

Моделирование надежности программных компонентов киберфизических систем

А.Н. Привалов¹, Е.В. Ларкин², А.В. Богомолов³✉

¹ Тульский государственный педагогический университет им. Л.Н. Толстого, г. Тула, 300026, Россия

² Тульский государственный университет, г. Тула, 300012, Россия

³ Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва, 119333, Россия

Ссылка для цитирования

Привалов А.Н., Ларкин Е.В., Богомолов А.В. Моделирование надежности программных компонентов киберфизических систем // Программные продукты и системы. 2025. Т. 38. № 1. С. 47–54. doi: 10.15827/0236-235X.149.047-054

Информация о статье

Группа специальностей ВАК: 2.3.5

Поступила в редакцию: 22.07.2024

После доработки: 16.08.2024

Принята к публикации: 23.08.2024

Аннотация. Актуальность данного исследования обусловлена тем, что надежность программных компонентов киберфизических систем является ключевой составляющей их эффективного функционирования. Ее адекватное математическое моделирование имеет существенное значение для прогресса цифровизации экономики. Работа направлена на устранение недостатков известных подходов к моделированию надежности программных компонентов, при реализации которых оценки характеристик надежности формируются на основе эмпирических данных о количестве ошибок, выявленных при тестировании программ. Поэтому результаты тестирования существенно зависят как от его длительности, так и от полноты покрытия области обрабатываемых данных подобластью данных, генерируемых при тестировании, что снижает эффективность оценивания надежности. Предметом исследования стали методы моделирования надежности программных компонентов киберфизических систем, характеризующейся временем запаздывания в цепи обратной связи между компонентами. В работе использованы методы программной инженерии, теории надежности, теории вероятностей и марковских процессов. Основным результатом являются математические модели надежности программных компонентов киберфизических систем, объединяющей полумарковские модели программных компонентов, генерации их сбоев и отказов. Разработанные математические модели основаны на структурно-параметрической полумарковской модели сбоев и отказов программного обеспечения, параметры которой определяются вычислительной сложностью и требованиями, предъявляемыми к программному обеспечению с учетом его функционального назначения. Получены формализованные описания пуассоновских потоков сбоев и отказов программных компонентов киберфизической системы. Практическая значимость работы определяется ее ориентированностью на применение для определения надежности программных компонентов на всех этапах жизненного цикла киберфизических систем, элементы которых взаимодействуют, самонастраиваются и адаптируются к изменениям с помощью стандартных программно реализуемых протоколов.

Ключевые слова: киберфизическая система, программное обеспечение, надежность программы, сбой программы, отказ программы, моделирование надежности, полумарковский процесс

Благодарности. Работа выполнена при поддержке гранта РФФ № 24-29-20256

Введение. Ключевые достижения и тренды научно-технического прогресса связаны с цифровизацией, предполагающей повсеместное применение цифровых технологий сбора и обработки информации [1]. Ускоренное внедрение цифровых технологий в экономику и социальную сферу является одной из национальных целей развития России. Ее достижение необходимо в интересах создания условий для высокотехнологичного бизнеса, повышения конкурентоспособности страны на глобальном рынке, укрепления национальной безопасности и повышения качества жизни людей. Одним из приоритетов цифровизации является внедрение киберфизических систем, отличительная особенность которых в интеграции вычисли-

тельных ресурсов в инженерно-технические системы [2, 3]. Причем вычислительная компонента киберфизической системы распределена по всей системе и синергетически увязана с составляющими ее элементами [4, 5]. Элементы киберфизических систем и отдельные киберфизические системы взаимодействуют, самонастраиваются и адаптируются к изменениям с помощью стандартных программно реализуемых интернет-протоколов [6, 7]. Поэтому надежность программных компонентов киберфизических систем является ключевой составляющей их эффективного функционирования, а ее адекватное моделирование имеет существенное значение для прогресса цифровизации.

Обзор существующих подходов

Причиной сбоев/отказов любого ПО являются ошибки, допущенные человеком, в том числе новые, возникшие при исправлении ранее сделанных ошибок и приводящие к отказам/сбоям того же самого или другого типа [8, 9]. Концепция моделирования надежности программных компонентов киберфизических систем должна быть единой, например, привязанной к их аппаратной части, а ввиду специфики причин отказов программная часть должна исследоваться в контексте моделей и задач обработки данных, сопровождающих функционирование киберфизических систем [10–12].

Недостатком известных подходов к моделированию надежности программных компонентов является то, что оценки характеристик надежности формируются на основе эмпирических данных о количестве ошибок, выявленных при тестировании программ [2, 13, 14]. Поэтому результаты тестирования существенно зависят как от его длительности, так и от полноты покрытия области обрабатываемых данных под областью данных, генерируемых при тестировании [12, 15].

Программные компоненты киберфизических систем решают задачи обеспечения их взаимодействия, самонастройки и адаптации к изменениям [16, 17]. В простейшем случае обработка данных по заданному алгоритму осуществляется последовательно, а целью обработки является формирование управляющих воздействий, направленных на обеспечение заданных характеристик: устойчивости, времени достижения установившегося режима функционирования киберфизической системы, перерегулирования, точности поддержания установившегося режима и т.п. [1, 18, 19]. Кратковременный выход перечисленных характеристик за заданные пределы означает сбой функционирования программных компонентов киберфизической системы, а устойчивое несоблюдение требований – их отказ.

Структурно-параметрической моделью функционирования программных компонентов киберфизической системы является полумарковский процесс [20, 21], состояния которого – абстрактный аналог операторов алгоритма функционирования. Время пребывания в состояниях определяется вычислительной сложностью реализуемых алгоритмов, а вероятность переключения в сопряженные состояния – спецификой обрабатываемых данных и логическими условиями выбора каждого состояния [22].

Таким образом, моделирование надежности программных компонентов киберфизической системы сводится к синтезу структурно-параметрической модели отказов ПО, применимой на этапе разработки программных компонентов. Недостаточно полная разработка моделирования надежности программных компонентов киберфизических систем обуславливает актуальность проведенных исследований, отличительные особенности которых определяются ориентацией на устранение недостатков известных подходов к моделированию надежности программных компонентов, при реализации которых оценки характеристик надежности формируются только на основе эмпирических данных о количестве ошибок, выявленных при тестировании программ.

Метод исследования

Анализ опыта эксплуатации киберфизических систем показывает, что наиболее часто мониторинг состояния их элементов и компонентов реализуется с помощью циклического опроса (поллинга) [2, 22]. Поллинг реализует алгоритм, включающий множество операторов:

$$S = \{s_0, s_1, \dots, s_n, \dots, s_N, s_{N+1}\},$$

где s_0 и s_{N+1} – фиктивные (неисполняемые) операторы, соответствующие операциям «Начало» и «Конец» запуска цикла поллинга, а остальные операторы s_n – исполняемые (иницирующие действия) операторы. Обратная связь между двумя неисполняемыми операторами придает цикличность алгоритму поллинга, а общее количество обращений (N) к элементам и компонентам киберфизической системы в цикле поллинга определяется количеством связей (K) между ними:

$$N = 2K.$$

Поскольку цикл поллинга реализует случайный процесс, эволюция (порядок обращений к элементам и компонентам киберфизической системы) которого после любого s_n не зависит от эволюции, предшествовавшей выполнению s_n , а время выполнения операции s_n имеет произвольные функции распределения, процедура поллинга может быть представлена в виде полумарковского процесса:

$$\mu = \{S, h(t)\},$$

где S – множество состояний, совпадающих с множеством операторов $\{s_n\}$, $n \in [1, \dots, N]$; $h(t) = p \otimes f(t)$ – полумарковская матрица; $f(t) = \{f_{j,n}(t)\}$ – матрица плотностей распределе-

ния времени выполнения операторов поллинга; $p = \{p_{j,n}\}$ – стохастическая матрица.

При разорванной обратной связи (связи между s_0 и s_{N+1}) полумарковский процесс имеет одно стартовое (s_0) и одно поглощающее (s_{N+1}) состояния и будет эргодическим, только если для любой пары состояний $(s_j, s_n), j, n \in [0, N+1]$, существует хотя бы один путь из состояния s_j в состояние s_n и хотя бы один путь из состояния s_n в состояние s_j . Свойство эргодичности следует из требований к процедуре поллинга, которая в течение каждого цикла должна иметь возможность хотя бы по одному разу опросить каждый компонент киберфизической системы.

В общем случае плотности распределения $f_{j,n}(t)$ время пребывания полумарковского процесса в состоянии s_j , если априорно известно, что следующим его состоянием будет s_n , определяется сверткой

$$f_{j,n}(t) = f_{j,n}^c(t) \odot f_{j,n}^d(t),$$

где $f_{j,n}^c(t)$ – плотность распределения времени программной подготовки данных для обмена с j -м элементом киберфизической системы в процессе поллинга; $f_{j,n}^d(t)$ – плотность распределения времени активации программного драйвера j -го элемента киберфизической системы в процессе поллинга; \odot – операция свертки.

Вероятности переключения полумарковского процесса из состояния s_j в состояние s_n определяются плотностями распределения данных, обрабатываемых конкретным оператором, и логическими условиями перехода процедуры поллинга в сопряженные операторы (алгоритмом поллинга).

В простейшем случае поллинг представляет собой последовательный однократный опрос каждого элемента киберфизической системы, реализуемый подачей на вход вектора входных сигналов с последующим анализом времени получения и компонентов вектора выходных сигналов. Кортеж $\langle s_0, s_1, \dots, s_N, s_{N+1} \rangle$ образует на полном ориентированном графе процедуры поллинга гамильтонов (посещающий каждую вершину ровно один раз) путь из s_0 в s_{N+1} . Одна из очевидных реализаций гамильтонова пути получается исключением из кортежа состояний s_0 и s_{N+1} . Замыкание (связь) состояний s_1 и s_N гамильтонова пути порождает гамильтонов цикл, в соответствии с которым производится опрос элементов киберфизической системы при поллинге.

Конкретная последовательность опроса элементов определяется разработчиком алгоритма поллинга с учетом специфики эксплуатации конкретной киберфизической системы. Плотности распределения времени пребывания процесса в состояниях s_0 и s_{N+1} определяются вырожденным законом распределения:

$$f_{N+1,0}(t) = f_{0,j}(t) = \delta(t),$$

где $\delta(t)$ – δ -функция Дирака. Как и ранее, предполагается, что обработка данных производится в операторах $\{s_i\}, i \in [1 \dots N]$.

Плотность распределения времени возврата в любой из операторов $\{s_1, \dots, s_N\}$, образующих при замыкании цикл, равна

$$f_{s_j}(t) = L^{-1} \prod_{j=1}^N L(f_j(t)),$$

где $L[\dots]$ и $L^{-1}[\dots]$ – прямое и обратное преобразования Лапласа соответственно; $f_j(t) \in f(t)$ – плотность распределения времени выполнения оператора s_j , выбираемая из матрицы $f(t)$ в соответствии с построенным гамильтоновым циклом. Период цикла, характеризуемый оценкой математического ожидания времени возврата в начало после цикла поллинга, равен

$$T = \sum_{j=1}^N T_j = \sum_{j=1}^N \int_0^{\infty} t f_j(t) dt,$$

где T_j – математическое ожидание времени выполнения операции $s_j, j \in [1 \dots N]$.

Поскольку при опросе элементов киберфизической системы программа поллинга выполняет процедуру дискретизации входного сигнала, период T должен удовлетворять условию

$$\frac{2\pi}{T} > \Omega(k), k \in \{1, \dots, K\},$$

где $\Omega(k)$ – минимальная круговая частота дискретизации k -го параметра, определяемая теоремой Котельникова для спектра вектора входных сигналов [23, 24]. На практике это условие, как правило, не выполняется, поэтому ошибка дискретизации при ее реализации с помощью процедуры поллинга должна быть меньше допустимой, то есть удовлетворять условию

$$\varepsilon \leq \min_{k \in \{1, \dots, K\}} \varepsilon_k,$$

где ε – допустимая ошибка дискретизации; ε_k – допустимая ошибка дискретизации k -го параметра.

При выходе периода дискретизации за порог, оцениваемый величиной ε_k , возникает ситуация, которая может привести к сбою/отказу киберфизической системы вследствие накопления ошибки дискретизации. Вероятность появления такой ошибки вычисляется как

$$p_k = \int_{\varepsilon}^{\infty} f_{S_j}(t) dt.$$

При организации обратной связи в киберфизической системе плотность распределения времени запаздывания вывода значений выходного (получаемого в результате поллинга) сигнала относительно ввода значений входного сигнала определяется выражением

$$f_z(t) = L^{-1} \left[L \left[f_{S_j}(t) \right]^M \right],$$

где M – порядок конечно-разностного уравнения в случае, если вектор выходного сигнала определяется как решение системы конечно-разностных уравнений, или количество отсчетов, необходимых для вычисления свертки, если вектор выходного сигнала определяется через вычисление свертки. Тогда математическое ожидание времени запаздывания будет

$$T_z = \int_0^{\infty} t f_z(t) dt.$$

Временной интервал между вводом входного сигнала и выводом выходного представляет собой чистое запаздывание в контуре обратной связи [25–27]. С точностью, достаточной для практических целей, можно считать, что запаздывание по времени во всех цепях обратной связи одинаково и определяется как временной интервал, начинающийся от чтения из буфера входного сигнала и заканчивающийся выводом выходного сигнала.

Если τ_k^1, τ_k^2 – пороговые значения времени запаздывания в цепи обратной связи, при которых перерегулирование параметра входного сигнала достигает критических значений, а τ_k^3 – порог, при достижении которого киберфизическая система теряет устойчивость, то вероятность сбоя/отказа киберфизической системы определяется как

$$p_z = \int_{\tau}^{\infty} f_z(t) dt,$$

где

$$\tau = \min_{k \in \{1, \dots, K\}} \{ \tau_k^1, \tau_k^2, \tau_k^3 \}.$$

Обсуждение результатов

Оценки вероятностей p_k и p_z , а также плотностей распределения $f_k(t)$ и $f_z(t)$ являются основой для построения полумарковской модели отказов программных компонентов киберфизической системы. На рисунке показан алгоритм определения надежности программных компонентов киберфизической системы, харак-

теризуемой временем запаздывания в цепи обратной связи.

По результатам подсчета надежности программных компонентов надежность киберфизической системы может быть оценена как высокая (ни одного выхода, то есть бессбойная работа программных компонентов), невысокая (от одного до N выходов, перемежающихся с периодами бессбойной работы, то есть сбойная работа программных компонентов) или низкая (больше N выходов, то есть отказ программных компонентов).

С помощью полумарковской модели времени наработки программных компонентов киберфизической системы до сбоя (T_s) и до отказа (T_o) могут быть оценены как

$$T_s = \frac{T_z}{p_z},$$

$$T_o = NT_z + \frac{T_z(1-p_z)(1-p_z^N) \sum_{i=1}^N i p_z^{i-1}}{p_z^N},$$

где T_z – математическое ожидание времени цикла поллинга; p_z – вероятность отказа программных компонентов в текущем цикле наблюдения.

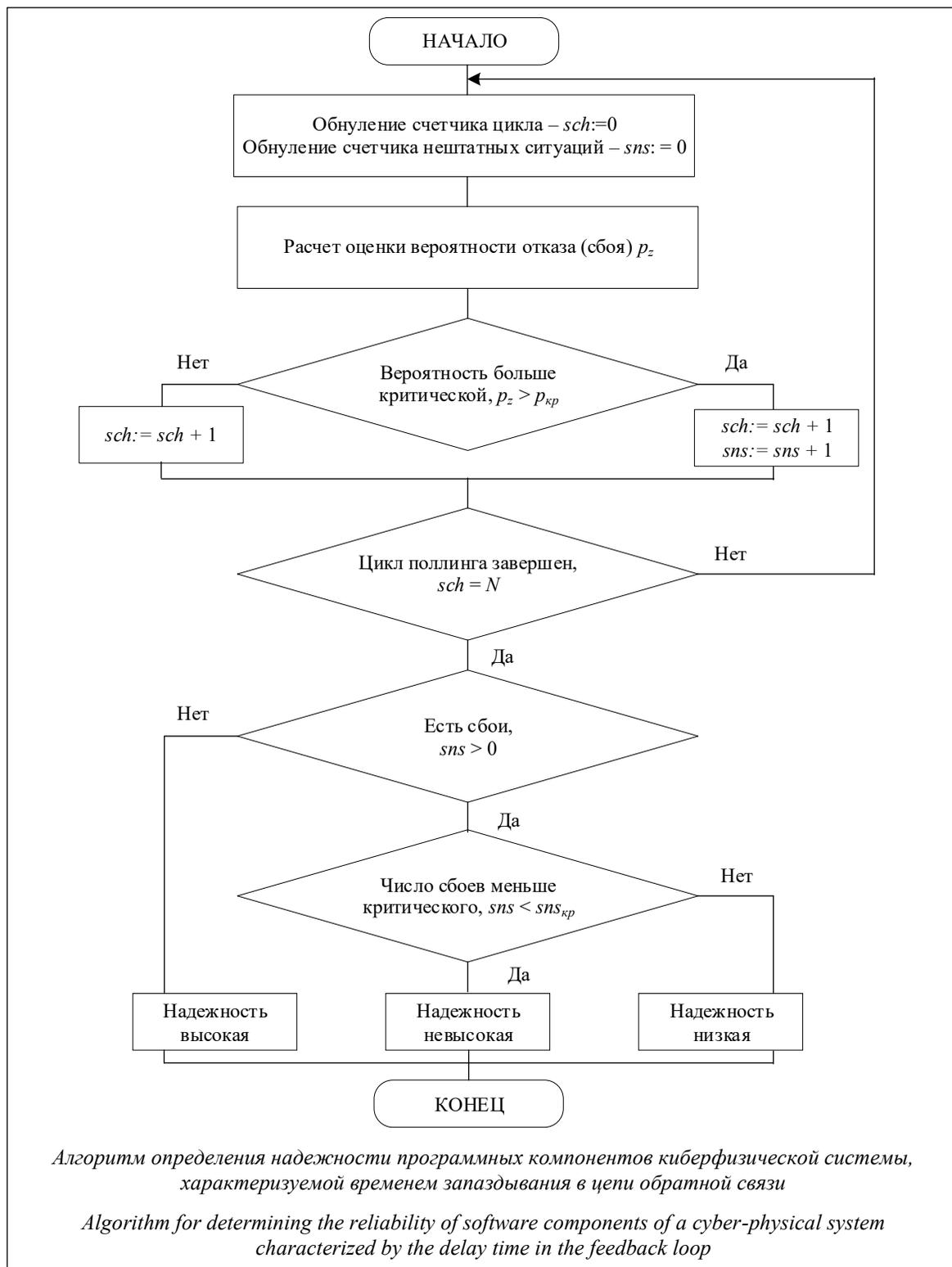
Поток выходов времени запаздывания формирования вектора выходных сигналов относительно вектора входных сигналов в цепи обратной связи за установленные пределы, представляющий собой сумму потоков с разными значениями времени запаздывания, стремится к пуассоновскому [28–30]. Плотность распределения времени между двумя выходами времени запаздывания за порог в пуассоновском потоке равна

$$f_{T_s}(t) = \frac{1}{T_s} e^{-\frac{t}{T_s}}, \quad f_{T_o}(t) = \frac{1}{T_o} e^{-\frac{t}{T_o}},$$

где $f_{T_s}(t)$ и $f_{T_o}(t)$ – распределения, описывающие пуассоновские потоки сбоев и отказов программных компонентов киберфизической системы.

Выводы

В результате исследования разработан подход к моделированию надежности программных компонентов киберфизических систем. Надежность определяется сбоями и отказами, обусловленными некорректным учетом временной сложности реализуемых алгоритмов функционирования. Предлагаемый подход основан на применении структурно-параметрической полумарковской модели сбоев/отказов



ПО, параметры которой определяются вычислительной сложностью и требованиями, пред-

ъявляемыми к ПО с учетом его функционального назначения.

Список литературы

1. Логинов И.В., Федоров В.И. Управление функциональным развитием многофункциональных киберфизических систем // ИСУ. 2023. № 2. С. 108–120.

2. Ларкин Е.В., Богомолов А.В., Привалов А.Н., Акименко Т.А. Математическое обеспечение иерархического цифрового управления сложным технологическим объектом // *Вестн. ЮУрГУ. Сер. Математика. Механика. Физика.* 2024. Т. 16. № 4. С. 43–55. doi: 10.14529/mmp240406.
3. Данилюк А.Ю., Минаков Е.П., Привалов А.Е., Александров М.А. Аналитический метод оценивания эффективности управления киберфизическими системами с учетом характеристик их цифровых двойников // *Изв. РАН.* 2023. № 4. С. 79–89.
4. Обычайко Д.С., Шихин В.А. Анализ и принятие решений по эксплуатационной надежности киберфизических систем // *Вестн. МЭИ.* 2023. № 3. С. 154–162. doi: 10.24160/1993-6982-2023-3-154-162.
5. Shatnawi O. Testing-effort dependent software reliability model for distributed systems. *IJDST*, 2013, vol. 4, no. 2, pp. 1–14. doi: 10.4018/jdst.2013040101.
6. Aital P., Sashikala P. Role of software reliability models in performance improvement and management. *J. of Software Engineering and Applications*, 2021, vol. 5, no. 9, pp. 737–742. doi: 10.4236/jsea.2012.59086.
7. Barack O., Huang L. Assessment and prediction of software reliability in mobile applications. *J. of software engineering and applications*, 2020, vol. 13, no. 9, pp. 179–190. doi: 10.4236/jsea.2020.139012.
8. Лысов Д.В. Анализ надежности в жизненном цикле программного обеспечения // *СУИТ.* 2020. № 2. С. 76–82.
9. Солдатов Е.С., Богомолов А.В., Ларкин Е.В., Солдатов А.С. Сенсорные сети контроля состояния авиационной техники при испытаниях и эксплуатации // *Авиакосмическое приборостроение.* 2024. № 2. С. 61–68.
10. Соловьев С.Ю. Об одном методе генерации страниц-карт для веб-сайтов // *Информационные процессы.* 2008. Т. 8. № 1. С. 24–29.
11. Соловьев С.Ю., Стельмашенко Д.Е. Метод экспертной классификации как инструмент анализа формальных понятий // *ИИИПР.* 2013. № 4. С. 57–61.
12. Ларкин Е.В., Привалов А.Н., Богомолов А.В. Дискретный подход к моделированию синхронизированных эстафет // *НТИ. Сер. 2: Информ. процессы и системы.* 2020. № 2. С. 17–26.
13. Golosovskiy M., Tobin D., Balandov M., Khlopotov R. Architecture of software platform for testing software of cyber-physical systems. In: *LNNS. Proc. CoMeSySo*, 2023, vol. 597, pp. 488–494.
14. Тельнов Ю.Ф., Казаков В.А., Данилов А.В., Брызгалов А.А. Разработка моделей производственных и бизнес-процессов сетевых предприятий на основе многоагентных систем // *Программные продукты и системы.* 2023. Т. 37. № 4. С. 632–643. doi: 10.15827/0236-235X.144.632-643.
15. Голосовский М.С. Информационно-логическая модель процесса разработки программного обеспечения // *Программные системы и вычислительные методы.* 2015. Т. 28. № 1. С. 59–68. doi: 10.7256/2305-6061.2015.1.14119.
16. Голосовский М.С., Богомолов А.В., Тобин Д.С. Алгоритм настройки систем нечеткого логического вывода на основе статистических данных // *НТИ. Сер. 2: Информ. процессы и системы.* 2023. № 1. С. 1–9. doi: 10.36535/0548-0027-2023-01-1.
17. Уласень А.Ф., Стальнов А.Н., Зуева А.Н. Надежность функционального программного обеспечения информационно-управляющих систем реального времени // *Информационно-измерительные и управляющие системы.* 2022. Т. 20. № 6. С. 67–71. doi: 10.18127/j20700814-202206-08.
18. Мальковский М.Г., Соловьев С.Ю. Конструирование отношения псевдохронологического порядка в терминологических сетях // *Открытые семантические технологии проектирования интеллектуальных систем.* 2016. № 6. С. 183–186.
19. Ларкин Е.В., Солдатов Е.С., Богомолов А.В. Математическое обеспечение мониторинга состояния и управления режимами эксплуатации систем хранения криогенных продуктов // *Вестн. ЮУрГУ. Сер.: Математика. Механика. Физика.* 2024. Т. 16. № 1. С. 23–31.
20. Bielecki T.R., Jakubowski J., Niewęłowski M. Conditional Markov chains: Properties, construction and structured dependence. *Stochastic Processes and their Applications*, 2017, vol. 127, no. 4, pp. 1125–1170. doi: 10.1016/j.spa.2016.07.010.
21. Lu H., Pang G., Mandjes M. A functional central limit theorem for Markov additive arrival processes and its applications to queueing systems. *QUESTA*, 2016, vol. 84, no. 3, pp. 381–406.
22. Larkin E., Privalov A., Bogomolov A., Akimenko T. Digital control of continuous production with dry friction at actuators. In: *SIST. Proc. Electromechanics and Robotics*, 2022, vol. 232, pp. 427–436. doi: 10.1007/978-981-16-2814-6_37.
23. Hayes M.H. *Statistical digital signal processing and modeling.* John Wiley & Sons Publ., NY, 1996, 624 p.
24. Stranneby D., Walker W. *Digital signal processing and applications.* Elsevier Publ., London, 2004, 357 p.
25. Briat C. Stability and performance analysis of linear positive systems with delays using input-output methods. *Int. J. of Control*, 2018, vol. 91, no. 7, pp. 1669–1692. doi: 10.1080/00207179.2017.1326628.
26. Li D., Chen G. Impulses-induced p-exponential input-to-state stability for a class of stochastic delayed partial differential equations. *Int. J. of Control*, 2019, vol. 92, no. 8, pp. 1805–1814. doi: 10.1080/00207179.2017.1412089.
27. Sanz R., García P., Albertos P., Fridman E. Robust predictive extended state observer for a class of nonlinear systems with time-varying input delay. *Int. J. of Control*, 2020, vol. 93, no. 2, pp. 217–222. doi: 10.1080/00207179.2018.1562204.
28. Григелиониш Б.И. О сходимости сумм ступенчатых случайных процессов к пуассоновскому // *Теория вероятностей и ее применения.* 1963. Т. 8. № 2. С. 189–194.
29. Ларкин Е.В., Акименко Т.А., Богомолов А.В. Моделирование надежности бортового оборудования мобильного робота // *Изв. Сарат. ун-та. Нов. сер. Сер.: Математика. Механика. Информатика.* 2021. Т. 21. № 3. С. 390–399 (на англ.). doi: 10.18500/1816-9791-2021-21-3-390-399.
30. Kobayashi H., Marl B.L., Turin W. *Probability, random processes and statistical analysis.* Cambridge University Press, London, 2011, 812 p. doi: 10.1017/CBO9780511977770.

Modeling the reliability of software components of cyber-physical systemsAleksandr N. Privalov¹, Evgeny V. Larkin², Aleksey V. Bogomolov³✉¹ Tolstoy Tula State Pedagogical University, Tula, 300026, Russian Federation² Tula State University, Tula, 300012, Russian Federation³ Federal Research Center “Computer Science and Control” of RAS, Moscow, 119333, Russian Federation**For citation**Privalov, A.N., Larkin, E.V., Bogomolov, A.V. (2025) ‘Modeling the reliability of software components of cyber-physical systems’, *Software & Systems*, 38(1), pp. 47–54 (in Russ.). doi: 10.15827/0236-235X.149.047-054**Article info**

Received: 22.07.2024

After revision: 16.08.2024

Accepted: 23.08.2024

Abstract. This relevance of the research is due to the reliability of software components of cyber-physical systems being a key component of their effective functioning. Its appropriate mathematical modeling is essential for the economy digitalization. The paper aims to eliminate the disadvantages of known approaches to modeling the reliability of software components, when the estimates of reliability characteristics are based on empirical data on the errors detected during the testing of programs. Hence, the testing results mostly depend on test duration and on the completeness of the processed data area coverage by the sub-area of the data generated during testing. This reduces the efficiency of reliability estimation. The research focuses on the reliability modeling methods for software components of cyber-physical systems. The reliability is characterized by the delay time in the feedback loop between components. The authors of the paper used methods of software engineering, reliability theory, probability theory and Markov processes. The main result is mathematical reliability models of software components of cyber-physical systems. They combine semi-Markov models of software components, generations of their faults and failures. The developed mathematical models are based on the structural-parametric semi-Markov model of software faults and failures. Its parameters are determined by the computational complexity and requirements to the software taking into account its functional purpose. The authors obtained formalized descriptions of Poisson flows of faults and failures of software components of a cyber-physical system. The practical relevance of the paper is due to its application for determining the reliability of software components at all stages of a cyber-physical system life cycle, where elements interact, self-adjust and adapt to changes using standard software-implemented protocols.

Keywords: cyber-physical system, software, program reliability, program fault, program failure, reliability modeling, semi-Markov process

Acknowledgements. The work was supported by the Russian Science Foundation grant no. 24-29-20256

References

1. Loginov, I.V., Fedorov, V.I. (2023) ‘Management of functional development of multifunctional cyber-physical systems’, *IS&CS*, (2), pp. 108–120 (in Russ.).
2. Larkin, E.V., Bogomolov, A.V., Privalov, A.N., Akimenko, T.A. (2024) ‘Mathematical support for hierarchical digital control of a complex technological object’, *Bull. of the SUrSU. Ser. Math. Mechanics. Physics*, 16(4), pp. 43–55 (in Russ.). doi: 10.14529/mmph240406.
3. Danilyuk, A.Yu., Minakov, E.P., Privalov, A.E., Aleksandrov, M.A. (2023) ‘Analytical method of evaluation of efficiency of control of cyberphysical systems taking into account characteristics of their digital counterparts’, *Bull. of RARAS*, (4), pp. 79–89 (in Russ.).
4. Obychaiko, D.S., Shikhin, V.A. (2023) ‘Analysis of and decision-making on the operational reliability of cyber-physical systems’, *Bull. of MPEI*, (3), pp. 154–162 (in Russ.). doi: 10.24160/1993-6982-2023-3-154-162.
5. Shatnawi, O. (2013) ‘Testing-effort dependent software reliability model for distributed systems’, *IJDST*, 4(2), pp. 1–14. doi: 10.4018/jdst.2013040101.
6. Aital, P., Sashikala, P. (2021) ‘Role of software reliability models in performance improvement and management’. *J. of Software Engineering and Applications*, 5(9), pp. 737–742. doi: 10.4236/jsea.2012.59086.
7. Barack, O., Huang, L. (2020) ‘Assessment and prediction of software reliability in mobile applications’, *J. of Software Engineering and Applications*, 13(9), pp. 179–190. doi: 10.4236/jsea.2020.139012.
8. Lysov, D.V. (2020) ‘Reliability analysis in the software life cycle’, *Control Systems and Inform. Tech.*, (2), pp. 76–82 (in Russ.).
9. Soldatov, E.S., Bogomolov, A.V., Larkin, E.V., Soldatov, A.S. (2024) ‘Sensor networks for monitoring the condition of aviation equipment during testing and operation’, *Aerospace Instrument-Making*, (2), pp. 61–68 (in Russ.).
10. Soloviev, S.Yu. (2008) ‘On one method of generating page maps for websites’, *Information Processes*, 8(1), pp. 24–29 (in Russ.).
11. Soloviev, S.Yu., Stelmashenko, D.E. (2013) ‘The expert classification method as a for formal concept analysis tool’, *AIDM*, (4), pp. 57–61 (in Russ.).
12. Larkin, E.V., Privalov, A.N., Bogomolov, A.V. (2020) ‘Discrete approach to modeling synchronized relay races’, *Sci. and Tech. Inform. Ser. 2: Inform. Processes and Systems*, (2), pp. 17–26 (in Russ.).
13. Golosovskiy, M., Tobin, D., Balandov, M., Khlopotov, R. (2023) ‘Architecture of software platform for testing software of cyber-physical systems’, in *LNNS. Proc. CoMeSySo*, 597, pp. 488–494.

14. Telnov, Yu.F., Kazakov, V.A., Danilov, A.V., Bryzgalov, A.A. (2023) 'Network enterprises: Production and business process models based on multi-agent systems', *Software & Systems*, 37(4), pp. 632–643 (in Russ.). doi: 10.15827/0236-235X.144.632-643.
15. Golosovsky, M.S. (2015) 'Information and logical model of the software development process', *Software Systems and Computational Methods*, 28(1), pp. 59–68 (in Russ.). doi: 10.7256/2305-6061.2015.1.14119.
16. Golosovsky, M.S., Bogomolov, A.V., Tobin, D.S. (2023) 'Algorithm for setting fuzzy logical inclusion systems based on statistical data', *Sci. and Tech. Inform. Ser. 2: Inform. Processes and Systems*, (1), pp. 1–9 (in Russ.). doi: 10.36535/0548-0027-2023-01-1.
17. Ulasen, A.F., Stalnov, A.N., Zueva, A.N. (2022) 'Ensuring the reliability of the functional software of informatively-managing systems real time', *Information-Measuring and Control Systems*, 20(6), pp. 67–71 (in Russ.).
18. Malkovsky, M.G., Soloviev, S.Yu. (2016) 'The designing of pseudo chronological order relation in the thermodynamical networks', *OSTIS*, (6), pp. 183–186 (in Russ.).
19. Larkin, E.V., Soldatov, E.S., Bogomolov, A.V. (2024) 'Mathematical support for monitoring the state and controlling the operating modes of cryogenic product storage systems', *Bull. of the SUrSU. Ser. Math. Mechanics. Physics*, 16(1), pp. 23–31 (in Russ.).
20. Bielecki, T.R., Jakubowski, J., Niewęglowski, M. (2017) 'Conditional Markov chains: Properties, construction and structured dependence', *Stochastic Processes and their Applications*, 127(4), pp. 1125–1170. doi: 10.1016/j.spa.2016.07.010.
21. Lu, H., Pang, G., Mandjes, M. (2016) 'A functional central limit theorem for Markov additive arrival processes and its applications to queuing systems', *QUESTA*, 84(3), pp. 381–406.
22. Larkin, E., Privalov, A., Bogomolov, A., Akimenko, T. (2022) 'Digital control of continuous production with dry friction at actuators', in *SIST. Proc. Electromechanics and Robotics*, 232, pp. 427–436. doi: 10.1007/978-981-16-2814-6_37.
23. Hayes, M.H. (1996) *Statistical Digital Signal Processing and Modeling*, NY: John Wiley & Sons Publ., 624 p.
24. Stranneby, D., Walker, W. (2004) *Digital Signal Processing and Applications*. London: Elsevier Publ., 357 p.
25. Briat, C. (2018) 'Stability and performance analysis of linear positive systems with delays using input-output methods', *Int. J. of Control*, 91(7), pp. 1669–1692. doi: 10.1080/00207179.2017.1326628.
26. Li, D., Chen, G. (2019) 'Impulses-induced p-exponential input-to-state stability for a class of stochastic delayed partial differential equations', *Int. J. of Control*, 92(8), pp. 1805–1814. doi: 10.1080/00207179.2017.1412089.
27. Sanz, R., García, P., Albertos, P., Fridman, E. (2020) 'Robust predictive extended state observer for a class of nonlinear systems with time-varying input delay', *Int. J. of Control*, 93(2), pp. 217–222. doi: 10.1080/00207179.2018.1562204.
28. Grigelionis, B.I. (1963) 'On the convergence of sums of step random processes to a Poisson process', *Theory of Probability and its Applications*, 8(2), pp. 177–182. doi: 10.1137/1108017.
29. Larkin, E.V., Akimenko, T.A., Bogomolov, A.V. (2021) 'Modeling the reliability of the onboard equipment of a mobile robot', *Izv. Sarat. Univ. Math. Mech. Inform.*, 21(3), pp. 390–399. doi: 10.18500/1816-9791-2021-21-3-390-399.
30. Kobayashi, H., Marl, B.L., Turin, W. (2011) *Probability, Random Processes and Statistical Analysis*. London: Cambridge University Press, 812 p.

Авторы

Привалов Александр Николаевич¹, д.т.н.,
 профессор, директор института,
 privalov.61@mail.ru
Ларкин Евгений Васильевич², д.т.н.,
 профессор, elarkin@mail.ru
Богомолов Алексей Валерьевич³, д.т.н.,
 профессор, ведущий научный сотрудник,
 a.v.bogomolov@gmail.com

Authors

Aleksandr N. Privalov¹, Dr.Sci. (Engineering),
 Professor, Director of the Institute,
 privalov.61@mail.ru
Evgeny V. Larkin², Dr.Sci. (Engineering),
 Professor, elarkin@mail.ru
Aleksey V. Bogomolov³, Dr.Sci. (Engineering),
 Professor, Leading Researcher,
 a.v.bogomolov@gmail.com

¹ Тульский государственный педагогический университет им. Л.Н. Толстого,
 г. Тула, 300026, Россия

² Тульский государственный университет,
 г. Тула, 300012, Россия

³ Федеральный исследовательский центр «Информатика и управление» РАН,
 г. Москва, 119333, Россия

¹ Tolstoy Tula State Pedagogical University,
 Tula, 300026,
 Russian Federation

² Tula State University, Tula,
 300012, Russian Federation

³ Federal Research Center
 "Computer Science and Control" of RAS,
 Moscow, 119333, Russian Federation