спусковых механизмов») событий.

Шаг 2. Описание идеального сценария S_0.

На этом шаге предполагается выделение логически завершенных стадий процесса с описанием результатов, которые должны получаться в конце каждой стадии.

Шаг 3. Реализация области события.

Назначение этого шага является определение фазы процесса/компонента системы, в которой/котором произошло событие. На этом шаге сокращается область поиска, т.е. исключается из рассмотрения функции/компоненты системы, в которых не могло произойти событие.

Шаг 4. Формулирование расширенной инвертированной проблемы в общем виде.

На этом шаге решаются следующие задачи:

4.1. Выявляются непосредственные причины и условия, приведшие к наблюдавшимся событиям.

4.2. Выявляются способы и условия реализации событий равных и превосходящих по последствиям те, что наблюдались.

Назначением шага является получение ответа на вопрос: «Что нужно сделать для того, чтобы в максимально возможной степени нарушить ход идеального процесса?».

Шаг 5. Поиск способов реализации инвертированной проблемы.

На этом шаге осуществляется поиск того, как можно создать причины и условия, увеличивающие возможность возникновения нежелательных событий. При этом происходит смещение акцентов исследования от вопроса «Что может произойти?» к вопросу «Как можно сделать?». Реализация этого шага предполагает получение ответов на следующие вопросы:

5.1. Поиск очевидных решений.

Существо этого вопроса сводится к определению функций/компонентов системы, события в которых будут решениями инвертированной проблемы.

5.2. Идентификация ресурсов.

Определяется перечень ресурсов, наличие которых необходимо для реализации очевидных решений.

5.3. Поиск способов получения ресурсов.

Ищутся способы получения ресурсов, в том числе за счет преобразования вторичных ресурсов, имеющихся в системе либо окружающей среде.

Шаг 6. Формулирование гипотезы по способам реализации инвертированной проблемы.

На этом шаге формулируются гипотезы о способах решения задач, определенных на шаге 5.

Шаг 7. Определение действий, препятствующих реализации инвертированной проблемы.

На этом шаге определяются барьеры, препятствующие реализации гипотез, определенных на шаге 6.

Пример. В составе системы управления имеется программный продукт, реализующий вычисление ряда функций (Рисунок 1).

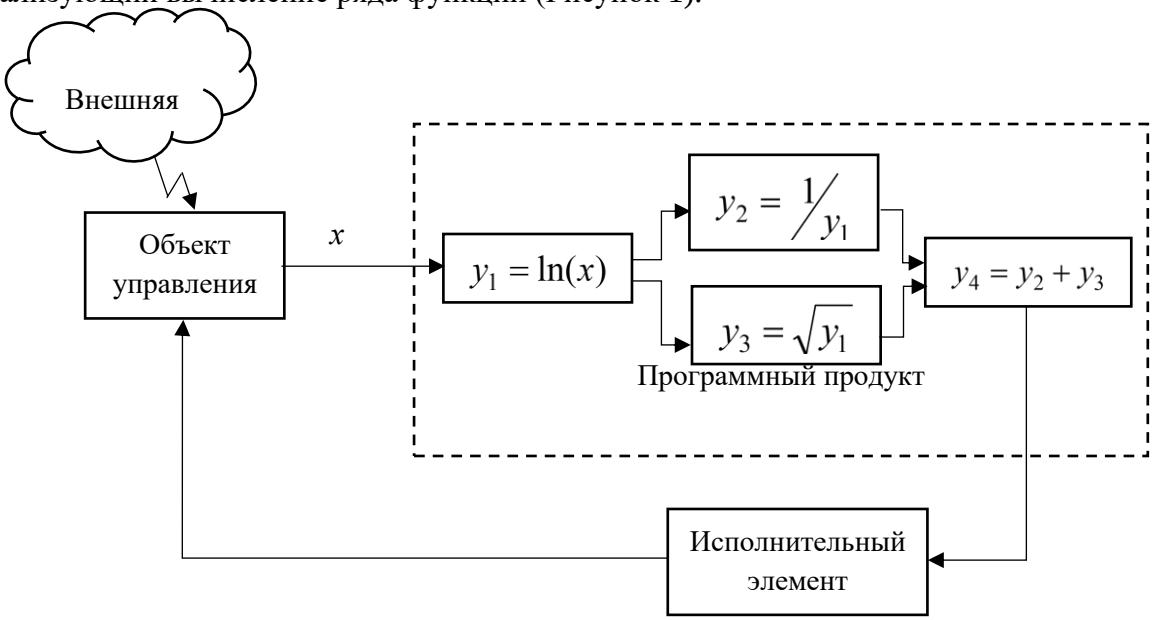

Рисунок 1 – Программный продукт в составе системы управления
Figure 1 – The software product as part of a control system

Исходные данные (значения x), поступающие от объекта управления, являются вещественными величинами. По оценкам экспертов областью фактических значений x, соответствующих штатному режиму функционирования объекта управления, являлись $x \in (3.5;4.5)$. В техническом задании на разработку программного продукта область возможных значений определена как $x \in (3;5)$, чему соответствуют значения $y_4 \in (y_4^{(н)}, y_4^{(в)})$. Работоспособность программного продукта длительное время не вызывала нареканий. Однако в последующем два раза произошло аварийное прерывание вычислений. К тому же в ряде случаев качество функционирования объекта управления падало, что было обусловлено тем, что значения $y_4 \notin (y_4^{(н)}, y_4^{(в)})$.

В ходе исследований было установлено, что из-за изменения состояния внешней среды объекта управления область возможных значений x стала $x \in (-1;10)$. Один из аварийных случаев связан с тем, что значение x оказалось $x = 0$. Другой – с тем, что $x = 1$. Схема устранения причин отказов свелась к тому, что в коды была добавлена проверка условия $x \in (3;5)$. Если это условие не соблюдается, будет выдаваться сообщение «недопустимое значение аргумента» и вычисления не производятся.

Использование схемы AFD-1

Шаг 1. Формулировка проблемы.

Имеется программный продукт, реализующий вычислительные операции:

$$y_1 = \ln(x); y_2 = 1/y_1; y_3 = \sqrt{y_1}; y_4 = y_2 + y_3 \quad (1)$$

Безаварийное завершение вычислений возможно при $x > 1$. На этапе разработки программного продукта предполагалось, что областью возможных значений аргумента всегда будут значения $x \in (3;5)$, в силу чего в тексте программы отсутствовала проверка условия $x > 1$, что и послужило причиной аварийных завершений вычислений, так как один раз x приняло значение $x = 0$, один раз – $x = 1$. Снижение качества функционирования объекта управления падало, так как хотя соблюдалось условие $x > 1$, в действительности значение x не всегда удовлетворяло условию $3 < x < 5$, а могло лежать в диапазоне $-1 < x < 10$.

Шаг 2. Описание идеального сценария S_0.

Идеальный сценарий состоит в получении значения $x \in (3;5)$ и проведении вычислений y_4 в соответствии с (1).

Шаг 3. Локализация области отказа.

Отказы были обусловлены тем, что не соблюдалось условие $x > 1$, т.е. отсутствовал контроль допустимости значений аргумента. Снижение качества функционирования объекта управления обусловлено тем, что при нарушении условия $x \in (3;5)$ не осуществлялся переход на иные алгоритмы расчета y_4, гарантировавшие выполнение условия $y_4 \in (y_4^{(н)}, y_4^{(в)})$.

Иными словами, не реализовывалась схема

$$y_4 = \begin{cases} A^{(1)} при 1 < x \le 3, \\ A^{(2)} при 3 < x < 5, \\ A^{(3)} при 5 \le x < 10, \end{cases}$$

где $A^{(i)}$ – алгоритм расчета y_4 при нахождении x в i-м из указанных диапазонов. Алгоритм $A^{(2)}$ совпадает со схемой расчета, представленной на Рисунке 1.

Шаг 4. Формулирование расширенной инвертированной проблемы.

4.1. Непосредственная причина отказов программного продукта состояла в том, что в тексте программы отсутствовал контроль допустимости значений входных параметров. Снижение качества информационной поддержки управления объектом было обусловлено тем, что не было обеспечено соответствие способов обработки входных данных свойствам данных, т.е. не был предусмотрен переход к разным алгоритмам обработки данных в зависимости от того, какому диапазону принадлежит значение x.

4.2. При создании программного продукта необходимо так организовать процесс его производства, чтобы в готовом продукте как можно чаще наблюдались аварийные завершения вычислений и в случае безаварийного завершения вычислений результаты расчетов не соответствовали состоянию бизнес-процесса.

Шаг 5. Поиск решения инвертированной проблемы.

5.1. Поиск очевидных решений.

а) В техническом задании описание бизнес-процесса, поддержку которого должен обеспечить программный продукт, привести в максимально общем виде, препятствующем определению допустимых значений x, при которых не происходит аварийных завершений вычислений.

б) Исключить в техническом задании требование перехода на разные схемы обработки данных в зависимости от свойств исходных данных. Оставить лишь описание схемы расчетов, соответствующих идеальному сценарию реализации бизнес-процесса.

5.2. Идентификация ресурсов.

В рассматриваемом случае условиями (ресурсами), способствующими реализации инвертированной проблемы, являются:

а) недостаточная формализация описания бизнес-процессов, обеспечивающих управление объектом;

б) недостаточная формализация условий выбора схемы расчетов в зависимости от свойств исходных данных.

5.3. Поиск способов получения ресурсов.

В рассматриваемом случае наибольшее число латентных дефектов можно обеспечить следующими способами:

а) Поручить разработку технического задания представителям заказчика и исключить из этого процесса представителей исполнителя. В этом случае в силу различия смыслового пространства специалистов в различных областях знаний возникает возможность недостаточно формального и детального (с точки зрения разработки программного продукта) описания особенностей бизнес-процессов.

б) Привлечение к разработке программного продукта специалистов, не владеющих в достаточной степени базовыми приемами разработки и испытания программных продуктов, а именно: обязательного определения области допустимых значений входных параметров; проверки поведения программного продукта как при допустимых, так и при недопустимых значениях входных параметров.

в) Выделение на реализацию программного проекта ресурсов (времени разработки), заведомо недостаточных для обеспечения качественной разработки и исследования функциональных и нефункциональных свойств программного продукта.

Шаг 6. Формирование гипотезы по способам реализации инвертированной проблемы.

В силу того, что программные продукты относятся к классу субъектоцентрических систем, можно утверждать, что причиной возникновения

латентных дефектов на разных стадиях жизненного цикла программных продуктов являются системные ошибки в организации программных проектов и различного рода персонифицированные ошибки, допускаемые разработчиками. В силу этого можно утверждать, что основной способ реализации инвертированной проблемы – обеспечение низкого качества управления программным проектом. Реалистичность такого подхода подтверждается многочисленными сведениями, представленными в разных литературных источниках.

Шаг 7. Действия, препятствующие реализации инвертированной проблемы.

Формирование барьеров (организационных, технологических), исключающих возможность возникновения условий (получение ресурсов), необходимых для реализации расширенной инвертированной проблемы, а именно:

1) Организационные барьеры

а) Разработка технического задания коллективом, в состав которого входят компетентные в своих профессиональных областях представители заказчика и исполнителя.

б) Контроль наличия в техническом задании формальных моделей управления объектом и моделей информационной поддержки управления как в расчетном состоянии окружающей среды, так и при его изменении.

2) Технологические барьеры

в) Исследование поведения программного продукта при непредсказуемых изменениях входного параметра (например, посредством ad-hoc тестирования).

г) Контроль значения входного параметра x и выбор схемы расчета y_4 с учетом того, какому из диапазонов принадлежит измеренное значение x (см. шаг 3).

Заключение

Цифровая экосреда является системообразующим фактором, обеспечивающим эффективную реализацию киберфизического управления. Особенностями киберфизического управления являются, во-первых, одновременная реализация адхократического, лоурархического и иерархического подходов к управлению распределенными динамическими объектами. Во-вторых, наличие противоречивых целей субъектов управления при наличии единой глобальной цели управления. В-третьих, неопределенность состояния объекта управления и изменчивость целей управления. Приведенный перечень особенностей киберфизического управления не является полным. Но даже отмеченные особенности позволяют сделать заключение о том, что существующие к настоящему времени методические основы обеспечения функциональной безопасности (ориентированные на создание аппаратно-программных комплексов для использования в заранее определенных условиях) в полной мере не позволяют решать задачи, связанные с формированием цифровой экосреды.

Вместе с тем, системообразующий характер цифровой экосреды делает необходимым выделить в качестве критического фактора функциональную безопасность инфраструктурных компонент цифровой экосреды. Это делает необходимым совершенствование теоретических, методических, модельных основ обеспечения функциональной безопасности компонент инфраструктуры цифровой экосреды.

Вопросам развития методологических и теоретических основ управления функциональной безопасностью, субъектоцентрических систем (к числу которых относятся аппаратно-программные комплексы) посвящены работы многих исследователей. Тем не менее, требуют дальнейшего развития теоретические основы, позволяющих выполнить научно обоснованную адаптацию разработок, подтвердивших свою эффективность при управлении функциональной безопасностью

субъектоцентрических систем иной, природы в область управления функциональной безопасностью распределенных динамических информационно-вычислительных систем.

Основу подхода, получившего в литературе наименование «барьерного мышления» (barrier thinking) составляет философия «defense-in-depth», разработанную в рамках проведения исследований, связанных с повышением функциональной безопасности атомной промышленности. Фокусом философии является разработка многослойных, эшелонированных систем защиты от агрессивных внешних воздействий. Наиболее известная метафора, отражающая существо «барьерного мышления» – «Модель Швейцарского Сыра - Swiss Cheese Model (SCM)», предложенная J.Reason. В рамках этой метафоры предотвратить трансформацию опасности (hazard) в потери (loses) можно за счет размещения между опасностью и потерями серии барьеров. Каждый из барьеров отождествляется с куском швейцарского сыра (знаменитого наличием в нем большого числа дырок – «holes»). Именно эта ассоциация дала название метафоре. «Дырки в слоях сыра» являются прообразом латентных дефектов, имеющих место в защитных барьерах, и обусловленных ошибками разной природы (организационной, технологической, ментальной), допускаемых разработчиками субъектоцентрических систем. Каждый отдельный барьер не способен полностью предотвратить негативные последствия, обусловленные опасностью. Вместе с тем, формирование системы барьеров делает возможным качественно усилить систему защиты за счет возникновения системного эффекта.

Одним из подходов к реализации концепции «барьерного мышления» с нашей точки зрения является описанный в литературе подход, известный как «диверсионный анализ» (AFD). AFD позволяет предложить систематическую процедуру для выявления уязвимых мест в конструкциях и организации использования объектов (т.е. позволяет выявлять места, в которых целесообразно устанавливать «барьеры»). Вместе с тем в современной литературе этот подход получил распространение применительно к техническим системам. Научная адаптация положений AFD в область управления функциональной безопасностью АПК требует проведения дополнительных исследований.

Ограничениями AFD с точки зрения управления функциональной безопасностью АПК являются:

- невозможность учета временного аспекта, ориентация на статические модели;
- неустойчивый характер оценок свойств защитных барьеров в условиях изменчивости свойств открытой информационно-вычислительной системы.

Перспективным направлением исследований видится развитие положений концепции «барьерного мышления» на случай статистической неопределенности свойств среды функционирования динамических информационно-вычислительных сетей.

БЛАГОДАРНОСТИ

Работа выполнена при поддержке РФФИ в рамках научного проекта № 19-08-00177 А «Методологические, теоретические и модельные основы управления функциональной безопасностью аппаратно-программных комплексов в составе распределенных сложных технических систем».

ЛИТЕРАТУРА

1. Кудж С.А., Цветков В.Я. Сетецентрическое управление и киберфизические системы. *Образовательные ресурсы и технологии*. 2017;2(19):86-92.
2. Черняк Л. Киберфизические системы. Cyber-Physical System (CPS). *К чему приведет слияние интернета, людей, вещей и сервисов.* 2017. URL: http://www.tadviser.ru/a/3748270(дата обращения: 12.02.2020).
3. *Revisiting the "Swiss Cheese" Model of Accidents*. EEC Note No. 13/06. European Organization for the Safety of Air Navigation, October 2006.
4. Thomas V. Perneger. The Swiss cheese model of safety incidents: Are there holes in the metaphor? *BMC Health Services Research*. 2005; 5(1). Available at: https://www.researchgate.net/publication/7488318_The_Swiss_cheese_model_of_safety_incidents_Are_there_holes_in_the_metaphor DOI: 10.1186/1472-6963-5-71 (accessed 12.01.2020).
5. Visnepolschi S., Zlotin B., Kaplan S., Zusman A. New tools for failure and risk analysis anticipatory failure determination (AFD) and the theory of scenario structuring. *Ideation Intl Inc*, 1999, 86 p.
6. Thurnes C., Zeihsel F., Visnepolschi S., Hallfell F. Using TRIZ to invent failures – concept and application to go beyond traditional FMEA. *Procedia Engineering*, 2015:426-450. Available at www.sciencedirect.com
7. Sunday E. Extension and Modification of Anticipatory Failure Determination Approach Based on I-TRIZ. *University of Stavanger, Department of Mechanical and Structural Engineering*, June 2014.
8. Klein G., Snowden D., Chew L.P. Anticipatory Thinking. *Proceedings of the Eighth International NDM Conference* (Eds. K. Mosier & U. Fischer), Pacific Grove, CA, June 2007.
9. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes, *Federal Technological University of Paraná (UTFPR)*, Curitiba, Brazil, January 2019. DOI: 10.1007/978-3-319-78075-7_12
10. Ritu Soni, Ashpinder Preet. Cognitive approach to root cause analysis for improving quality of life: a case study for IT Industry. *International journal of informative and futuristic research (Online)*. Vol. 1. Issue 1, August -September 2013.

REFERENCES

1. Kuj S.A., Tsvetkov V.Ya. Network-centric management and cyber-physical systems. *Obrazovatel'nye resursy i tekhnologii*. 2017;2(19):86-92 (In Russ).
2. Chernyak L.. Cyber-Physical System (CPS). What will the merger of the Internet, people, things and services lead to? 2017. (In Russ) URL: http://www.tadviser.ru/a/37482720(accessed 12.02.2020).
3. *Revisiting the "Swiss Cheese" Model of Accidents.* EEC Note No. 13/06. European Organization for the Safety of Air Navigation, October 2006.
4. Thomas V. Perneger. The Swiss cheese model of safety incidents: Are there holes in the metaphor? *BMC Health Services Research*. 2005; 5(1). Available at: https://www.researchgate.net/publication/7488318_The_Swiss_cheese_model_of_safety_incidents_Are_there_holes_in_the_metaphor DOI: 10.1186/1472-6963-5-71 (accessed 12.01.2020).

5. Visnepolschi S., Zlotin B., Kaplan S., Zusman A. New tools for failure and risk analysis anticipatory failure determination (AFD) and the theory of scenario structuring. *Ideation Intl Inc*, 1999.
6. Thurnes C., Zeihsel F., Visnepolschi S., Hallfell F. Using TRIZ to invent failures – concept and application to go beyond traditional FMEA. *Procedia Engineering*, 2015:426-450. Available at www.sciencedirect.com
7. Sunday E. Extension and Modification of Anticipatory Failure Determination Approach Based on I-TRIZ. *University of Stavanger, Department of Mechanical and Structural Engineering*, June 2014.
8. Klein G., Snowden D., Chew L.P. Anticipatory Thinking. *Proceedings of the Eighth International NDM Conference* (Eds. K. Mosier & U. Fischer), Pacific Grove, CA, June 2007.
9. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes, *Federal Technological University of Paraná (UTFPR)*, Curitiba, Brazil, January 2019, 24p. DOI: 10.1007/978-3-319-78075-7_12
10. Ritu Soni, Ashpinder Preet. Cognitive approach to root cause analysis for improving quality of life: a case study for IT Industry. *International journal of informative and futuristic research (Online)*. Vol. 1. Issue 1, August -September 2013.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Гвоздев Владимир Ефимович, д.т.н., профессор кафедры технической кибернетики ФГБОУ ВО «Уфимский государственный авиационный технический университет», Уфа, Российская Федерация
e-mail: wega55@mail.ru

Vladimir E. Gvozdev, Doct. Sci. (Technical), Professor Of The Department Of Engineering Cybernetics, Ufa State Aviation Technical University, Ufa, Russian Federation

Гузаиров Мурат Бакеевич, д.т.н., профессор кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет», Уфа, Российская Федерация
e-mail: guzairov@ugatu.su

Murat B. Guzairov, Doct. Sci. (Technical), Professor Of The Department Of Computing And Information Security, Ufa State Aviation Technical University, Ufa, Russian Federation

Бежаева Оксана Яковлевна, к.т.н., доцент кафедры технической кибернетики ФГБОУ ВО «Уфимский государственный авиационный технический университет», Уфа, Российская Федерация.
e-mail: obezhaeva@gmail.com

Oxana Y. Bezhaeva, Cand.Sci. (Technical), Associate Professor Of The Department Of Engineering Cybernetics, Ufa State Aviation Technical University, Ufa, Russian Federation.

Давлиева Алия Салаватовна, соискатель, кафедра технической кибернетики ФГБОУ ВО «Уфимский государственный авиационный технический университет», Уфа, Российская Федерация.
e-mail: aliyasr21@gmail.com

Aliya S. Davlieva, Degree Applicant, Department Of Engineering Cybernetics, Ufa State Aviation Technical University, Ufa, Russian Federation.

Галимов Роберт Ришатович, аспирант кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет», Уфа, Российская Федерация.
e-mail: rrgalimov@gmail.com

Robert R. Galimov, Graduate Student Of The Department Of Computing And Information Security, Ufa State Aviation Technical University, Ufa, Russian Federation